Porque o fruto da luz consiste em toda bondade, e justiça e verdade.

Efésios 5.9

INTELIGÊNCIA GOVERNAMENTAL:

CONTEXTOS NACIONAIS E DESAFIOS CONTEMPORÂNEOS

Marco Cepik
Organizador

INTELIGÊNCIA GOVERNAMENTAL:

CONTEXTOS NACIONAIS E DESAFIOS CONTEMPORÂNEOS

EDITORA IMPETUS
Niterói, RJ
2011

Editora Impetus Ltda
Rua Alexandre Moura, 51 – Gragoatá – Niterói – RJ
CEP: 24210-200 – Telefax: (21) 2621-7007

Editoração Eletrônica: Editora Impetus Ltda.
Capa: Rafael Brum
Revisão de Português: Marcos Roque
Impressão e encadernação: Editora e Gráfica Vozes Ltda.
Série: Inteligência, Segurança e Direito
Coordenador da Série: Denilson Feitoza

I48

Inteligência governamental : contextos nacionais e desafios contemporâneos / Marco Cepik, organizador. – Niterói, RJ: Impetus, 2011.
352 p. ; 16cm x 23cm.

ISBN: 978-85-7626-569-6

1. Serviços de inteligência – Brasil. 2. Segurança nacional - Brasil. I. Cepik, Marco.

CDD- 363.240981

DEDICATÓRIA

Dedico o livro à minha equipe de assistentes de pesquisa,
orientandos e estudantes.

AGRADECIMENTO

Agradeço aos colegas, Dr. Denilson Feitoza, Dra. Priscila Brandão e Dr. Carlos Arturi, bem como a Christiano Ambros, Luíza Schneider, Gustavo Vernier, Gustavo Moller e Bruno Kern. Agradeço ainda a toda a equipe da Editora Impetus.

Agradeço também o apoio do CNPq.

OS AUTORES

Marco Cepik é professor associado na Universidade Federal do Rio Grande do Sul (UFRGS), onde desenvolve atividades de pesquisa, ensino, orientação e consultoria em três áreas: Estudos sobre Inteligência, Segurança Internacional e Governo e Digitalização. Pesquisador do Núcleo de Estratégia e Relações Internacionais (NERINT-UFRGS), do Centro de Estudos Internacionais sobre Governo (CEGOV-UFRGS) e do Centro de Estudos de Inteligência Governamental (CEIG-UFMG), Cepik publicou oito livros, 23 capítulos de livros e 21 artigos científicos até 2010. Marco Cepik foi pesquisador / professor visitante na Indiana University of Pennsylvania (1997-98), na FLACSO Ecuador (2003 e 2006), na National Defense University em Washington-DC (2000 e 2002) e na Naval Post Graduate School em Monterey-CA (2004), entre outras instituições no Brasil e no exterior. Em 2005, foi bolsista de pós-doutorado do CNPq na Universidade de Oxford, no Reino Unido.

Carlos Arturi é professor associado do Departamento de Ciência Política da UFRGS. Obteve seu doutorado no Institut d'Etudes Politiques de Paris (Sciences Po) e realizou seu pós-doutoramento na Universidade de Lisboa. Coordena o Grupo de Pesquisa "Contestação Transnacional e Controles Democráticos", credenciado pelo CNPq, integra o Núcleo de Estratégia e de Relações Internacionais (NERINT) do Instituto Latino-Americano de Estudos Avançados (ILEA), da UFRGS, e está associado ao LABMUNDO, da Universidade Federal da Bahia (UFBA). É docente e orientador de mestrado e doutorado nos programas de Pós-Graduação em Ciência Política e em Relações Internacionais da UFRGS, bem como professor-convidado do Mestrado em Ciência Política da Universidade Federal do Paraná (UFPR).

Júlio Cóssio Rodriguez possui graduação em Relações Internacionais pela UFRGS (2007) e mestrado em Ciência Política pela mesma universidade (2009). Atualmente, é doutorando em Ciência Política pela Universidade de Lisboa, com vínculo no Instituto de Ciências Sociais (ICS). É bolsista de doutorado da Fundação para a Ciência e Tecnologia – Portugal (FCT).

Gabriel Pessin Adam possui mestrado em Relações Internacionais pela UFRGS e atualmente é doutorando do Programa de Pós-Graduação em Ciência Política da mesma universidade. Pesquisador do Núcleo de Estratégia e Relações Internacionais (NERINT-UFRGS).

Alexander Arciniegas Carreño é advogado formado pela Universidad Industrial de Santander (UIS), Colômbia, e mestre em Ciência Política pela UFRGS. Atualmente, é doutorando em Ciência Política pela mesma universidade.

Mamadou Alpha Diallo possui graduação em Administração pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) (2008) e mestrado em Ciência Política pela UFRGS (2011). Atualmente, é doutorando do Programa de Estudos Estratégicos Internacionais da UFRGS e pesquisador do Núcleo de Estratégia e Relações Internacionais (NERINT-UFRGS).

Igor Castellano da Silva é doutorando em Estudos Estratégicos Internacionais pela UFRGS, pesquisador vinculado ao Núcleo de Estratégia e Relações Internacionais (NERINT) e bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). Possui graduação em Relações Internacionais e mestrado em Ciência Política pela mesma universidade (UFRGS).

Nathaly Xavier possui graduação em Relações Internacionais pela UFRGS (2008). É mestre e doutoranda em Ciência Política pela mesma universidade.

Marília Bortoluzzi Severo é doutoranda em Ciência Política pela UFRGS, pela linha de pesquisa em Política Internacional. É mestre em Ciência Política pela mesma instituição e possui graduação em Direito pela Universidade Federal de Santa Maria (UFSM).

Fabrício Ávila possui graduação em História (bacharelado) pela PUCRS (2005), graduação em História (licenciatura plena) pela PUCRS (2005) e mestrado em Relações Internacionais pela UFGRS 2008. É doutorando em Ciência na UFGRS, onde pesquisa a dissuasão nuclear no século XXI.

Marcos Carra possui graduação em Física (bacharelado) (1990), graduação em História (licenciatura) (1995), graduação em Ciências Econômicas (2002), graduação em História (bacharelado) (2003), graduação em Ciências Sociais (bacharelado) (2006) e mestrado em Relações Internacionais, todos pela UFGRS (2008). Doutorando em Ciência Política pela mesma universidade.

Christiano Ambros possui graduação em Relações Internacionais pela UFRGS (2010). Atualmente, é mestrando do Programa de Pós-Graduação em Ciência Política da mesma universidade. É bolsista sênior e coordenador do Grupo de Trabalho - Teoria e Inteligência Comparada do Núcleo de Estratégia e Relações Internacionais (NERINT) da UFRGS.

Jussara de Oliveira Machado possui especialização *Lato Sensu* em Inteligência de Estado e Inteligência de Segurança Pública pela Fundação Escola Superior do Ministério Público de Minas Gerais (FESMPMG) (2010); especialização *Lato Sensu* em Gestão Pública pelo Praetorium (2009) e graduação em Direito pela Pontifícia Universidade Católica de Minas Gerais (PUC Minas) (2002). Pesquisadora estudante do Centro de Estudos Estratégicos e Inteligência Governamental da Universidade Federal de Minas Gerais (CEEIG/UFMG) (desde 2010).

APRESENTAÇÃO DA SÉRIE

A atividade de inteligência é essencial ao desenvolvimento e à preservação do Estado Democrático de Direito brasileiro. Todos os países economicamente desenvolvidos, com democracias consolidadas, possuem serviços de inteligência responsáveis, legais e fortes.

Há uma imensa "massa de informações" com a qual o Estado tem de lidar cotidianamente, seja quanto à execução de ações específicas, seja quanto ao estabelecimento de suas políticas e estratégias institucionais.

No Brasil, o princípio constitucional da eficiência (art. 37, *caput,* da Constituição da República) veda que o Estado trabalhe com essa "massa de informações" de forma meramente empírica, com desperdício de recursos humanos, materiais e financeiros. O Estado deve utilizar-se de métodos, técnicas e ferramentas adequados para lidar com as informações necessárias ao desempenho de suas finalidades constitucionais, superando a fase individualista e amadorística de seus agentes públicos e políticos e alcançando a racionalidade gerencial exigida pelo princípio constitucional da eficiência.

Os modelos estatais de inteligência constituem uma certa ordenação, adequação e organização de métodos, técnicas e ferramentas de gestão da informação e do conhecimento, especialmente destinados ao processo decisório estatal.

Nessa linha, a inteligência de Estado (ou inteligência "clássica") é voltada, principalmente, ao assessoramento do processo decisório. Por exemplo, nos termos legais, o Sistema Brasileiro de Inteligência (Sisbin) tem a finalidade de fornecer subsídios ao Presidente da República nos assuntos de interesse nacional (art. 1º da Lei nº 9.883/1999), possuindo, como órgão central, a Agência Brasileira de Inteligência (Abin), subordinada ao Gabinete de Segurança Institucional da Presidência da República.

Todavia, sendo sobretudo método, a noção de inteligência de Estado passou a ser aplicada a órgãos públicos em geral, adequando-se a suas finalidades estatais específicas, notadamente no âmbito da segurança pública e da fiscalização.

Isso ocorreu nos Estados Unidos da América, em que, até a Segunda Guerra Mundial, a atividade de inteligência era utilizada, basicamente, como inteligência "clássica", ou seja, com fins militares (inteligência militar) e políticos. Entre 1900 e 1950, gradualmente, a inteligência criminal (*criminal intelligence*) obteve reconhecimento como ferramenta efetiva de combate ao crime, até que, em 1956, foi formada, com 26 agências estatais e locais, a Unidade de Inteligência

de "Segurança Pública" (L.E.I.U – *Law Enforcement Intelligence Unit*), que possui, atualmente, mais de 250 agências, nos Estados Unidos, Canadá, Austrália e África do Sul.

Esse mesmo processo tem ocorrido, atualmente, no Brasil, em que se desenvolvem as atividades de inteligência de segurança pública (denominação recente que abrange, por exemplo, a inteligência policial), inteligência ministerial (Ministério Público), inteligência fiscal, inteligência prisional/penitenciária etc.

De maneira irreversível, apesar das resistências culturais e institucionais, a inteligência de segurança pública e, de modo geral, novas inteligências (como a ministerial, a fiscal e a prisional) têm firmado sua "dupla natureza", como "inteligência estratégica" (processo decisório – natureza consultiva) e "inteligência tática" (produção de provas – natureza executiva), destinadas tanto à produção de provas para investigações e processos criminais, cíveis e fiscais (inteligência tática), especialmente em situações mais complexas como combate às organizações criminosas, programas de controle de crimes e defesa de interesses coletivos, quanto à produção de conhecimento destinado a processos decisórios estratégicos.

Entretanto, de um lado, a inteligência "consultiva" (ou seja, inteligência "clássica" ou inteligência de Estado, voltada a subsidiar o processo decisório do tomador de decisão no mais alto nível estratégico, precipuamente nas áreas de defesa externa, segurança interna e relações internacionais), e, de outro lado, a inteligência "executiva" (ou seja, voltada a subsidiar, com "provas", atividades de natureza executiva, em casos complexos e/ou difíceis, como na inteligência policial, inteligência ministerial, inteligência fiscal, inteligência penitenciária etc.) são significativamente distintas e demandam marcos regulatórios diferentes. Além disso, a atividade de inteligência não deve se confundir com investigações ou processos, sejam cíveis, criminais, fiscais ou administrativos.

Considerando que há vinte e sete unidades federativas no Brasil, cada uma com Polícia Civil, Polícia Militar, Ministério Público, Corpo de Bombeiros Militar, Sistema Prisional e Secretaria da Fazenda, além dos órgãos da União (Exército, Marinha, Aeronáutica, Ministério da Defesa, Abin, Secretaria da Receita Federal do Brasil, Ministério Público da União etc.) e dos municípios (Guardas Municipais), facilmente se verifica que há, desenvolvidas ou embrionárias, mais de 150 "agências" ou "serviços" de inteligência brasileiros, mais da metade dos quais surgiu ou se desenvolveu nos últimos oito anos.

Essa rápida expansão deve continuar nos próximos anos.

A sociedade, a imprensa, os centros de ensino e pesquisa e o próprio Estado finalmente despertaram para essa nova realidade, com o que se renovaram e ampliaram os questionamentos sobre a eficiência e a legalidade das atividades de inteligência, bem como sobre sua "capacidade" de respeitar direitos humanos e direitos fundamentais.

Há uma verdadeira efervescência na área da inteligência, com realização de pesquisas acadêmicas, edição de estudos, surgimento de pós-graduações, publicação de longas reportagens críticas, declarações de importantes personalidades públicas (como as dos chefes dos Poderes da União), discussões legislativas no Congresso Nacional, imensa repercussão na mídia de ações estatais atribuídas à inteligência (como as da Polícia Federal e da Abin) etc.

A prospectiva para a inteligência, nos próximos cinco a dez anos, indica cenários com significativas transformações:

a) diante do déficit legal sobre a inteligência, vários aspectos da inteligência deverão ser regulamentados por lei *stricto sensu,* como leis ordinárias ou, possivelmente, até emenda à Constituição;

b) novos "serviços de inteligência" continuarão a surgir, inclusive "sistemas" de inteligência constitucionalmente "autônomos" (como Ministérios Públicos, Poder Judiciário, Poder Legislativo e Municípios), demandando que a "Comunidade de Inteligência" se antecipe no planejamento de sua integração ou cooperação;

c) a inteligência procurará justificar-se e adequar-se como método proporcional, controlável, eficiente e federativo-cooperativo, bem como desenvolver-se como método pluriagencial, interdisciplinar e interparadigmático, adequado a fenômenos complexos e dialéticos;

d) a inteligência de segurança pública e novas inteligências firmarão sua "dupla natureza", como "inteligência estratégica" (processo decisório – natureza consultiva) e "inteligência tática" (produção de provas – natureza executiva);

e) a inteligência tenderá a atuar de forma cooperativa, seguindo a tendência mundial ao compartilhamento informacional;

f) a inteligência aumentará sua participação em investigações criminais e civis, seja auxiliando ou integrando órgãos investigativos;

g) a inteligência de segurança pública e outras inteligências orientadas para a investigação procurarão desenvolver e consolidar seu devido processo legal;

h) a inteligência buscará padronização, inclusive com desenvolvimento de normas de qualidade e sistemas de certificação de qualidade;

i) a inteligência buscará educação (capacitação, treinamento e aperfeiçoamento, permanentes e continuados), segundo parâmetros internacionais, mas adequada à realidade nacional atual e futura. Por exemplo, a Fundação Escola Superior do Ministério Público de Minas Gerais (FESMPMG) lançou a primeira Pós-Graduação brasileira de Especialização em Inteligência de Estado e Inteligência de Segurança Pública, que já está na quinta turma, tendo, como alunos, Delegados da Polícia Federal, Oficiais de Inteligência da Agência Brasileira de Inteligência (ABIN), Delegados da Polícia Civil, Oficiais da Polícia Militar, Agentes da Polícia Federal, Promotores de Justiça, Procuradores de Justiça, Procurador da República, Procuradores do Trabalho, Auditores Fiscais estaduais e federais, Analista do TCU, Juiz Federal, Juiz de Direito, Agentes Penitenciários etc.

A Editora Impetus, com o apoio da Fundação Escola Superior do Ministério Público de Minas Gerais (FESMPMG), em face desses cenários de relevantes transformações, lançou a série brasileira sobre inteligência, denominada "Inteligência, Segurança e Direito".

A série "Inteligência, Segurança e Direito" objetiva contribuir para o desenvolvimento e o aperfeiçoamento da inteligência e da segurança, por meio da publicação de estudos, pesquisas, ensaios, manuais, cursos, tratados, coletânea de artigos e outras obras de qualidade, nacionais ou estrangeiros, produzidos por profissionais de inteligência e segurança, pesquisadores, professores, especialistas e estudiosos em geral. Ademais, a série também incorpora o novo campo de estudos e pesquisas do direito sobre a inteligência e a segurança.

A série "Inteligência, Segurança e Direito" tem demonstrado sua vitalidade e relevância, chegando à 2ª edição de sua primeira obra e a esta quarta obra (*Inteligência governamental*: contextos nacionais e desafios contemporâneos), com grande sucesso.

Dr. Denilson Feitoza

Pós-Doutorado em Inteligência, Segurança e Direito (Canadian Centre of Intelligence and Security Studies – CCISS)

Pós-Doutorado em Ciência da Informação (UFMG)

Doutor em Direito, Mestre em Direito e Master of Arts in Open and Distance Education

Coordenador da Série "Inteligência, Segurança e Direito"

Presidente da Associação Internacional de Analistas de Inteligência de Segurança Pública – Capítulo Brasil – IALEIA-BR

Coordenador da Pós-Graduação de Especialização em Inteligência de Estado e Inteligência de Segurança Pública da Fundação Escola Superior do Ministério Público de Minas Gerais (FESMPMG)

Pesquisador doutor do Centro de Estudos Estratégicos e Inteligência Governamental, da Universidade Federal de Minas Gerais (CEEIG/ UFMG)

Diretor acadêmico da Associação Brasileira de Professores de Ciências Penais (ABPCP)

Membro da International Association of Law Enforcement Intelligence Analysts (IALEIA)

Membro da International Association for Intelligence Education (IAFIE)

Membro da International Association of Crime Analysts (IACA)

Ex-Presidente do Instituto Brasileiro de Inteligência Criminal (INTECRIM)

Ex-Secretário-Geral do Grupo Nacional de Combate às Organizações Criminosas (GNCOC)

Ex-Coordenador do Centro de Segurança e Inteligência Institucionais (CESIN), do Ministério Público de Minas Gerais

Ex-Coordenador nacional do Grupo de Inteligência dos Ministérios Públicos

Procurador de Justiça

www.impetus.com.br

www.fesmpmg.org.br

www.inteligenciabr.com

www.denilsonfeitoza.com

APRESENTAÇÃO

A inteligência governamental é uma parte do Estado contemporâneo com profundas implicações para a democracia e a segurança. Se, por um lado, a desconfiança perante esses órgãos tem sido recorrente em diferentes contextos políticos, por outro não é possível uma ordem democrática sem serviços de inteligência institucionalizados, ou seja, efetivos e legítimos. Eles são essenciais na função de governo, ao subsidiar governantes em seus processos diários de tomada de decisão. Além desses dilemas já tradicionais, contudo, novos focos de tensão surgem com os avanços tecnológicos e as mudanças históricas recentes. Nesse sentido, este livro tem o intuito de contribuir com esse debate, através da exposição de casos relevantes para o sistema internacional e para a política externa brasileira, na Parte I, e também por meio de uma discussão teórica a respeito dos novos desafios enfrentados pela inteligência governamental, na Parte II.*

No primeiro capítulo, Carlos Arturi e Júlio Rodriguez comparam os casos de Portugal e Brasil, analisando o tipo de transição política efetuado nas respectivas democratizações e o padrão resultante para as relações civis-militares e para as organizações de inteligência e de segurança internas. Além de contribuir com o importante caso brasileiro, os autores concluem que o tipo de transição política – bastante diferente nos dois casos – tem papel preponderante no resultado. No caso português, em que a transição aconteceu de forma abrupta, através da Revolução dos Cravos, de 1974, os atores não ficaram constrangidos pelo legado do período anterior e conseguiram efetuar o controle civil sobre os militares de forma mais profunda, institucionalizando os serviços de inteligência e segurança internas sob controles democráticos – embora, evidentemente isso não tenha sido isento de conflitos. Já no caso brasileiro, os autores demonstram a dificuldade dos civis de institucionalizar e de instituir o controle democrático sobre os militares, devido à lenta, gradual e pactuada transição da ditadura brasileira, mostrando, contudo, que o processo tem avançado paulatinamente nas últimas décadas.

***** Embora compartilhando leituras e uma agenda de pesquisa orientada para a explicação de aspectos institucionais, analíticos e operacionais da área de inteligência, os textos reunidos neste volume refletem as fontes que estiveram disponíveis a cada autor e expressam as convicções e interpretações de seus autores. Trata-se, pois, de um volume pluralista, onde coexistem diferentes opiniões, sempre provisórias e sujeitas aos resultados de pesquisas adicionais. O editor do volume não endossa, necessariamente, as afirmações contidas nos diferentes capítulos. Tampouco eles refletem, necessariamente, qualquer posição institucional da UFRGS ou do CNPq, a quem agradecemos o apoio à pesquisa por meio da concessão de bolsas e auxílios de pesquisa.

Já no capítulo 2, Gabriel Adam apresenta com o estudo de caso da Rússia, a atuação dos serviços de inteligência russos no pós-Guerra Fria. O autor faz um breve histórico dos sistemas de inteligência russos desde o tempo dos czares, e aponta a continuidade expressiva nos métodos e comportamentos ao longo da história russa. Mesmo em momentos políticos bastante distintos, como no caso da descentralização e enfraquecimento durante o governo de Boris Yeltsin e no fortalecimento e centralização da era Putin, o padrão de atuação é bastante recorrente. Segundo o autor, portanto, os desafios ainda são grandes em termos de institucionalização, do estabelecimento de controles democráticos e de uma conduta condizente com a preservação dos direitos humanos.

O capítulo 3, de Alexandre Arciniegas Carreño, propõe uma reflexão sobre a irredutibilidade da segurança nacional e as tensões inevitáveis entre segurança coletiva/segurança individual e segredo/transparência, através da análise das instituições de inteligência da Colômbia. O autor descreve como as complexidades da sociedade colombiana influenciam diretamente a agência de inteligência, a qual se vê muitas vezes como instrumento de interesses específicos, minada pela corrupção e pelo patrimonialismo. Nesse sentido, ele defende uma reforma no setor de inteligência que consiga superar essa situação delicada, e coloque a inteligência colombiana em posição de cumprir seu papel enquanto tal.

Nos capítulos 4 e 5, Mamadou Alpha Diallo e Igor Castellano, respectivamente, analisam os casos da Nigéria e da República Democrática do Congo, demonstrando os desafios não apenas da institucionalização dos serviços de inteligência e segurança na África, mas seu papel no delicado processo de construção do Estado. A difícil equação entre o passado colonial e o estabelecimento do monopólio do uso da força, muitas vezes ainda não atingida no continente africano, se combina com os dilemas próprios dos sistemas de inteligência e segurança – tornando esses processos ainda mais complexos. Contudo, se por um lado esses dilemas estão na pauta diária dos países africanos, por outro, o esvaziamento das funções de inteligência e segurança também pode ser complicado, uma vez que, como demonstra Castellano no caso da RDC, esses órgãos podem ser ilhas de capacidade estatal em um mar de ineficácia e inação. Nesse sentido, o equilíbrio parece encontrar grandes obstáculos nos países africanos.

Terminados os estudos de caso, tem início a Parte II do livro, que reúne trabalhos teóricos a respeito dos novos desafios enfrentados pelas atividades de inteligência no mundo contemporâneo. No capítulo 6, Nathaly Xavier trata do papel da inteligência nas Operações de Paz da ONU no pós-Guerra Fria. A autora demonstra como, em um contexto de ampliação quantitativa e qualitativa das operações de paz da ONU, as atividades de inteligência são cada vez mais necessárias para o sucesso das missões. Por meio do estudo de alguns casos, fica clara a tensão entre a necessidade da inteligência, de um lado, e o caráter

multinacional das Nações Unidas, de outro. Como parte de conflitos armados, a inteligência é fundamental para o sucesso de operações e sua ausência muitas vezes compromete o sucesso das operações, como no caso de Srebrenica. Por outro lado, os países membros relutam em ceder suas prerrogativas soberanas e a própria ONU não atua com a mesma liberdade que os Estados nacionais, não admitindo, por exemplo, a obtenção de informações por meios ilegais ou antiéticos. Nesse sentido, a autora tenta identificar como os novos desafios colocados pelo pós-Guerra Fria geraram mudanças institucionais na organização internacional.

No capítulo 7, Marília Bortoluzzi Severo problematiza os conceitos de propaganda, inteligência e operações encobertas, demonstrando ao leitor como o componente "informação" presente nesses conceitos permite que se considere propaganda como pertencente ao âmbito das operações de inteligência. Atividade há séculos largamente utilizada por governos dos mais diversos tipos, a propaganda é instrumento de persecução de interesses nacionais. Segundo a autora, o capítulo se propõe a investigar onde se encaixam os meios de propaganda e de mídia nas atividades de inteligência, desfazendo a confusão conceitual em torno do termo "propaganda" e mostrando que tal instrumento não constitui uma operação informacional do tipo operação psicológica, mas sim do tipo operação encoberta.

No capítulo 8, Fabrício Ávila demonstra como as novas tecnologias e o processo de digitalização têm impactado diretamente o sistema internacional por meio de dois fenômenos. Em primeiro lugar, o barateamento dos custos faz com que mais países tenham acesso a determinadas capacidades, o que aumenta a possibilidade de um balanceamento sistêmico. Em segundo lugar, essas novas tecnologias têm impactado diretamente nas capacidades de IMINT, por meio da geração e disponibilização de imagens de satélite. Essas, por sua vez, não apenas cumprem seu papel clássico como atividade de inteligência, no fornecimento de informação para a tomada de decisão, mas também influenciam diretamente a opinião pública a respeito de conflitos internacionais. Nesse sentido, o autor demonstra, através do caso recente do Iraque, da tensão com o Irã e a Coreia da Norte e também de tensões mais profundas como aquelas entre Estados Unidos, China e Rússia, como a IMINT e a digitalização vêm transformando e sendo transformadas nas últimas décadas.

No capítulo 9, Marcos Carra discorre sobre a utilidade da Teoria dos Jogos para as atividades de inteligência. Além de discorrer sobre a teoria dos jogos em si, o autor demonstra que, de um lado, a teoria dos jogos pode auxiliar o tomador de decisões, contribuindo diretamente para as atividades de inteligência. Através da teoria dos jogos, é possível compreender melhor a natureza do jogo, as motivações dos rivais e as ações e reações dos competidores antes de desenvolver e implementar sua própria estratégia. Contudo, o autor alerta que, por outro

lado, a aplicação da Teoria dos Jogos enfrenta diversos problemas, desde a matematização até a definição de alguns pressupostos caros a essa teoria, como o da maximização dos ganhos e o do comportamento racional.

No capítulo 10, Christiano Ambros colabora com uma interessante discussão a respeito dos vieses cognitivos na tomada de decisão. As atividades de inteligência, cujo objetivo reside no fornecimento de informação para a tomada de decisão, precisam levar em consideração esses possíveis vieses, como demonstra o autor. Embora sejam de difíceis detecção e prevenção, pois intrínsecos e automáticos na mente humana, o conhecimento a seu respeito é fundamental, para que a decisão seja ainda mais bem embasada. Além disso, o autor analisa a forma pela qual as emoções interferem diretamente na tomada da decisão – outro fator profundamente relevante nas atividades de inteligência, visto o estresse e a pressão sob os quais atuam os consumidores de inteligência.

Por fim, no capítulo 11, Jussara de Oliveira Machado retoma o tema das tecnologias digitais abordado no capítulo 8, porém sob nova perspectiva – talvez um dos desafios contemporâneos mais iminentes para a inteligência e a humanidade como um todo: as ameaças provenientes do ciberespaço. A autora mostra como a inteligência enfrentará obstáculos ainda mais complexos que aqueles próprios de sua natureza, com o aumento do volume de informação, a dificuldade de rastrear responsáveis, o anonimato e as guerras não-declaradas, além das novas possibilidades de terrorismo por meio de sua versão cibernética. Ainda restam intactos os dilemas da legitimidade e da privacidade. A cibernética traz novos desafios para a sociedade como um todo, mas principalmente para aqueles que têm de encontrar informações confiáveis e abrangentes em um mar de incerteza e anonimato.

Este livro, portanto, tenta suprir algumas lacunas na área de inteligência governamental de duas formas: analisando casos significativos de uma perspectiva institucional, de um lado, mas também casos normalmente deixados de lado e sobre os quais o pesquisador tem dificuldades de encontrar informações; e, em segundo lugar, trazendo discussões teóricas a respeito do papel da inteligência no século XXI e os novos desafios a serem enfrentados por ela, para além de sua própria complexidade intrínseca.

Marco Cepik
Organizador da obra

LISTA DE SIGLAS E ACRÔNIMOS

As siglas e acrônimos utilizados ao longo do livro seguem a forma mais comum pelos quais os órgãos e conceitos são conhecidos no Brasil. Assim, por exemplo, a Agência Central de Inteligência dos Estados Unidos da América aparece registrada sob a sigla CIA e não ACI. Quando for possível ou necessário para auxiliar a compreensão, registra-se também o termo por extenso em língua estrangeira entre parênteses.

ABIN – Agência Brasileira de Inteligência
ACP – África, Caribe e Pacífico
AFDL – Aliança das Forças Democráticas para Libertação do Congo-Zaire (Alliance de Forces Democratique pour la Liberation du Congo-Zaire)
AID – Agência para o Desenvolvimento Internacional (Agency for International Development) (organismo do Banco Mundial)
ANC – Exército Nacional Congolês (Armée Nationale Congolaise)
AND – Agência Nacional de Documentação Congolesa (Agence Nationale de Documentation)
ANI – Agência Nacional de Imigração do Congo (Agence Nationale d'Immigration)
ANI – Agência Nacional de Inteligência (Chile)
ANI – Agência Nacional de Inteligência (Nigéria)
ANP – Academia Nacional de Polícia (Brasil)
ANR – Agência Nacional de Informação da República Democrática do Congo (Agence Nationale de Renseignements)
AOF – África Ocidental Francesa
AOFI – Associação Nacional dos Oficiais de Inteligência (Brasil)
AR – Assembleia da República (Portugal)
ARENA – Aliança Renovadora Nacional (Brasil)
ASAT – Arma Anti-satélite (Anti-satellite weapon)
AWAC – Sistema Aerotransportado de Alerta e Controle (Airborne Early Warning and Control)
C2W – Guerra de Comando e Controle (Command and Control Warfare)
CA – Operações Encobertas (Covert Actions)
CAE – Comissão de Assuntos Econômicos (Brasil).
CCAI – Comissão Mista de Controle das Atividades de Inteligência (Brasil)
CDN – Conselho de Defesa Nacional (Brasil)
CEDEAO – Comunidade Econômica dos Estados da África Ocidental (Communauté Économique des États de l'Afrique de l'Ouest)

CENIMAR – Centro de Informações da Marinha (Brasil)
CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CETS – Sistema de Rastreamento de Exploração Infantil (Child Exploitation Tracking System)
CGT – Confederação Geral do Trabalho (Portugal)
CIA – Agência Central de Inteligência dos Estados Unidos da América (Central Intelligence Agency)
CIE – Centro de Informações do Exército (Brasil)
CIM – Centro de Inteligência da Marinha (Brasil)
CISA – Centro de Informações de Segurança da Aeronáutica (Brasil)
CMC – Comunicações Mediadas por Computador
CND – Centro Nacional de Documentação Congolês (Centre Nationale de Documentation)
CNDP – Congresso Nacional para a Defesa do Povo da República Democrática do Congo (Congrès National pour la Défense du Peuple)
CNE – Exploração de Redes de Computador (Computer Network Exploitation)
CNI – Infraestruturas Críticas Nacionais (Critical National Infrastructure)
CNI – Conselho Nacional de Inteligência da Espanha (Consejo Nacional de Inteligencia)
CNJ – Conselho Nacional de Justiça (Brasil)
CNMP – Conselho Nacional do Ministério Público (Brasil)
CNO – Operações de Redes de Computadores (Computer Network Operations)
CNS – Gabinete de Coordenação de Segurança Nacional da Nigéria
COAF – Conselho de Controle de Atividades Financeiras (Brasil)
CODI – Centros de Operações de Defesa Interna (Brasil)
COPEI – Coordenação Geral de Pesquisa e Investigação (Brasil)
CSE – Conselho de Segurança do Estado (Congo)
CSI – Conselho Superior de Informações (Portugal)
CSIS – Centro de Estudos Estratégicos e Internacionais (Center for Strategic & International Studies)
CSN – Conselho de Segurança Nacional (Zaire)
CSSI – Superior de Segurança Interna (Portugal)
C**HEKA** – Comissão Extraordinária Panrussa para o Combate da Contrar-revolução, Sabotagem e Especulação
DAS – Departamento Administrativo de Segurança da Colômbia (Departamento Administrativo de Seguridad)
DAS – 4ª Direção de Serviços Administrativos (Portugal)
DCAF – Controle Democrático das Forças Armadas (Geneva Centre a for the Democratic Control of Armed Forces)
DEMIAP – Detecção Militar das Atividades Antipatrióticas (congolês) (Détection Militaire des activités Anti-Patrie)
DEOPS – Departamentos Estaduais de Ordem Política e Social (Brasil)
DFS – Departamento de Suporte das Nações Unidas (United Nations Department of Field Support)

DFSP – Departamento Federal de Segurança Pública (Brasil)
DGM – Direção Geral de Migração do Congo (Direction Générale de Migration)
DGS – Direção Geral de Segurança (Portugal)
DI – Departamento de Inteligência (Brasil)
DIE – Departamento de Inteligência Estratégica (Brasil)
DIM – Direção de Inteligência Militar (Nigéria)
DINFO – Divisão de Informações (Portugal)
DIP – Departamento de Investigações e Propaganda (Brasil)
DNS – Sistema de Nomes de Domínio (Domain Name System)
DOD – Departamento de Defesa Norte-americano (Department of Defense)
DOI – Destacamentos de Operações de Informações (Brasil)
DOPS – Delegacia de Ordem Política e Social (Brasil)
DPA – Departamento de Assuntos Políticos das Nações Unidas (United Nations Department of Political Affairs)
DPF – Departamento de Polícia Federal (Brasil)
DPKO – Departamento de Operações de Paz da ONU (Department of Peace Keeping Operations)
DPRF – Departamento de Polícia Rodoviária Federal (Brasil)
DPS – Divisão de Polícia Política e Social (Brasil)
DRGS – Direção de Informações Gerais e Serviços Especiais da Polícia da República Democrática do Congo (Direction des Renseignements Généraux et Services Spéciaux de la Police)
DSEF – 3ª Direção de Serviços de Estrangeiros e Fronteiras (Portugal)
DSI – 1ª Direção de Serviços de Informação (Portugal)
DSI – Divisão de Segurança e Informações (Brasil)
DSIC – 2ª Divisão de Serviços de Investigação e Contencioso (Portugal)
DSIC – Departamento de Segurança da Informação e Comunicações (Brasil)
DSN – Doutrina de Segurança Nacional (Brasil)
DSP – Divisão Presidencial Especial do Zaire (Division Spéciale Présidentielle)
DTEC – Departamento Técnico (Portugal)
ECOMOG – Grupo de Monitoramento da Comunidade Econômica dos Estados dos Estados do Oeste Africano (Economic Community of West African States Monitoring Group)
ECPS – Comitê Executivo para Paz e Segurança da ONU (Executive Committee on Peace and Security)
EIS – Sistema de Informação da Europol (Europol Information System)
ELINT – Inteligência Eletrônica (Eletronic Intelligence)
ELN – Exército de Libertação Nacional da Colômbia (Ejército de Liberación Nacional de Colombia)
EMC-FA – Estado-Maior Conjunto das Forças Armadas (Brasil)
EMGFA – Estado-Maior-General das Forças Armadas (Portugal)
EMGRM – Estado-Maior de Inteligência Militar (congolês) (Etat-Major Général du Renseignement Militaire)
ENASP – Nacional de Justiça e Segurança Pública (Brasil)

ESG – Escola Superior de Guerra (Brasil)
EUA – Estados Unidos da América
EUPOL – Polícia da União Europeia
EUROSUR – Sistema Europeu de Vigilância das Fronteiras Externas (European External Border Surveillance System)
EW – Guerra Eletrônica (Eletronic Warfare)
FAC – Forças Armadas Congolesas
FAPSI – Agência Federal de Comunicação e Informação Governamental (URSS)
FARC – Forças Armadas Revolucionárias da Colômbia
FARDC – Forças Armadas da República Democrática do Congo (Forces Armées de la République Democratique du Congo)
FAZ – Forças Armadas Zairianas (Forces Armées Zaïroises)
FDLR – Forças Democráticas de Libertação de Ruanda
FNP – Força Nacional da Polícia (Nigéria)
FPS – Serviço Federal das Fronteiras da Rússia (Federal'naya Pogranichnaya Sluzhba)
FRONTEX – Agência Europeia de Gestão da Cooperação Operacional nas Fronteiras Externas dos Estados-Membros da União Europeia (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union)
FSB - Serviço Federal de Segurança da Rússia (Federal'naya Sluzhba Bezopasnosti)
FSK – Serviço Federal de Contraespionagem da Rússia (Federal'naya Sluzhba Kontrrazvedki)
FSNP – Serviço Federal de Polícia de Impostos da Rússia
FSO – Serviço de Proteção Federal da Rússia
FSS – Forças e Serviços de Segurança (Portugal)
GC – Guarda Civil do Zaire (Garde Civile)
GIG – Rede de Informação Global (Global Information Grid)
GKU – Diretoria Principal de Controle do Kremlin (URRS)
GN – Polícia Nacional do Zaire (Gendarmerie Nationale)
GNR – Guarda Nacional Republicana (Portugal)
GON – Grupo de Observação Nacional e Internacional da Colômbia (Grupo de Observación Nacional e Internacional)
GR – Guarda Republicana da República Democrática do Congo (Garde Républicaine)
GRU – Serviço de Inteligência do Exército da Rússia (Glavnoye Razvedyvatelnoye Upravleniye)
GSI – Gabinete de Segurança Institucional (Brasil)
GSIPR – Gabinete de Segurança Institucional da Presidência da República (Brasil)
GUGB – Chefia de Administração de Segurança do Estado da Rússia (Glavnoye Upravleniye Gosudasrtvennoy Bezopasnosti)
GUSP – Diretoria Principal de Programas Específicos do Presidente da Rússia
HEWS – Sistema de Alerta Humanitário Antecipado (Humanitarian Early Warning Service)

HSPD-23 – Diretiva Presidencial de Segurança Interna dos EUA (Homeland Security Presidential Directive 23)
HUMINT – Inteligência Humana (Human Inteligence)
IBW – Guerra Baseada na Inteligência (Intelligence Based Warfare)
ICBM – Míssil Balístico Intercontinental (Inter-Continental Ballistic Missile)
IEW – Guerra de Informação Econômica (Informational Economic Warfare)
IGAI – Inspeção-Geral da Administração Interna (Portugal)
IMINT – Inteligência de Imagens (Imagery Intelligence)
INSS – Instituto para Estudos de Segurança Nacional (Institute for National Security Studies)
INTERPOL – Organização Internacional de Polícia Criminal (International Criminal Police Organization
IO – Operações Informacionais (Information Operations)
IPES – Instituto de Pesquisas e Estudos Sociais (Brasil)
ISE – Elemento de Suporte de Inteligência (Intelligence Support Element)
IW – Guerra de Informação (Information Warfare)
IWS – Site sobre Guerra Informacional (The Information Warfare Site)
JAI – Justiça e Assuntos Internos (Portugal)
JCS – Junta de Chefes de Pessoal dos EUA (Joint Chiefs of Staff)
JDISS – Sistema de Suporte de Inteligência Destacável Conjunta (Joint Deployable Intelligence Support System)
JMAC – Centro de Análise Conjunta de Missões da ONU (Joint Mission Analysis Center)
JSN – Junta de Salvação Nacional (Portugal)
KGB – Comitê de Segurança do Estado (URSS) (Komitet Gosudasrtvennoy Bezopasnosti)
LP – Legião Portuguesa
LRA – Exército de Resitência do Lorde (Lord's Resistance Army)
MAD – Destruição Mútua Assegurada (Mutual Assured Destruction)
MAI – Ministério da Administração Interna (Nigéria)
MAI – Ministério da Administração Interna (Portugal)
MB – Ministério da Segurança (Rússia)
MDB – Movimento Democrático Brasileiro
MFA – Movimento das Forças Armadas (Portugal)
MILDEC – Dissimulação Militar (Military Deception)
MINUSTAH – Missão das Nações Unidas para Estabilização do Haiti (United Nations Stabilization Mission in Haiti)
MIPONUH – Missão de Polícia Civil das Nações Unidas no Haiti (United Nations Civilian Police Mission In Haiti)
MONUC – Missão das Nações Unidas para Organização e Estabilização na Repúblicia Democrática do Congo (United Nations Organization Stabilization Mission in the Democratic Republic of the Congo)
MPS – Serviço de Planejamento Militar da ONU (Military Planning Service)
MSB – Serviço Inter-republicano de Segurança (Rússia)

MVD – Ministério do Interior da Rússia (Ministerstvo Vnutrennikh Del)
NCP – Polícia da Costa do Níger (Niger Coast Police) (Nigéria no período colonial)
NEPAD – Nova Parceria pelo Desenvolvimento (Nigéria)
NF-E – Nota Fiscal Eletrônica
NKGB – Comissariado do Povo para a Segurança do Estado (URSS) (Narodnyy Komitet Gosudasrtvennoy Bezopasnosti)
NKVD – Comissariado dos Assuntos Internos do Povo (URSS) (Narodnyy Komissariat Vnutrennikh)
NPC – Conselho de Polícia da Nigéria (Nigeria Police Council)
NPF – Forças da Polícia Nigeriana
NPS – Escola de Pós-graduação Naval (Naval Postgraduate School; Monterey, California, EUA)
NSPD-54 – Diretiva Presidencial de Segurança Nacional dos EUA (National Security Presidential Directive 54)
OCHA – Escritório para Coordenação de Questões Humanitárias das Nações Unidas (United Nations Office for the Coordination of Humanitarian Affairs)
OGPU – Administração Unida da Polícia Estatal (URSS) (Obyedinennoye Gosudarstvennoy Politicheskie Upravlenyie)
OMA – Escritório de Assuntos Militares da ONU (Office for Military Affairs)
ONS/NSO – Organização Nigeriana de Segurança (Nigerian Security Organization)
OPEP – Organização dos Países Exportadores de Petróleo
OPSEC – Operações de Segurança (Operations Security)
OSINT – Inteligência de Fontes Abertas (Open Source Intelligence)
OTAN – Organização do Tratado do Atlântico Norte
OUA – Organização da União Africana
PCB – Partido Comunista Brasileiro
PCP – Partido Comunista Português
PDA – Polo Democrático Alternativo
PDN – Política de Defesa Nacional (Brasil)
PDS – Partido Democrático Social (Brasil)
PDSD – Política de Defesa e Segurança Democrática da Colômbia (Política de Defensa y Seguridad Democrática)
PFL – Partido da Frente Liberal (Brasil)
PFS – Polícia Federal de Segurança (Brasil)
PIAPS – Plano de Integração e Acompanhamento dos Programas Sociais de Prevenção da Violência (Brasil)
PIDE – Polícia Internacional de Defesa do Estado (Portugal)
PMDB – Partido do Movimento Democrático Brasileiro
PNC – Polícia Nacional Congolesa (Police Nationale Congolaise)
PSDB – Partido da Social Democracia Brasileira
PSP – Polícia de Segurança Pública (Portugal)
PSYOP – Operações Psicológicas (Psychological Operations)

PT – Partido dos Trabalhadores (Brasil)
PVDE – Polícia de Vigilância e Defesa do Estado (Portugal)
RDC – República Democrática do Congo
RNC – Royal Niger Company (Nigéria período colonial)
RNCP – Royal Niger Company Police (Nigéria período colonial)
SAC – Comando Aéreo Estratégico dos EUA (US Strategic Air Comand)
SADEN – Secretaria de Assuntos de Defesa Nacional (Brasil)
SAE – Secretaria de Assuntos Estratégicos (Brasil)
SAP – Setor Especial da Polícia Sul-Africana (Special Branch of the South Afican Police)
SARM – Serviço de Ação e de Informação Militar do Zaire (Service d'Action et de Renseignements Militaire)
SCI – Serviço Central de Investigação (Portugal)
SDCI – Serviço Diretor e Coordenador de Informação (Portugal)
SECINT – Secretaria de Inteligência (Brasil) (Aeronáutica)
SENAD – Secretaria Nacional Antidrogas (Brasil)
SENASP – Secretaria Nacional de Segurança Pública (Brasil)
SFICI – Serviço Federal de Informações e Contrainformações (Brasil)
SGSSI – Secretário-Geral do Sistema de Segurança Interna (Portugal)
SI – Serviços Internacionais (Portugal)
SIC – Serviço de Inteligência Colombiano (Servicio de Inteligencia Colombiano)
SIED – Serviço de Informações Estratégicas de Defesa (Portugal)
SIEDM – Serviço de Informações Estratégicas de Defesa e Militares (Portugal)
SIGINT – Inteligência de Sinais (Signals Intelligence)
SIN – Serviço de Inteligência Nacional da Colômbia (Servicio de Inteligencia Nacional)
SINAI – Sistema Nacional de Inteligência da Colômbia (Sistema Nacional de inteligencia)
SINDE – Subsistema de Inteligência de Defesa (Brasil)
SIRP – Sistema de Informações da República Portuguesa
SIS – Serviço de Informações de Segurança (Portugal)
SISBIN – Sistema Brasileiro de Inteligência (Brasil)
SISC – Sistema de Segurança e Credenciamento (Brasil)
SISNI – Sistema Nacional de Inteligência (Brasil)
SISP – Subsistema de Inteligência de Segurança Pública (Brasil)
SISSEGIN – Sistema de Segurança Interna (Brasil)
SM – Segurança Militar do Congo (Sécurité Militaire)
SMI – Serviço de Informações Militares (Portugal)
SN – Segurança Nacional do Congo (Sûreté Nationale)
SNI – Serviço Nacional de Informação (Brasil)
SNIP – Serviço Nacional de Inteligência e Proteção Congolês (Service Nationale d'Inteligence e Protection)
SPEAI – Secretário de Política, Estratégia e Assuntos Internacionais do Ministério da Defesa (Brasil)

SRF – Secretaria da Receita Federal (Brasil)
SRM – Serviço de Informação Militar da República Democrática do Congo (Service de Renseignement Militaire)
SSI – Sistema de Segurança Interna (Portugal)
SSR – Reforma do Setor de Segurança (congolês)
SSS – Serviço de Segurança do Estado (Nigéria) (State Security Service)
STF – Supremo Tribunal Federal (Brasil)
SVR – Serviço de Inteligência Estrangeira da Rússia (Sluzhba Vneshney Razvedki)
UA – União Africana
UAV – Veículo Aéreo não Tripulado (Unmanned Aerial Vehicle)
UE – União Europeia
UNITAF – Força Tarefa Unificada das Nações Unidas (United Task Force)
UNMIH – Missão das Nações Unidas no Haiti (United Nations Mission in Haiti)
UNMIK – Missão das Nações Unidas para Administração Provisória do Kosovo (United Nations Interim Administration Mission in Kosovo)
UNOSOM – Operação das Nações Unidas na Somália (United Nations Operation in Somalia)
UNPROFOR – Força de Proteção das Nações Unidas (United Nations Protection Force)
UNSC – Conselho de Segurança das Nações Unidas (United Nations Security Council)
UNSMIH – Missão de Suporte das Nações Unidas no Haiti (United Nations Support Mission In Haiti)
UNTMIH – Missão de Transição das Nações Unidas no Haiti (United Nations Transition Mission In Haiti)
URSS – União das Repúblicas Socialistas Soviéticas
USIA – Agência de Informação dos Estados Unidos (United States Information Agency)
WMD – Arma de Destruição em Massa (Weapon of Mass Destruction)

SUMÁRIO

PARTE I
CASOS NACIONAIS

PARTE I

CASOS NACIONAIS

Capítulo 1

OS SERVIÇOS DE INTELIGÊNCIA E DE SEGURANÇA INTERNA NO BRASIL E EM PORTUGAL

Carlos S. Arturi e Júlio C. Rodriguez

Este capítulo analisa, sob uma perspectiva comparada, o desenvolvimento das instituições de inteligência e de segurança pública de Portugal e do Brasil, a partir do início de seus processos de democratização, em meados da década de 1970. O interesse na comparação advém de uma semelhança fundamental para nosso trabalho: as transições de regime em ambos os países integram as três dezenas de casos semelhantes que formam a "terceira onda de democratizações" (HUNTINGTON, 1991). O fato de terem iniciado a mudança de regime no mesmo momento histórico facilita a comparação do desenvolvimento dos órgãos de inteligência e de segurança interna durante a consolidação da democracia. A comparação permitirá igualmente qualificar melhor algumas hipóteses que relacionam o tipo de regime anterior e o modo de transição como variáveis explicativas para os constrangimentos à consolidação dos novos regimes democráticos, particularmente, aqueles dilemas que se referem à institucionalização dos serviços de inteligência e de segurança pública, com legitimidade e sob controle democrático.[1]

Compartilhamos a premissa, explicitada por diversos pesquisadores (BRANDÃO, 2002; CEPIK & BRANDÃO, 2003; CEPIK, 2003, 2005, 2009; NUMERIANO, 2010; BRANDÃO, 2010; MENDONÇA, 2010; PINTO, 2010), de que serviços de inteligência e de segurança interna institucionalizados, legitimados e eficazes são fundamentais para que os regimes democráticos cumpram as

[1] Este capítulo contou com a valiosa colaboração dos alunos Joana Oliveira de Oliveira e Fernando Preusser de Mattos, respectivamente bolsistas de Iniciação Científica da Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS) e do Conselho Nacional de Pesquisa e Desenvolvimento Tecnológico (CNPq).

funções essenciais de manter a ordem interna, a soberania do país e a eficácia na formulação de políticas de segurança pública. O problema crucial do tema em análise é a tensão, sempre existente nos regimes democráticos, entre as funções coercitivas dos órgãos de segurança pública e as liberdades e direitos civis dos cidadãos, bem como entre as necessidades do segredo das funções de inteligência e os controles democráticos de suas atividades. Esses dilemas são particularmente importantes para aqueles países que saíram de longos períodos ditatoriais, como Portugal e Brasil (CEPIK, 2005:68-69).

Com efeito, nos países da "terceira onda" de democratizações, seus atuais órgãos de inteligência e de segurança interna são, frequentemente, herdeiros ou mera continuação daqueles que operavam durante as ditaduras, estreitamente vinculados aos imperativos da repressão política e das contingências da Guerra Fria; ao contrário, nas democracias mais tradicionais, os serviços de inteligência desenvolveram-se primordialmente sob a forte influência da diplomacia e da guerra (CEPIK, 2003). Assim, o amálgama entre segurança pública e segurança nacional, bem como entre inimigo externo e interno, impregnou os passos iniciais da institucionalização dos serviços de inteligência e de manutenção da ordem interna na maioria dos países recentemente democratizados, muitas vezes com efeitos deletérios para as liberdades civis.

Uma das teses de *path-dependency* mais difundidas na literatura especializada (O'DONNELL, 1988) sobre transições para democracia, argumenta que quanto maior apoio político auferisse o regime autoritário no início da transição, mais gradual e controlado seria esse processo e, portanto, maiores seriam as dificuldades de consolidação da democracia, em virtude da presença de "resíduos autoritários" no novo regime. Embora, para Share e Mainwaring (1988), a maneira pela qual a democracia é instalada não determine totalmente seu desenvolvimento posterior, as condições iniciais do novo regime estabelecem as regras do jogo, as modalidades de interação e os limites ao comportamento dos atores e às mudanças políticas. No que concerne ao estudo dos serviços de inteligência e de segurança pública após a "terceira onda" de democratização, examinados neste capítulo, a perspectiva analítica da "path-dependency" foi igualmente muito utilizada, explícita ou implicitamente, em valiosos estudos comparados (CEPIK, 2005; NUMERIANO, 2010; BRANDÃO, 2010; MENDONÇA, 2010; PINTO, 2010). Todavia, é difícil discernir a real influência das diversas variáveis explicativas deste modelo, como argumentaremos ao longo do capítulo.

Nesse sentido, os dilemas afrontados pelos regimes democráticos, decorrentes de transições pactuadas, constituem-se de obstáculos políticos que, ou originaram-se desse modo de transição, ou constituíam características tradicionais do sistema político, e que foram reforçados pelo processo de democratização gradual e controlado pelos dirigentes autoritários. Este foi o

caso do Brasil, mas não o de Portugal. Entender as causas dessa dessemelhança fundamental permitirá melhor compreender os casos singulares em estudo (BADIE & HERMET, 1990).

As principais semelhanças entre os casos português e brasileiro consistem no fato de que as organizações de inteligência e de segurança pública concentraram-se, primordialmente, durante as respectivas ditaduras, na repressão à oposição política, o que torna especialmente problemática sua legitimação nos novos regimes democráticos. As divergências entre ambos os países são, entretanto, mais numerosas. Em Portugal, no período salazarista, houve as guerras coloniais, uma revolução com ruptura entre o antigo e o novo regime, a descolonização, bem como a inserção do país na União Europeia após a redemocratização. Dessa inserção decorreram reformas de sua organização da segurança interna que afastaram a tutela militar e, posteriormente, se enquadraram nas respostas políticas aos atentados terroristas perpetrados na Europa após aqueles de 11 de setembro de 2001 nos Estados Unidos. Essas reformas visam promover maior cooperação interestatal para a segurança regional. Portanto, a institucionalização dos serviços de inteligência portugueses está solidamente implantada nas regras do regime democrático, sob coordenação civil e controle parlamentar.

Por sua vez, o Brasil vivenciou uma transição negociada sob controle dos dirigentes autoritários, que resultou em um regime democrático com alta continuidade política, prerrogativas militares muito importantes e baixo controle civil sobre as organizações de inteligência e segurança. Essas características, associadas à incipiente capacidade estatal para garantir os direitos dos cidadãos e ao estigma de polícia política granjeado pelos serviços de inteligência do passado, dificultam sobremaneira a legitimação e a institucionalização do sistema de informações e de segurança do país no novo regime democrático, apesar das importantes reformas realizadas nos últimos anos para aperfeiçoá-los (CEPIK, 2009; BRANDÃO, 2010; MENDONÇA, 2010).

A questão que buscamos responder, portanto, é em que medida os atuais regimes democráticos de Portugal e Brasil conseguiram equacionar e/ou resolver esses dilemas e tensões entre segurança e liberdade? Como estão constituídos e atuam seus sistemas de inteligência e de segurança interna? Qual o padrão estabelecido das relações entre civis e militares? Qual o grau de controle político democrático sobre as organizações de inteligência e de segurança? Os limites, atribuições, os mandatos legais e a coordenação desses órgãos estão claramente definidos?

Nossa principal hipótese é de que as principais variáveis explicativas da configuração e evolução recente dos sistemas de inteligência e de segurança nos dois países são: as características das ditaduras, o modo de transição política,

as mudanças ocorridas durante a consolidação da democracia, o desenho institucional inicial desses órgãos, a interação entre os diversos atores envolvidos e suas escolhas estratégicas, bem como as relações entre civis e militares. Essas variáveis possuem pesos diferenciados e incidem diferentemente na configuração dos atuais serviços de inteligência, conforme a história política de cada país, como argumentaremos ao longo do capítulo, à luz dos trabalhos realizados por outros pesquisadores sobre o tema. Igualmente, esse esforço analítico permitirá aquilatar o grau atual de institucionalização e de legitimidade dos sistemas portugueses e brasileiros de inteligência e de segurança interna, à luz da ainda escassa, mas qualificada, literatura científica a respeito do tema nos dois países.

Adotamos a definição de "serviços de inteligência" elaborada por Marco Cepik, que enfatiza o caráter estatal e conflituoso de suas funções, demarcando-se de concepções excessivamente amplas e genéricas:

> "(...) organizações permanentes e atividades especializadas na coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, a defesa nacional e a garantia da ordem pública de um país. (...) São organizações que desempenham atividades ofensivas e defensivas na área de informações, em contextos adversariais em que um ator tenta compelir o outro à sua vontade. Nesse sentido, pode-se dizer que essas organizações de inteligência formam, juntamente com as Forças Armadas e a polícia, o núcleo coercitivo do Estado contemporâneo" (CEPIK, 2003:75-76).

Este trabalho aborda principalmente os serviços nacionais de inteligência externa e de segurança interna (voltada crescentemente para atividades de caráter policial e de manutenção da ordem, para as "novas ameaças" e para a luta antiterrorismo) e, em menor medida, de inteligência militar e de estruturas de cooperação regional e internacional. No caso do Brasil, federação cujos estados possuem secretarias estaduais de segurança pública que comandam suas próprias polícias judiciárias e ostensivas (polícias militares), o nível estadual tampouco será priorizado na análise.

Embora não seja objeto da análise, as políticas de defesa militar serão abordadas apenas quando incidirem sobre a segurança interna, através da militarização crescente da luta antiterrorista, da erosão da distinção entre inimigo interno e inimigo externo, e da atenção devotada às denominadas "novas ameaças" (criminalidade transnacional, imigração ilegal, contestação internacional etc.). Atenção semelhante será dedicada à verticalização das atividades de inteligência e de segurança, que formam sistemas nacionais e regionais, e à sua horizontalização, criada pela expansão de organizações especializadas. As fontes de dados utilizadas na pesquisa são provenientes de documentos oficiais, de material de imprensa e da bibliografia especializada.

O capítulo está estruturado em duas partes principais: a primeira consiste de uma descrição histórica do desenvolvimento das organizações de inteligência

e de segurança interna, desde sua origem até sua consolidação nas ditaduras de Portugal e do Brasil. A segunda parte trata da configuração atual do sistema e das organizações de inteligência, conforme elas se desenvolveram ao longo do processo de democratização até o final da primeira década do século XXI nos dois países. Finalmente, faremos algumas considerações finais sobre o tema do trabalho, em uma perspectiva comparativa.

1.1. A Evolução dos Serviços de Inteligência e de Segurança em Portugal

Em maio de 1926, um golpe militar iniciou o período ditatorial em Portugal, o qual, com a ascensão de Salazar ao poder no início dos anos 1930, se tornou conhecido como Estado Novo ou, ainda, período Salazarista. A intenção dos golpistas era promover a restauração da ordem, tendo em vista a turbulência social e política do início do século XX, propósito que amalgamou militares da direita radical, monárquicos e, também, republicanos conservadores, e deu início ao processo de "Revolução Nacional". As grandes manifestações da Confederação Geral do Trabalho (CGT) em 1924 e 1925, bem como a atuação da legião vermelha, simbolizam o cenário de desordem política e social para os militares golpistas. O primeiro período da ditadura teve como presidente o General Carmona (1926-1951). Contudo, após disputas no interior do regime militar, principalmente no âmbito do chamado "Reviralho", que provocou insurreições em 1927, 1928 e 1931, o Ministro das Finanças, António Salazar chega ao poder para institucionalizar a ditadura e transformá-la em Estado Novo (PINTO, 2000; NUMERIANO, 2010; PALACIOS CEREZALES, 2008). Em 1933 é apresentada uma constituição que institucionaliza, enfim, o regime sob o comando de António Salazar. Essa constituição, apesar de apresentar formalidades liberais, colocava o poder legislativo sob o comando do executivo e continha uma legislação de caráter repressivo, além de suprimir controles sobre o governo. Salazar assumiu o comando do Conselho de Ministros e, embora houvesse um presidente (General Carmona), quem chefiou o regime até 1968 foi o próprio Salazar.

1.1.1 A polícia política em Portugal durante o salazarismo

Durante o início do período salazarista houve a "produção" do aparelho repressivo do Estado, com sua reorganização e ampliação (PALACIOS CEREZALES, 2008). Ainda com os acontecimentos do "Reviralho" vivos na memória, corpos policiais (Polícia de Segurança Pública - PSP e Guarda Nacional Republicana - GNR) foram organizados, com reforço da lealdade e de suas funções para com o Estado Novo. Ocorre igualmente a organização da PVDE (Polícia de Vigilância e Defesa do Estado), que mais tarde se tornará a famigerada PIDE (Polícia

Internacional de Defesa do Estado), esta última criada logo após a II Guerra Mundial. Já sob o governo de Marcello Caetano (1969-1974), a PIDE muda de denominação para DGS (Direção Geral de Segurança). Pode-se ainda destacar o papel da legião portuguesa (LP) no Estado Novo, como "auxiliar" dos aparatos repressivos e com perfil nitidamente fascista (ROSAS, 1998).

O processo de constituição da polícia política no início da ditadura do Estado Novo salazarista remetia a organizações criadas no período da I República (1910-1926) que, até então, "eram fundamentalmente polícias de 'ordem pública'" (RIBEIRO, 1995:35). A partir da reestruturação policial de 29 de agosto de 1933, é criada a Polícia de Vigilância e Defesa do Estado (PVDE). O período anterior a 1926, em que se inicia o período ditatorial em Portugal, já apresentava estruturas policiais que seriam reorganizadas e incorporadas à PVDE e, posteriormente, à PIDE. No entanto, deve ser considerado que a forma de atuação, subordinação e suas demais características estruturais e institucionais se modificaram no decorrer dos anos.

O período de maior relevância para a compreensão da PVDE-PIDE, para Maria da Conceição Ribeiro, é o da ditadura de Sidónio Pais, a partir de 1917. Isto se deve às reformas da Polícia Preventiva do sidonismo, que modifica sua denominação duas vezes até 1922. Em outubro de 1922, modifica-se novamente sua designação para Polícia Preventiva e de Segurança do Estado. O decreto de outubro, segundo Ribeiro (1995), organiza essa polícia como polícia política da I República. Portanto, "a Polícia Preventiva criada durante a ditadura de Sidónio Pais surge como a primeira tentativa sistemática de organização de uma polícia política considerada peça-chave do aparelho de Estado e dotada de amplos poderes, incluindo o poder de detenção, de que nenhuma das suas congêneres anteriores parece ter disposto" (RIBEIRO, 1995:51).

No período de 1926 a 1933 ocorrem diversas modificações nas denominações e atribuições das polícias que compõem o aparato repressivo da ditadura. Com a ascensão de Salazar ao poder, em setembro de 1930, é extinta a Polícia Internacional (imigração e estrangeiros) e sua estrutura é inserida na Polícia de Investigação Criminal, que passa a ser subordinada ao Ministério da Justiça e Cultos. Em junho de 1931, por sua vez, é igualmente extinta a Polícia de Informações, que passa a ter suas atribuições destinadas à Polícia de Segurança Pública, ligada ao Ministério do Interior. Nota-se, aqui, a centralidade do Ministério do Interior em assuntos de inteligência interna e de polícia política, que ainda permanece atual, sob a égide do Ministério da Administração Interna. Em maio de 1932, ocorre a primeira tentativa de unificação policial. Um ano depois, é criada a Polícia de Defesa Política e Social, subordinada ao Ministério do Interior. Esse fato é relevante porque, em agosto de 1933, é feita a fusão entre a Polícia de Defesa Política e Social com a Polícia Internacional Portuguesa e há

a criação da Polícia de Vigilância e Defesa do Estado (PVDE), também submetida ao Ministério do Interior (RIBEIRO, 1995).

Após a Guerra Civil Espanhola, o "perigo vermelho" passa a estar no centro das preocupações da PVDE. Entre 1936 e 1939, ocorre a "Cruzada" anticomunista, que induziu a uma escalada da violência repressiva. Com efeito, a defesa da ordem adquire especial atenção, com foco na repressão ao comunismo. Como destaca Pimentel (2009), após o fim da Segunda Guerra, as outras polícias políticas fascistas ou nacional-socialistas foram extintas; em Portugal, contudo, com a manutenção do regime ditatorial, a polícia política adquiriu novos poderes e nova denominação. O Decreto-Lei nº 35.046, de 22/10/1945, cria a Polícia Internacional de Defesa do Estado (PIDE).

> Centralizando no seu seio todos os organismos com funções de prevenção e repressão política dos crimes contra a segurança interna e externa do Estado, a PIDE conservou a instrução preparatória dos processos respeitantes àqueles delitos e ficou ainda com a capacidade de determinar, com quase total independência, o regime de prisão preventiva (PIMENTEL, 2009:31).

Nos anos 1940, a PIDE era composta por três divisões: 1ª Divisão – Serviços Internacionais (SI), 2ª Divisão – Serviço Central de Investigação (SCI), 3ª Divisão – Serviço de Segurança do Estado. Na Guerra Colonial (1960-1962) foram criadas subdelegações e postos de fronteira e vigilância em Angola e Moçambique, colocando a PIDE, "em relação ao ultramar, tal como se encontravam as forças armadas" (PIMENTEL, 2009:40). O recrutamento para Ultramar adquire relevância nesta fase e, em 1962, o número de funcionários da PIDE no ultramar ultrapassa o número no Continente e Ilhas.

As referências encontradas dão conta de que a PIDE não se militariza,[2] como a GNR e PSP, para atuar nas colônias. Segundo Palacios Cerezales (2008) e Pimentel (2009) há o recrutamento de mais agentes para atuar contra os movimentos políticos na Colônia. Costa Pinto (2006, 2010) aponta para uma desmilitarização da PIDE na reestruturação pós-1974. Numeriano também destaca que a PIDE/DGS, mesmo após o golpe de 1974, segue com atividades nas províncias, como organismo de informações militares (NUMERIANO, 2010). Podemos inferir que houve uma militarização parcial devido à amplitude de seu papel no policiamento político. Pimentel e Numeriano também destacam o papel da PIDE na fiscalização dos militares de esquerda e direita dentro do regime. A atuação deste órgão, portanto, era ampla e atingia todas as esferas do poder.

Marcello Caetano, que substitui Salazar em 1968 por motivos de saúde do velho ditador, extingue a PIDE e cria a Direção-Geral de Segurança (DGS), com o

[2] "Militarização" de instituições de inteligência civis deve ser entendida, neste trabalho, na definição de Priscila Brandão: "(...) estamos fazendo alusão ao fato de os postos de comando estarem, em sua maioria, concentrados nas mãos de militares, sejam eles da ativa ou da reserva" (BRANDÃO, 2010:8).

Decreto-Lei nº 49.401, de 19 de novembro de 1969. A nova instituição continuou sob a tutela do Ministério do Interior, com exceção de sua implantação nas colônias, que ficou sob o comando do Ministro do Ultramar. Embora Marcelo Caetano tenha feito diversas críticas à PIDE, a condução e a práticas da DGS foram mantidas como no período salazarista. Em 1972, dois Decretos-Lei modificaram a DGS e formataram a organização, que permaneceu como tal até o final, em 1974. O Ministério dos Negócios Estrangeiros também atuou como grande colaborador da PIDE. O Ministério da Justiça julgava os crimes identificados pela PIDE, porém sempre em acordo com a documentação proveniente desta última.

O fim da 2ª Guerra Mundial anunciou para a oposição ao Estado Novo o "fim dos fascismos" – como se dá no Brasil com a queda de Getúlio Vargas, em 1945 – o que provocou algumas manifestações sociais contra o regime, contidas pelo sistema policial estruturado por Salazar. Porém, após o fim da guerra, algumas modificações têm lugar na imagem e na estrutura do regime, como é o caso da modificação do nome da polícia política do regime, de PVDE para PIDE e do retorno de alguns presos políticos. No entanto, as modificações servem apenas para dar suporte legal para o recrudescimento da repressão, agora sob comando da PIDE. A política externa de Salazar produziu alguns efeitos no pós-guerra que permitiram um prolongamento do regime, mesmo com o aumento da pressão internacional pelo fim do regime corporativista português. O ingresso de Portugal na OTAN simbolizou que a imagem externa do regime não o impedia de ingressar no rol das "democracias" da Europa Ocidental (PINTO & TEIXEIRA, 2007).

O cenário do início da Guerra Fria é de relativa estabilidade social e política em Portugal, com certo grau de desenvolvimento econômico. Nesse período, se dá a campanha presidencial de 1958, em que se enfrentam dois candidatos oriundos do regime, porém com plataformas distintas: o General Humberto Delgado, de "oposição", e Américo Tomás, de situação. Durante e após as eleições, houve diversas manifestações em apoio a Humberto Delgado, que simbolizava, para uma parcela da população, inclusive para o PCP (Partido Comunista Português), uma perspectiva de abertura política. Contudo, a eleição é fraudada a favor de Américo Tomás e os protestos são reprimidos com violência até 1962. Os cenários de fraude, violência repressiva e o advento das lutas anticoloniais põem o país na pauta mundial.

A subida ao poder nos EUA de John F. Kennedy fez com que as iniciativas de descolonização adquirissem amplitude mundial. Os blocos Afro-asiático e soviético foram de grande relevância, como destacam Antônio Costa Pinto e Nuno Severiano Teixeira (2007), no fortalecimento e apoio à causa anticolonial. Há o endurecimento do regime militar no continente e a ampliação do papel das polícias e da PIDE nas colônias (PALACIOS CEREZALES, 2008). A mudança social

no país continua com maior crescimento econômico até a crise do petróleo de 1973, que afeta muito negativamente o país.

Nesse ínterim chega ao poder, em 1968, em substituição ao adoentado Antônio Salazar, Marcello Caetano. O novo governo tem um discurso de "abertura" política, mas o novo cenário social do país e a Guerra Colonial são os principais complicadores do período "marcelista". As manifestações recrudescem, assim como a repressão, que agora fica a cargo da DGS. Como forma de evidenciar esse recrudescimento, o número de prisões da polícia política atinge 766 indivíduos em 1973. É nesse mesmo ano que se iniciam as tratativas para a elaboração do golpe de 25 de abril de 1974, que põe fim ao regime militar e inicia a transição para a democracia em Portugal (PALACIOS CEREZALES, 2008).

1.1.2 O 25 de abril de 1974 e a transição para democracia em Portugal

Após o Golpe Militar de 25 de abril de 1974, que põe fim ao regime salazarista, tem início o período conturbado de transição para a democracia, que apenas se institucionaliza, de fato, após a revisão constitucional de 1982. Segundo Lobo, Magalhães e Pinto (2009), o contexto de transição no qual ocorre o Golpe pode ser caracterizado pela falta de apoio internacional ao regime, no cenário de Guerra Fria, e pelo ambiente de crise do Estado e de descolonização. A singularidade do papel dos militares no caso português se destaca por configurar um golpe militar para levar o país à democracia. Trata-se, portanto, de um golpe em prol da democracia e da descolonização. A incapacidade de Marcello Caetano em pôr fim à Guerra Colonial é salientada com uma das principais razões para o 25 de abril.

Entre 1974 e 1976 desenvolve-se um dinâmico período de transição, repleto de incongruências e conflitos entre as lideranças e grupos que apoiaram o golpe. O processo de transição é caracterizado por uma crise no interior das elites revolucionárias, principalmente entre o Movimento das Forças Armadas (MFA) e alguns generais conservadores que resistiam ao final do império colonial português. A clivagem em torno da descolonização, motor inicial do conflito entre capitães dirigentes do golpe e o General Spínola e outros oficiais generais conservadores, marcou a emergência política do MFA. Esse fator abriu um espaço de mobilização política e social e concomitante crise do Estado, que pode explicar a incapacidade das elites moderadas dominarem "por cima" a rápida institucionalização da democracia representativa (PINTO, 2006:39).

A transição por ruptura com o regime salazarista passa a se tornar visível, principalmente com o chamado "saneamento" da administração pública e empresas, uma purga de sessenta generais das forças armadas e, também, com a extinção da PIDE/DGS (PINTO, 2010). Todavia, o primeiro órgão de informações da Revolução dos Cravos teve breve duração, pois o Serviço Diretor e Coordenador

de Informações (SDCI), criado no dia 23 de maio de 1975, foi extinto em 21 de maio de 1976, deixando acéfala a área de inteligência civil (NUMERIANO, 2010:192-193).

Nesse período ocorrem algumas clivagens na sociedade portuguesa das quais emergem novos partidos, que representam a direita e a centro-direita no país (CDS e PPD). Os movimentos sociais e partidos de esquerda recrudescem suas manifestações, principalmente pela atuação do Partido Comunista Português (PCP). A estrutura de governo após o golpe era composta por um Conselho de Ministros e, subordinados a este, encontravam-se o presidente da República (General Spínola) e a Junta de Salvação Nacional. Relacionados com o presidente da República estavam o I Governo Provisório (Palma Carlos), o chefe de Estado Maior (Costa Gomes) e o Comitê de Coordenação do MFA.

O Movimento de Forças Armadas passa a atuar nesse período como balizador dos conflitos e configura-se como um movimento revolucionário de esquerda. Essa guinada à esquerda pode ser notada pela promoção da Reforma Agrária e de grandes nacionalizações. O golpe militar transforma-se, então, em processo revolucionário com a centralidade do MFA na condução da vida política e social do país. Uma tentativa de golpe para reconduzir os conservadores ao poder, em março de 1975, não é bem-sucedida e provoca, de forma indireta, um pacto entre os militares e partidos acerca da constituição. Garante-se o poder de veto aos militares sobre o texto constitucional que seria aprovado pela Assembleia Constituinte, a ser eleita em 1975 (PALACIOS CEREZALES, 2008).

Após o chamado Verão Quente de 1975 (LISI, 2004, 2005) – quando houve diversas mobilizações antirrevolucionárias, de esquerda e de direita, e uma tentativa de golpe comunista por parte do PCP, que contou com apoio da União Soviética (PINTO, 2006) – as forças moderadas venceram os radicais em 25 de novembro de 1975. Foram eleitos, em 1976, para governar Portugal, após a aprovação da Constituição, o presidente General Ramalho Eanes e o Primeiro-Ministro socialista Mario Soares.

As manifestações e a efervescência política da sociedade portuguesa geraram discursos oficiais dos novos governantes em prol da pacificação e reconciliação do país. Nesse contexto de intensas manifestações políticas, a influência do MFA no processo constitucional pode ser notada pela organização do poder Executivo, no qual há um presidente e um órgão regulador – o Conselho da Revolução. Portanto, entre as condições impostas pelos militares, estavam a escolha de um presidente militar e a criação do Conselho da Revolução, que funcionou, então, como garantidor do processo revolucionário proposto pelo MFA.

Nesse contexto de intensas manifestações políticas é aprovada a nova Constituição da República Portuguesa com todos os elementos acordados em seu texto (LOBO, MAGALHÃES e PINTO, 2009).

A adaptação dos aparatos repressivos e policiais do período ditatorial ao novo contexto de transição é também turbulenta e, como considera Diego Palacios Cerezales (2008), há um recrudescimento da violência policial em resposta ao "novo" ambiente de maior liberdade social e política. Num curto período de tempo, a radicalização das forças policiais (PSP e GNR) provocou algumas mortes. O início da desmilitarização não impediu que abusos sejam cometidos, principalmente pela cultura de violência das polícias herdeiras do período ditatorial. Era intenção do MFA expandir os expurgos nas forças policiais com a criação do Comando Operativo do Continente (COPCON), organização que representava a desconfiança dos revolucionários em relação às forças policiais. A ruptura, entretanto, ocorre de forma mais abrupta e perceptível com as organizações ligadas ao policiamento político, ou seja, PIDE/DGS, cujos membros envolvidos em atos ilegais são expurgados do governo nos primeiros momentos da transição.

Após a aprovação da nova Constituição, inicia-se a consolidação do processo democrático, já que a revisão constitucional de 1982 extingue o Conselho da Revolução, determina a diminuição dos poderes do presidente e cria duas novas instituições democráticas: o Conselho de Estado e o Tribunal Constitucional. A Assembleia da República, por sua vez, constitui o poder legislativo na estrutura de poder do Estado. Após essa revisão constitucional, pode-se afirmar que houve, finalmente, a subordinação dos militares ao poder político-partidário (LOBO, MAGALHÃES E PINTO, 2009). Essa afirmação está relacionada diretamente com a extinção do Conselho da Revolução e da Lei de Defesa Nacional na revisão constitucional.

Assim, em 1982, é criada a nova Lei de Defesa Nacional e das Forças Armadas (Lei nº 29/82) e reformulado o sistema de informações. Para diferenciar do antigo sistema de policiamento político, é criado, também, em 1984, o Sistema de Informações da República Portuguesa (SIRP), pela Lei nº 30/84.[3] Faziam parte do SIRP: Conselho Superior de Informações (CSI), o Serviço de Informações de Segurança (SIS), o Serviço de Informações Estratégicas de Defesa (SIED) e o Serviço de Informações Militares (SMI). Em relação às informações ou serviços de inteligência no período anterior à revisão constitucional de 1982, podemos destacar dois organismos relevantes – SDCI (Serviço Diretor e Coordenador de Informação, ligado ao Conselho da Revolução), o posterior DTEC (Departamento Técnico), e a DINFO (Divisão de Informações, vinculada ao Estado-Maior-General das Forças Armadas – EMGFA). No contexto, a criação de um serviço de informação para a democracia foi também posta em debate, assim como a da Lei de Segurança Interna, o que só ocorrerá em 1987.

[3] Alterada apenas em 2004, com a Lei Orgânica nº 4. A regulamentação desta última ocorreu pela aprovação da Lei nº 9/2007, que promove a reforma do SIRP.

Se no plano das relações civis-militares a transição se consolidava num eixo democrático, na esfera dos serviços de Inteligência isto vai começar somente em 1984. Nos primeiros dez anos do golpe dos capitães, a esfera civil da área de informações permanecera suspensa em um limbo institucional. A Junta de Salvação Nacional extinguiu a PIDE/DGS em 1974, e, nos anos seguintes, os governos provisórios não criaram nenhum órgão civil para a atividade de Inteligência e Contrainteligência (NUMERIANO, 2010).

Em relação aos Serviços de Informações durante a transição, como mencionado anteriormente, há a criação e a extinção de diversas estruturas, bem como a reforma ou alteração de outras. Roberto Numeriano (2010) afirma que entre 1974 e 1984 há o "medo" e a "acefalia" nos serviços de informações – serviço de inteligência em Portugal. Isso se deve à herança dos abusos das polícias políticas do período do Estado Novo e às mudanças nas estruturas do Estado.[4] O "saneamento" posto em prática no pós-1974 e o rompimento com o legado autoritário dessas estruturas se consolida como prioridade da gestão do governo durante a transição. Somente em 1984, com a criação do SIRP, é que se inicia o período de formação das novas estruturas de informações do Estado Português democrático. Contudo, a Lei de Segurança Interna é aprovada apenas em 1987, que confere ao SIS (Sistema de Informações de Segurança) atribuições relevantes para seu funcionamento como órgão de inteligência civil.

O período entre 1982 e 1995 é marcado inicialmente pela Revisão Constitucional de 1982 e finda com as eleições de 1995. Nessa campanha política, a pauta de ampliação dos controles sobre as forças policiais adquire destaque na política nacional. É criada, então, a Inspeção-Geral da Administração Interna (IGAI), com autonomia em relação ao Ministério da Administração Interior. Este organismo fiscalizador passa a atuar decisivamente no controle dos abusos e desvios de conduta das forças de segurança interna do Estado Português.

Nos anos 1990, outra alteração na legislação modifica a Lei-Quadro do SIRP. Essa nova legislação cria o SIEDM (Serviço de Informações Estratégicas de Defesa e Militares), que será extinto e substituído pelo SIED (Serviço de Informações Estratégicas de Defesa) em 2004. Portanto, durante o período de transição para democracia, entre 1975 e 1982, ocorrem revisões constitucionais e reformas constitucionais que alteram substancialmente as estruturas de segurança interna e externa do Estado Português. As mais recentes modificações dessas estruturas serão analisadas mais adiante.

[4] Esta situação de acefalia da inteligência civil, durante uma década, é semelhante à do Brasil quando Fernando Collor assume a Presidência (1990-1992) e extingue o Serviço Nacional de Informações (SNI), mas não cria outro órgão para substituí-lo. Isso só iria a ocorrer em 1999, no início do segundo mandato de Fernando Henrique Cardoso, com a regulamentação da Agência Brasileira de Inteligência (ABIN).

1.2. Os Serviços de Segurança e Inteligência no Brasil até a Redemocratização

De forma ainda embrionária, a atividade de Inteligência institucionalizada no Brasil teve início em 29 de novembro de 1927, com o Decreto nº 17.999, que instituiu o Conselho de Defesa Nacional (CDN) – primeira repartição pública federal criada com o objetivo exclusivo de processar informações em proveito da Presidência da República (FIGUEIREDO, 2005). Ao final da República Velha (1889-1930), o país assistia ao acirramento de rivalidades políticas e ao fortalecimento dos movimentos operários e de contestação contra as elites governantes, como as grandes greves de 1917 e 1918 no Rio de Janeiro e em São Paulo, bem como a fundação, em 1922, do Partido Comunista Brasileiro (PCB). Com a Revolução de 1930, Getúlio Vargas assume a Presidência da República e, quatro anos mais tarde, reorganiza duas vezes o Conselho de Defesa Nacional. Além de dotá-lo de uma assessoria técnica, o Decreto nº 23.873, de 15 de fevereiro de 1934, cria, para cada ministério, as Seções de Defesa Nacional; em agosto de 1934, o CDN é renomeado Conselho Superior de Segurança Nacional.

A mudança na nomenclatura denota o emprego de um conceito mais amplo, o de segurança, que pode ser aplicado a questões internas ou externas, em situações de guerra ou de paz, em detrimento do conceito mais restrito de defesa. Esse processo revela a organização do Estado face aos grupos e movimentos de massa, por meio da tipificação de crimes contra a ordem política e social e da criminalização, principalmente, de comunistas e de estrangeiros. Com a instauração da ditadura do Estado Novo (1937-1945), a atividade de Inteligência e os serviços de polícia passaram a se constituir, claramente, como polícia política, instrumentalizando a repressão aos opositores e inimigos do regime brasileiro.

A institucionalização da inteligência brasileira começa efetivamente após a II Guerra, embora suas estruturas estivessem voltadas para as atividades internas e exercessem funções de polícia desde o Estado Novo varguista. Também desse período resulta a criação de um Departamento Federal de Segurança Pública (DFSP), submetido ao Ministério da Justiça e Negócios Interiores, pelo Decreto-Lei nº 6.378, de 28/3/1944. Fruto de uma reforma do Poder Judiciário, a criação do DFSP consistiu, de fato, na transformação da Polícia do Distrito Federal (à época, o Rio de Janeiro) em um Departamento que se pretendia federal, embora inicialmente restrito ao território do antigo DF. Somente em 1946, o Departamento estenderia sua atuação nacionalmente, dotado de três divisões e de seis delegacias especializadas (ROCHA, 2004:66). Sob responsabilidade da Divisão de Polícia Política e Social (DPS), estavam não apenas as funções de Inteligência, mas também a repressão aos opositores da ditadura de Vargas. Posteriormente ao Estado Novo, o DFSP passou a operar mais com o objetivo de coordenação do que propriamente como polícia investigativa. Mesmo assim,

conforme Rocha (2004: 76), "não é exagero repetir que o 1º DFSP, como agência de segurança pública mais importante no regime de democracia competitiva pós-Estado Novo, obteve seu eixo central através da polícia política". A polícia política por excelência, à frente da repressão política, bem como máquina de propaganda e censura do Estado Novo, foi o Departamento de Investigações e Propaganda, o famigerado DIP.

A atividade de Inteligência vinculada diretamente ao Estado e responsável por assessorar o poder Executivo surgiu em 1946, com a criação do SFICI (Serviço Federal de Informações e Contrainformações). Com efeito, até então, as atividades sigilosas de interesse do Estado brasileiro vinham sendo desenvolvidas por órgãos policiais – sob coordenação do DFSP – e caracterizavam-se pelo aspecto de polícia política do regime vigente (RORATTO & CARNIELLI, 2006). A experiência brasileira na 2ª Guerra Mundial oportunizara o inter-relacionamento entre os exércitos Aliados e a Força Expedicionária Brasileira, o que se mostrou determinante para que os militares brasileiros percebessem a importância da Inteligência para o assessoramento do governo. O presidente e general Eurico Dutra, ex-ministro da Guerra do Estado Novo, que sucede Vargas, ao ser eleito em 1946, cria em setembro daquele mesmo ano, por meio do Decreto-Lei nº 9.775-A, o SFICI, subordinado ao Conselho de Segurança Nacional (nova denominação para o Conselho de Defesa Nacional) e dirigido por oficiais superiores das Forças Armadas. Nota-se, já então, a militarização dos serviços de inteligência civis no Brasil.

Todavia, o SFICI seria estruturado somente em 1956, por meio da determinação do presidente Juscelino Kubitschek, sediado na segunda seção da Secretaria Geral do Conselho de Segurança Nacional. Em setembro de 1958 foram estabelecidas a chefia do SFICI e suas subseções do Exterior, do Interior, de Segurança Interna e de Operações, tendo a existência do órgão "um papel discreto e de pouca significação" (RORATTO & CARNIELLI, 2006:7), uma vez que as forças policiais, e especialmente a Divisão de Polícia Política e Social, ainda representavam a principal fonte de informações político-sociais.

A atividade de Inteligência brasileira passou a ter proporções inéditas a partir do golpe militar de 31 de Março de 1964. Pouco mais de dois meses após a deposição pelas armas do então presidente João Goulart (1961-1964), foi criado o Serviço Nacional de Informações (SNI), pela Lei nº 4.341, de 13 de junho daquele ano. A justificativa principal para a criação do órgão que simbolizou e coordenou a "comunidade de informações" do regime autoritário brasileiro, e que sobreviveu cinco anos após o fim da ditadura, foi a de que o novo governo buscava implantar um serviço de Inteligência que estivesse em conformidade com a Doutrina de Segurança Nacional (DSN), idealizada no âmbito da Escola Superior de Guerra (ESG), desde 1949. Essa doutrina traçava, basicamente, um

diagnóstico das debilidades e capacidades nacionais no contexto da Guerra Fria, enquanto destacava a vulnerabilidade do país ao comunismo, tornando-se necessário, segundo seus proponentes, precaver-se ativamente contra essa ameaça (FICO, 2001:39-42).

A estrutura do SNI contava com uma Secretaria Administrativa, uma Inspetoria Geral de Finanças e uma Agência Central, sediada no Palácio do Planalto, em Brasília, e dividida entre seções de Informações Estratégicas, Operações Especiais e Segurança Interna. O órgão passou a contar também com agências regionais, divididas nas mesmas seções que a Agência Central, inicialmente nas principais capitais, Rio de Janeiro e São Paulo, e em seguida nas demais. A chefia do SNI ficaria, inicialmente, com o General Golbery do Couto e Silva, até a transição presidencial de 1967, quando o General Costa e Silva assumiu o posto do General Castelo Branco (1964-1967) e nomeou o General Emílio Médici como o novo chefe do órgão. Conforme Carlos Fico (2001:42), "não surpreende, portanto, que Golbery tenha se tornado o primeiro chefe do SNI", afinal coube principalmente a ele a elaboração intelectual da DSN, além de ter sido um dos principais proponentes da criação de um órgão de informações deste tipo, desde a década de 1950. O General Golbery também atuou intensamente durante a conspiração contra o governo Goulart, a frente do Instituto de Pesquisas e Estudos Sociais (IPES).

O Departamento Federal de Segurança Pública (DFSP), sofreu reformulações à época do golpe militar. Com a extinção do SFICI e o surgimento do SNI, o próprio DFSP se viu quase extinto. No entanto, o Departamento se manteve e assumiu posição secundária, por assim dizer, no exercício da repressão política, centrando suas atividades na geração de inquéritos judiciais, na autuação e no controle do acesso de estrangeiros, bem como no combate ao tráfico de entorpecentes – função esta em que se especializaria. Mais além, caberia também ao DFSP a execução da censura, por meio da proibição, da busca e da apreensão de materiais e de produtos culturais proibidos pelo regime.

A Academia Nacional de Polícia (ANP), fundada em 1961, pelo General Osmar Soares, surge nesse contexto como instituição de ensino policial, ainda que dirigida pelos militares. Em 1964, ocorre a transferência completa do DFSP para a nova capital do país, sendo rebatizado de Polícia Federal de Segurança (PFS). Até esse momento, contudo, a maior Divisão do departamento, a DPS, permanecia no Rio de Janeiro. Essa mesma Divisão seria transformada, ainda em 1962, na Delegacia de Ordem Política e Social (DOPS).

A garantia do protagonismo militar nos órgãos de segurança pública se deu, portanto, com a implantação de um modelo integrado: as polícias de base municipal – como as guardas civis – foram dissolvidas, enquanto se unificaram nas Polícias Militares estaduais (PMs) todas as polícias ostensivas, sob o comando

dos governadores dos estados. Às PMs seria destinada a função de policiamento ostensivo, muitas vezes sob comando de oficiais do Exército, enquanto a função repressiva destinava-se aos DEOPS estaduais, diretamente vinculados aos secretários estaduais de segurança pública, muitos deles militares, da ativa e da reserva. Os diretores gerais da Polícia Federal, por sua vez, seriam todos oriundos do Exército, em sua maioria generais.

A nacionalização da então PFS somente seria institucionalizada em novembro de 1964 (ROCHA, 2004).[5] Em fevereiro de 1967, a PFS assume definitivamente o nome de Departamento de Polícia Federal (DPF) e se constitui como embrião da estrutura atual da Polícia Federal. Não se pode desconsiderar que, ao longo de toda a década de 1960, as reestruturações do DFSP-PFS-DPF seriam marcadas pela presença dos Estados Unidos na "transferência profissional" e nos programas de intercâmbio e de ajuda, principalmente por meio da Agency for International Development (AID).

A partir de 1968, com o surgimento de ações armadas por grupos de esquerda e com o recrudescimento da repressão, o governo proclama o Ato Institucional nº 5 em 13 de dezembro de 1968. O AI-5 seria a legislação mais repressiva do regime – começam os "anos de chumbo" (1968-1976) da ditadura. Nessa perspectiva, em 1970, o SNI passava a fazer parte de uma estrutura maior de atividades de Inteligência, o Sistema Nacional de Inteligência (SISNI). Coordenado formalmente pelo SNI, o SISNI era composto ainda pelos Sistemas Setoriais de Informações dos Ministérios Civis, pelos Sistemas Setoriais dos Ministérios Militares e por outros órgãos, como assessorias de informações situadas em empresas estatais e esferas da administração pública. Nos ministérios civis, o órgão central de informações passava a ser a Divisão de Segurança e Informações (DSI) – a qual substituía as Seções de Segurança Nacional dos ministérios civis, existentes até 1967 –, aliado a diversas Assessorias de Segurança e Informações (presentes em órgãos da administração pública).

Quanto aos ministérios militares, órgãos específicos da Marinha, do Exército e da Aeronáutica compunham os Sistemas Setoriais de Informações. A Marinha contava com o Centro de Informações da Marinha (CENIMAR), fundado ainda na década de 1950; o Exército, com o Centro de Informações do Exército (CIE), o mais forte e mais atuante dentre os órgãos militares de informações, criado em 1967, justamente para combater as organizações armadas de esquerda. Na Aeronáutica, a estrutura de informações era similar, dotada de um Centro de Informações de Segurança da Aeronáutica (CISA).

Como constava no decreto criador do SNI, sua finalidade distanciava-se da aplicação do poder de polícia, no entanto, estava isento da prestação de contas

[5] Oficialmente, 16 de novembro de 1964 é tida como a data de fundação da Polícia Federal (ROCHA, 2004: 83).

ao Congresso sobre sua organização, suas operações e seu pessoal. A chefia do SNI mostrava-se cada vez mais influente nas decisões da Presidência, a tal ponto que dois dos cinco generais que chefiaram o órgão – Emílio Médici e João Figueiredo – tornaram-se presidentes da República. Muito embora, portanto, a execução da repressão policial à dissidência política não dissesse respeito ao órgão, formalmente, o SNI virou o símbolo do serviço de inteligência interna da ditadura no Brasil.

O fortalecimento do Conselho de Segurança Nacional, em 1968, e o estabelecimento do Sistema de Segurança Interna (SISSEGIN), seguindo a escalada de repressão do regime militar, buscavam, por sua vez, institucionalizar a função propriamente repressiva. Integravam o SISSEGIN os Destacamentos de Operações de Informações (DOI) dos Centros de Operações de Defesa Interna (CODI), órgãos de repressão política e de combate direto à esquerda armada, formados a partir de 1970, organizados segundo as grandes regiões militares e comandados por oficiais do Exército. Os DOI-CODIs eram integrados por oficiais e suboficiais das três armas, membros das polícias militares e judiciária dos estados e também da polícia federal. O conjunto dos DOI-CODIs estava vinculado ao ministro do Exército.

É digno de registro que as funções de polícia política e de combate à oposição armada – em que a tortura era utilizada de forma sistemática, bem como o assassinato e o "desaparecimento" de opositores foram rotineiros no auge da repressão – eram igualmente asseguradas pelos Departamentos Estaduais de Ordem Política e Social (DEOPS), órgãos das secretarias de segurança pública dos Estados brasileiros, onde se destacou, pela importância na repressão e também pela brutalidade, o de São Paulo. Todos estes órgãos e seus funcionários formavam a "comunidade de segurança" do regime, que foi responsável por quase quatro centenas de mortos e desaparecidos políticos e por milhares de torturados, a maioria na primeira metade da década de 1970.

1.2.1 A liberalização política e as divisões da "comunidade de segurança"

Um processo de democratização totalmente finalizado envolve genericamente três etapas: o início da dissolução do regime autoritário, a criação da democracia e a consolidação do novo regime (BERMEO, 1992:273). A longa e gradual transição no Brasil permite distinguir com clareza esses períodos. O primeiro se estende de março de 1974 a março de 1985, e abrange os dois últimos governos militares, as presidências dos generais Ernesto Geisel (1974-1979) e João Figueiredo (1979-1985). A segunda etapa – a construção da democracia – desenvolve-se durante o governo civil de José Sarney (1985 - 1990). Quanto ao processo de consolidação do novo regime democrático, uma espécie de segunda transição, ela inicia-se com a presidência de Fernando Collor

de Mello, em 15 de março de 1990, eleito por sufrágio universal e afastado do poder por um processo de *impeachment* em dezembro de 1992. A partir da substituição de Collor por seu vice-presidente, Itamar Franco (1992-1994), e dos dois mandatos presidenciais de Fernando Henrique Cardoso, a democracia como regime político vai se consolidando no país. Com a posse do presidente eleito Luís Inácio Lula da Silva, em 2003, que significou uma real alternância política no poder, consideramos que o atual regime democrático encontra-se consolidado, embora ainda persistam fatores que o fragilizam, como é o caso do poder real e das prerrogativas que gozam os militares nas atividades relativas aos assuntos de defesa, inteligência e manutenção da ordem interna.[6]

Uma particularidade importante a ser ressaltada, que diferencia a autocracia brasileira de regimes similares na região, foi o fato de apresentar a mais longa duração dentre todos, de ser o mais bem sucedido do ponto de vista econômico, o menos repressivo entre seus congêneres e aquele no qual "os militares como corporação, e não um militar, assumiram a responsabilidade pelo poder e adaptaram as instituições políticas à nova ordem autoritária" (SOARES, 1994:13). De fato, seus dirigentes sempre consideraram o autoritarismo como formato político transitório e mantiveram, praticamente durante todo o período, a existência de partidos políticos, um calendário eleitoral e o Congresso em funcionamento, embora com restrições políticas importantes, como veremos adiante. Esta ambiguidade institucional da ditadura no Brasil se revela extremamente importante para a análise, pois as características do regime autoritário precedente podem, de fato, ser consideradas como uma macro variável política fundamental para a determinação do modo de transição e do tipo de democracia que resultará deste processo. O processo de democratização brasileiro apresenta também como uma de suas características centrais o fato de ter se desenvolvido através de negociações sob forte controle dos dirigentes autoritários. Sob este aspecto, ele é similar ao caso espanhol, como ressaltam Share e Mainwaring (1988), e se diferencia, como mencionamos, do caso português.

O estudo da tentativa que os detentores do poder fizeram para liberalizar gradual e controladamente o regime autoritário e para institucionalizar uma democracia "forte", em que os militares mantivessem um direito de veto sobre a vida política do país, revelou que eles foram relativamente bem sucedidos em seus propósitos. Isto, não obstante as dificuldades encontradas pelo general Figueiredo para conduzir o processo político e sua sucessão nos últimos anos de

[6] A consolidação da democracia é uma espécie de segunda transição e a avaliação da estabilização e o enraizamento deste regime em um determinado país requer um considerável recuo temporal. Para uma posição crítica e bem fundamentada sobre os problemas para a consolidação da democracia no Brasil, centrada basicamente nas relações civis-militares, ver Zaverucha (2005, 2000).

governo, devido às pressões e à mobilização crescente da oposição e de amplos setores sociais que exigiam a democratização efetiva e imediata do país.

A longa duração e a evolução extremamente gradual da fase de liberalização política, assim como a utilização da competição eleitoral como recurso institucional privilegiado da transição, criaram no mundo político brasileiro uma percepção de "normalização" do processo conduzido sob o controle e segundo as regras impostas unilateralmente pelos detentores do poder. Essas regras foram como que "naturalizadas" nas avaliações, cálculos e elaboração de estratégias pelos principais atores políticos ao longo do período. Esse fator "tempo" revelou-se fundamental para o alargamento progressivo do setor moderado da oposição e daquele reformista do regime. Nesse sentido, a perda de controle sobre a transição, ao final da presidência Figueiredo, significou a autonomização da lógica desse processo (LESSA, 1989; LAMOUNIER, 1988), originado por uma estratégia voluntarista dos dirigentes do regime e modelado pelas características mais tradicionais da vida política brasileira: uma "práxis autoritária associada a uma lógica liberal" (TRINDADE, 1985), a centralidade política dos militares e a tradição de conciliação "pelo alto" das elites políticas (ARTURI, 2001).

O alto grau de continuísmo das elites autoritárias na Nova República pode ser ilustrado pelo fato de que, por ocasião das eleições gerais de 1986, que formaram a Assembleia Constituinte, foram eleitos 217 deputados que pertenciam ao antigo partido de apoio ao regime autoritário (ARENA) e apenas 212 provenientes da antiga oposição democrática (MDB) durante o período do bipartidarismo imposto (1966-1979). Este resultado também se deve ao prestígio e apoio significativos de que ainda desfrutava o regime autoritário e suas lideranças na época, em virtude do desenvolvimento econômico alcançado durante o período autoritário e das posições de poder que mantiveram após seu término. Aliás, a presença no poder da elite política civil do regime autoritário após a instauração da democracia foi maior do que no governo Sarney. De fato, o PFL, a partir de 1990 passa a ser o principal partido de sustentação dos governos Collor e Itamar Franco e, em 1994, forma com o PSDB (Partido da Social Democracia Brasileira), a aliança que elegeu o presidente Fernando Henrique Cardoso e como vice-presidente, Marco Maciel (PFL), ex-senador e ex-líder do governo Geisel na Câmara dos Deputados. Em suma, os reformistas do regime autoritário foram os herdeiros políticos privilegiados do processo de transição.

As forças armadas conseguiram prerrogativas políticas extraordinárias, que as mantêm como um dos atores políticos centrais, com grande poder informal, sobretudo em momentos de crise política. Os antigos dirigentes autoritários também obtiveram a garantia de que não haveria "revanchismo" contra os agentes do Estado que cometeram crimes no exercício da repressão contra a oposição,

outro problema candente para a consolidação dos novos regimes democráticos instaurados nas duas últimas décadas.

A partir do início do processo de liberalização política "lenta, gradual e segura", impulsionada pelo General Ernesto Geisel, logo após assumir a Presidência da República, em 1974, o SNI expandiu paradoxalmente suas atividades, passando a desfrutar de grande autonomia já no final dessa década. Muitas vezes, o SNI se confrontou com os DOI-CODIs e com os DEOPS em defesa do projeto de abertura política das presidências Geisel e Figueiredo contra a "linha-dura" militar, encastelada nesses últimos órgãos, que se opunha à liberalização do regime. Um momento grave desse conflito ocorreu durante a acirrada luta política pela sucessão de Geisel, que opôs como pretendentes o chefe do SNI de então, General João Figueiredo (o preferido de Geisel e do General Golbery), e o Ministro do Exército, General Sylvio Frota. Ambos usaram os serviços de inteligência sob seu comando, respectivamente o SNI e o CIE, para reforçar suas posições e recursos e enfraquecer a candidatura oposta. Esta disputa foi selada com a dramática demissão de Frota por Geisel em 12 de outubro de 1977.

O General João Figueiredo toma posse em março de 1979, mas recebe o poder sem contar com a legislação mais repressiva do regime, abolida em dezembro de 1978, e simultaneamente com a eclosão de manifestações de estudantes e de trabalhadores pela redemocratização do país. A extrema-direita, boa parte localizada nos órgãos de inteligência e de repressão, especialmente nos DOI-CODIs e nos escritórios regionais do CIE, começou a praticar uma série de atentados após a promulgação da anistia política, em agosto de 1979, e do retorno dos exilados ao país. Inconformada com a abertura política continuada pelo presidente Figueiredo e temerosa de ser judicialmente perseguida no futuro, em virtude dos crimes cometidos durante o auge da repressão, a extrema-direita reagia. Ocorreram atentados contra revistarias que vendiam jornais de esquerda, contra personalidades, organizações da oposição e da sociedade civil, que resultaram na morte da secretária da Associação Brasileira de Imprensa, em 1980. Figueiredo coloca um general próximo, Octavio Medeiros, na chefia do SNI e reforça a estrutura deste último, justamente na época de abertura política e na ausência de grupos de contestação armada ao regime. O general Medeiros tentou ser o terceiro presidente oriundo da chefia do SNI, mas suas pretensões foram atropeladas pelo "caso Riocentro", em 1981, no Rio de Janeiro. De fato, a explosão de uma bomba no interior de um automóvel ocupado por militares, que resultou na morte de um deles, no estacionamento do centro de convenções Riocentro, onde tinha lugar um show para milhares de pessoas, em 30 de abril, teve consequências múltiplas e importantes para o futuro político do país (ARTURI, 2000; BRANDÃO, 2002). Em primeiro lugar, o episódio significou o fim dos atentados perpetrados pela extrema-direita inconformada com o processo de transição, que ocorriam desde o final de 1979.

O segundo efeito importante do caso Riocentro foi a demissão do General Golbery do Couto e Silva, fundador do SNI, de seu cargo de ministro-chefe da Casa Civil, que ocupava desde o início da Presidência Geisel, já que ele exigia a apuração completa dos fatos e a punição dos responsáveis pelos atentados. Ao não conseguir seu intento, teria pronunciado a célebre frase: "Criei um monstro [SNI]". Ao que se saiba, o SNI não esteve envolvido no caso Riocentro, obra provável agentes do DOI-CODI e do CIE, associados a civis extremistas. A dúvida é se o SNI conhecia há mais tempo a identidade dos autores desses ataques; em caso positivo, se não teria sido complacente com os atentados terroristas para, eventualmente, justificar a escolha do chefe do serviço de informações como sucessor do General Figueiredo, após 1985. Ora, os planos do General Golbery e de Geisel eram os de que o próximo presidente fosse um civil originado dos quadros do partido do regime, o Partido Democrático Social (PDS) e, assim, afastar gradualmente os militares do exercício direto do poder político.

Os resultados das eleições para governador de estado e para deputados estaduais e federais em 1982 dão uma vitória política expressiva para a oposição e são diretamente responsáveis pela perda do controle do processo de transição pelo regime. Graças aos senadores escolhidos indiretamente em 1978, o partido governamental mantém ainda a maioria no Congresso e no Colégio Eleitoral que irá se reunir em janeiro de 1985 para eleger o próximo presidente da República. Mas a partir da eleição de 1982, na qual os partidos de oposição conquistam dez governos estaduais entre os mais importantes do país e a maioria das cadeiras na Câmara dos Deputados, o governo deve administrar o país negociando diretamente com poderosos governadores da oposição e fazer face ao seu desgaste político crescente. A oposição partidária e a sociedade civil organizada começaram, assim, a tolher gradativamente a margem de manobra do regime e a inverter o domínio político da transição, sempre na estrita observância da legislação político-eleitoral imposta pelos governos militares. Esse quadro político complexo, somado ao sentimento de segurança da oposição quanto à irreversibilidade da transição, notadamente após a neutralização da extrema-direita militar devido ao caso Riocentro em 1981, provocaram uma multiplicação de estratégias visando à sucessão presidencial, com um objetivo político igual ao do governo: eleger o futuro presidente no Colégio Eleitoral em janeiro de 1985.

É nesse contexto que surge a surpreendente mobilização pelas eleições diretas à Presidência da República em 1984, conhecida como movimento "Diretas-já". Ela foi a reivindicação mais forte e concreta pela democratização do país após 1964 e pôs em cheque, momentaneamente, a estratégia política do regime e os planos das lideranças oposicionistas mais conservadoras, que já negociavam possíveis alianças com setores do partido governista. O movimento pelas eleições diretas para presidente da República mobilizou milhões de pessoas por todo o país, mas não conseguiu impedir a rejeição, em abril de 1984, do

projeto de emenda constitucional que a implantaria. Entretanto, esse movimento foi fundamental para estimular e justificar o apoio da dissidência do regime, a Frente Liberal, ao candidato do PMDB à Presidência, Tancredo Neves. A grande campanha pelas "Diretas-Já", e sua impotência para alterar as regras impostas pelo regime autoritário, é paradigmática da liberalização "pelo alto" através de acordos e cisões no seio das elites políticas no Congresso, pois, se ela facilitou a dissidência governista e impediu um hipotético recuo político-institucional, foi, todavia, incapaz de dar um desfecho verdadeiramente democrático ao processo de transição, pelo simples fato de que a maioria das lideranças oposicionistas e do próprio governo estavam, naquela conjuntura, satisfeitos com a "legalidade autoritária" e com os ganhos políticos vislumbrados.

Finalmente, a oposição democrática, que conseguiu provocar uma dissidência nas forças políticas e militares do regime, elege indiretamente, no Colégio Eleitoral, em janeiro de 1985, o líder oposicionista moderado Tancredo Neves como presidente da República. Os eventos posteriores são bem conhecidos: a eleição da chapa Tancredo Neves e José Sarney em janeiro de 1985; a internação hospitalar de Tancredo, gravemente doente, na véspera de sua posse em 15 de março; sua morte em 21 de abril. Assim, a fortuna e as opções dos príncipes tornaram José Sarney, ex-presidente do PDS, o partido da ditadura, o primeiro presidente civil desde 1964, resultado muito próximo daquele almejado pelo grupo militar "castelista" que iniciara e controlara, durante quase todo o período, a liberalização do regime uma década antes. O pacto político, que certamente ocorreu, entre o candidato oposicionista e os militares, para impedir qualquer turbulência política na reta final da liberalização, garantiu àqueles últimos prerrogativas e salvaguardas políticas excepcionais para um regime democrático. O continuísmo político e o excesso de "garantismo" tornaram-se as marcas da democratização no Brasil. A lentidão, o gradualismo e o controle exercido nesse período pelos detentores do poder legaram "resíduos autoritários" e reforçaram práticas políticas tradicionais do país, que problematizaram fortemente a fase seguinte de democratização, sob o governo Sarney, e constrangeram o processo de consolidação do novo regime democrático a partir de 1990.

1.2.2 A Presidência Sarney e o Serviço Nacional de Informações (1985-1990)

A fase de democratização no Brasil desenvolve-se durante a Presidência civil de José Sarney (1985-1990), intitulada "Nova República", na qual, em maio de 1985, foi levantada a proibição dos partidos comunistas, deu-se a expansão máxima do sufrágio, com a permissão ao voto dos analfabetos e foi convocada uma Assembleia Nacional Constituinte, eleita em 1986. Posteriormente, a Assembleia Constituinte (1987-1988) redige e aprova a nova Constituição

democrática, em 8 de outubro de 1988, e realizam-se eleições diretas para presidente da República em 1989, pela primeira vez após 1961. Durante a Presidência Sarney, os constrangimentos postos à construção e à consolidação do novo regime são múltiplos e interdependentes: persistência da crise econômica com forte crescimento da inflação, fragilidade política da "Aliança Democrática", falta de legitimidade do novo presidente, eleito indiretamente, aos olhos da maioria da população, e presença de importantes resíduos autoritários oriundos da transição "pelo alto".

Os acordos da oposição com os militares, que permitiram a passagem do poder sem maiores riscos, foram de fato centrados numa série de garantias quanto à não punição dos crimes cometidos pelos órgãos de segurança do antigo regime e à manutenção de prerrogativas das forças armadas, que lhes permitiram ampla autonomia em relação às instituições políticas e influência sobre o processo de constituição da nova ordem democrática, com a manutenção de seis ministérios militares. A tutela militar sobre o sistema político vigorou durante o governo Sarney, em que os ministros militares, sobretudo o do Exército, pressionaram fortemente o presidente e o Congresso constituinte no sentido de restringir as reformas sociais e políticas propugnadas pela oposição de esquerda, bem como para manter parte de suas prerrogativas políticas no novo regime democrático.

Há autores que sustentam que os militares no Brasil perderam muito do poder político que detinham no momento da posse do presidente Sarney em 1985. Wendy Hunter (1997) afirma que a razão desta erosão do poder e das prerrogativas políticas dos militares, durante os governos Sarney, Collor e Itamar Franco, foi o desenvolvimento de uma dinâmica política eleitoral típica dos regimes democráticos no período. Esse processo, associado ao fim da Guerra Fria e à falência da esquerda radical, teria provocado um esforço dos políticos para reduzir tanto o orçamento, como as esferas de influência dos militares, transferindo recursos econômicos e de poder para a arena partidário-eleitoral. Todavia, Zaverucha (2000, 2005) demonstra que o controle civil democrático sobre os militares ainda não se verifica, de fato, no Brasil, onde as forças armadas continuam detendo largas prerrogativas e considerável autonomia política até os dias de hoje. O autor alerta ainda que a dimensão militar na transição e na consolidação democrática tem sido subestimada pelos analistas políticos. Outros autores têm uma opinião mais relativizada que Zaverucha a respeito do poder dos militares após a transição, pois destacam os avanços democratizantes que ocorreram nas relações civis-militares nos últimos anos (OLIVEIRA, 2000), bem como o despreparo e o descaso das elites civis em relação aos assuntos militares e de defesa (D'ARAÚJO & CASTRO, 2001).

No que concerne aos serviços de inteligência, o Serviço Nacional de Informações continuaria, de fato, em funcionamento durante o governo de José Sarney (1985-1990), que assumira o cargo diante dos problemas de saúde do

primeiro presidente civil eleito após o regime militar, Tancredo Neves. Feita a transição política e restabelecida a eleição direta para presidente da República, a ser realizada no final de 1989, a situação interna do país mostrava-se muito menos violenta se comparada às décadas anteriores. Ao contrário dos DOI-CODIs e dos escritórios regionais do CIE, extintos durante a Presidência Sarney, o SNI, sob a chefia do General "geiselista" Ivan de Souza Mendes, manteve a mesma denominação e permaneceu praticamente intacto à redemocratização, inclusive à promulgação de uma nova Constituição em 1988, situação provavelmente inédita na "terceira onda de democratizações".

O SNI continuava concentrado em grupos contrários aos interesses do governo, produzia relatórios mensais a respeito da segurança interna do país e monitorava as greves que se multiplicavam no período (CEPIK & BRANDÃO, 2003). O reflexo dessa situação é a manutenção de uma hegemonia do *ethos* militar – ainda hoje – na condução das atividades de Inteligência civil, na forma de práticas e de legados instituídos durante a ditadura (NUMERIANO, 2010). Somente em 15 de março de 1990, no primeiro dia da Presidência de Fernando Collor de Mello, o SNI seria abolido, como veremos adiante. A partir de 1986, com a Diretriz de Segurança Interna, ficava a cargo do Departamento de Polícia Federal (DPF) e das polícias estaduais a responsabilidade central pela segurança interna (ROCHA, 2004:100). Entre as atribuições previstas na Constituição de 1988 (art. 144) para a DPF, destacam-se: a) o exercício com exclusividade das funções de polícia judiciária da União; b) a apuração de crimes contra a ordem política e social – papel exercido anteriormente pelos órgãos do SISSEGIN; c) prevenir e reprimir o tráfico internacional de entorpecentes e de outras drogas afins, o contrabando e o descaminho; d) exercer as funções de polícia marítima, aeroportuária e de fronteiras; e) realizar ações de Inteligência destinadas à prevenção e à repressão criminal.

Quanto ao último tópico, nota-se que há uma atividade paralela entre o DPF e a atual Agência Brasileira de Inteligência (ABIN), fundada em 1999, como órgãos de Inteligência federais. A distinção, ao menos legalmente, reside no objetivo da coleta, da análise e da difusão das informações: ao contrário da ABIN, a atividade de Inteligência exercida pela PF volta-se à apuração de crimes e ao exercício de polícia judiciária, e não ao fornecimento de informações estratégicas à Presidência com o objetivo de assessorar o Chefe de Estado. Apesar disso, houve casos em que a atuação paralela mostrou-se, de fato, concorrencial (ROCHA, 2003); em outro, uma operação conjunta, denominada "Satiagraha", em 2008, originou um "escândalo" político com sérias repercussões a ABIN e para PF até os dias de hoje, como veremos mais adiante.

1.3. A Configuração Atual do Sistema de Inteligência em Portugal

As principais estruturas de policiamento em Portugal estão ligadas diretamente ao Ministério da Administração Interna, enquanto a Polícia Judiciária, devido ao seu atributo de investigação criminal, está ligada ao Ministério da Justiça. Note-se ainda que o Sistema de Informações de Segurança (SIS) remete-se diretamente ao Primeiro-Ministro, ligado, também, ao Secretário-Geral do SIRP. O controle sobre as atividades de inteligência é externo e parlamentar. O principal fiscalizador do SIRP, após a reforma de sua Lei Quadro em 2004, é o Conselho de Fiscalização, que, conforme consta nesta Lei, deve ser composto por "três cidadãos de reconhecida idoneidade e no pleno gozo dos seus direitos civis e políticos, eleitos pela Assembleia da República por voto secreto e por uma maioria de dois terços dos deputados presentes". Como destaca Numeriano (2010:307):

> Em Portugal, a accountability da atividade de Inteligência é processada pelos três poderes da República: Executivo, Legislativo e Judiciário. O SIS e o SIED são controlados externamente pelo Conselho de Fiscalização dos Serviços de Informação. O Conselho é integrado por três representantes eleitos pela Assembleia da República (AR), por voto secreto e maioria de dois terços – o que significa na prática a escolha de nomes originários das maiorias partidárias no parlamento. O mandato dos conselheiros é de quatro anos e só pode ser revogado por decisão da maioria dos deputados da Assembleia. Outro órgão de controle externo é a Comissão de Fiscalização dos Centros de Dados, integrada por três magistrados do Ministério Público, designados pelo Procurador-Geral da República.

Deve-se ainda mencionar que a fiscalização dos serviços de informação em Portugal, promovida pelo Conselho de Fiscalização, não se restringe à Inteligência Civil, pois o SIRP é também composto por órgãos que desempenham função de inteligência militar – SIED. O controle sobre as atividades de inteligência em Portugal está, após 2004, com um grau de institucionalização elevado, devido ao seu histórico de rompimento com a herança do autoritarismo, principalmente em relação à Polícia Política, e apresenta uma consistente desmilitarização. As reformas constitucionais ou aprovações de diplomas relacionados à segurança, no período recente, estão ligadas diretamente à integração regional europeia.

Contudo, o legado autoritário é maior em relação às forças de segurança interna, pois, como demonstra Diego Palacios Cerezales (2010), a desmilitarização igualmente ocorre, porém de forma mais lenta que no âmbito dos serviços de informação. Embora a transição por ruptura tenha como conduta padrão o expurgo, o saneamento e a dissolução das estruturas do regime salazarista, em algumas áreas, em especial, nas forças de segurança pública (PSP e GNR) o processo não foi tão rápido e radical.

A reformulação do Sistema de Segurança Interna (SSI) entrou na agenda política recente de Portugal e, em 29 de agosto de 2008, foi aprovada a Lei de

Segurança Interna (Lei nº 53/2008), que define a nova Política de Segurança Interna, o Sistema de Segurança Interna, as forças e serviços de segurança e as medidas de polícia. Com a aprovação desta lei alterou-se, portanto, a organização da Segurança Interna em Portugal. O objetivo central desta alteração, que modifica o diploma de 1987 (nº 20/87), é o de responder ao contexto atual de segurança nacional e regional, que se alterou profundamente na última década. A nova lei visou também a permitir uma maior coordenação e cooperação dos órgãos responsáveis pela execução da segurança interna.

O órgão central do novo SSI é o Conselho Superior de Segurança Interna (CSSI), o qual é composto por representantes da Assembleia da República, o Secretário-Geral do SIRP, o Chefe Estado-Maior General das Forças Armadas, o Representante do Sistema Integrado de Operações de Proteção e Socorro e o Diretor-Geral dos Serviços Prisionais. Institui-se o Secretário-Geral do Sistema de Segurança Interna (SGSSI), que se remete diretamente ao Primeiro-Ministro, o qual por sua vez deve relatar ao Presidente as ações principais do sistema. Entre as principais mudanças promovidas pela reforma do SSI está a centralização de atividades na Secretaria-Geral de SSI, que passa coordenar as Forças e Serviços de Segurança (FSS), sob a tutela do Ministério da Administração Interna (MAI) e do Ministério da Justiça.

As mudanças promovidas na organização do SSI também se relacionam com a integração regional e as novas demandas de organização e cooperação securitária regional no âmbito da União Europeia. O combate ao terrorismo relacionado com o pilar de Justiça e Assuntos Internos (JAI) é destaque neste aspecto, pois a cooperação policial entre as forças de segurança portuguesas e o Serviço Europeu de Polícia (EUROPOL), que ficou instituída a partir de 2010, adquire relevância na promoção de segurança na região. Além da cooperação policial com esta agência europeia, há o reforço da necessidade de troca de informações e controle de fronteiras, principalmente com a colaboração do SSI com o FRONTEX e o EUROSUR, ambos relacionados com o controle do trânsito de pessoas entre fronteiras na União Europeia.

Foram aprovadas na sequência da nova Lei de Segurança Interna as novas leis orgânicas das principais forças de segurança interna, a Guarda Nacional Republicana (GNR) e a Polícia de Segurança Pública (PSP). Também, aprova-se a Lei de Organização da Investigação Criminal e altera-se a Lei Quadro do SIRP (Sistema de Informações da República Portuguesa), de 2004, com a Lei nº 9/2007, que estabelece a organização da Secretaria-Geral do SIRP, do SIED e do SIS. Esta lei também regulamenta o regime jurídico ao qual serão submetidas as estruturas do SIRP. Contudo, a organização anterior, dada pela Lei nº4/2004, permanece praticamente inalterada; apenas foram criadas as Secretarias-Gerais acima mencionadas. Assim, o SIRP está sob a tutela de três instâncias de poder

que exercem a fiscalização deste serviço. Cabe ao Conselho de Fiscalização do SIRP da Assembleia da República regular e fiscalizar este serviço. Além dessa fiscalização, a Procuradoria Geral da República, por intermédio da Comissão de Fiscalização de Dados do SIRP, também exerce controle institucional. Contudo, o SIRP é vinculado diretamente ao Primeiro-Ministro, que se remete ao Presidente da República. Há dois conselhos – Consultivo e Superior de Informações – também vinculados ao Primeiro-Ministro. Portanto, o Secretário-Geral do SIRP remete-se a esses dois conselhos e ao Primeiro-Ministro.

Fica, enfim, destacado que as reformas e modificações na Segurança Interna de Portugal respondem a diversos aspectos e promovem uma adequação ao novo contexto pós-11 de setembro, de fortalecimento da integração regional. Nota-se ainda que a militarização diminui e acompanha o avanço da consolidação democrática. A institucionalização desses serviços e sua legitimidade perante a população também crescem, com a criação e regulamentação de estruturas de controle mais efetivas das forças de segurança e de informações. A estrutura e o funcionamento do atual sistema de inteligência brasileiro, como veremos a seguir, encontra-se ainda distante da institucionalização democrática alcançada em Portugal.

1.4. A Trajetória do Sistema de Inteligência do Brasil após a Democratização

A extinção do Serviço Nacional de Informações (SNI) foi instituída pela Medida Provisória nº 150, de 15 de março de 1990 e, posteriormente, pela Lei nº 8.028, de 12 de abril de 1990, nas quais o presidente eleito Fernando Collor, no dia de sua posse, empreendeu uma série de modificações na estrutura da Presidência da República. A Lei nº 8.028 também extinguiu a Secretaria de Assuntos de Defesa Nacional (SADEN), que havia sido criada durante o governo de José Sarney, e criou a Secretaria de Assuntos Estratégicos (SAE), que passou a integrar, dentro de sua estrutura organizacional, o Departamento de Inteligência (DI). Foi na recém-criada SAE, então sob comando de um civil neófito nos assuntos da área e amigo pessoal do presidente Collor, que boa parte dos antigos funcionários do SNI foi realocada. Na realidade, essa Secretaria atuou mais como sucessora da Secretaria Geral do Conselho de Segurança Nacional do que propriamente do SNI (BRANDÃO, 2010). Ao que tudo indica, o presidente Collor extinguiu o SNI movido, sobretudo, por sentimentos pessoais em relação à instituição, e não orientado por uma verdadeira intenção de reforma do setor de inteligência nacional. Esse fato, aliado ao descaso com os assuntos de inteligência, de segurança e de defesa por parte do Congresso, bem como pelo estigma político que as organizações do setor gozavam junto à sociedade civil (BRANDÃO, 2002), foram responsáveis por uma década de inexistência de um serviço de inteligência

estratégica e civil no Brasil. Os serviços militares, por sua vez, continuavam intatos e sem nenhuma regulamentação que não fossem as originadas pelas suas próprias iniciativas. De fato, a verdadeira instituição sucessora do SNI foi a Agência Brasileira de Inteligência (ABIN), implementada apenas em 1999.

A estrutura da Presidência da República passou mais uma vez por alterações com o novo presidente Itamar Franco (1992-1994), após o *impeachment*. De certa forma, Collor havia, com a extinção do SNI e outras medidas, afastado a tutela militar da presidência da República, embora não houvesse tocado nos serviços de inteligência militares. Em novembro de 1992, a Secretaria de Assuntos Estratégicos foi reformulada e incorporou a recém-criada Subsecretaria de Inteligência (SSI), através da Lei nº 8.490. Segundo Brandão (2010) houve um retrocesso nas relações civis-militares durante o governo Itamar Franco, com a reintegração de militares afastados por Collor na SSI, bem como pela ausência de diretrizes para o setor. A indicação para ministro-chefe da SAE de um almirante da reserva colocou novamente a inteligência civil sob comando de um militar, embora a SAE permanecesse vinculada à Secretaria-Geral da Presidência da República.

Nos dois mandatos do presidente Fernando Henrique Cardoso (1995-2002) houve uma tentativa articulada de requalificar as relações civis-militares, através da criação de um Ministério da Defesa, a elaboração da Política de Defesa Nacional (PDN), a formação da Comissão sobre Desaparecidos políticos durante o regime autoritário e a criação da ABIN (BRANDÃO, 2010:143). A PDN constituiu, na avaliação de Diniz e Proença (1997), mais uma declaração de princípios genérica do que uma política de defesa propriamente, mas se tornou um avanço, já que foi o primeiro documento do gênero. A Comissão dos Desaparecidos, por sua vez, conseguiu lançar luz sobre centenas de casos de mortes e desaparecimentos cometidos pelos órgãos de repressão política da ditadura e serviu de base para as indenizações posteriores efetuadas pelo estado brasileiro, embora não tenha havido julgamentos por estes crimes. A Lei da Anistia "recíproca" de 1979, que perdoava os crimes políticos da oposição e aqueles cometidos pelos dirigentes e agentes da repressão, teve sua validade reiterada pela Constituição de 1988 e confirmada por decisão, em 2010, do Supremo Tribunal Federal.

A criação da ABIN teve início em 1995, no início da presidência de Fernando Henrique Cardoso (1995-2002), através da Medida Provisória nº 813. O processo de criação da Agência, contudo, alongou-se devido a resistências políticas – relacionadas à imagem negativa que granjearam os serviços de inteligência no meio político e na sociedade durante a ditadura – e também a pressões corporativas, até que, em 7 dezembro de 1999, foi sancionada pelo presidente Fernando Henrique Cardoso a Lei nº 9.883, que efetivava, de fato, o novo órgão. Essa lei instituiu igualmente o Sistema Brasileiro de Inteligência (SISBIN), que

estrutura esse setor até o início de 2011, pelo menos, e cuja responsabilidade é a de "integrar as ações de planejamento e execução das atividades de inteligência do país". A ABIN foi designada como o "órgão central do SISBIN e com missão de 'planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do país'", diretamente vinculado ao presidente da República e, preferencialmente, sob direção civil.

Sobre as competências da ABIN, a Lei determinou que a agência deveria "planejar e executar ações relativas à obtenção e análise de dados para a produção de conhecimentos destinados a assessorar o presidente da república, planejar e executar a proteção dos conhecimentos sensíveis, relativos aos interesses e à segurança do Estado e da sociedade, avaliar as ameaças à ordem constitucional, tanto no nível interno quanto externo e promover aperfeiçoamento dos recursos humanos e da doutrina de inteligência" (BRANDÃO, 2010:176), não versando sobre contrainteligência e ações encobertas. Merecem atenção dois pontos relevantes e bastante positivos da Lei, aquele que regulamenta a participação do Poder Legislativo na análise da Política Nacional de Inteligência, fixada pelo Presidente da República, e o que estabelece a responsabilidade de fiscalização, por parte do Congresso, sobre as atividades da ABIN. Ainda, são destacados como princípios do sistema "a preservação da soberania nacional, a defesa do Estado democrático de direito e a dignidade da pessoa humana".

Ainda durante o ano de 1999, alterações importantes para a área de inteligência provocaram a relativização de alguns avanços da legislação que criou o SISBIN, como a extinção da SAE, em janeiro, e a criação do Gabinete de Segurança Institucional (GSI) da Presidência da República, em setembro, cujas responsabilidades estavam relacionadas à extinta Casa Militar. O GSI passa a granjear poderes crescentes durante as presidências de Fernando Henrique Cardoso – sob forte influência de seu ministro-chefe, o General Alberto Cardoso – e, igualmente, durante as de Luís Inácio Lula da Silva (2003-2010). Hoje, seu titular, que por determinação legal deve ser um oficial-General nomeado pelo presidente da República, possui *status* de ministro e a ABIN, cujo diretor-geral deve ser aprovado pelo Congresso, passa a ser subordinada ao GSI. Esse arranjo institucional subordina a principal agência do sistema de inteligência civil do país – a ABIN –, cujo diretor-geral pode e deve preferencialmente ser um civil, a um órgão obrigatoriamente comandado por um militar. A militarização, agora, é formal e legal, e a ABIN permanece sem contato direto com a Presidência da República.

Apesar de representar a oficialização da atividade de inteligência no Brasil, a Lei deixou lacunas na regulamentação de pontos muito importantes ao apresentar definições genéricas e deixar temas implícitos. No art. 2º, por exemplo, não fica claro quem são os componentes do SISBIN, a Lei apenas define que "os

órgãos e entidades da Administração Pública Federal que, direta ou indiretamente, possam produzir conhecimentos de interesse das atividades de inteligência, em especial aqueles responsáveis pela defesa externa, segurança interna e relações exteriores, constituirão o Sistema Brasileiro de Inteligência, na forma de ato do presidente da República". Ainda, não há clareza no estabelecimento da área de competência da atividade, do que deveria ser protegido por segredo governamental, e, mais importante, a quem o SISBIN seria subordinado. Por fim, outra falha identificada por Priscila Brandão, é de que a Lei "regulamenta a atuação da ABIN dentro do SISBIN. Não são regulamentadas as atividades de inteligência e contra-inteligência das polícias estaduais, dos comandos maiores e nem mesmo da Polícia Federal, que são de importância fundamental para o funcionamento de nossas bases institucionais" (BRANDÃO, 2010:178).

O estabelecimento dos órgãos citados supra não significou o fim da institucionalização da atividade de inteligência no Brasil. Nos anos seguintes, e até o presente momento, a área continua a passar por mudanças estruturais importantes, algumas positivas para a consolidação da democracia e para o controle democrático sobre as atividades de inteligência, outras, não. Não sendo possível fazer uma análise de todas as alterações já realizadas no campo legal, buscaremos analisar algumas que se destacam. Marco Cepik, em "Regime Político e Sistema de Inteligência no Brasil: Legitimidade e Efetividade como Desafios Institucionais", lista e analisa cinco destas modificações. Primeiramente, a subordinação da ABIN ao Gabinete de Segurança Institucional foi uma das alterações que acarretou o aumento das responsabilidades do GSI, o qual, no governo de Fernando Henrique Cardoso, "transformou-se no principal instrumento agregador dos fluxos informacionais vindos de vários órgãos federais e no locus de gestão de crises nas áreas de segurança interna e externa" (CEPIK, 2005:84).

Em segundo lugar, a criação da Comissão Mista de Controle das Atividades de Inteligência (CCAI), através do Projeto de Resolução do Congresso Nacional nº 08, de 2001, implementou o já previsto Órgão de Controle e Fiscalização Externo. Todavia, esta Comissão é bastante inoperante; seu projeto de regulamento interno ainda não havia sido aprovado até o fechamento deste capítulo (2011). Em terceiro lugar, o Decreto Executivo nº 4.376, de 13 de setembro de 2002, regulamentou a participação dos ministérios no âmbito do SISBIN através da determinação das unidades de cada ministério que fariam a interação com o Sistema, contribuindo assim para a delimitação da organização dele. Ainda, o Ministério da Defesa criou, em 2002, o Subsistema de Inteligência de Defesa (SINDE) com a finalidade de articular, com o Ministério da Defesa, os centros de inteligência da Marinha, Exército, Aeronáutica e Estado-Maior de Defesa. Por fim, a última mudança aqui destacada, é a criação do Subsistema de Inteligência de Segurança Pública (SISP), em 21 de dezembro de 2000.

Cepik ressalta que, até 2005, "seu potencial integrador de fluxos de informação nas áreas de inteligência criminal, inteligência de segurança (interna), contra-inteligência e contraterrorismo foi pouco desenvolvido" (CEPIK, 2005:89).

A expansão do SISBIN, através da criação dos dois subsistemas mencionados supra, deveria incrementar a cooperação entre as agências. Persistem, contudo, sobreposições de interesse, além de baixa especialização formal – características que dificultam a integração de fluxos informacionais. O SISP é coordenado pela Secretaria Nacional de Segurança Pública (SENASP), do Ministério da Justiça, e tem entre seus principais componentes operacionais: o Departamento de Polícia Federal (DPF) e o Departamento de Polícia Rodoviária Federal (DPRF), do Ministério da Justiça; Conselho de Controle de Atividades Financeiras (COAF), Coordenação Geral de Pesquisa e Investigação (COPEI) e Secretaria da Receita Federal (SRF), do Ministério da Fazenda; além do Ministério da Integração Regional, Ministério da Defesa (SPEAI) e Gabinete de Segurança Institucional da Presidência da República (ABIN e SENAD), bem como polícias civis e militares dos 26 estados e do Distrito Federal. Nessa lista incompleta de organizações vinculadas fica evidente a abrangência desse subsistema que, na prática, transforma-se em um sistema apenas parcialmente integrado ao SISBIN (CEPIK, 2009).

Já o segundo subsistema, o SINDE, é coordenado pelo Departamento de Inteligência Estratégica (DIE) do Ministério da Defesa e foi uma tentativa de articular este ministério com os centros de inteligência da Marinha, Exército, Aeronáutica e Estado-Maior de Defesa. Ao Ministério de Defesa estão subordinados formalmente os serviços de inteligência de cada força, bem como secretarias e chefias responsáveis pela inteligência estratégica e operacional. Os serviços militares de inteligência e, portanto, o SINDE, não constituem o foco deste trabalho, mas é significativo que todos eles mudaram de denominação com a democratização do país, estigmatizados que estavam por terem participado diretamente da repressão política – ao contrário do SNI, que manteve a sua denominação durante todo governo Sarney. A Força Aérea Brasileira foi a primeira a iniciar seu processo de reorganização, quando o Ministério da Aeronáutica criou sua Secretaria de Inteligência (SECINT), em janeiro de 1991, na mesma época em que a Marinha cria o Centro de Inteligência da Marinha (CIM), em substituição ao CENIMAR. Posteriormente, em 2004, a SECINT transforma-se em Centro de Inteligência da Aeronáutica (CIAer), sua atual denominação. O serviço de informações do Exército foi o mais demorado dos três órgãos a esvaziar suas atribuições, talvez pelo fato de ele ter sido um dos maiores órgãos de informação e repressão política durante o regime militar. Em 1992, o CIE mantém a sigla, mas passa a utilizar o termo Inteligência em seu nome, tornando-se o Centro de Inteligência do Exército. Mais tarde ocorreu a criação da Escola de Inteligência

Militar do Exército, com o objetivo de reabilitar antigos servidores e preparar novos analistas de inteligência.

Esse é o período, portanto, em que os órgãos da "comunidade de informações" brasileira começam a substituir o termo "informações", utilizado durante a ditadura, por "inteligência" em seus documentos e em suas denominações, possivelmente como forma de se desvencilhar do estigma do passado, além de acompanhar a modernização da denominação do setor (BRANDÃO, 2002). Mendonça (2010) descreve detalhadamente a formação de subsistemas de inteligência de cada força armada singular, no qual cada um integra vários órgãos sem controle civil.

Por fim, houve a criação do Ministério da Defesa, em 9 junho de 1999, e a transformação dos Ministérios da Marinha, Exército e Aeronáutica em Estados-Maiores, cuja repercussão na área de inteligência militar foi sua subordinação aos comandantes de cada Estado-Maior. O Ministério da Defesa possui também uma Subchefia de Inteligência, a qual cabe a função de propor as bases para a doutrina, além de coordenar o Departamento de Inteligência Estratégica (DIE), atualmente pertencente à Secretaria de Política, Estratégia e Assuntos Internacionais (SPEAI), a quem estava designada a função de execução. O Ministério da Defesa, além de racionalizar custos e melhor integrar as forças armadas singulares, significou um passo importante para o relacionamento mais democrático entre civis e militares e diminuiu igualmente a presença militar no centro do poder político. Seu desenvolvimento, entretanto, ocorreu de forma muito dificultosa, com grande resistência dos militares, cujas forças singulares perderam o status de ministério. Houve vários ministros, todos civis, durante sua ainda curta existência, mas a maioria se demitiu em decorrência de crises mais ou menos abertas com a hierarquia militar.

A Presidência Lula, em seus dois mandatos (2003-2010), deixou um legado ambíguo a respeito da institucionalização das organizações e atividades de inteligência e de segurança internas. No primeiro mandato, Lula praticamente nada alterou no setor, mas estabeleceu formalmente, por intermédio da Lei nº 10.683, de 28/5/2003, a coordenação da ABIN pelo GSI, comandado por um general. Igualmente, não realizou alterações na inteligência militar, pelo contrário, aumentou paulatinamente as atribuições de inteligência do Ministério da Defesa (MD) (MENDONÇA, 2010). É apenas em julho de 2007, com a posse do Ministro Nelson Jobim, ex-presidente do STF e um dos principais redatores da Constituição de 1988, que o MD começa a ganhar estatura política, influência nos assuntos de defesa e a subordinar os respectivos comandos militares. O ministro Jobim se tornou um intermediário de confiança entre os militares e o governo de esquerda durante o governo Lula. A atual presidente Dilma Roussef, que tomou posse em 1º de janeiro de 2011, o manteve inicialmente como ministro da

pasta.[7] Foram ainda elaborados, durante a Presidência Lula, a Política Nacional de Defesa, em junho de 2005, e a Estratégia Nacional de Defesa, em dezembro de 2008, que, gradativamente, auxiliam a institucionalização democrática do setor.

Todavia, a alteração mais significativa nas relações institucionais entre poder civil e militar ocorreu recentemente, com as modificações legislativas introduzidas pela Lei Complementar nº 136, em 25/8/2010, que transforma o antigo Estado-Maior de Defesa – que era subordinado ao MD, mas até então com poderes limitados em relação às Forças Armadas – em Estado-Maior Conjunto das Forças Armadas (EMC-FA), doravante "responsável pelo emprego, e aos Comandantes das Forças Singulares, o preparo do Poder Militar. Em razão dessas competências, o Chefe do EMC-FA situa-se na mesma hierarquia e linha de prioridade dos Comandantes das três Forças. (...) Com efeito, o ministro da Defesa passou a estar inserido na cadeia de comando das Forças Armadas. Pela legislação anterior, ele ficava na lateralidade como um [mero] chefe administrativo'" (MENDONÇA, 2010:60). Adicionalmente, a legislação permitiu não apenas que o ministro nomeasse indiferentemente civis ou militares para as Secretarias do MD, antes restritas aos militares, como também adquirisse mais prerrogativas na promoção dos generais.

Essas importantes modificações legais para a alteração das relações civis-militares no Brasil – em que, desde 1985, os militares exerciam efetivamente autonomia no que dizia respeito às políticas de defesa e ao funcionamento de suas instituições – não foram acompanhadas por medidas semelhantes na área de inteligência. Ao contrário, o escopo da inteligência militar foi ampliado e a inteligência civil, cujo órgão máximo é a ABIN, que coordena legalmente o SISBIN, encontra-se em crise, após o envolvimento em mais um escândalo político, a Operação Satiagraha, em 2008. Esse epíteto designa uma operação policial-judiciária, comandada por um delegado da Polícia Federal, sobre um escândalo financeiro que envolvia um banco de investimentos, companhias telefônicas e a luta entre eles pela obtenção do controle acionário das companhias estatais que haviam sido privatizadas no fim da década de 1990. A investigação policial se utilizou de dezenas de agentes da ABIN, apesar de dirigida por um delegado da PF, e acabou resultando no escândalo e na crise institucional das supostas escutas clandestinas. Estas teriam sido realizadas por agentes da ABIN, que teriam igualmente gravado conversas do Presidente do Supremo Tribunal Federal e de outras autoridades.

[7] Contudo, o ministro deu declarações que incomodaram o governo de Dilma, desgastando sua posição até torná-la insustentável. Em 4 de agosto de 2011, a presidente Dilma convidou o ex-chanceler Celso Amorim para comandar a pasta da Defesa, o que foi recebido com desconfiança pelos militares, principalmente pelas posições políticas de Amorim diante do Itamaraty.

O envolvimento da ABIN, em tal escala, com questões policiais de ordem interna é, de fato, esdrúxulo e nunca foi bem explicado.[8] Há o fato de que o então diretor-geral da ABIN também era delegado da PF; e, em decorrência do escândalo, foi substituído no posto. Mendonça utiliza-se, como Priscila Brandão, do recurso analítico de *path-dependency* (COLLIER & COLLIER, 1991) – mas, ao contrário da autora, em nível puramente organizativo e institucional – para demonstrar como o "caso Satiagraha" foi um momento crítico para o conjunto ABIN/SISBIN. Este pesquisador, e oficial de inteligência concursado da ABIN, como fez questão de esclarecer em sua dissertação da ESG, escora-se também no argumento de Wolfgang Krieger (2009) de que o mais poderoso controle das atividades de Inteligência é o controle legislativo e suas comissões específicas. Todavia, segundo este autor, o legislativo é geralmente ineficiente e mesmo negligente até a eclosão de um escândalo político ou de um erro de "inteligência" grave no setor. Nesse momento, o poder legislativo reage, quer estabelecendo comissões de inquérito, quer formando comissões para reformas do sistema de inteligência, como veio a acontecer a partir do caso Satiagraha, no Brasil, e dos atentados de 11 de setembro de 2001 nos Estados Unidos, situações que Mendonça compara em seu trabalho.

Após a denúncia da suposta escuta clandestina do presidente do STF, o presidente Lula decide afastar a cúpula da ABIN e cria, em fevereiro de 2009, um Comitê Ministerial para Elaboração da Política Nacional de Inteligência e Reavaliação do Sistema Brasileiro de Inteligência, com prerrogativa de sugerir medidas e reformas em todo o sistema (MENDONÇA, 2010:120). A Comissão virou palco de disputa burocrática que envolvia primordialmente o MD e o GSI, bem como, secundariamente, o Ministério das Relações Exteriores. A Comissão Ministerial (GT-SISBIN), onde a ABIN estaria sub-representada, realizou cerca de quarenta reuniões entre março e agosto de 2009, e apresentou seus resultados ao presidente da República em novembro do mesmo ano. A principal sugestão do GT-SISBIN é a de uma reformulação profunda do sistema de inteligência brasileiro e do papel da ABIN nele, pois essa agência deixaria de ser o órgão coordenador do sistema de inteligência nacional, em prol de "um colegiado de mais alto nível". Assim, a proposta sugere a criação de uma nova camada superior, a cargo do GSI, seguindo a tendência de expansão vertical do sistema de inteligência (CEPIK, 2003). Esta nova superestrutura coordenaria quatro subsistemas (estratégica, defesa, segurança pública e econômica), cabendo à ABIN apenas a coordenação do subsistema de inteligência estratégico. Esta proposição contraria, de fato, o espírito da lei que instituiu a agência e o SISBIN,

[8] A ABIN já havia sido envolvida, direta ou indiretamente, em outros escândalos, que lhe fizeram perder graus de liberdade no sistema de inteligência, como sua subordinação ao GSI logo após o caso das gravações clandestinas de empresários e autoridades durante o processo de privatização de algumas empresas estatais, no final da década de 1990. Ver BRANDÃO (2002).

em 1999, que garantia, via ABIN, a coordenação civil de todo o sistema de inteligência nacional (MENDONÇA, 2010:131).

O problema principal da institucionalização da inteligência civil não seria, portanto, o estigma que sofre a ABIN de ser a herdeira do SNI [9] ou sua militarização interna – que, segundo Mendonça, está declinante – mas a de ser impedida de se tornar a principal instituição civil de coordenação da inteligência de Estado. Em suas palavras: "[A ABIN] é alvo de críticas e disputas intragovernamentais as quais, em princípio, têm suas origens no que se convencionou chamar de 'competição burocrática' por poder ou autonomia no âmbito do sistema estatal de decisão estratégica" (MENDONÇA, 2010:125). Nesse caso, os militares procuram ampliar seu "território" e os diplomatas, por sua vez, aliam-se ou com eles ou com os agentes da ABIN, ao sabor de suas conveniências (Idem, 2010:153).

Além dos problemas relativos à institucionalização do SISBIN sob controle civil e democrático e às prerrogativas militares remanescentes da transição pactuada, é na inefetividade do Estado de Direito democrático para boa parte da população, explicitada pela violência generalizada e pela falência da segurança pública, que reside, em nosso entender, a característica mais insidiosa para o aprofundamento do regime democrático no Brasil. Inefetividade e violência que atingem primordialmente os mais pobres. Com efeito, o Estado não consegue exercer o monopólio da violência e impor a ordem político-democrática no conjunto do território nacional. Por sua vez, as agências estatais resistem em atender com equidade e em reconhecer os direitos da população mais pobre e das minorias sociais; especialmente os órgãos de segurança pública, que persistem no emprego de métodos arbitrários e violentos sobre estes setores. O'Donnell utiliza-se do conceito de "cidadania de baixa intensidade" e de "democracia iliberal" para descrever a situação na qual "se respeitam os direitos participativos e democráticos da poliarquia, mas se viola o componente liberal da democracia. (...) Esta bifurcação constitui o reverso da moeda da complexa mescla de componentes democráticos e autoritários nestes estados" (O'DONNELL, 1993).

Sinal dos tempos, em 2010, forças do Exército e da Marinha, juntamente com as polícias estaduais do Rio de Janeiro e da PF, participaram de uma grande operação de policial em uma favela do Rio de Janeiro, indício de militarização também na segurança pública, bem como de "federalização" das secretarias de segurança pública estaduais, cujos titulares são, hoje, em boa parte delegados de polícias federais. A PF, baseada em seus recursos e em sua reputação de probidade e eficiência, estende sua influência sobre a inteligência interna e de segurança pública e sobre as polícias estaduais, o que demonstra a falência das estruturas de ordem pública da maioria dos entes federados no Brasil.

[9] Ver Priscila BRANDÃO (2002) e obra mais recente da mesma autora (BRANDÃO, 2010).

No recente período de redemocratização, a primeira tentativa de formulação de um plano nacional de segurança pública veio à tona no segundo mandato do presidente Fernando Henrique Cardoso (1999-2002), quando ele lançou um documento que trazia importantes contribuições à formulação de políticas de segurança pública, distanciando-se da reprodução acrítica da tradição autoritária que caracterizara os governos anteriores: prevenção da violência, por meio da implementação de programas sociais, o Plano de Integração e Acompanhamento dos Programas Sociais de Prevenção da Violência (PIAPS), bem como pela afirmação da agenda de Direitos Humanos, enfatizada com a criação da Secretaria Nacional de Direitos Humanos e com o primeiro Plano Nacional de Direitos Humanos. Paralelamente, a atuação da Secretaria Nacional de Segurança Pública (SENASP) e a criação de um Fundo Nacional de Segurança Pública exemplificam a atenção dada pelo governo FHC ao setor, muito embora a falta de sistematização e de coordenação entre as instituições, bem como a carência de verbas e os atritos políticos, tenham inviabilizado muitos dos objetivos propostos. Em suma, foi na presidência de Fernando Henrique Cardoso que tiveram lugar as iniciativas mais importantes para alterar as relações civis militares, com a criação do Ministério da Defesa, e institucionalizar a inteligência estratégica civil, através da ABIN e do SISBIN.

No primeiro mandato do presidente Lula (2003-2006), um novo Plano Nacional de Segurança Pública foi incorporado ao programa de governo, tendo início a sua execução por meio da SENASP. Por sua vez, sucessivas ações da Polícia Federal foram levadas a cabo e amparadas por ampla cobertura da mídia, o que contribuiu para a construção de uma identidade – perante a opinião pública – de competência e destemor. Em agosto de 2007, o governo federal lança o Programa Nacional de Segurança Pública com Cidadania (Pronasci), propondo envolver dezenove ministérios e articular estados e municípios nas suas 94 ações. Menos do que uma alternativa aos planos anteriores na área de segurança pública, "o Pronasci reitera o Plano Nacional de Segurança Pública do primeiro mandato do presidente Lula, o qual, por sua vez, incorporava, sistematizava e explicitava o que já estava, embrionária ou tacitamente, presente no Plano Nacional do governo Fernando Henrique Cardoso" (SOARES, 2007:92). Em acréscimo à iniciativa do Pronasci, o Ministério da Justiça – em parceria com o Conselho Nacional do Ministério Público (CNMP) e o Conselho Nacional de Justiça (CNJ) – formulou, em fevereiro de 2010, a Estratégia Nacional de Justiça e Segurança Pública (ENASP). Todavia, ainda falta muito para avançar os princípios e procedimentos democráticos nesta área.

1.5. Considerações Finais

O objetivo central do trabalho consistiu na comparação entre os arranjos institucionais dos serviços de inteligência e de segurança interna de Portugal e Brasil, que permitisse uma melhor compreensão do desenvolvimento dessas instituições e de seus desafios atuais, a partir dos processos de democratização nos dois países. Alguns estudiosos dos processos de democratização na América Latina destacam, com efeito, uma forte afinidade entre tipos de regimes autoritários precedentes, modos de transição à democracia e dilemas decorrentes das características destes processos para a consolidação dos novos regimes democráticos (NOHLEN & THIBAUT, 1994), o que caracteriza um padrão de *path-dependency*. Este debate enquadra boa parte dos estudos realizados sobre os serviços de inteligência e manutenção da ordem interna após a redemocratização, embora com nuances significativas entre eles.

Ao tratar de Portugal, António Costa Pinto (2010), ressalta igualmente a importância do modo de transição, se por ruptura ou pactuada, para a definição das características e dos dilemas do novo regime democrático. O autor descreve a grande ruptura, em Portugal, com a ordem anterior – a Revolução dos Cravos de abril de 1974 – que implicou o desmantelamento do aparato de inteligência e de polícia política da ditadura e o afastamento da tutela militar sobre o sistema político já em 1982, marco inicial da consolidação democrática do país. Portugal torna-se, assim, uma espécie de caso de controle exemplar da democratização dos serviços de inteligência e de consolidação da democracia, durante poucos anos, em contraste com o caso brasileiro (NUMERIANO, 2007). Entretanto, como bem demonstra António Costa Pinto, a democratização no país não se desenvolveu de forma linear, nem sem conflitos agudos, devido ao peso do "duplo legado" da revolução de Abril: o protagonismo dos militares e a forte influência do Partido Comunista Português.[10]

Nesse caso, a *path-dependency* é muito evidente e a variável explicativa fundamental para a institucionalização democrática daquelas organizações reside mais no tipo de transição do que nas características do regime anterior, na "natureza da ruptura", como bem explica António Costa Pinto (2010:407); ruptura que foi exemplar em Portugal, inclusive com golpe de estado militar para instaurar a democracia. Cremos que, efetivamente, nos modos de transição por ruptura com o regime anterior, a variável modo de transição é decisiva, pois os novos dirigentes buscam conscientemente romper com as instituições e práticas do passado; portanto, o tipo de regime anterior perde importância no desenho das novas instituições políticas e coercitivas. Naqueles países onde as ditaduras caíram por colapso, como na Argentina, ou por golpe, como em Portugal, o novo regime democrático possui menos constrangimentos e legados autoritários da transição, o que lhe permite impor uma ruptura política e institucional profunda

[10] Para uma análise mais detalhada da Revolução do Cravos e seus desdobramentos, ver Schmitter (1999).

em relação ao *ancien régime*, sobretudo no que concerne aos órgãos coercitivos e de inteligência.

Mesmo assim, o novo sistema de inteligência português demorou quase uma década para ser criado após a Revolução de Abril, e foi antecedido pela afastamento da tutela militar e pelo início da consolidação da democracia, com a reforma constitucional de 1982. Fenômeno semelhante ocorreu no Brasil, entre a extinção do SNI da ditadura, no início da presidência Collor, em 1990, e a efetiva criação da ABIN no final de 1999, no início do segundo mandato de Fernando Henrique Cardoso. Esta coincidência pode ter várias causas, mas certamente traduz a dificuldade das novas democracias – mesmo naquelas que rompem definitivamente com o antigo regime, como em Portugal – para lidar com o estigma dos serviços de inteligência criados nos tempos de repressão política.

Conforme os diversos autores, as variáveis explicativas que relacionam democratização e novas instituições de inteligência e segurança interna mudam de relevância para a explicação dos constrangimentos ao controle civil e democrático sobre as organizações de inteligência brasileiras pós-democratização. Para aqueles, como Zaverucha (2000, 2005) e Numeriano (2010), que privilegiam na análise as relações civis-militares, o fator mais importante é a desmilitarização dos órgãos de inteligência externa e interna, condição necessária para a consolidação do regime democrático, a qual, para estes autores, não foi ainda alcançada no Brasil. Numeriano (2007:283) considera que "a inteligência civil brasileira está ainda em transição", sob hegemonia dos militares, e lembra Boraz & Bruneau (2006), para quem a consolidação da democracia só estará confirmada com o controle civil sobre a área de inteligência.

Já Cepik (2005, 2009), Priscila Brandão (2010) e Mendonça (2010) estão mais atentos aos fatores institucionais, aos interesses e à interação entre os principais atores da área. Todavia, há nuanças entre todas estas interpretações. Priscila Brandão atribui ao legado da transição e às escolhas feitas pelos atores relevantes nos "momentos críticos" destes processos – que, no caso brasileiro, teve lugar no ano de 1984, quando da grande campanha popular frustrada por eleições diretas para presidente da República – as principais origens dos constrangimentos à institucionalização do setor de inteligência civil no Brasil. Nessa interpretação, também calcada no modelo de *path-dependency*, o tipo de regime anterior teria menor valor explicativo que o modo de transição, processo que deixou legados autoritários (militarização, estigma dos órgãos de inteligência, descaso político e social para com o setor etc.) que ainda dificultam, no seu entender, a institucionalização legitimada dos serviços de inteligência e a supremacia política civil sobre os militares. Segundo a autora, na estrutura atual dos serviços de inteligência ainda preponderam os interesses militares sobre os civis (BRANDÃO, 2010). A pesquisadora conclui que a forma de transição

influencia mais o padrão das relações civis-militares no novo regime democrático que a reforma das instituições de inteligência, "cujos resultados encontram-se muito mais ligados ao desempenho da sociedade política do que aos acordos celebrados na transição" (Idem, 2010:257).

Assim, para Brandão, o interesse civil e legislativo torna-se "uma variável mais relevante do que os constrangimentos institucionais no processo de refundação das agências nacionais civis de inteligência no Brasil, no Chile e na Argentina" (Idem, 2010:259). No caso brasileiro, a extinção do SNI no início do governo Collor bem o demonstrou, embora o governo não tivesse um projeto alternativo. Quando o governo de Fernando Henrique Cardoso iniciou uma reforma mais profunda nas relações civis-militares e criou uma agência civil que coordenasse o sistema de inteligência do país, enfrentou resistências ideológicas, corporativas e o descaso da sociedade política com estas alterações, ainda inconclusas e indefinidas.

A argumentação de Cepik distancia-se das teses que estabelecem vínculos fortes entre o modo de transição e seus efeitos sobre a institucionalização dos serviços de inteligência e segurança pública, embora reconheça a repercussão daqueles processos sobre os constrangimentos atuais que pesam sobre o setor.[11] Este pesquisador, em trabalho sobre as agências de inteligência brasileiras, baseado em modelo de Peter Gill (1994), conclui que, em 2004, "as reformas estruturais brasileiras na área de inteligência foram em larga medida bem-sucedidas do ponto de vista de sua adequação ao contexto de um regime democrático consolidado" (CEPIK, 2005:97). Todavia, ele alerta que "a profissionalização dos serviços de inteligência no Brasil ainda depende de um longo percurso no que diz respeito às Forças Armadas e à polícia" (Idem, 2005:96) e que a inteligência doméstica está superdimensionada em relação à externa, bem como muito próxima das questões que envolvem a segurança do Estado e a criminalidade violenta (CEPIK, 2009:vi).

Mendonça (2010), por sua vez, é o único autor que não inclui os processos de democratização como uma variável que influencia a configuração atual dos órgãos de inteligência. Este autor analisa a evolução da legislação que instituiu o Sistema de Inteligência Brasileiro e a Agência Brasileira de Inteligência, em 1999, que consagrava a supremacia do poder civil sobre a inteligência de estado (2010:129). A situação atual do setor, no entender do autor, caracteriza-se por uma "hipertrofia da inteligência militar" (2010:77) e por uma profunda disputa intercorporativa entre militares, diplomatas e civis da ABIN, na qual os dois

[11] Marco Cepik utiliza, em estudo sobre a origem dos serviços de inteligência (2003), as conclusões de Amy Zegart (1999), para quem as variáveis explicativas com maior influência na evolução dos órgãos de segurança nacional são de caráter político e institucional.

primeiros atores tentam impedir que este serviço desempenhe efetivamente o papel de órgão coordenador do SISBIN.

O projeto de Programa Nacional de Inteligência, realizado pelo GT-SISBIN ainda não foi aprovado, pois o presidente Lula sugeriu que a Comissão Mista de Controle dos Assuntos de Inteligência (CCAI) do Congresso elaborasse um parecer sobre o documento. Entretanto, mesmo com a troca de governo, a dinâmica da reforma não arrefece. A nova presidente da República, Dilma Roussef, que tomou posse em 1º de janeiro de 2011 já removeu a Secretaria Nacional Antidrogas (SENAD) do Ministério da Defesa para o da Justiça, o que sinaliza uma desmilitarização do setor de segurança pública. Os atores interessados tampouco se desmobilizam. Assim, representantes da Associação Nacional dos Oficiais de Inteligência (AOFI) entregaram uma carta endereçada à presidente Dilma, em fevereiro de 2011, onde reivindicam o fim da subordinação "militar" ou "policial" da ABIN e acesso direto ao chefe de governo. A missiva teria sido uma reação a supostas tentativas de interferência do novo ministro-chefe do GSI, um general do Exército, na ABIN (*ZERO HORA*, 9/2/2011, p. 6). De todo modo, os oficiais da agência, ao também se referirem à tutela policial, sugerem que tampouco preferem que seu diretor-geral seja um delegado da PF, como ocorreu nos últimos anos.

Percebe-se que o sistema de inteligência brasileiro evolui com avanços e recuos, no que concerne a sua coordenação civil e a seu controle democrático, e encontra-se, no início de 2011, em mais um momento crítico de sua institucionalização. No que diz respeito aos modelos de *path-dependency* baseados nos processo de democratização, podemos afirmar que no caso das transições pactuadas e graduais, como a brasileira, torna-se muito difícil discernir o peso das variáveis ligadas ao tipo de regime anterior, modo de transição e dinâmica da consolidação democrática, pelo grau de influência de uma fase sobre outra. Há a necessidade de mais estudos empíricos e comparativos para o avanço da teoria sobre o tema.

Em suma, a estrutura do sistema de inteligência brasileiro, ao contrário daquela de Portugal, defronta-se ainda com o desafio de se institucionalizar, em período de conflito e de indefinição aguda em relação ao seu futuro próximo, embora as primeiras atitudes do novo governo sejam alvissareiras. No que concerne ao provimento da ordem pública democrática, segundo Luiz Eduardo Soares (2007:86), pesquisador e ex-secretário de segurança pública do estado do Rio de Janeiro, "a transição democrática não se estendeu à segurança pública", a qual se mostra ainda, "do ponto de vista dos interesses da cidadania, ineficiente". Dessa constatação, emerge como prioridade fundamental para o setor, na atualidade, a reforma profunda na estrutura e nas instituições de segurança pública do país (federais e estaduais), bem como o desenvolvimento

institucional das organizações de inteligência e de manutenção da ordem, sob direção e controle político civil.

REFERÊNCIAS

ALENTE, Manuel Monteiro Guedes (Coord). (2005). *I Colóquio de Segurança Interna*. Instituto Superior de Ciências Policiais e Segurança Interna. Coimbra, Edições Almedina.

ARTURI, Carlos S. (2000). *Le Brésil*: une tentative de démocratisation octroyée (1974-1985). Villeneuve d'Ascq, Presses Universitaires du Septentrion, 502 p.

_____. (2001). O Debate sobre Mudança de Regime Político à Luz do Caso Brasileiro. *Revista de Sociologia e Política*, Curitiba, n. 17.

BADIE, Bertrand; HERMET, Guy. (1990). *Politique Comparée*. Paris, PUF.

BERMEO, Nancy. (1992). *Democracy and the Lessons of Dictatorship*. Comparative Politics, v. 24, n. 3.

BORAZ, Steven & BRUNEAU, Thomas. (2006). "Democracy and Effectiveness". *Journal of Democracy*, v. 17, n. 3, National Endowment for Democracy and The Johns Hopkins University Press.

BRANDÃO, Priscila C. (2002). *SNI & ABIN*: uma leitura da atuação dos serviços ao longo do século XX. Rio de Janeiro, Editora FGV.

_____. (2010). Serviços Secretos e Democracia e no Cone Sul: premissas para uma convivência legítima, eficiente e profissional. Niterói, Impetus.

BRUNEAU, Thomas C. & MATEI, Florina C. (2008). Hacia una Nueva Conceptualización de la Democratización y las Relaciones Civiles Militares. *Democratization*, v. 15, n. 5, p. 909-929. ISSN 1351-0347 print/1743-890X online. DOI: 10.1080/13510340802362505 # 2008 Taylor & Francis.

CARRILHO, Maria. (2000). Forças Armadas e Democracia. In: PINTO, António Costa (Coord). *Portugal Contemporâneo*. Madri, Edições Seguitur, p.143-159.

CEPIK, Marco. (2001). *Espionagem e democracia*: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro, Editora FGV.

_____. (2003). Sistemas nacionais de Inteligência: Origens, Lógica de Expansão e Configuração Atual. *Dados* (Rio de Janeiro), Rio de Janeiro, v. 46, n. 01, pp. 75-128.

_____.; BRANDÃO, Priscila Carlos. (2003). The New Brazilian Intelligence System: An Institutional Assessment. *International Journal of Intelligence and Counter Intelligence*, Nova York - NY, v. 16, n. 2, p. 167-194.

_____. (2005). Regime Político e Sistema de Inteligncia no Brasil: legitimidade e efetividade como desafios institucionais (1999-2004). *Dados* (Rio de Janeiro), Rio de Janeiro, v. 48, n. 01, p. 67-113.

_____. 2009. Prólogo. In: SWENSON, Russel G. & LEMOZY, Susana C. (2009). *Democratización de la Función de Inteligencia*. El Nexo de la Cultura Nacional y la Inteligencia Estratégica. Washington, National Defense Intelligence College.

COLLIER, David & COLLIER, Ruth. (1991). *Shaping the Political Arena*. Princeton, Princeton University Press.

CRUZ, Manuel Brada da. (2000). A Evolução da Democracia Portugues. In: PINTO, António Costa (Coord). *Portugal Contemporâneo*. Madri, Edições Seguitur, p. 122-142.

D'ARAÚJO. Maria Celina & CASTRO, Celso. 2001. *Militares e Política na Nova República*. Rio de Janeiro, Editora FGV.

FICO, Carlos. (2001). *Como eles agiam*. Rio de Janeiro, Record.

FIGUEIREDO, Lucas. (2005). *Ministério do Silêncio* – A história do serviço secreto brasileiro de Washington Luís a Lula (1927-2005). Rio de Janeiro, Editora Record.

GILL, Peter. (1994). *Policing Politics*: Security Intelligence and the Liberal Democratic State. London, Frank Cass.

GOUVEIA, Jorge Bacelar & PEREIRA, Rui (Coords). (2007). *Estudos de Direito e Segurança*. Coimbra, Edições Almedina.

HUNTER, Wendy. (1997). *Eroding Military Influence in Brazil*: Politicians Against Soldiers. Chapel Hill, The University of North Carolina Press.

HUNTINGTON, Samuel P. (1991). The Third Wave: Democratisation in the Late Twentieth Century. Norman, University of Oklahoma Press.

KRIEGER, Wolfgang. (2009). Oversight of Intelligence: A Comparative Approach. In: TREVERTON, Gregory & AGRELL, Wilheim. *National Intelligence System*: Current Research and Future Prospects. Cambridge (UK), Cambridge University Press.

LAMOUNIER, Bolivar. (1988). O Brasil autoritário revisitado : o impacto das eleições sobre a Abertura. In: STEPAN, Alfred. *Democratizando o Brasil*. São Paulo, Paz eTerra, p. 92-115.

LESSA, Renato. (1989). Reflexões sobre a gênese de uma democracia banal. In: DINIZ, E., BOSCHI, R., e LESSA, R. (1989). *Modernização e Consolidação Democrática no Brasil*: dilemas da Nova República. São Paulo, Vértice.

LISI, Marco. 2007. "O PCP e o processo de mobilização entre 1974 e 1976". *Análise Social*, vol. XLII (182), p. 181-205.

LOBO, MAGALHÃES & PINTO. (2009). As Instituições Políticas da democracia portuguesa. In: CABRAL, M; LOBO, M; FEIJÓ, R. (Orgs.) *Portugal*: uma democracia em construção: ensaios de homenagem a David B.Goldey. Lisboa, ICS, Imprensa de Ciências Sociais, p. 141-174.

LOFF, Manuel & PEREIRA, Maria da Conceição Meireles. (2006). *Portugal 30 Anos de Democracia (1974 – 2004)*. Actas do Colóquio realizado na Faculdade de Letras da Universidade do Porto. Porto, Editora da Universidade do Porto.

MENDONÇA, Ariel M. de. (2010). *A Proposta de Reformulação do Sistema Brasileiro de Inteligência (SISBIN)*: similaridades e diferenças com o processo de reforma na Comunidade de Inteligência dos Estados Unidos da América. Dissertação de Conclusão do Curso de Altos Estudos de Política e Estratégia da Escola Superior de Guerra (ESG) (Brasil).

MORLINO, L. (1992). Consolidações Democráticas na Europa Meridional. Indicações teóricas para análise empírica. *DADOS*, v. 35, n. 2.

NOHLEN, D. & THIBAUT, B. (1994). *Investigación sobre la transición em América Latina*: enfoques, conceptos, tesis. Arbeitspapier, n. 11, Universidade de Heidelberg.

NUMERIANO, Roberto. 2010. *Serviços Secretos. A sobrevivência dos legados autoritários*. Recife, Editora da UFPE.

O'DONNELL, G. (1988). Transições, continuidades e alguns paradoxos. In: REIS, F. W. e O'DONNEL, G. *A democracia no Brasil*: dilemas e perspectivas São Paulo, Vértice.

_____. (1993). Acerca del estado, la democratización y algunos problemas conceptuales. Una perspectiva latinoamericana com referencias a países poscomunistas. *Desarollo Económico*, v. 33, n.130.

OLIVEIRA, E. R. de & CORREA, S. (2000). Forças Armadas, direção política e formato institucional. In: D'ARAUJO, M. C. & CASTRO, C. *Democracia e Forças Armadas no Cone Sul*. Rio de Janeiro, Editora da FGV.

PALACIOS CEREZALES, Diego. (2008). *Estado, régimen y orden público en el Portugal contemporáneo (1834–2000)*. Tese Doutorado, Complutense University of Madrid. Disponível em: <http://eprints.ucm.es/8075/>.

_____. (2010). Repressive Legacies and the Democratisation of Iberian Police Systems, *South European Society and Politics*, 15: 3, p. 429-448.

PIMENTEL, Irene Pimentel. (2009). *A História da PIDE*. Lisboa: Círculo de Leitores e Temas e Debates. 6ª edição.

PINTO, António Costa (Coord). (2000). *Portugal Contemporâneo*. Madri, Edições Seguitur.

_____. (2006). O Legado Autoritário e a Transição Portuguesa para a Democracia, 1974-2004. In: LOFF, Manuel e PEREIRA, Maria da Conceição Meireles. *Portugal 30 Anos de Democracia (1974 – 2004)*. Actas do Colóquio realizado na Faculdade de Letras da Universidade do Porto. Porto, Editora da Universidade do Porto, p. 37-72.]

_____.; TEIXEIRA, Nuno Severiano (Org.). (2007). *Portugal e a Integração Europeia 1945-1986*: A perspectiva dos actores. Lisboa, Temas e Debates.

_____. (2010). Coping with the Double Legacy of Authoritarianism and Revolution in Portuguese Democracy', *South European Society and Politics*, v. 15, n. 3, p. 395-412.

RIBEIRO, Maria da Conceição. (1995). *A Polícia Política no Estado Novo (1926-1945)*. Lisboa: Editorial Estampa.

ROCHA, B. L. (2003). *O grampo do BNDES*: quando o complemento da ABIN é a mídia oficiosa. Rio de Janeiro, Sotese.

ROCHA, Bruno L. (2004). *Polícia Federal após a Constituição de 1988*: polícia de governo, segurança de Estado e polícia judiciária. Dissertação apresentada como requisito parcial para a obtenção do título de Mestre em Ciência Política no Programa de Pós-Graduação em Ciência Política da Universidade Federal do Rio Grande do Sul, 2004.

RORATTO, J.M. & CARNIELLI, B.L. (2006). O pensar e a criação de um organismo de Inteligência Federal no Brasil: antecedentes históricos. *Revista Brasileira de Inteligência*, Brasília, Abin, v. 2, n. 2.

ROSAS, Fernando. (1998). O Estado Novo. MATTOSO, José. (Dir.). *História de Portugal*. Vol. 7. Lisboa, Estampa.

_____. (2000). Salazarismo e Desenvolvimento Económico nos anos 30 e 40. In: PINTO, António Costa (Coord). *Portugal Contemporâneo*. Madri, Edições Seguitur, p. 93-110.

_____. (2006). A Revolução Portuguesa de 1974/75 e a Institucionalização da Democracia. In: LOFF, Manuel e PEREIRA, Maria da Conceição Meireles. *Portugal 30 Anos de Democracia (1974 – 2004)*. Actas do Colóquio realizado na Faculdade de Letras da Universidade do Porto. Porto, Editora da Universidade do Porto. p. 15-36.

SCHMITTER, Philippe C. (1999). *Portugal*: do Autoritarismo à Democracia. Lisboa: ICS.

SHARE, Donald e MAINWARING, Scott. (1986). "Transições pela transação: a democratização no Brasil e na Espanha", *Dados*, Rio de Janeiro, v. 29, n. 2, pp. 207-235.

SOARES, Gláucio A. D. (1994). O Golpe de 64. In: SOARES, G. A. D. & D'ARAUJO, M. C. *21 anos de regime militar*: balanços e perspectivas. Rio de Janeiro, Editora da FGV.

SOARES, L. E. (2007). A Política Nacional de Segurança Pública: histórico, dilemas e perspectivas. *Estudos Avançados*, v. 21, n. 61.

SWENSON, Russel G. & LEMOZY, Susana C. (2009). *Democratización de la Función de Inteligencia*. El Nexo de la Cultura Nacional y la Inteligencia Estratégica. Washington, National Defense Intelligence College.

TEIXEIRA, Nuno Severiano. (2000). A Política Externa Portuguesa. 1890-1986. In: PINTO, António Costa (Coord). *Portugal Contemporâneo*. Madri, Edições Seguitur, pp.61-93.

TRINDADE, Helgio. (1985). Bases da democracia brasileira: lógica liberal e práxis autoritária. In: ROUQUIÉ, A., LAMOUNIER, B., SCHWARCZ, J. *Como renascem as democracias*. São Paulo: Brasiliense.

ZAVERUCHA, Jorge. (2000). *Frágil democracia*: Collor, Itamar, FHC e os militares (1990-1998). Rio de Janeiro, Civilização Brasileira.

_____. (2005). *FHC, Forças Armadas e Polícia*. Entre o autoritarismo e a democracia (1999-2002). Rio de Janeiro, Record.

ZEGART, Amy. (1999). *Flawed by Design*: The Evolution of the CIA, JCS and NSC. Stanford, Stanford University Press.

ZERO HORA [jornal diário], Porto Alegre, 9/2/2011, p. 6.

Capítulo 2

OS SERVIÇOS DE INTELIGÊNCIA RUSSOS APÓS 1991

Gabriel Pessin Adam

A Guerra Fria, para além de sua inegável e profunda relevância histórica, foi pródiga em criar imagens, formar mitos e sedimentar símbolos no imaginário popular internacional, ao menos no mundo ocidental. Entre as agências ligadas aos serviços de inteligência das duas superpotências mundiais, duas receberam enorme destaque: a CIA pelo lado norte-americano e o KGB representando a União Soviética.

No ano de 1991, a URSS foi extinta e a Guerra Fria acabou formalmente. A Federação Russa foi a sucessora, em muitos aspectos, da URSS. Assim como os serviços de inteligência da Rússia eram anteriores ao Estado soviético, eles sobreviveram à derrocada deste, sendo reformulados. O presente trabalho almeja investigar como foram estruturados os serviços de inteligência russos desde 1991, com especial atenção ao período de Vladimir Putin na presidência do país (2000-2008). Conforme será visto, essa reestruturação esteve inserida no contexto de centralização do poder na Rússia, espelhando-o até certa medida, bem como fez parte de um objetivo maior: revalorizar o sistema de segurança do país em sua integralidade. Outro ponto a ser abordado é a relação entre as reformas dos serviços de inteligência e a concepção das metas de política externa da Federação Russa, traçadas no início do governo Putin.

O estudo será dividido em quatro seções. A primeira é composta de uma pequena reconstituição histórica dos serviços de inteligência da Rússia e da União Soviética. A seguir serão abordadas as reestruturações efetuadas naquelas agências efetuadas pelos presidentes russos após o fim da União Soviética, com destaque especial para o período de Vladimir Putin, conforme já salientado. Por fim, as ligações entre as mudanças nos serviços de inteligência e a concepção de segurança nacional da Federação Russa serão brevemente analisadas.

2.1. A Tradição dos Serviços de Segurança na Rússia

O histórico de polícias secretas formadas pelos governantes russos vem de longa data. Desde os tempos dos czares, corporações foram criadas como ferramenta de manutenção do poder. Por certo, não se pode afirmar que fossem serviços de inteligência, como hoje são concebidos, mas algumas das atividades que desenvolveram foram incorporadas no rol de funções de órgãos como o KGB e seus sucessores. De modo rápido podem ser aqui citadas organizações em cujo ventre é possível verificar o embrião dos atuais serviços de inteligência russos.

A primeira organização russa que desenvolvia funções de segurança e perseguição a rivais políticos, denominados de traidores, foi a *Oprichina*, criada pelo Imperador Ivan, o Terrível, no longínquo 1565. Composta por seis mil membros (os *oprichiniki*, vestidos de preto e cavalgando cavalos de mesma cor), tal força servia ao propósito de manter a ordem interna e salvaguardar o poder do Czar contra movimentos de insurgência.

Após 1572, ano do fim da *Oprichina*, foi somente no reinado de Pedro, o Grande, que a Rússia testemunhou a existência de uma organização de mesmo tipo. Isto se deu com a criação do Gabinete Preobrazhenski, cuja principal função era investigar a subversão política (RICHELSON, 1986:02). Sucessivamente, cada czar que assumiu o controle do Império Russo aboliu o serviço de segurança interna de seu antecessor e criou o seu próprio. Uma importante alteração qualitativa ocorreu em 1826, quando Nicolau I fundou a Terceira Seção. A organização de polícia secreta possuía poderes que lhe permitiam realizar investigações sobre qualquer assunto de interesse do Governo. Seu campo de atuação originário era prioritariamente Moscou e as maiores cidades russas (RICHELSON, 1986:03). Entretanto, a partir de 1832 seus agentes começaram a realizar missões além das fronteiras russas, especialmente na Polônia. A última das organizações de segurança russa do período czarista que merece destaque é a *Okhrana* (1880-1917), cujos poderes lhe permitiam agir sem mandado contra os cidadãos, expulsar indivíduos para a Sibéria sem julgamento, conduzir investigações contra qualquer um e até mesmo impor a pena de morte sem o crivo do judiciário em casos considerados especiais.

A Revolução Russa de 1917 jogou o país em uma guerra civil entre os Bolcheviques revolucionários e os Mencheviques. A necessidade dos bolcheviques de manter o poder conquistado os levou a empreender violentas respostas contra seus opositores, os quais eram apoiados por potências estrangeiras temerosas com os resultados da experiência comunista que se anunciava. Questionado acerca destas medidas, Trotsky afirmou: "protestais contra o terror brando que estamos a aplicar contra os nossos inimigos de classe. Mas devíeis saber que antes que se passe um mês o terror assumirá formas muito mais violentas, segundo o exemplo dos grandes revolucionários franceses" (CARR, 1977:182).

No dia 20 de dezembro de 1918, menos de dois meses depois de tal declaração, foi criada a *Cheka*, ou Comissão Extraordinária Panrussa para o Combate da Contrarrevolução, Sabotagem e Especulação. No início, os poderes da *Cheka* se limitavam a suprimir e liquidar todas as tentativas e atos de contrarrevolução e sabotagem em solo russo; trazer aos tribunais revolucionários para julgamento todos os sabotadores e contrarrevolucionários e trabalhar em meios para combatê-los; e empreender investigações preliminares. Contudo, o acirramento das disputas internas na Rússia e o assédio que o país sofria das potências estrangeiras levaram ao aumento do rol de atividades da organização, o que se deu concomitantemente a uma maior liberdade de ação.[1] O resultado disto foi a semelhança de poderes e métodos da *Cheka* com a *Okhrana,* estabelecendo-se, assim, uma continuidade de métodos entre a polícia interna czarista e a soviética. Apesar de sua relevância, a *Cheka* possuía uma organização rival, o Comissariado para Assuntos Internos, gestado ainda em 1917. A manutenção de dois organismos que se espelhavam em muitos aspectos e comungavam de objetivos, competências e organização institucional era uma conduta típica do governo soviético, baseada na regra de dividir para governar (SUVOROV, 1984: 18). Com duas agências em constante competição era mais fácil às lideranças bolcheviques impedirem que uma delas se tornasse muito poderosa a ponto de ameaçar o *status quo.* O fim da guerra civil, e a consequente vitória definitiva dos bolcheviques, acarretaram o esvaziamento da *Cheka*.

A criação da União das Repúblicas Socialistas Soviéticas (URSS) como um ente federal composto por quinze repúblicas, em dezembro de 1922, gerou nova alteração de nomenclatura da principal agência de segurança e inteligência interna. Assim, em novembro de 1923, surgiu a Administração Unida da Polícia Estatal (*Obyedinennoye Gosudarstvennoy Politicheskie Upravlenyie* - OGPU). A criação da OGPU representou um avanço institucional aos serviços de segurança e inteligência da polícia interna soviética. Pela primeira vez, suas atribuições estavam previstas na Constituição Federal. O caráter transitório da *Cheka,* nascida no momento de Guerra Civil e utilizada prioritariamente para salvaguardar a vitória bolchevique, dava lugar à institucionalização incontestável decorrente da constitucionalização de tais serviços e agências (RICHELSON, 1986:11).

Posteriormente, em 1934, a OGPU foi absorvida pelo Comissariado dos Assuntos Internos do Povo (*Narodnyy Komissariat Vnutrennikh* - NKVD). Suas funções foram atribuídas a um novo órgão, a Chefia de Administração de

[1] Horizontalmente, a Cheka recebeu várias novas funções em um curto espaço de tempo. Entre elas estavam a fiscalização das fronteiras (tropas terrestres, marítimas e um regimento aéreo) e a proteção das lideranças e das principais instalações do país. Para além das atividades estritamente de segurança, a agência passou a atuar em qualquer área em que houvesse algum interesse do governo soviético. George Leggett, citado por Richelson, afirma que a Cheka se tornou uma ferramenta indispensável para todos os propósitos do Partido e o Governo (RICHELSON, 1995:08)

Segurança do Estado (*Glavnoye Upravleniye Gosudasrtvennoy Bezopasnosti* - GUGB). A criação da GUGB coincidiu com o aprofundamento dos expurgos dentro do próprio Partido Comunista, almejando à eliminação dos chamados inimigos do povo e da Revolução. Via de consequência, a perseguição e os julgamentos realizados pelos órgãos de segurança se avolumaram.[2]

No ano de 1941, já em meio a II Guerra Mundial, Stalin retirou uma parcela da estrutura e do pessoal da NKVD e formou o Comissariado do Povo para a Segurança do Estado (*Narodnyy Komitet Gosudasrtvennoy Bezopasnosti* – NKGB). A possível motivação para tanto fora a impossibilidade do NKVD e da GUGB de dar conta dos desafios relacionados às ações de contrainteligência da época (RICHELSON, 1986:15). Ainda em 1941, as duas agências se fundiram de novo, como NKVD. Dois anos depois, a GUGB foi retirada do NKVB e incorporada na nova NKGB. Depois da II Guerra Mundial, em 1946, a NKGB foi unida ao Ministério de Segurança do Estado. Tal situação perdurou até 1953, ano da morte de Stalin.

Apenas dois dias depois do falecimento de Stalin, seu sucessor, Nikita Krushchev definiu que o Ministério do Interior (*Ministerstvo Vnutrennikh Del* - MVD) incorporaria os quadros e funções do Ministério de Segurança.[3] Em 1954, o MVD teve suas atribuições divididas com um novo órgão, o Comitê de Segurança do Estado (*Komitet Gosudasrtvennoy Bezopasnosti* - KGB). Vale lembrar que além do MVD e do KGB, ainda havia o Serviço de Inteligência do Exército (*Glavnoye Razvedyvatelnoye Upravleniye* - GRU), que, apesar de ser um órgão ligado diretamente ao Exército Vermelho, em virtude de suas tarefas cotidianas, muitas vezes competia com as demais organizações de inteligência por informações e privilégios.[4]

As primeiras funções do KGB eram limitadas à inteligência voltada para o exterior, contrainteligência, e contrassubversão. O Ministério de Segurança permaneceu com a administração das tropas internas, das fronteiras e dos campos de prisioneiros. Em 1957, o KGB assumiu o controle das fronteiras. No aspecto institucional, a agência também obteve ganhos, eis que seu líder passou

[2] Apenas entre 1945 e 1953 (morte de Stalin), os órgãos de segurança (NKVD/MVD e MGB) emitiram 626.373 sentenças. Destas, 12.155 foram condenações à morte, 585.592 à prisão em campos de trabalhos forçados, 24.007 ao exílio e 4.619 a outras penas (READ, 1996:15).

[3] Kruschev desejava minar o poderio do Ministério do Interior, uma vez que durante os anos de Stalin os agentes de inteligência daquela organização formavam um grupo fechado, relativamente grande e dotado de consideráveis privilégios – uma verdadeira casta separada da sociedade pela imposição do medo (TSYPKIN, 2007:271).

[4] Viktor Suvorov lembra que o líder principal do GRU sempre era um ex-dirigente do KGB. Com isto, procurava-se estabelecer um equilíbrio no qual, por um lado, o GRU não se submetia completamente aos interesses do exército, pois seu líder não era um militar de carreira, e, por outro lado, com o passar dos anos, esse mesmo líder se tornava um defensor de sua organização ante o KGB. Por sua vez, o KGB sabia que o chefe do GRU era um ex-integrante de suas fileiras, razão pela qual conhecia seus métodos (SUVOROV, 1984:22).

a fazer parte do Politburo e do Secretariado Geral do Partido Comunista da União Soviética.[5] A organização interna do órgão possuía cinco diretorias-chefe, seis diretorias e seis departamentos. A extensão da agência russa de segurança era bastante ampla. Em comparação com a subdivisão das agências de inteligência e segurança norte-americanas, o KGB assumia várias funções que eram distribuídas entre diferentes organizações dos EUA.

De modo geral, os poderes do KGB e formas de atingir suas metas eram bastante assemelhados aos dos serviços de segurança que o antecederam, como a *Cheka* e, antes dela, a *Okhrana*.[6] Tal fato não deve causar surpresa, eis que tanto o governo czarista quanto o governo soviético não eram democráticos. Num ambiente como esse, as atividades de repressão interna e de inteligência a ela correlata não são fiscalizadas pela sociedade, mas apenas por parte das lideranças políticas, justamente quem patrocina a dominação social. Este ciclo concede uma grande liberdade de ação ao KGB e similares na história russa. De acordo com Michael Tsypkin, nas duas últimas décadas de existência da URSS, o KGB pôde como em nenhum outro momento de sua história, desfrutar de liberdade para buscar os seus próprios interesses. Isto se deveu à relativa fraqueza da liderança política russa após a saída de Krushchev do poder (TSYPKIN, 2007: 273). Todavia, o controle sobre a sociedade soviética viria a sofrer um relaxamento a partir de 1985, com a nomeação de Mikhail Gorbachev para o cargo de Secretário-Geral do Partido Comunista.

---

[5] O dissidente Viktor Suvorov aponta que a URSS era governada por uma espécie de triunvirato, formado pelo Partido Comunista, o KGB e o exército. O autor sustenta que um intricado jogo de poder se estabelecia entre as três organizações, sendo que as duas primeiras procuravam aumentar o controle sobre o Estado enquanto a última nunca tentou fortemente adquirir tal proeminência, dados os freios externos gerados por KGB e PCUS. O exército servia como uma espécie de algodão entre cristais (SUVOROV, 1984:17-19). Ainda que talvez Suvorov exagere na força do KGB, tendo em vista o poder do Politburo e do Secretário-Geral do Partido Comunista ao longo da experiência soviética, seu testemunho vale, ao menos, como indício das ramificações da agência de polícia interna e inteligência no núcleo duro do comando da URSS.

[6] Uma inovação de método repressivo empregado pelo KGB que vale ser ressaltada foi o envio de determinados presos a hospitais psiquiátricos. Os cidadãos passíveis de serem internados nestes hospitais eram diagnosticados por médicos a serviço do KGB, sendo que a "perturbação mental" mais comum nos prontuários era esquizofrenia. Os casos considerados mais "graves" eram tratados pelo MVD. Ainda que os resultados de isolamento e maus tratos fossem os mesmos, o método de enviar aos hospitais psiquiátricos parecia, externamente, menos cruel que os trabalhos forçados. Além disto, era muito mais cômodo ao governo, pois ao serem diagnosticados como detentores de uma doença psíquica, os presos não podiam se manifestar nos julgamentos, condição especialmente interessante no caso dos dissidentes. Além dessas internações, o KGB continuou empregando as medidas já tradicionais nos serviços de segurança russo-soviéticos, tais como ameaças, grampeamento de telefones, buscas na casa de suspeitos, métodos psicológicos de vigilância ostensiva, isolamento social do indivíduo, deportação, condenação a trabalhos forçados em prisões nas quais as condições de vida eram péssimas, tortura física e abusos a fim de conseguir confissões de culpa. As prisões, detenções, mortes e deportações constituem a ponta final da atividade dos órgãos de segurança soviéticos.

No mesmo ano que foi empossado, Gorbachev lançou os projetos da *Perestroika* e da *Glasnost*. A tradução de *Glasnost* é "transparência", sendo tal plano voltado para os aspectos políticos do regime. Já a *Perestroika*, ou "reconstrução", tinha como meta revitalizar a economia soviética.[7] Depois de detonado, o processo de modificação econômica e política do sistema fugiu ao controle de seus líderes, e resultou no desmantelamento da URSS.

O lapso compreendido entre a subida ao poder de Gorbachev e o fim da URSS foi um período de mudanças para o KGB. Os olhos do mundo estavam voltados para o processo iniciado na URSS. Parte de sua credibilidade dependia de uma minoração dos atos de perseguição política empregados pelo Politburo.[8] Diante disto, o KGB teve de se adaptar à situação. A organização se tornou mais flexível quanto aos métodos de investigação e prisão empregados. As atividades de inteligência e contra-inteligência também foram afetadas. A hostilidade e o medo do inimigo se tornaram menores, o que ocasionou até mesmo cooperação em algumas áreas. Contudo, isto não significou o sumiço dos adversários, os quais foram beneficiados pela abertura política, pois vislumbraram o aumento das possibilidades de empregar operações de inteligência em solo soviético (GARTHOFF, 1996:240). O desgosto do KGB pela sua nova situação pôde ser medido pela tentativa de golpe de Estado praticada em agosto de 1991, no qual a organização teve importante participação. O fracasso do golpe levou à discussão acerca do futuro do KGB. A esta altura, Boris Yeltsin, presidente russo, já detinha mais poder em suas mãos do que Gorbachev, então presidente soviético.[9] Optou-se, num primeiro momento, pela reformulação do KGB. Todavia, em 03 de dezembro de 1991, Gorbachev assinou uma lei que reorganizava os órgãos de segurança do Estado. O KGB foi abolido e substituído por duas novas agências: o Serviço Inter-republicano de Segurança (MSB) e o Serviço Central de Inteligência Estrangeira da URSS. Como resposta, em 19 de dezembro, Boris Yeltsin, já presidente russo, criou o Ministério de Segurança e de Assuntos Internos da República Socialista Soviética Federal Russa. No dia 31 de dezembro de 1991, a própria URSS foi extinta.

---

[7] Angelo Segrillo aponta que "no contexto da experiência histórica soviética de meados dos anos 1980, o melhor termo para tradução talvez seja o de reestruturação" (SEGRILLO, 2000:17).

[8] Os relatórios anuais do KGB fornecidos a Gorbachev contêm dados que exemplificam o relaxamento das atividades de contra-insurgência. As ações de "trabalho preventivo profilático" que tinham como objetivo a contenção de atividade subversiva estrangeira foram realizadas, em 1985 e 1986, contra 15.274 e 10.275 cidadãos soviéticos, respectivamente. Já em 1988, tais ações visaram apenas 711 pessoas e no ano seguinte 338 (GARTHOFF, 1996:236)

[9] Dentre os alvos internos da Quinta Diretoria-Chefe do KGB, Yeltsin era o número 1. Seu apartamento havia sido grampeado e todas as suas comunicações eram interceptadas (GORDIEVSKY, 1993:69).

2.2. Da Reestruturação Pós-URSS: Período Yeltsin

Com o fim da URSS, a Federação Russa se tornou um Estado soberano. Transformações de grande monta foram impingidas à sociedade. Economicamente, o país passou do sistema de economia planificada para o capitalismo e, no aspecto político, o totalitarismo soviético foi formalmente substituído pela democracia. No pertinente aos serviços de segurança internos e de inteligência, a estrutura dos mesmos foi alterada pelo Governo Yeltsin logo em seu início. Ao invés de contar com uma grande e poderosa organização que centralizava boa parte das atividades de inteligência, distribuindo-as em suas ramificações internas, o Kremlin decidiu criar um conjunto de órgãos, cada qual responsável por uma especialidade.

Entre 1992 e 1993, os serviços de segurança soviéticos ficaram a cargo do Ministério da Segurança (MB). Em dezembro de 1993, Yeltsin aboliu o MB e criou diversos órgãos responsáveis pela segurança e inteligência do país. O principal sucessor do KGB foi o Serviço Federal de Contraespionagem (*Federal'naya Sluzhba Kontrrazvedki* - FSK), que dois anos depois seria substituído pelo Serviço Federal de Segurança (*Federal'naya Sluzhba Bezopasnosti* - FSB). A organização responsável pela inteligência externa era o Serviço de Inteligência Estrangeira (*Sluzhba Vneshney Razvedki* - SVR), que era baseado na Primeira Diretoria-Chefe do KGB.[10] O Comitê de Informação Governamental, depois Agência Federal de Comunicação e Informação Governamental (*Federal'noye Agentstvo Pravitelstvennoy Svyazi I Informacii* - FAPSI) era encarregado da inteligência eletrônica (ELINT). As pessoas mais importantes do Estado eram protegidas pelo Serviço de Proteção Federal (*Federal'naya Sluzhba Orhani* - FSO), função que era desempenhada pela Nona Diretoria do KGB,[11] ao passo que a segurança de objetos de grande relevância ficava a cargo da Diretoria Principal de Programas Específicos do Presidente (*Glavnoye Upravlenie Specialnih Program* - GUSP). Por seu turno, a proteção das fronteiras ficou nas mãos do Serviço de Proteção de Fronteiras (*Federal'naya Pogranichnaya Sluzhba* - FPS), encargo que nos tempos soviéticos era de responsabilidade da Nona Diretoria-Chefe do KGB.[12] Além destes, o GRU continuou sendo a organização responsável pela inteligência militar. O organograma de Yeltsin espelhava a prática de estabelecer certa rivalidade entre instituições de segurança, a fim de que nenhuma detivesse o monopólio da informação na Federação Russa. Assim, o GRU competia com o

[10] A Primeira Diretoria do KGB era responsável pela coleta e análise da inteligência exterior, pela contra-inteligência ofensiva e por medidas de ação. Era subdividido em três diretorias, três serviços e dezesseis departamentos (RICHELSON, 1986:23).

[11] Os agentes da Nona Diretoria do KGB eram os únicos que podiam portar armas na presença dos principais líderes do Partido Comunista da URSS. Foram membros deste grupo que dificultaram o retorno de Gorbachev a Moscou quando do golpe de agosto de 1991.

[12] Devido à extensão da URSS, a Nona Diretoria-Chefe do KGB possuía um contingente superior a 300 mil agentes.

SVR, da mesma forma que o FSB competia com a FAPSI (SOLDATOV, 2008: 481). Cabe destacar, contudo, que a pulverização das atribuições antes centralizadas no KGB não significava apenas o renascimento do tradicional método russo/soviético de "dividir para governar", nem somente uma tentativa de copiar o sistema adotado pelos norte-americanos; ela reflete muito a forma de governar de Yeltsin. A dispersão de poder no período foi uma constante. A fim de se manter no controle do jogo político, Yeltsin fez acordos e promessas a diferentes setores da sociedade, tais como lideranças e governadores regionais, oligarcas que compunham a nova elite econômica, políticos influentes (membros da chamada "família Yeltsin"), e alguns setores das forças armadas. Diante disso, não constitui surpresa que Yeltsin tenha aprofundado a estratégia de manter mais de um órgão de inteligência com o intuito de evitar o controle de informação por determinado setor do governo. Da mesma forma, não causa espanto que a relevância entre estas agências tenha oscilado durante o seu governo, pois este foi basicamente reativo aos acontecimentos sistêmicos e domésticos, nunca tendo demonstrado possuir uma estratégia de ação delineada.

No começo de seu primeiro governo, Yeltsin procurou se aproximar das potências ocidentais, sobretudo dos Estados Unidos e dos principais membros da União Europeia. Para que estes laços fossem fortificados, a Rússia deveria passar uma imagem de um Estado desprovido de arroubos imperialistas em relação aos países do espaço pós-soviético.[13] Uma consequência indireta desta fase ocidentalista da política externa russa, que tinha Andrey Kosyrev no cargo de Ministro das Relações Exteriores, foi maior atenção aos assuntos domésticos de segurança, em detrimento dos externos. Isto se verificou, em primeiro lugar, porque a manutenção de uma maciça presença de agentes realizando serviços de espionagem nos "parceiros ocidentais" deporia contra os esforços russos de se integrar na comunidade internacional. Em segundo lugar, devido ao fato já referido de que o governo permitiu-se ser pressionado por diferentes grupos políticos, circunstância que obrigava o Kremlin a socorrer a seus serviços de inteligência para realizar suas manobras e evitar a perda total de controle. Cumpre ponderar, todavia, que o fato de o maior foco de preocupação de Yeltsin estar voltado para os problemas internos da Rússia não significou o abandono completo das atividades internacionais de inteligência e coleta de informações.[14]

[13] O espaço pós-soviético é composto pelos países que um dia foram Repúblicas Socialistas Soviéticas (Azerbaijão, Armênia, Belarus, Cazaquistão, Federação Russa, Geórgia, Moldávia, Quirguistão, Tadjiquistão, Turcomenistão, Ucrânia e Uzbequistão), excluindo-se os países bálticos (Lituânia, Estônia e Letônia), pois logo após a independência, estes logo se voltaram para a União Europeia, tornando-se membros do bloco regional em 2005.

[14] O caso de Robert Hansen, um funcionário da CIA que passava segredos norte-americanos para os soviéticos e continuou com seus atos clandestinos depois do final da Guerra Fria, até ser pego, em 2001, demonstra a continuidade na disputa por dados secretos por parte de russos e norte-americanos, mesmo diante de declarações de amizade e apoio formuladas em profusão no início da década de 1990.

As mudanças nos rumos da política externa de Yeltsin impactaram na relevância dos serviços de inteligência russos para o Kremlin. Desde 1993, após perder as eleições legislativas, Yeltsin procurara relativizar a aproximação estreita com União Europeia e EUA antes buscada. Entretanto, foi somente a partir de 1996 que a política externa russa sofreu alterações de maior relevo. O marco disto foi a nomeação de Yevgeni Primakov ao cargo de Ministro das Relações Exteriores. O novo chanceler defendia uma maior aproximação com os países emergentes do oriente (como Irã, China e Índia), a retomada do controle russo sobre o espaço pós-soviético, e a relativização dos laços de "amizade" com as potências ocidentais. No concernente às questões de segurança e inteligência, a nomeação do novo Chanceler também foi impactante. Ex-membro do KGB, especializado na região do Oriente Médio, Primakov havia sido, desde 1991 até então, o chefe do SVR. Ao nomeá-lo como Ministro das Relações Exteriores Yeltsin, indicava não somente a necessidade de alteração da política externa do país, como também que a questão da segurança internacional voltava a ser uma preocupação central do Kremlin, o que, consequentemente, valorizava o SVR. Mais tarde, em 1998, Primakov foi nomeado primeiro-ministro, fato que inaugurou no Governo Yeltsin a prática de preencher o cargo com homens oriundos dos serviços de segurança ou de inteligência do país, o que culminou com a indicação de Vladimir Putin, em setembro de 1999.

2.3. Os Serviços de Segurança na Era Putin

Vladimir Putin assumiu a condição de presidente russo eleito em março de 2000, mas já ocupava o posto interinamente desde a renúncia de Boris Yeltsin, em 31 de dezembro de 1999. O começo da carreira de Putin no serviço público soviético se deu no KGB (1975-1991), pelo qual atuou na Alemanha Oriental (1985-1991).[15] Posteriormente, Putin trabalhou na administração de São Petersburgo, até retornar aos serviços de segurança, primeiro na Diretoria Principal de Controle do Kremlin (GKU), e, depois, no FSB, sendo nomeado chefe deste órgão em 1998. Ficou no cargo até ser apontado primeiro-ministro. O breve histórico da carreira política de Putin é pertinente, pois o fato de ter pertencido aos quadros soviéticos, especificamente no KGB, influenciou sua visão da *res* pública, o que se refletiu na condução de seu governo, na formação de seu grupo de aliados, bem como nas reformas implantadas nos serviços de inteligência ao longo de seus dois mandatos. Por óbvio, não é apenas a personalidade de um presidente que impacta a formulação de suas políticas de governo; eventos ocorridos nos âmbitos doméstico e sistêmico igualmente

[15] Putin se desligou do KGB em 20 de agosto de 1991, segundo dia do Golpe de Estado contra Gorbachev. Em declaração posterior, ele afirmou que logo no início de tal acontecimento, sabia de que lado deveria ficar (SAKWA, 2008:13).

trazem importantes consequências que definem caminhos a serem trilhados. No caso da Rússia, por exemplo, a Guerra da Chechênia no plano interno e o avanço do fundamentalismo islâmico no nível internacional foram temas que influenciaram diretamente a reestruturação dos serviços de inteligência do país no início do século XXI.

Antes de abordar a reforma dos serviços de inteligência, convém trazer à tona os atos de Putin voltados para a centralização do poder político do país no Governo Federal, e, em especial, na figura do Presidente. Conforme mencionado alhures, durante o governo Yeltsin ocorreu uma grande dispersão de poder: o Parlamento era controlado pela oposição (majoritariamente o Partido Comunista); os líderes regionais ganharam tantas prerrogativas em troca de apoio ao presidente que em alguns casos o governo federal perdera a capacidade de impor sua vontade às elites locais; e nos corredores do Kremlin, os oligarcas (detentores do poderio econômico) detinham enorme influência, a qual não se furtavam de usar em prol de seus interesses, nem sempre coincidentes com os do Estado. O objetivo principal de Putin era reconstruir o sistema de verticalização de poder, recorrente na história política russa desde os tempos dos czares. Tal sistema pressupõe uma cadeia vertical de poder em que cada nível fica subordinado ao que lhe é superior, não havendo quase espaço para questionamento ou infidelidade. Vale destacar que a Constituição Federal da Federação Russa vigente, escrita com base na vontade de Yeltsin após sua disputa com o Parlamento em 1993, estabelece o princípio deste sistema, ao estabelecer maiores prerrogativas ao Poder Executivo, em detrimento dos Poderes Executivo e Judiciário.

Com o intuito de atingir o objetivo traçado, Putin agiu em três frentes. Primeiramente, iniciou uma perseguição seletiva a determinados oligarcas que poderiam atrapalhar os seus planos de fortalecer o Estado.[16] O segundo passo era garantir a governabilidade junto ao Parlamento, composto por duas casas, o Conselho da Federação (alta) e a Duma (baixa). Na Câmara Baixa, o desafio era evitar ataques desestabilizadores das duas principais correntes de oposição, a comunista e a liberal. Para tanto, Putin fundou um partido, o Rússia Unida, o qual, mediante a formação de alianças, conseguiu obter cadeiras que garantiram

[16] Os primeiros oligarcas que foram afastados dos corredores do Kremlin foram Boris Berezovski e Vladimir Gusinski. Grandes responsáveis pela eleição de Yeltsin, ambos eram muito poderosos econômica e politicamente. Gusisnki já era rival de Putin desde a eleição de 2000, na qual apoiou Primakov. Após ser afastado de Moscou, buscou abrigo em Israel. Por sua vez, Berezovski havia apoiado Putin, mas não ganho sua confiança. Foi exilado em Londres e de lá procurou atacar o governo, seja por intermédio de seus veículos de mídia, seja fomentando a oposição liberal. Mais tarde, o caso de derrocada de um oligarca pelas mãos do governo mais notório foi o de Mikhail Khodorkovski, que acabou preso, enviado para a Sibéria e se tornou inelegível por oito anos. Sua empresa petrolífera, Yukos, adquirida em meio aos processos de privatização escusos comandados pelo Governo Yeltsin, foi confiscada e acabou como propriedade das empresas estatais Rosneft e Gazprom.

a maioria simples ao governo entre 2000 e 2003.[17] Nas eleições legislativas de 2003 e 2007, após a aprovação de novas leis eleitorais que lhe favoreciam, o partido governista conseguiu a maioria absoluta das cadeiras, o que deu grande liberdade de ação para o Kremlin. Já o Conselho da Federação foi conquistado através de uma mudança na lei. Antes de Putin, o órgão era composto pelos governadores regionais. A regra foi alterada, e os governadores passaram a indicar seus representantes, o que significou a perda de uma parcela de seus poderes, entre eles a imunidade parlamentar. Desde que esta modificação foi introduzida, em nenhuma votação do Conselho Federal realizada durante o Governo Putin os interesses do Kremlin foram contrariados. O último vértice da estratégia de centralização de poder era recuperar a proeminência da esfera federal sobre as regiões. Logo no princípio de seu governo, o presidente criou sete governos suprarregionais, os quais abarcavam todas as regiões da Rússia. Os ocupantes destes cargos até hoje são nomeados pelo Kremlin e detêm ascendência sobre os governantes regionais. Cabe destacar que a primeira leva de *supergovernadores* era composta por cinco ex-generais do exército russo. Ao obter sucesso nos seus planos, Putin conseguiu restabelecer a verticalização do poder na Rússia.

2.3.1 O fortalecimento do FSB (Federal'naya Sluzhba Bezopasnosti)

Semelhante processo de centralização de funções e poder foi posto em prática por Putin no que diz respeito aos serviços de inteligência do país. No ano de 2003 quando a situação do governo no Parlamento já era bastante favorável e o presidente gozava de crescente apoio popular, foi editada lei que iniciou um processo de valorização do FSB, o qual passou a abarcar órgãos e funções que pertenciam a outras agências de segurança. Num primeiro momento, o Serviço Federal de Polícia de Impostos (*Federal'naya Sluzhba Nalogovoy Policii* - FSNP) foi transformado no Comitê Estatal para Conter a Circulação Ilegal de Narcóticos (*Federal'naya Sluzhba po Kontrolyu za Oborotm i Exportnogo Controlya* – FCTEK). A FAPSI, que durante o Governo Yeltsin disputava prestígio e poder com o FSB, acabou por ter parte de sua estrutura incorporada pelo "rival". Outra parcela ficou sob encargo do FSO, ao passo que os ramos responsáveis pela inteligência de sinais (SIGINT) e pela ELINT foram repassados ao GRU. O FPS foi extinto, sendo integralmente incorporado ao FSB. Com todas essas modificações, o FSB passou a contar com um total de 286 mil funcionários, sendo que destes, 92 mil se dedicam exclusivamente às atividades de inteligência e 54 mil à interceptação de sinais (JANE's, 2009:310). Andrei Soldatov fornece um exemplo significativo do prestígio do FSB: o Ministério

[17] A criação de partidos político governistas foi uma estratégia utilizada tanto por Yeltsin quanto por Putin. Já Medvedev não fez o mesmo, sendo o governo representado na Duma e nas regiões e localidades pelo Rússia Unida.

do Interior (MVD) não foi abolido no processo de reformas, mas ficou sob controle do FSB, uma vez que os principais postos daquele órgão passaram a ser ocupados por oficiais deste (SOLDATOV, 2008: 482). Além do abarcamento de funções de outras agências e da penetração em outras, o FSB aumentou seu poder ao desenvolver um aparato analítico próprio, com o qual pode não somente prover informações às lideranças do país, mas também fornecer estimativas, prerrogativa que o KGB, por exemplo, não possuía.

No tocante as suas atribuições, o FSB passou, também, a se dedicar à contenção de dissidentes políticos, ao combate ao tráfico de drogas, à corrupção estatal e, notadamente, às ações de antiterrorismo, atuando em solo russo e no exterior. Além destas novas atividades, o FSB manteve as alçadas que lhe eram tradicionais, como a contra-inteligência, considerada por Mikhail Tsypkin a principal função da agência dentro da estrutura dos serviços de segurança russo (TSYPKIN, 2007:279). Vale dedicar algumas linhas a duas das funções desempenhadas pelo órgão, o antiterrorismo e a contrainteligência, dada a relevância que adquiriram (no caso da primeira) ou mantiveram (no caso da segunda) na concepção de segurança do governo russo.

Após a declaração do governo russo de que a Guerra da Chechênia estava acabada, em meados de 2000, os atentados de 11 de setembro de 2001 nos Estados Unidos trouxeram novamente à tona a ameaça de terrorismo. No caso russo, o temor era dobrado. Na seara doméstica havia o risco de que o movimento separatista na Chechênia recobrasse seus ataques, tendo em vista o caráter fundamentalista que adquiriu ao longo dos anos, o que acabou por se concretizar em uma série de ações terroristas praticadas por guerrilheiros chechenos fora de sua República desde 2002. Vale citar os eventos mais impactantes. Em 2002, um grupo checheno invadiu o teatro Moscou Drubovna durante a apresentação de uma peça de grande sucesso na época, e fez oitocentos reféns. Os sequestradores desejavam a retirada das tropas russas da Chechênia. Depois de dois dias, o governo russo invadiu o teatro utilizando um gás venenoso desconhecido. Todos os terroristas foram mortos, mas com eles pereceram 129 reféns.[18] No mês de agosto de 2004, dois aviões que partiram do aeroporto de Domodedovo, em Moscou, foram derrubados, sacrificando um total de 90 passageiros. Apenas um mês depois, ocorreu a invasão da Escola nº 1 de Beslan, localizada na República da Ossétia do Norte, por parte de um grupo islâmico leal ao líder checheno Samil Basayev. Entre alunos, professores e pais, foram mantidos 1.128 reféns na escola. Após dois dias, as forças russas invadiram a escola. O saldo foi a morte de 331 reféns, entre eles 186 crianças, 12 soldados das tropas especiais e 31

[18] Externamente, a Rússia foi muito criticada, pois ao se recusar a divulgar a composição do gás utilizado impediu que os médicos salvassem muitas vítimas. Contudo, no plano doméstico, Putin reforçou sua imagem de líder forte, que não se rende aos terroristas, recebendo grande apoio popular a suas medidas.

sequestradores. Duas semanas depois, Basayev assumiu a responsabilidade pelo atentado. Em 2005, um grupo de militantes realizou ataque a instalações militares e de serviços de segurança na cidade de Nalchik, República de Kabardino-Balkaria. Faleceram 92 rebeldes, 12 civis e 35 policiais. Recentemente, no dia 29 de março de 2010 foram feitos novos ataques terroristas, em duas estações de metrô de Moscou, deixando 38 mortos e dezenas de feridos. Foi o primeiro ataque na capital russa desde 2004, quando o metrô moscovita também havia sido vítima de bombas, cujo resultado foi a morte de 41 pessoas. Um detalhe interessante referente aos ataques de 2010 é que um deles ocorreu na Estação Lubianka, muito próximo da ex-sede do KGB e onde hoje o FSB tem suas principais instalações. Não é difícil imaginar a intenção dos autores do evento de desmoralizar o governo russo de Medvedev e Putin.

A relevância dos atos perpetrados pelas forças chechenas em todo o território russo fez com que todas as agências de inteligência deslocassem parte de seus efetivos para o Cáucaso do Norte. Com o FSB não foi diferente. Aliás, o órgão comandou os trabalhos entre as várias agências até 2003, quando o encargo foi delegado ao MVD. Contudo, segundo Andrei Soldatov, o MVD não possuía experiência em lidar com os chechenos, razão pela qual tinha dificuldades de infiltrar agentes nos grupos terroristas. Em função disto, o FSB, mesmo sem ser o principal órgão na região, permaneceu com uma atuação destacada, ao lado da Guarda de Kadyrov, força criada pelo Governo Federal e formada por recrutas escolhidos pelo presidente checheno da época, Akhmad Kadyrov. Após os ataques a Beslan, Moscou empreendeu nova modificação na estrutura das forças antiterrorismo. O resultado foi a lei "Oposição ao Terrorismo", a qual previa a criação do Comitê Nacional Antiterrorismo (*Nacionalny Antiterroristichesky Komiter* –NAK), órgão que a partir de então se tornou responsável pela centralização da luta contra o terrorismo. O NAK possui um diretório federal e vários diretórios regionais. Quase todos ficaram a cargo de diretores do FSB. A única e curiosa exceção era o diretório do Cáucaso do Norte, cuja liderança ficou com agentes do MVD até meados de 2009, quando foi repassada ao chefe do departamento do FSB na Chechênia.

Apesar de não ser a agência especializada em inteligência no exterior, a atuação do FSB na luta contra o terrorismo não se restringe ao território russo. Uma importante iniciativa exterior é a de arquitetar uma rede de serviços de inteligência com os países da Comunidade dos Estados Independentes (CEI), na qual compartilhassem uma base de dados. Em 2004, após os eventos em Beslan, foi formada a Diretoria de Combate ao Terrorismo Internacional do FSB, cuja principal missão é identificar e destruir células de insurgentes localizadas além das fronteiras russas. No mesmo ano, foi assinado um memorando de cooperação entre o FSB e a Estrutura Regional Antiterrorista da Organização de Cooperação

de Xangai, o qual concedeu alguma efetividade à última, criada em 2001. Andrei Soldatov sustenta que a Diretoria de Combate ao Terrorismo Internacional do FSB possui conexões com agências de outros Estados, como o FBI, por exemplo, mas realiza pouca troca de informação, limitando os contatos a algumas áreas táticas (SOLDATOV, 2008:493).

As atividades de contrainteligência do FSB também ocorrem tanto na Rússia quanto em outros Estados. No ambiente doméstico, um dos principais alvos de investigação da agência russa são os cidadãos oriundos de países membros da OTAN, o que revela a permanência do clima de desconfiança em relação às potências ocidentais, em que pese o fim da Guerra Fria. Na linha dos hábitos que não mudaram desde a URSS, cumpre destacar que o exército russo continua sendo objeto de ações de contrainteligência por parte do FSB, encargo que cabe à sua Terceira Diretoria (TSYPKIN, 2007:279). Além das ações e avos tradicionais, no Governo Putin novos atores passaram a receber atenção especial dos agentes do FSB. Aqui, o caso das ONGs merece ser citado. O fim do Estado soviético proporcionou a penetração em solo russo de várias organizações não governamentais, das mais variadas origens e com múltiplas finalidades. Durante o período de Putin na presidência, houve grande desconfiança por parte do Kremlin acerca das "reais intenções" das ONGs estrangeiras atuantes na Federação Russa. Elas foram consideradas uma maneira de intromissão dos países ocidentais nos assuntos e interesses russos. O temor de que as ONGs conseguissem fragilizar o governo perante a sociedade gerou lei que proibia que atuassem no país.

Outro tema que ganhou destaque entre as tarefas do FSB foi o combate à espionagem industrial, praticada tanto pelas potências do Ocidente, como pelos países do Oriente, como a Coreia do Sul, por exemplo. No âmbito externo, os novos membros da OTAN, em especial os Países Bálticos e aqueles oriundos do pacto de Varsóvia, constituem o foco principal do setor internacional de contra-inteligência do FSB (JANE´s 2009:313).[19]

2.3.2 O SVR (Sluzhba Vneshney Razvedki)

Sucessor da Primeira Diretoria do KGB, o SVR é o órgão de inteligência russo especializado em missões no exterior (ainda que o FSB e o GRU também exerçam atividades fora do território russo). Com um quadro estimado de 15 mil funcionários, internamente é dividido em três setores. O primeiro é composto pelas diretorias operacionais, responsável pelas seguintes funções: planejamento

[19] Entre os novos Estados surgidos com o fim da URRS, os Países Bálticos (Estônia, Letônia e Lituânia) foram aqueles que mais fortemente procuraram se afastar da influência russa. Eles foram os únicos que nunca pertenceram à CEI. No ano de 2005, os Países Bálticos ingressaram na União Europeia, tornando-se alguns dos principais opositores da aproximação do bloco regional com Moscou.

operacional, análises, inteligência técnica, não-proliferação de armamentos, terrorismo, inteligência econômica e contrainteligência. O segundo abriga as diretorias regionais espalhadas pelo território russo. O terceiro responde pelos serviços de apoio que dão sustentação aos dois primeiros, aglutinando funções de gerenciamento pessoal, ligações internacionais, finanças, questões jurídicas e guarda de arquivos.

No transcorrer do governo de Vladimir Putin, a Rússia praticou o que pode ser denominado de *economização de sua política externa*. Em breves linhas, o conceito pode ser definido como o uso dos recursos energéticos russos (gás natural e petróleo) e, em menor extensão, de armamentos, para obter capital necessário à recuperação (e à reforma, num plano ideal) da combalida economia russa do início dos anos 2000, e para conseguir vantagens políticas nos níveis regional (espaço pós-soviético) e sistêmico. Tais movimentos tinham como fim último a recuperação do papel de grande potência da Federação Russa. A relevância, até certo ponto inédita, dada aos fatores econômicos como meio de angariar poder no sistema internacional influenciou a delegação das funções do SVR. O cerne de sua atuação passou a ser a inteligência econômica, a investigação de políticos no exterior e a espionagem industrial, restando diminuída a importância das ações com fins meramente políticos. A comunhão entre o direcionamento dado ao SVR e a tática de política eterna russa é ainda mais perceptível quando se leva em conta que o órgão está cada vez mais voltado para a proteção dos interesses das companhias estatais russas dos setores de defesa, do gás e do petróleo. Não é por outro motivo que desde os anos 1990, o SVR vem desenvolvendo redes de espionagem científico-tecnológicas, necessárias no competitivo mercado de comercialização de armas e recursos energéticos (JANEs 2009:315).

Tendo em vista seus novos e antigos objetivos, o SVR possui um leque de atuação bastante amplo. Regionalmente, os países da CEI perfazem um espaço de atuação destacado do SVR, que procura, da mesma forma que o FSB, manter trocas de informações com os serviços de inteligência daqueles Estados.[20] No Leste Europeu e na Europa Central os Países Bálticos e aqueles que pertenceram ao Pacto de Varsóvia também merecem atenção especial do SVR. Além destes, os alvos tradicionais, como os EUA e seus aliados, Japão e China permanecem como prioridades dos agentes do serviço de inteligência russo.

A atuação externa do SVR (e dos demais órgãos de inteligência russos) teve destaque em pelo menos dois eventos ocorridos no ano de 2010. No mês de junho, onze cidadãos russos foram acusados de serem espiões infiltrados nos EUA. Dez foram capturados em solo norte-americano (em Montclair, New Jersey; Yonkers, New York; e Arlington, Virgínia) e outro no Chipre, mas este fugiu da

[20] Seguindo o que se enxerga nas relações bilaterais entre governos, o aliado mais próximo da agência russa dentre seus pares estrangeiros é o serviço de inteligência bielo-russo.

cadeia. Algumas semanas depois, Moscou e Washington acordaram uma troca de dez espiões russos presos por dez espiões norte-americanos presos; a maior permuta do gênero desde o fim da Guerra Fria. Em novembro de 2010, uma jovem russa, Katia Zatuliveter, assistente do deputado do Parlamento Britânico Michael Hancock, foi acusada pela seção de contrainteligência do MI-5 britânico de ser uma espiã. Não houve provas de que Zatuliveter de fato trabalhava para o SVR. Tal fato, aliado à defesa intransigente que Hancock fez de sua assistente, levaram o MI-5 a alegar que ela ainda estava no estágio de "agente adormecida", logo ainda não enviara informações importantes à Rússia. De qualquer sorte, a carência de comprovação dos atos de espionagem alegados impediu que o assunto tomasse as proporções dos fatos ocorridos nos Estados Unidos. Mesmo que o segundo caso não seja tão elucidativo como o primeiro das ações do SVR nos países ocidentais, ambos evidenciam que a agência russa mantém uma rede de inteligência no exterior bastante ativa.

Conforme já salientado anteriormente, o SVR igualmente se envolve na luta contra o terrorismo. Mesmo que não atue diretamente na Chechênia, cabe à agência monitorar as atividades dos chechenos residentes na Europa e nos Estados Unidos que possam representar uma fonte de apoio aos separatistas ou trazer algum risco à situação do governo russo na República.

2.3.3 O GRU (Glavnoye Razvedyvatelnoye Upravleniye)

Único dos serviços de inteligência da Federação Russa que manteve sua nomenclatura desde o período soviético, o GRU detém algumas peculiaridades em relação ao FSB e ao SVR, dada a sua condição de ser a agência de inteligência do Departamento de Defesa Russo. A principal delas é o fato de que o chefe da agência se reporta ao Líder dos Generais da Federação Russa, e não ao presidente, como ocorre com o diretor principal dos dois outros órgãos referidos. Talvez esta autonomia do GRU ajude a explicar porque o FSB ainda mantém uma seção voltada para observação do exército russo. Outra parte da explicação por certo reside na rivalidade de décadas entre GRU e KGB, antes referida, a qual se mantém após a substituição do último pelo FSB.

A estrutura do GRU atualmente é dividida por região e por tarefas. Neste último quesito, são três diretorias principais: a Primeira Diretoria é responsável pela inteligência encoberta; a Segunda Diretoria responde pela inteligência militar; a Terceira Diretoria, por sua vez, realiza atividades de SIGINT, ELINT e IMINT (inteligência de imagens). Vale destacar que, com a extinção da FAPSI, a Sexta Diretoria do GRU obteve controle sobre os satélites de espionagem Kosmos e sobre a base Ros Kosomo de ELINT, situada no Yêmen. Quanto à distribuição espacial, as Unidades de Destinação Especial (*Spetsnaz*) do GRU estão localizadas nas seguintes regiões: Região de Psov (2ª Brigada); Distrito Militar do Ural

(3ª Brigada); Território de Krasnoyarsk, Distrito Militar do Cáucaso do Norte (10ª Brigada); Distrito Militar do Oriente Longínquo (14ª Brigada); Distrito Militar de Moscou (16ª Brigada); Região de Rosov, Distrito Militar do Cáucaso do Norte (22ª Brigada); e Distrito Militar da Sibéria (24ª Brigada).[21]

No tocante às atribuições do GRU, lhe cabe coletar informações acerca do poderio militar de outros países, tais como armas e estratégias, assim como avanços das indústrias de defesa (TSYPKIN, 2008:277). Para tanto, possui uma rede de escritórios militares espalhados no exterior. Quanto aos alvos da agência, estes são parecidos com os do SVR, mas com proeminência dos países da CEI e dos Estados ocidentais.[22] Aliás, um reflexo visível da Guerra Fria nas atitudes do GRU é o seu antiocidentalismo arraigado. Por causa desta particularidade, foi com certo assombro que seus agentes e diretores acompanharam as Guerras dos Bálcãs e do Golfo, pois em tais ocasiões constataram a grande diferença tecnológica dos armamentos dos EUA e da OTAN (munições guiadas, lasers, veículos de reconhecimento, desenvolvimento e fabricação de sistemas avançados de fiscalização para aviões) em relação ao material de guerra russo. A conclusão a que chegaram foi de que a diminuição das diferenças existentes perante a OTAN nos armamentos convencionais somente poderia ser atingida com o acúmulo de inteligência militar.

O GRU também está envolvido no conflito contra os separatistas chechenos. Sua tarefa primordial entre os órgãos de segurança que operam na região é combater os rebeldes situados nas montanhas. Possui dois esquadrões compostos por chechenos que realizam missões de identificação e eliminação de militantes ativos.

2.3.4 Órgãos do Departamento de Defesa da Federação que possuem seções próprias de inteligência

2.3.4.1 Serviço de Proteção Federal (FSO - Federal'naya Sluzhba Okhrany)

O FSO possui como função primordial resguardar os membros do Governo e da Duma de Estado (Parlamento Baixo da Federação Russa), sendo sucessor da Nona Diretoria do KGB, na sua época responsável pela proteção de VIPs e vigilância de suspeitos. Durante a presidência de Vladimir Putin, o FSO ganhou certa importância, pois na disputa por atenção e orçamentos entre os serviços de inteligência russos, ele detinha a prerrogativa de produzir análises

[21] Como parte da Reforma Militar, a 12ª e a 67ª s Brigadas Spetsnaz foram dissolvidas, assim como a 3ª Brigada foi cortada.

[22] As forças de inteligência do GRU estiveram envolvidas no Conflito da Ossétia do Sul, em agosto de 2008, quando o Exército russo enfrentou as forças armadas da Geórgia. As Brigadas que tiveram participação ativa no enfrentamento foram as localizadas no Distrito Militar do Cáucaso do Norte (10ª e 22ª) e a Brigada lotada no Distrito Militar Leningrado (2ª).

diretamente para o Presidente e para a elite da administração federal. No período das eleições parlamentares de 2007 e presidenciais de 2008, o FSO teve parte de suas atribuições alargada, pois lhe foi destinada a investigação política, tanto da oposição, quanto de membros da situação.

2.3.4.2 Unidades com destinação especial (*Spetsnaz*) das tropas interiores

Dentro das tropas vinculadas ao Ministério do Interior russo (MVD), há um contingente denominado "Unidades de Destinação Especial", criadas especialmente para garantir a segurança dos Jogos Olímpicos de Moscou, em 1980. No começo dos anos 1990, as *Spetsnaz* detinham três diretorias, duas relacionadas com questões de combate e outra que tratava da inteligência. Em 1993, os setores responsáveis pela inteligência se separaram das *Spetsnaz* e se tornaram membros autônomos das Tropas Interiores. Com a subida de Putin ao poder, houve mudanças. As divisões e os batalhões das *Spetsnaz* voltaram a ter setores de inteligência próprios. Isto não significou o fim das seções de inteligência das Tropas Interiores, que se mantiveram ativas.

No ano de 2008, foi criado o Centro de Propósitos Especiais 604, o qual inclui um grupo de operações especiais, subgrupo militar anfíbio responsável por defender os bens do Estado, mas que também efetua tarefas antidiversionárias e antiterroristas em ambientes aquáticos. Segundo Kozlov, o Centro permitiu às Tropas Interiores desenvolverem suas atividades relacionadas à inteligência. Assim, por exemplo, foram criadas subseções de equipamentos de vigilância de rádiocomunicação utilizada em ELINT; além de subseções de SIGINT (KOZLOV, 2010).

Da mesma forma que outros serviços de inteligência russos, as Tropas Interiores participam da luta contra o terrorismo na Chechênia. Vale lembrar que as tropas interiores do MVD foram a primeira força antiterrorista a se engajar nos conflitos do Cáucaso do Norte. Num primeiro momento, suas seções de inteligência encontraram dificuldades para conseguir informações e penetrar nos grupos terroristas, o que motivou o Kremlin a enviar reforço proveniente de outros serviços de inteligência. Não houve, todavia, o abandono da região pelas Tropas Interiores do MVD e seus setores de inteligência, os quais hoje têm como objetivos o sequestro e a destruição de integrantes de células militantes adormecidas.

2.4. A Continuidade no Governo Medvedev

Dmitri Medvedev foi eleito presidente russo em 2008, apoiado na ampla popularidade de Vladimir Putin, nomeado Primeiro-Ministro após as eleições parlamentares de 2007. Nos primeiros anos de seu governo (2008 a 2010) não houve uma grande reestruturação dos serviços de inteligência, ainda que tal

hipótese tenha sido aventada em meados de 2009. Uma decisão importante tomada pelo Kremlin no período foi o aumento dos poderes do FSB, não especificamente em relação às demais agências antes citadas, mas perante as pessoas físicas e jurídicas residentes e estabelecidas na Rússia. Vale dedicar algumas linhas a tais fatos.

Acerca das possibilidades de mudança na estrutura dos serviços de inteligência, no mês de abril de 2009, o General Valentin Korabelnikov do GRU pediu demissão do posto que ocupava desde 1997. Na época, houve suspeitas de que a demissão possuía raízes na sua discordância quanto à reforma nas forças armadas colocada em curso por Putin e seguida por Medvedev. Sua contrariedade diria respeito à possibilidade de que várias das atribuições do GRU passariam para o SVR, entre elas as unidades de interceptação de rádio e os satélites espaciais. Até mesmo o risco de submissão do GRU ao SVR não era inteiramente descartada naquele momento (KRAMNIK, 2010). Os rumores não se confirmaram, e o sucessor de Korabelnikov, General Shlyakhturov, não viu o GRU sofrer perda de funções ou poder no sistema de defesa russo. Tal situação não deve ser alterada no futuro, pois por mais que o processo de reformulação das forças armada russas seja profundo e polêmico, e que seus resultados ainda sejam incertos, o histórico do GRU aponta uma forte autonomia desde os tempos soviéticos. Logo, é difícil crer que ele um dia recaia sobre o controle de serviços russos de inteligência civis, como o FSB, o SVR ou qualquer outro que porventura possa vir a ser criado.

Após os ataques ao metrô de Moscou em março de 2010, Medvedev submeteu ao Parlamento russo emenda à lei sobre o FSB, a qual foi aprovada no Poder Legislativo. A partir de então, os agentes do FSB detêm a prerrogativa de adotarem medidas preventivas contra indivíduos ou pessoas jurídicas consideradas executoras (ou em vias de executar) atos ofensivos aos artigos da lei que proíbe atos de extremismo. A pena para as pessoas físicas que descumprirem a lei é uma multa de 500 a 1.000 rublos e a prisão por 15 dias.[23] Caso o indivíduo seja um oficial, a multa aumenta para 3.000 rublos. Já as pessoas jurídicas podem receber multas de 10.000 a 50.000 rublos.[24] A polêmica lei gerou muita discussão e acusações por parte de partidos oposicionistas de significar um retorno a métodos soviéticos de perseguição política e pessoal. Em outubro de 2010, nova lei relacionada aos serviços de inteligência foi aprovada, desta feita voltada para as relações desses com a imprensa russa. Ela "limita as atividades de coleta de informação relacionada ao terrorismo junto ao pessoal de segurança do governo, mesmo que estes tenham escolhido entrar em contato com a imprensa, oficial ou

[23] Segundo o site do Banco Central do Brasil, em dezembro de 2010, 500 rublos equivalem a R$ 27,56. Para fins de mensuração da multa, vale destacar que no ano de 2009, os russos tiveram uma renda per capita mensal de 16.887 rublos.

[24] Segundo o site do Banco Central do Brasil, 500 rublos equivalem a R$ 551,30.

extraoficialmente" (SOLDATOV, 2010). Na prática, o que o dispositivo legal faz é dificultar aos jornalistas a checagem das informações divulgadas pelos serviços de segurança.[25] A mesma legislação estipulou que todas as informações relativas ao financiamento das atividades antiterroristas são classificadas como secretas. Assim, se torna impossível haver o controle externo sobre o quanto está sendo gasto (e eventualmente desperdiçado) no combate ao terrorismo. Ainda que o orçamento total desta espécie de atividade, via de regra, não seja integralmente divulgado ao público, a norma em questão impede que até mesmo uma noção aproximada das despesas estatais direcionadas para os atos de antiterrorismo seja obtida.

Em suma, no campo da inteligência, as esperanças que uma parcela da mídia russa e estrangeira compartilhava acerca de uma menor influência do FSB (e dos demais serviços de segurança) no Kremlin e na sociedade durante o Governo Medvedev não foram correspondidas. O FSB pode não ter aumentado suas funções administrativas após o fim do período Putin, mas elas também não foram diminuídas. Ao mesmo tempo, sua capacidade de agir contra os cidadãos russos e a imprensa em geral foi acrescida a partir da edição das leis referidas. Aliás, é possível traçar um paralelo entre a legislação proposta por Putin após os atentados de Beslan, a qual revogou a eleição direta para governadores das regiões administrativas russas, e as normas elaboradas por Medvedev depois do atentado no metrô de Moscou.

2.5. Os Serviços de Inteligência e a Política Externa Russa

Conforme referido anteriormente, a diminuição do número de serviços de inteligência na Federação Russa e o recrudescimento de funções e poderes delegados ao FSB podem ser comparados aos movimentos de centralização de poder na política doméstica russa.[26] Ou seja, as reformas dos serviços de segurança

[25] A diminuição das prerrogativas da imprensa perante os serviços de inteligência da Federação Russa é um processo que vem sendo observado desde o início dos anos 1990. No Governo Yeltsin, a Lei da Mídia obrigava o FSB e o SVR a responder questões formuladas pela imprensa no prazo de dez dias após a divulgação de comunicados oficiais. Em função disto, as duas agências criaram assessorias de imprensa, mesmo que nem sempre o dispositivo legal em questão fosse respeitado. Posteriormente, durante o Governo Putin, FSB e SVR passaram a divulgar apenas *press releases* noticiando seus projetos e ações, razão pela qual suas assessorias de imprensa foram desmanteladas (SOLDATOV, 2008: 488). A lei de Medvedev representa um passo adiante no cerceamento do trabalho dos jornalistas, pois procura obstaculizar o acesso destes a fontes que eventualmente pudessem contestar, ampliar ou comentar os boletins divulgados.

[26] A verticalização de poder mais acentuada do Governo Putin deu lugar a uma diarquia entre o agora primeiro-ministro Vladimir Putin e o presidente Dmitri Medvedev. As funções de governo e política externa são repartidas entre ambos da política russa atual. O arranjo estabelecido não apresentou fissura nos três primeiros anos do Governo Medvedev, eis que os dois têm atuado no mesmo compasso em todas as questões relevantes e prioritárias para o governo. Caso consideremos os dois como principais expoentes do grupo político que chegou ao poder por intermédio de Putin (e é por este

estão inseridas dentro uma política de governo bastante clara implementada por Vladimir Putin a partir de 2000 e seguida por seu pupilo político e sucessor Dmitri Medvedev, chegando até mesmo a refleti-la, sob determinado ponto de vista. A reformulação realizada igualmente faz parte de outro movimento iniciado no Governo Putin e mantido em andamento desde então: a reestruturação do sistema de segurança russo, notadamente as forças armadas.[27] Estas e outras políticas postas em funcionamento desde o início da primeira década dos anos 2000 possuem um propósito maior, qual seja, a retomada, por parte da Federação Russa de seu papel de grande potência no sistema internacional. Em que pese a importância que concederam ao fator econômico e à comercialização de recursos energéticos no mercado mundial na política externa russa, os governos de Putin e Medvedev concederam a devida importância ao complexo de segurança e defesa do país, considerado elemento essencial para a meta sistêmica a ser alcançada.

Antes mesmo de ser eleito presidente da Federação Russa, mas já ocupando o cargo interinamente, Vladimir Putin publicou via Decreto Presidencial a Concepção de Segurança Nacional da Federação Russa. Nesse documento, algumas das principais diretrizes implantadas em seu governo foram expostas. A principal delas era a defesa da construção de um mundo multipolar. Segundo a visão do Kremlin, a multipolaridade é uma das tendências conflitantes e excludentes que emergiam no sistema internacional após o fim do confronto bipolar da Guerra Fria. A outra tendência é a de um mundo dominado pelos países ocidentais desenvolvidos, liderados pelos Estados Unidos. A Federação Russa, a despeito de suas dificuldades da época, era compreendida como um país que objetivamente continuava a desempenhar um papel importante nos processos mundiais, tendo em vista seu considerável potencial econômico, militar e de pesquisa tecnológica, sem esquecer sua condição única no continente eurasiano. Ou seja, a Rússia reunia condições de ser uma grande potência no mundo multipolar que almejava ajudar a construir.

No concernente aos serviços de inteligência do país, eles são mencionados diretamente em apenas uma passagem do documento, a qual os classifica como "de especial significado para a garantia da segurança nacional da Federação Russa é o uso efetivo e o desenvolvimento das capacidades de inteligência e contra-inteligência com o propósito de prontamente revelar ameaças e determinar suas origens".[28] Contudo, a leitura de todo o texto permite que se façam ligações entre, de um lado, a concepção do governo russo acerca dos objetivos do país e ameaças contra ele dirigidas, e de outro, as modificações concebidas nos organismos de inteligência russos. Cumpre trazer à tona algumas dessas aproximações.

---

liderado) e que hoje controla a Presidência e o Parlamento, não é impossível falar na manutenção da centralização de poder no Governo Medvedev, ainda que de outro tipo.

27 Para maiores detalhes das reformas das forças armadas russas, ver HERSPRING, 2006 e 2010.

28 Tradução do autor a partir do National Security Concept of the Russian Federation.

O terrorismo, nacional e internacional, é mencionado seis vezes ao longo do documento, quase sempre com um tom de séria ameaça aos cidadãos russos, à Federação Russa como um todo e até mesmo à estabilidade do sistema internacional. Convém lembrar que no período da edição do Decreto Presidencial a segunda fase da Guerra da Chechênia estava em plena conflagração, o que explicaria o excesso de preocupação com o terrorismo. Todavia, como referido anteriormente, o terrorismo checheno e internacional (especialmente o proveniente do Afeganistão e da Ásia Central) continuou sendo uma poderosa fonte de dor de cabeça para as autoridades russas. Dentro de tal contexto, o envolvimento de todos os principais organismos de inteligência do país no combate ao terrorismo ao longo dos dez anos que se seguiram à publicação da Concepção de Política Externa da Federação Russa resta plenamente justificado.

A OTAN é outra fonte de preocupação citada textualmente no documento. As ameaças provenientes da organização militar referidas são basicamente duas: o alargamento para o leste (até as fronteiras russas) e a sua tendência a usar força militar além da área de sua responsabilidade sem a chancela da ONU, fator encarado como potencial causador de desestabilidade da situação estratégica do mundo. Os riscos representados pela OTAN e pelos Estados Unidos, bem como o esforço de Washington para fazer prevalecer a tendência de um mundo unipolar, foram constantemente relembrados durante o Governo Putin, sobretudo no seu segundo mandato. Por certo, não são outras as razões que motivaram o Kremlin a destinar boa parte da atenção dos principais serviços de inteligência russos para os países da OTAN, seja investigando os atos dos cidadãos dos mesmos em território russo, seja mantendo ativas células clandestinas e agentes nos Estados que compõem a organização militar. Neste ínterim, os exemplos já citados de acusações de espionagem dirigidas à Rússia por Estados Unidos e Inglaterra em 2010 podem ser mais uma vez lembrados.

Por fim, as atividades desenvolvidas por FSB, SVR e GRU junto aos países da CEI, mediante busca de parcerias e permuta de informações, ou por intermédio de espionagem, também estão conectadas à concepção de segurança nacional da Rússia. Nas suas diretrizes de política externa, Moscou declara que seus interesses primordiais no espaço formado pela CEI são o fortalecimento da integração do bloco regional e o afastamento de outros Estados que procuram penetrar na região com o intuito de fortalecerem suas posições e, em semelhante medida, diminuir a presença russa. Em outras palavras, os países oriundos da União Soviética devem continuar sendo encarados como pertencentes a uma esfera de influência de Moscou.

Pelo exposto, a partir da análise de algumas das principais ameaças identificadas pelo Kremlin à Federação Russa, é possível constatar que a reestruturação dos organismos de inteligência do país não ocorreu a esmo. A escolha dos novos alvos, a busca de tecnologia e as reformas administrativas

efetivadas tiveram como um de seus nortes os objetivos de política externa de Moscou. É claro que as questões de política doméstica também estão presentes, como, por exemplo, a manutenção de diferentes agências com funções sobrepostas a fim de que nenhuma delas se torne poderosa o bastante para significar uma ameaça ao governo, o que é uma tradição de décadas em solo russo. Porém, não obstante a permanência da rivalidade interna, assim como as falhas ainda existentes nos organismos de inteligência russa, é inegável que após a conturbada década de 1990, os serviços secretos russos voltaram a ter uma importância efetiva não negligenciável na perseguição dos objetivos regionais e sistêmicos da Federação Russa.

2.6. Considerações Finais

A evolução dos organismos de segurança russos após a Guerra Fria pode ser comparada, de certo modo, com a trajetória da própria Federação Russa nos últimos vinte anos. Os confusos anos 1990, período quase de exceção na história do país bicontinental, deram lugar a uma Rússia mais confiante, que possui um objetivo definido, qual seja, retomar a condição de grande potência, desta vez em um sistema que vislumbra em direção à multipolaridade. Os organismos de inteligência, por sua vez, recobraram o papel de destaque na estrutura de segurança da Rússia, deixando de servir prioritariamente aos interesses da elite política, como em grande parte do período Yeltsin, e passando a ser incorporados na estratégia de crescimento do poder sistêmico do país.

Portanto, a semelhança de trajetórias não é apenas coincidência. Os serviços de inteligência participaram do avanço da Federação Russa em busca do prestígio perdido. Isto foi verificado não somente pela comunhão entre as ameaças e metas traçadas na Concepção de Segurança Nacional Russa e as funções e alvos que foram àqueles destinadas pelo Kremlin. Conforme referido, desde o início dos anos 2000, houve uma destacada ocupação de cargos da esfera federal por membros e ex-membros dos serviços de segurança, em especial do FSB. Ou seja, para além da concentração de poder em tais órgãos, não é incorreto afirmar que a ideologia que permeia os serviços de inteligência russos tenha, de algum modo, influenciado a administração federal da Rússia. Situação que por si só, destaque-se, não representa uma carência democrática do país ou um Estado policial, muito menos um retorno ao período soviético, como é referido por alguns analistas.

Porém, há ressalvas a serem feitas. Assim como a Federação Russa tem enfrentado percalços na busca de seus objetivos, tais como a excessiva dependência de sua economia da venda de recursos energéticos, ou a diminuição acentuada de sua população, razão pela qual precisa fazer correções de rumo em suas táticas, o trabalho de reconstituição da área de inteligência está em

curso, e, portanto, é incompleto. Os erros cometidos por seus agentes no exterior, bem como a incapacidade debelar definitivamente o movimento checheno de insurgência demonstram que a eficiência que tornou o KGB reconhecido e temido ainda não se vê presente no FSB e seus pares. Todavia, a importância que os governos Putin e Medvedev deram não somente aos órgãos de inteligência, mas às forças armadas e ao complexo de segurança russo como um todo, permitem esperar uma melhora considerável nestas áreas nos próximos anos. Situação que se concretizada, melhorará as chances russas de se firmar como grande potência, apesar das dificuldades estruturais e conjunturais do país.

REFERÊNCIAS

CARR, Edward Hallett. (1977) *História da Russa Soviética:* A Revolução Bolchevique, vol. 1. Porto: Edições Afrontamento, 494 p.

CEPIK, Marco Aurélio Chaves. (2003). *Espionagem e Democracia*. Rio de Janeiro: Editora FGV, 232 p.

DUNLOP, John D. (2005). *Beslan:* Russia´s 9/11? Jameson Fundation, 52 p.

_____. (2009). *The September 2004 Beslan Terrorist Incident:* New Findings. Stanford University, 20 p.

GARTHOFF, Raymond. (1996). The KGB Reports to Gorbachev. *Intelligence and National Security* vol. 11 nº 2, p. 224-244.

GORDIEVSKY, Oleg (1993). The KGB After the Coup. *Intelligence and National Security* vol. 8, nº 3, p. 68-71.

HERSPRING, Dale R. Putin, Medvedev and the Russian Military. In WEGREN, Stephen and HERSPRING, Dale R. *After Putin´s Russia:* Past Imperfect, Future Uncertain. New York: Rowman & Littlefield, 2010 (p. 265 a 289), 318 p.

_____. *The Kremlin and the High Command:* Presidential Impact on the Russian Military from Gorbachev to Putin. Kansas: University Press of Kansas, 2006, 242 p.

KEEP, John. (2005). *A History of Soviet Union*. London: Oxford, 480 p.

KOZLOV, Sergei. *Internal Troops Spetsnaz: the 2000s*. Moscou: Agenta. Disponível em: <http://www.agentura.ru/english/spetsnaz/Internaltroops/>. Acesso em: out./2010.

KRAMNIK, Ilya. *Expanding FSB Powers: Treating the Symptoms not the Disease?* Moscou: Ria Novosti. Disponível em: <http://en.rian.ru/analysis/20100803/160057479.html>. Acesso em: ago/2010.

NATIONAL SECURITY CONCEPT OF THE RUSSIAN FEDERATION. Full English Translation from Rossikaya Gazeta, January, 2000, 18 p.

READ, Chistopher. *From Tsars to Soviets*. (1996). London: Routdlege, 330 p.

RICHELSON, Jeffrey T. (1986) *Sword and Shield: Soviet Intelligence and Security Apparatus*. Massachussets: Ballinger Publishing Company, 279 p.

_____. (1995). *A Century of Spies*. New York: Oxford University Press, 534 p.

SAKWA, Richard. (2008). *Putin*: Russia´s Choice. New York: Routlegde, 388 p.

SEGRILLO, Angelo (2000). *O Fim da URSS e a Nova Rússia*. Rio de Janeiro: Vozes, 152 p.

SERVICE, Robert. (2003) *A History of Modern Russia*. Cambrige: Harvard University Press, 659 p.

SOLDATOV, Andrei and BOROGAN, Irina. *In Counterrorism, Medvedev Follows Putin's Road*. Moscow: Ezhednevny Journal, 08/04/2010.

SOLDATOV: Andrei. (2008). *Russia*. In FARSON, Stuart, GILL, Peter, PHYTIAN, Mark e SHPIRO, Shlomo. *PSI Handbook of Global Security and Intelligence*. London: Praeger Security International, 700 p.

SUVOROV, Viktor (1984). *A Espionagem Militar Soviética*. Rio de Janeiro: editora Record, 226 p.

TRENIN, Dmitri e MALASHENKO, Aleksei (2004). *Russia's Restless Frontier*. Washington, Carnegie Press, 265 p.

TSYPKIN, Mikhail (2007). *Terrorism's Threat to New Democracies; The Case of Russia*. In BRUNEAU, Thomas C. e BORAZ, Steven C., eds. Reforming Intelligence: Obstacles to *Democratic Control and Effectiveness*. Texas: University of Texas Press, 407 p.

WARNER, Michael (2009). *Building a Theory of Intelligence System*. In AGRELL, Wilhelm e TREVERTON, Gregory F., eds. *National Intelligence System:* Current Research and Future Prospects. Cambridge University Press, 302 p.

Capítulo 3

INTELIGENCIA EN DEMOCRACIAS: LA CRISIS DEL SERVICIO DE INTELIGENCIA COLOMBIANO

Alexander Arciniegas Carreño

Este capítulo contiene un recorrido por los antecedentes y configuración del sistema de inteligencia en Colombia a partir del cual se contextualiza la crisis que desde 2004 sacude al Departamento Administrativo de Seguridad DAS, la agencia civil de inteligencia colombiana. Con ello se espera alcanzar por lo menos con dos finalidades: la primera, ofrecer una visión general a cerca de la evolución, realizaciones y límites de la actividad de inteligencia y de la comunidad de inteligencia (IC) en el país. Y en segundo lugar, subrayar como la manera en que se desarrolla la inteligencia dentro de un determinado Estado repercute sobre la calidad de la democracia. Se parte aquí de la premisa que la necesidad de sortear la compleja tensión entre los requerimientos de la seguridad nacional – derivados de la estructura anárquica del sistema internacional – y los criterios mínimos de la poliarquía, no debe conducir a que los Estados abdiquen del uso de capacidades de inteligencia, sino a que mejoren su profesionalismo y eficacia, cuidando al mismo tiempo de mejorar o establecer dispositivos de control. Al fin y al cabo y como sucede en otras áreas de la seguridad, en inteligencia efectividad y legitimidad son no solo dos caras de la misma moneda, sino prerrequisitos de la estabilidad del régimen democrático y la viabilidad de un Estado con mínimas pretensiones de autonomía en el sistema internacional contemporáneo.

En este orden, la estructura del ensayo presenta en primer momento algunos conceptos básicos sobre la actividad de inteligencia, al igual que los impedimentos y esfuerzos identificados por algunos teóricos en relación con la tarea de reformar las organizaciones de inteligencia en el contexto de naciones democráticas. A partir de allí, en un segundo momento se caracterizan con base en el registro de algunos de las principales publicaciones periodísticas

colombianas, las dificultades vividas por el DAS en los últimos seis años, presentando también algunas decisiones implementadas desde la dirección de la agencia y desde el gobierno para encararla; lo mismo que la manera como han operado los principales mecanismos de control público, con especial atención con el papel cumplido por el Poder Legislativo. Para en tercer lugar, formular breves observaciones finales orientadas a ofrecer una síntesis de las cuestiones abordadas, lo mismo que a mencionar la experiencia de otros países que pueden servir como punto de referencia en el camino de construir en Colombia una inteligencia más profesional, eficiente y democrática.

3.1. La Reforma de Inteligencia y el Dilema entre Poliarquía y Seguridad Nacional

La actividad de inteligencia es un área sobre la cual se escribe poco, talvez por esta razón popularmente se le asocia con la cara más oscura de los regímenes totalitarios que imperaron durante la Guerra Fría. Por eso mismo a continuación se intenta precisar algunas nociones básicas que permiten defender la necesidad de que los Estados cuenten con organizaciones de inteligencia, lo mismo que subrayar a partir del caso colombiano que la supervisión y la reforma de los distintos sistemas y agencias continua siendo una tarea desafiante, no solo para las democracias de "tercera onda".

Pero ¿Qué es precisamente inteligencia? De acuerdo con Mark Lowenthal (2008) inteligencia pude significar un producto, un proceso y una organización. Como producto, Inteligencia es ante todo el resultado de aquellas actividades y como organización está referida a las agencias que las ejecutan. En cuanto proceso se pone en marcha a iniciativa de los gobiernos, en busca de recopilar, analizar y difundir cierto tipo de informaciones requeridas, al tiempo que constituye el rubro por el cual se planifican y ejecutan acciones encubiertas. (BORAZ & BRUNEAU, 2006).

En cualquiera de los anteriores significados la inteligencia se orienta a dos objetivos: informar la política y/o apoyar operaciones (militares, policiales o de naturaleza encubierta) en defensa de la seguridad nacional. Para cumplir estas dos misiones, las organizaciones de inteligencia ejecutan de manera integrada las funciones de colecta, análisis, contrainteligencia o "security intelligence" y acciones encubiertas. Es decir, los encargados de la colecta de información por fuentes humanas o técnicas (señales o imágenes), dependen de los analistas para reunir información y discernir su significado; el personal de contrainteligencia – responsable de proteger los secretos del Estado – dependerá de los analistas para contrarrestar espías y el personal de operaciones encubiertas requerirá de recolección, análisis y contrainteligencia de buena calidad. (BORAZ & BRUNEAU, 2006).

De las cuatro funciones anteriores talvez la más polémica desde el punto de vista ético y jurídico sea la relacionada con acciones encubiertas. Según Boraz & Bruneau (2008:30), estas actividades van desde la propaganda hasta acciones propiamente de fuerza con el fin de influir en otro Estado por medios difíciles de rastrear o susceptibles de ser negados. Es a través de las acciones encubiertas que las agencias de inteligencia van más allá de la mera recopilación e interpretación para hacer uso de la fuerza, hecho que las aproxima de las operaciones militares – con la diferencia de que aquellas implican un mayor y más sistemático nivel de secreto. Esto último sirve para ilustrar como aunque la inteligencia hace parte de la coerción estatal, mantiene particularidades como secreto y conocimiento.

Luego de una corta aproximación sobre lo que la inteligencia es y puede hacer, resulta conveniente, con fundamento en (CEPIK, 2003: 138-139), introducir en esta parte del trabajo definiciones mínimas en relación a cuestiones como seguridad, seguridad nacional y amenazas, como punto de partida para la reflexión. Seguridad sería entonces, una condición relativa de protección en la cual se es capaz de neutralizar amenazas discernibles contra la existencia de alguien o de algo con razonable expectativa de éxito. En términos organizacionales, seguridad significa patrones y medidas de protección para conjuntos definidos de informaciones, sistemas, instalaciones, comunicaciones, personal, equipos y operaciones – siendo que tales medidas para no tornarse ellas mismas en una amenaza deben guardar proporcionalidad en relación a las amenazas percibidas en contra de quien está siendo protegido.

La proporcionalidad en cuanto limite a cualquier pretensión totalitaria permite ahora abordar la noción de seguridad nacional, aclarando que la naturaleza controversial del concepto en buena medida responde a su frecuente utilización como justificativa de prácticas políticas represivas por ejemplo, en las dictaduras latinoamericanas del Cono Sur. Esta categoría se entiende aquí como una condición relacionada con la protección colectiva e individual de los miembros de una sociedad contra amenazas a su sobrevivencia y autonomía. Seguridad Nacional implica así mismo una dimensión vital de la existencia individual y colectiva en el contexto moderno de sociedades complejas delimitadas por Estados de base territorial. De manera que estar seguro implica vivir en un Estado capaz de neutralizar amenazas mediante la negociación, la obtención de informaciones sobre capacidades e intenciones, a través del uso de medidas extraordinarias y de las opciones relativas al uso de la fuerza.

Por otro lado, las amenazas, pueden ser de naturaleza externa (agresiones militares, espionaje, invasión del territorio o bloqueo económico) o interna (apoyos internos a amenazas externas), binomio al que en casos como el de Colombia deben agregarse dinámicas de subversión y en las últimas décadas amenazas transnacionales: crimen organizado, narcotráfico y terrorismo. Es por ello que, como se dijo antes, todos los Estados se ven forzados a realizar

inteligencia y a poseer algún tipo de organización responsable de proveerla, de la misma manera que mantienen ejércitos y policías. Sin embargo, y como subraya Cepik (2003: 150), tales organizaciones no son solo parte del esfuerzo gubernamental para proveer seguridad y reducir incertidumbre ya que a menudo son también parte del problema.

Semejante paradoja da lugar a los siguientes dilemas: ¿Cómo conciliar la autonomía de los gobernantes para velar por los intereses y la seguridad de los gobernados con el funcionamiento de mecanismos democráticos en virtud de los cuales los primeros deben responder a la voluntad de los segundos? ¿Cómo enfrentar la doble tensión: sigilo / derecho a la información y seguridad individual / seguridad colectiva? Y en relación a los servicios de inteligencia, ¿qué hacer frente a los riesgos de su instrumentalización por parte de los gobernantes y/o de su automatización al punto de que se conviertan en un poder dentro del Estado?

Estas tensiones y dilemas pueden sin embargo, ser reducidos a través de los mecanismos institucionales propios de las poliarquías [1], instrumentos que buscan aumentar el grado de control ciudadano de modo que sea posible tener democracia allí donde existen servicios de inteligencia, al igual que compatibilizar secreto y transparencia.[2] De allí la necesidad de optimizar dispositivos de control [3] como: elecciones, prensa, mandatos legales, control judicial, coordinación y supervisión por parte del Poder Ejecutivo y supervisión y prestación de cuentas en el Legislativo. Según Cepik (2003: 159), cuidando así mismo de la eficacia a través de la intelligence reform [4], es una tarea desafiante no solo para democracias en consolidación, sino para aquellas más antiguas. [5] La complejidad de una

[1] Las poliarquías o "democracias reales" pueden ser pensadas como regímenes que fueron sustancialmente popularizados y liberalizados, esto es fuertemente inclusivos y abiertos a la contestación política. Dahl (2003:31).

[2] El secreto gubernamental es compatible con la transparencia de los actos del gobierno solo cuando la justificación de su necesidad puede ser pública. Ver Cepik (2003:151-152).

[3] Para detallar un poco mejor la idea del control sobre inteligencia el texto se vale aquí de Boraz & Bruneau (2006:33) quienes ofrecen una buena síntesis. En dicha perspectiva el poder ejecutivo normalmente establece la misión y organización básica de la IC, como principal consumidor de inteligencia; a su turno el legislativo crea mecanismo claves de supervisión organizacional, presupuestario y de personal, al poder judicial le cabe el rol de salvaguardar los derechos de los ciudadanos contra eventuales intromisiones del gobierno; en cuanto a los mecanismos legales de rendición de cuentas algunas democracias establecen estos al interior de las propias organizaciones en forma de consejos internos, inspectores generales. Mientras los controles internos incluyen cuestiones como el ethos profesional de las IC, normas institucionales o la existencia de múltiples agencias; los controles externos reúnen prensa, lobbies, think tanks y ONGs.

[4] En términos ideales el resultado de una reforma bien concebida dará lugar no solo a una IC más "democracy-friendly", sino más eficaz en su misión de ayudar a proteger la nación de enemigos reales y potenciales que normalmente intentan ocultar la verdad en relación con sus intenciones y capacidades. Al respecto ver Boraz & Bruneau (2006: 29).

[5] De hecho, Boraz & Bruneau (2008:39) refieren la reciente experiencia de EUA y Gran Bretaña para ilustrar en qué medida la reforma de inteligencia como la propia democracia requiere constante atención, supervisión e ingeniería institucional para ser efectiva.

reforma de inteligencia y el intenso debate que suscita en todo el mundo tiene que ver para Bruneau & Dombroski (2006: 157-158) con cuatro razones. En primer lugar, la inteligencia opera a partir del secreto, tendiendo a eludir los checks and balances en que se basa la democracia. En segundo lugar, las agencias de inteligencia colectan y analizan información lo cual en últimas significa poder para promover sus propias agendas y propósitos, o beneficiar a sus "amigos" en el gobierno. En tercer lugar, los oficiales de la inteligencia rutinariamente realizan en el extranjero actos que están fuera de la ley (robo de documentos, interceptaciones teléfonos etc.) lo que hace difícil la distinción entre romper las leyes en el extranjero y acatarlas en casa. Finalmente, quienes hacen inteligencia tienden siempre a usar como auto justificación el argumento de que su trabajo es crítico para la defensa de la nación.

De modo más específico la reforma de inteligencia tendría según (BORAZ & BRUNEAU, 2006:32-33) obstáculos más específicos en la medida que: a) en nuevas democracias funcionarios electos evitarían cualquier relación con aparatos de inteligencia percibidos como instrumentos de represión en el antiguo régimen; b) políticos civiles pueden, negar su conocimiento de operaciones para evitar aparecer como tolerantes frente a actividades ilegales; c) los políticos pueden no conocer suficientemente a cerca de inteligencia para enfrentar una tarea que suele ser difícil y peligrosa; d) los legisladores a menudo carecerían de incentivos para comprometerse en una reforma de inteligencia; y e) existiría una equivocada definición en cuanto al rol de los legisladores en materia de seguridad nacional. Estos autores igualmente identifican obstáculos provenientes del recelo que cualquier tentativa de control externo puede despertar en la (IC). En este sentido, los profesionales de la inteligencia pueden creer que los civiles no conocen los suficiente sobre su trabajo y sin embargo aspiran a ejecutar un rol de supervisión legal y presupuestal. Frecuentemente las organizaciones de inteligencia supondrían que mayor libertad presupuestal y legal mejora la seguridad del país y en lo que podría ser el mayor problema, el personal de inteligencia puede considerar que los políticos fallan al hacer de la seguridad nacional su prioridad y puede dudar de que tengan la capacidad necesaria para manejar información secreta o temer que inevitablemente acaben culpando a la inteligencia ante cualquier falla. Desconfianza que tiende a intensificarse en países donde los partidos políticos incluyen antiguas guerrillas.

Frente a los obstáculos y con fundamento en (BORAZ & BRUNEAU, 2006), existen varios campos en los es necesario avanzar para conseguir el control democrático en materia de inteligencia: elevar el interés y la presión pública quebrando la apatía y el miedo a la inteligencia; incrementar en los civiles consciencia y competencia en asuntos de inteligencia, en el entendido que las democracias deben asegurar a los civiles carreras viables en ese campo de la seguridad; institucionalizar procesos que soporten transparencia y eficacia:

comités de supervisión en el legislativo, cambios institucionales que enfrenten "luchas internas" y enfaticen operaciones conjuntas, normas de inteligencia en democracia toda vez que mejor coordinación, profesionalismo, transparencia y confianza llevaran a una más efectiva (IC) sirviendo a políticos conocedores. Así mismo, sería necesario fomentar la profesionalización (expertise, corporateness, responsibility) de los servicios de inteligencia como elemento de control interno.

Las anteriores tareas en relación con la reforma de inteligencia son mencionadas aquí no para sugerir acríticamente un rígido plan de trabajo aplicable a todos los casos, pues se considera por al contrario que el debate relacionado con la estructura de inteligencia que requerida por un determinado país y los mecanismos para su control cabe en primera instancia a cada sociedad nacional. Lo que interesa delante de aquella lista de "buenas prácticas" es la manera como subraya la importancia del control democrático, brindando también la máxima atención al problema de la eficacia para la consolidación democrática, eficacia que se torna aun más imperiosa en aquellos países que como Colombia son sacudidos por guerras internas, crimen organizado o narcotráfico. Es por ello que se propone enseguida relacionar las cuestiones generales detalladas hasta aquí con la evolución de la (IC) en Colombia y sobre todo de la más reciente crisis del DAS, intentando justificar la necesidad de una reforma de inteligencia. Esta finalidad dará sentido a la descripción de cuestiones como los problemas de automatización e instrumentalización en la principal agencia civil de inteligencia, algunas decisiones implementadas desde la dirección de la agencia y desde el gobierno para encararla; lo mismo que al rol cumplido por controles externos como el legislativo y la prensa entre otros.

3.2. El Departamento Administrativo de Seguridad (DAS)

Si bien la historia de los servicios secretos en América Latina tiene principio a mediados de los años cuarenta, cuando Argentina, Brasil y México crearon organizaciones de inteligencia que estaban inspiradas en las policías políticas de Europa Oriental en la Guerra Fria. (GÓMEZ, 2009). En Colombia esto ocurrirá casi una década después. Así en 1953 durante el gobierno del General Rojas Pinilla (1953-1957) se constituirá el Servicio de Inteligencia Colombiano SIC, organismo que en 1960 pasa a ser el Departamento Administrativo de Seguridad DAS.[6] Según Porch (2009), el DAS tendrá por lo menos tres problemas congénitos: uno de ellos será la incapacidad de definir una núcleo de misiones,

[6] El gobierno de Rojas Pinilla fue una solución de arbitraje para detener el desbordamiento del conflicto político conocido como "La Violencia" Este episodio de la historia colombiana por el cual los jefes de los principales partidos colombianos, liberal y conservador, instrumentalizaron el fanatismo político entre sus bases se agudizo luego del 9 de abril de 1948 - cuando es asesinado en Bogotá el caudillo liberal Jorge Eliecer Gaitán - y que extenderá su influjo hasta 1965, dejando como saldo cerca de 200.000 víctimas." Pearce (1992).

el segundo aludirá a deficiencias burocráticas como: alta rotación de personal, bajos salarios y ausencia de estructura de carrera y en tercer lugar, una elevada politización, inherente al régimen de poder dividido – Frente Nacional (1958-1974) – en el que nació. De esta manera anclado en el clientelismo del sistema político colombiano y con carencias misionales y organizacionales, el DAS no solo restringirá sus posibilidades de eficacia sino que rápidamente ganará una reputación de corrupción. Tales deficiencias resistirán la reorganización administrativa impulsada por el gobierno de Misael Pastrana en 1974 y la restructuración con ambiciones modernizantes y de tecnificación ejecutada por el Presidente Virgilio Barco en 1989, pudiendo decirse lo mismo en relación a los problemas de duplicidad, falta de coordinación y desperdicio de recursos que desde los años setenta serán visibles no solo en el DAS, sino en la inteligencia militar e inteligencia policial.

Fue con un sistema de inteligencia descoordinado, poco profesional y corrupto que el Estado debió enfrentar a partir de 1984 la guerra contra el Cartel de Medellín y la persecución de Pablo Escobar Gaviria. Sin embargo, en esa coyuntura la fragilidad del DAS, se vio temporalmente disimulado sobre todo durante la dirección de Miguel Masa Marques (1986-1992) y con mayor razón en virtud de la participación del organismo en el operativo que eliminó a Escobar Gaviria el 2 de diciembre de 1993. Así, la guerra contra el narcotráfico no solo no serviría para enfrentar los problemas estructurales del DAS sino que contribuyó a agravarlos como consecuencia de la estrategia heterodoxa implementada por entonces (asistencia técnica norteamericana, alianzas con agrupaciones delictivas entre ellas la conformada por los enemigos de Pablo Escobar conocida como los "PEPES" etc.) que toleró una cultura de violación a los derechos humanos (PORCH, 2009).[7]

Por tanto, los problemas de la inteligencia continuarían sin solución de continuidad y como anota (BORAZ, 2008), ni la Constitución de 1991 o los gobiernos de Cesar Gaviria (1990-1994), Ernesto Samper (1994-1998) y Andrés Pastrana (1998-2002) materializaron una restructuración del DAS y de la (IC) en su conjunto.[8] En cuanto a la Constitución de 1991 propuesta para robustecer al Estado y al régimen político a partir del paradigma de la democracia participativa, aunque incluyó en materia de seguridad importantes novedades al intentar contrarrestar la hegemonía que desde 1958 ostentaban los militares en materias de seguridad y defensa, no introdujo cambios sustanciales en materia de inteligencia (LEAL BUITRAGO, 1994). Durante el gobierno de Cesar Gaviria tal vez la cuestión a destacar sea la creación de un comité asesor para la coordinación

[7] La sigla PEPES significa perseguidos por Pablo Escobar.

[8] En Colombia la IC comprende además del DAS, la inteligencia del ejército, la fuerza aérea y la marina, la Dirección de Inteligencia de la Policía Nacional, DIPOL, la Unidad de Información y Análisis Financiero UIAF y el Cuerpo Técnico de Investigaciones CTI, de la Fiscalía General de la Nación, Boraz (2008).

nacional de inteligencia del que participaron los Ministros del Interior, Defensa, Relaciones Exteriores, el Comandante de las Fuerzas Armadas y los directores de la Policía Nacional y el DAS. Más adelante, el gobierno de Ernesto Samper a través del Decreto 2233 de 1995 buscó, crear el Sistema Nacional de inteligencia SINAI del que también hacían parte las carteras de Defensa, Justicia, intentando unificar y coordinar una política de inteligencia que fortaleciera la cooperación y la eficiencia, lo mismo que inovar el ciclo de inteligencia (planificación, dirección, recolección, análisis y diseminación). Sin embargo durante su mandato los modestos alcances de estas iniciativas contrastaron con los controvertidos episodios que rodearon la salida de dos directores del DAS, Ramiro Bejarano y Marco Tulio Gutiérrez, el primero por negarse a monitorear enemigos del gobierno y el segundo por valerse de una firma privada para hacerlo. Finalmente, mediante el Decreto ley 218 de 2000 el gobierno de Andrés Pastrana, intentó especificar las funciones del DAS y encargó a las organizaciones de inteligencia la tarea de producir la información que el Estado requería para la toma de decisiones y la formulación de la política relativa a la seguridad interna y externa. Aunque, tales reformas no estuvieron integradas en una estrategia más amplia.

En la Administración de Álvaro Uribe Vélez (2002-2010), que a diferencia de sus antecesores optó por una estrategia militar en el control del orden público y vino a profundizar la cooperación militar con EUA iniciada por Pastrana, la presión por resultados traería un efecto perjudicial para la (IC) que se tradujo en: deterioro de los protocolos mínimos de inteligencia; intensificación de la falta de coordinación y las rivalidades históricas entre policía y ejército, imposibilitando de paso la posibilidad de cruzar, procesar y analizar información; continuarán así mismo, deficiencias crónicas como la reiteración entre las funciones de las agencias y la confusa mezcla de tareas del DAS, llevando por ejemplo a que con frecuencia colisionen la inteligencia con la investigación criminal (PORCH, 2009; BORAZ, 2008).[9] Por estas razones a pesar de que a lo largo de los seis apartes de la Política de Defensa y Seguridad Democrática PDSD adoptada en 2003 se concede un importante rol al DAS, la agencia no tardaría en convertirse en el talón de Aquiles de la administración Uribe Vélez.[10]

---

[9] La consecuencia más sobresaliente de esa cooperación en términos de inteligencia es la Central de Inteligencia Conjunta localizada en la base aérea de Tres Esquinas (Departamento del Caquetá) creada en 1999 bajo los auspicios de Comando Sur (El Tiempo, 1999a). Incluye una plataforma de unas 1.500 has. a poco más de 3.000 metros sobre el nivel del mar, entre los ríos Caquetá y Orteguaza, posee una pista de 2.500 metros para el aterrizaje y despegue de aviones dedicados a labores de inteligencia y alerta temprana: AWACS-E3, Orión P-3, RC-7 («avión fantasma»), y aeronaves Galaxy C-5, para el transporte masivo de tropas. Cuenta así mismo, zonas para entrenamiento y ubicación de personal; radares conectados a sistemas satelitales, radares de vigilancia basados en tierra (GMR) y de vigilancia aérea (AEW), para monitorear el país, con proyección hacia el Atlántico y el Pacífico, desde Putumayo, isla de San Andrés, la Guajira, Vichada, San José del Guaviare, Leticia. Serrano Torres (2005).

[10] http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/DIFP/Cap.%202%20Web.pdf

La crisis del DAS durante el gobierno Uribe en virtud de la cual se anunció a fines de 2009 la extinción de la agencia (Semana, 2009a), comienza durante la dirección de Jorge Noguera Cotes (2002-2005).[11] Noguera en su calidad de director del DAS no solo incluyo dentro de sus "asesores externos" generales cuestionados por sus vínculos con el paramilitarismo como Rito Alejo del Rio y Iván Ramírez Quintero, sino permitió que la infiltración de narcotraficantes, paramilitares y en menor escala guerrillas de izquierda como el ELN (Ejército de Liberación Nacional), dentro de la inteligencia civil alcanzara niveles insólitos.[12] De hecho, tanto Noguera como el subdirector del DAS tendrán que salir de la institución en octubre de 2005 en medio de una grave denuncia según la cual el Director de Inteligencia Enrique Arriza habría intentado comprar el expediente del narcotraficante Wilber Varela alias "jabón" e instalar una central de inteligencia paralela al servicio de Carlos Mario Jiménez, jefe del bloque Central Bolívar de los paramilitares (El Espectador, 2010a).

Enseguida y cuando todo hacía suponer que el final de la administración Noguera Cotes precipitaría las reformas indispensables, un nuevo escándalo se encargó de revelar el carácter limitado de los correctivos implementados por las direcciones de Andrés Peñate (2005-2007) y María del Pilar Hurtado (2007-2008). El comienzo del episodio conocido en los medios periodísticos como "las chuzadas" fue revelado a partir de octubre de 2008 cuando el senador del Gustavo Petro, miembro del partido opositor Polo Democrático Alternativo (PDA), denunció hechos de espionaje realizados por el DAS en contra miembros de la oposición, periodistas, defensores de derechos humanos, etc. (El Espectador, 2009b). En relación con las revelaciones de Petro, la Fiscalía General de la Nación establecería después que los seguimientos habrían sido ejecutados por "G-3", una estructura creada en 2004 con la misión de monitorear personas y organizaciones opositoras que eran considerados como una amenaza. Según la Fiscalía, el "G-3" era una estructura informal que dependía del jefe de inteligencia y había sido usado incluso para espiar miembro del propio gobierno como el Vicepresidente y el viceministro de Defensa. Una vez extinto en 2006 dará lugar al GONI (grupo de

[11] El nombramiento de Jorge Noguera (jefe de la campaña presidencial de Uribe en el Departamento del Magdalena en 2002) habría ocurrido a pesar de sus vínculos con paramilitares de su desconocimiento en materia de inteligencia. Algunos de los episodios más polémicos de su gestión incluyen: suprimir archivos que comprometían la responsabilidad de líderes paramilitares en graves delitos; patrocinar el fraude electoral en beneficio de partidarios de Uribe; recibir propinas de parte de narcotraficantes por informaciones relacionadas con operaciones de la policía; suministrar listados de sindicalistas y profesores de izquierda a los paramilitares para que posteriormente fueran asesinados; eliminar la Unidad de Investigación Financiera en 2002 para cubrir aparentes vínculos entre compañías petroleras y carboníferas norteamericanas con las Autodefensas Unidas de Colombia Ver Porch (2009).

[12] "En 2008 el Ejército encontró un computador perteneciente a integrantes del ELN en Arauca. Para sorpresa de los militares, entre los documentos que tenía el portátil estaban los informes completos enviados a la Dirección General Operativa del DAS en Bogotá con detalles sobre una operación contra estructuras del ELN en esa zona del país (Semana, 2009b).

Observación Nacional e Internacional), a su vez comprometido en seguimientos ilegales a los Magistrados de la Corte Suprema de Justicia (El Tiempo, 2009b). En relación con la Corte Suprema, órgano judicial con el que el Ejecutivo sostuvo tensas relaciones [13], en 2009 fue también denunciada la participación de Martha Leal alta funcionaria de la dirección de inteligencia del DAS en reuniones celebradas en la Casa de Nariño (Sede del Gobierno Nacional), entre un enviado del jefe paramilitar conocido como "Don Berna" y funcionarios del gobierno, cuya finalidad era reunir información en contra de los miembros del alto tribunal (Revista Semana, 2009b). Corroborando la aparente instrumentalización del DAS por parte del Ejecutivo, recientes declaraciones obtenidas dentro de la investigación que la Fiscalía General de la Nación sigue por estos hechos, han llegado a comprometer la responsabilidad del Presidente de la Republica de cuyo despacho depende directamente el DAS. De acuerdo con el testimonio del ex director del Área de Inteligencia del DAS, a principios de septiembre de 2007 el Secretario General de la Presidencia manifestó a la directora del DAS María del Pilar Hurtado, el interese del Presidente para que lo mantuviera informado acerca de: la Corte Suprema de Justicia, los senadores de oposición Piedad Córdoba, Gustavo Petro y el periodista Daniel Coronell (El Espectador, 2010c). En el mismo sentido la Fiscalía sugirió que las interceptaciones practicadas a miembros de la Corte Suprema obedecían a las importantes investigaciones que allí se adelantaban en especial a sus decisiones en relación con la "parapolítica" – proceso que como ya fue señalado comprometió judicialmente a la coalición uribista. Un día después de lo dicho por la Fiscalía, el propio Jefe del Estado tuvo que salir a negar la responsabilidad del Ejecutivo en relación con espionajes ilegales, en lo que puede ser un uso de la negación plausible. Uribe afirmó: "Si el gobierno ordenara espionajes ilegales tendría cárcel, empezando por el Presidente" (El Tiempo, 2010c).

De cualquier manera es bueno subrayar que las irregularidades ocurridas en el DAS durante los últimos años, tienen un carácter estructural y recurrente a la luz de los antecedentes y la evolución de la actividad de inteligencia del país. Lo que no significa que lo que ha venido ocurriendo durante los últimos años pueda ser visto como un asunto menor. La automatización de la inteligencia como fuente de información que se vende a los intereses de narcos y paramilitares o su instrumentalización por el Ejecutivo afectan la calidad de las instituciones poliárquicas ya que por ejemplo, usar la inteligencia para seguir irregularmente a la oposición limita la competición política, una de las dimensiones claves

[13] Esta tensión tiene como antecedente un enfrentamiento entre el Presidente de la Republica y el Magistrado Iván Velásquez iniciado en 2007 cuando este inició sus investigaciones sobre "parapolítica", proceso que desde 2006 indaga la penetración de los paramilitares en el Legislativo y cuyos resultados afectaron particularmente a los partidos Uribistas. Por parapolítica fue condenado entre otros congresistas el Senado Mario Uribe Escobar primo del Presidente de la Republica. Jane's (2009).

de la democratización según Dahl (2005). En la misma perspectiva teórica, la infiltración del crimen organizado en el aparato de inteligencia resulta problemático a la luz de la octava condición para la poliarquía, esto es: contar con instituciones para hacer que las políticas del gobierno dependan de las elecciones o de otras manifestaciones de preferencias y no de grupos de poder no electos (DAHL, 2005). De allí la necesidad de una reforma que logue conciliar control democrático y eficacia no solo en el DAS, sino en el conjunto de la (IC).

Detallada la naturaleza de la crisis de la inteligencia en Colombia, lo mismo que subrayadas sus implicaciones para la democracia colombiana, conviene presentar brevemente la manera como algunos dispositivos de control han venido respondiendo a la situación. En lo que respecta los medios de comunicación y aun coincidiendo con (CEPIK, 2003) en cuanto a que estos no son un "agente perfecto" de lo público y presentan limites endógenos y exógenos para vigilar al gobierno, es necesario reconocer el papel de publicaciones nacionales como el periódico Espectador, y las revistas Semana y Cambio, medios que durante los últimos años han venido haciendo una importante labor investigativa y un cubrimiento sistemático de las irregularidades dentro del DAS. [14] La dirección del organismo con Andrés Peñate buscó recobrar el control institucional de la organización a través de varias estrategias entre las que se destacan: un sistema de contrainteligencia; trasladar funcionarios en las direcciones regionales más afectadas por la influencia paramilitar; elaborar un mapa de riesgo para la institución; implementación el polígrafo; requisitos más estrictos (exámenes, entrenamientos) para promoción; priorizar la misión de producir inteligencia (con la publicación de un boletín de inteligencia dirigido alto gobierno y oficiales militares) y finalmente, mejorar los niveles de cooperación con la inteligencia militar (suministro de HUMINT e inteligencia financiera) (PORCH, 2009). Con Felipe Muñoz, quien desde 2008 remplazo en la dirección a María del Pilar Hurtando, continuó el proceso de ajuste institucional dirigido a focalizar al DAS en inteligencia estratégica. En este camino pueden destacarse cuestiones como el desmonte de labores no misionales (protección de personalidades y la coordinación de la oficina de INTERPOL Bogotá), redacción de un Manual Nacional de Inteligencia ajustando los manuales de inteligencia y contrainteligencia, creación del Grupo Centro de Protección de Datos y Archivos de inteligencia y contrainteligencia y la promoción ante el Congreso en noviembre de 2009 de un proyecto de ley que suprime la actual estructura para dar forma a una nueva agencia, en relación con esta última finalidad fue también elaborado un libro Blanco de Inteligencia, hoja de ruta en

[14] De hecho un grupo de periodista de la revisa Semana se hizo acreedor al Premio Latinoamericano de Periodismo de Investigación, por el trabajo titulado "Espionaje e interceptaciones ilegales en el DAS", El galardón, entregado por Transparency International y el Instituto Prensa y Sociedad de Perú. (El Espectador, 2010d).

la creación de la nueva institución. [15] En lo que se refiere al papel del Legislativo, este muestra una postura contradictoria, ya que si bien ha servido de escenario para intensos debates en torno a las irregularidades del DAS [16] y tramitó la ley 1288 de 2009 [17], marco legal que establece límites, fines, mecanismos de control sobre las actividades de inteligencia y contrainteligencia, así como regula el uso de las bases de datos en que se apoyan y promueve la cooperación y coordinación al interior de la (IC). Por otro lado ha eludido el debate con argumentos poco claros el proyecto de ley que confiere facultades al Ejecutivo para eliminar la actual estructura del DAS [18] y crear una nueva institución de inteligencia (El Espectador, 2010e), comportamiento que parece ilustrar aquello que se comentó en la primera parte del ensayo en relación como la falta de incentivos de los legisladores para comprometerse [19] con reformas de inteligencia. Finalmente, en lo que se refiere al rol de la Rama Judicial si bien, la Fiscalía General de la Nación sobresale por la tarea investigativa que viene desarrollando y en virtud de las cuales se ha podido enjuiciar altos funcionarios del gobierno; habría que decir así mismo, que el control previo sobre la legalidad o razonabilidad en el área de seguridad e inteligencia continua siendo limitado aun después de la entrada en vigencia de la ley 1288 de 2009, instrumento que no contempló nada semejante a lo que existe en países como Perú, donde virtud

---

15 Tomado del Informe del DAS al Congreso de la Republica de Colombia 2009-2010 "Inteligencia al servicio del país".

16 El más reciente fue promovido por la Comisión Primera del Senado y buscaba esclarecer el paradero de dos de las siete plataformas móviles de inteligencia y vigilancia compradas por el DAS en 2007, al igual que esclarecer irregularidades relacionadas con la existencia de intermediarios y sobornos en la negociación.

17 Uno de los aspectos más destacados de esta ley tiene relación con la institucionalización del control parlamentario creando la Comisión legal parlamentaria de Seguimiento a las actividades de Inteligencia y Contrainteligencia.

18 La actual estructura orgánica del DAS está compuesta por La Dirección del Departamento dependencia a la cual están asignados los empleos de Secretario Privado y Asesores del Despacho; una oficina de Asuntos Internacionales; 27 seccionales: Amazonas, Antioquia, Arauca, Atlántico, Bolívar, Boyacá, Caldas, Caquetá, Casanare, Cauca, Cesar, Córdoba, Cundinamarca, Chocó, Guajira, Huila, Magdalena, Meta, Nariño Norte de Santander, Quindío, Risaralda, San Andrés, Santander, Sucre, Tolima. Valle del Cauca; veinte 20 Puestos Operativos: Apartado, Tame, Sogamoso, Aguazul, Aguachica, Planeta Rica, Fusagasuga, Facatativa, Girardot, Maicao, Pitalito, Granada, Puerto Carreño, Ipiales, Tumaco, Mocoa, Providencia, Barrancabermeja, Magangue, Buenaventura; 12 Puestos de Seguridad Rural: Paz de Ariporo, Tauramena, Orocue, Caucasia, Sahagun, Fonseca, Fundación, San Martín, Puerto López, Guamo, Mariquita, Trujillo y 37 Puertos Migratorios: Leticia (3), Medellín, Turbo, Apartado, Capurgana, Arauca [2], Barranquilla [2], Cartagena [2], Coveñas, Bogota, Riohacha, Puerto Nuevo, Maicao, Paraguachon, Santa Marta, Puerto Carreño, Tumaco, Ipiales, Mocoa, San Miguel, Cúcuta [2], Pereira, San Andrés [2], Providencia [2], Bucaramanga, Cali, Buenaventura, Bahia Solano, Base Militar de Apiay. Ver, http://www.das.gov.co/

19 De acuerdo con la acusación presentada por la Fiscalía ante el Juez de Conocimiento, desde finales del 2007 y durante el 2008, Mario Aranguren, quien se desempeñaba como director de la Unidad de Información y Análisis Financiero UIAF - encargada de prevenir y detectar operaciones de lavado de activos - realizó junto con funcionarios del DAS actividades ilegales de investigativas sobre algunos magistrados de la Corte Suprema, encaminadas a establecer vínculos con agentes del narcotráfico o con cualquier persona o conducta al margen de la ley, (El Tiempo,2010d).

de una ley análoga, dos Vocales Superiores Ad Hoc deben ser designados por la Corte Suprema para autorizar o negar solicitudes de la DINI en relación con operaciones especiales (CHIRI, 2006:15). [20]

3.3. Consideraciones Finales

El contradictorio cuadro de la realidad colombiana – elecciones razonablemente libres y competitivas desde 1958 y el desafío de organizaciones guerrilleras, paramilitares y narcotraficantes a las instituciones democráticas y la legitimidad estatal, dentro del cual se enmarca la crisis vivida por el DAS durante sus casi seis décadas de existencia – ofrece la justificación para llevar adelante una reforma de inteligencia que avance en el propósito de construir una comunidad de inteligencia más eficiente desde el punto de vista estratégico y compatible con las exigencias de la democracia, proceso que como se mostró está cercado de impedimentos y desafíos en cualquier democracia. La manera como el tema de la inteligencia se ignoró durante la discusión y promulgación de la Constitución de 1991 proceso que busco liberar al régimen político de las estreches introducidas desde el Frente Nacional para consolidar la Democracia y que inexplicablemente postergó la solución a los problemas endémicos de la inteligencia colombiana, trajo como correlato los fenómenos de infiltración criminal y espionaje político que la opinión viene conociendo desde 2004.

En el contexto de la transición por la que pasa el DAS desde finales de 2009 la actual dirección de la institución tiene a su favor haber dado continuidad a los esfuerzos por resolver la histórica dispersión de funciones conjurando los riesgos potenciales que una crisis de semejantes proporciones puede representar para la seguridad nacional: vacio de inteligencia, fugas de información sensible, etc. Sin embargo, es necesario evitar que esta parsimonia conduzca a un simple cambio de nombre con el que se preserve la misma estructura, los mismos recursos, mentalidad y desde luego los mismo defectos. Razón por la cual se torna necesario el compromiso no solo del Ejecutivo, que por cuenta de la centralidad que hasta febrero de este año otorgó dentro de su agenda a impulsar una segunda reelección acabó relegando esta y otras cuestiones cruciales, sino del Legislativo que también pareció tener pocos incentivos para discutir la reforma de inteligencia. En este propósito puede ser útil revisar experiencias latinoamericanas como las de Mexico, Ecuador, Chile y Brasil. En relación a estos dos últimos países en Chile luego de la transición a la democracia fue creada la ANI (Agencia Nacional de Inteligencia) en la que predominan los analistas de formación universitaria;

[20] La ausencia de una reforma sustantiva habría ocurrido en el Perú durante la transición del Servicio de Inteligencia Nacional (SIN) al Consejo Nacional de Inteligencia (CNI).

subordinada al Ministerio del Interior, asesora al gobierno y encabeza el sistema de inteligencia (Fundación Ideas para la Paz, 2006). Mientras Brasil desde 1999 viene rediseñando su inteligencia creando la Agencia Brasilera de Inteligencia ABIN, el Sistema Brasilero de Inteligencia SISBIN, el Sistema de Inteligencia de Seguridad Publica SISP, el Sistema de Inteligencia de Defensa y en 2004 el plan de carrera para los analistas de informaciones de la ABIN, (Cepik, 2005). La necesidad de una agencia colombiana de inteligencia especializada en suministrar inteligencia estratégica se hace más clara considerando que según el diagnóstico del gobierno, de los 6500 funcionarios que integran la actual planta de personal del DAS, únicamente el 17% desempeña funciones de inteligencia contrainteligencia y extranjería (Revista Semana, 2010c).

En este camino, la ley 1288-2009 es un instrumento útil aunque insuficiente, pues por el momento no se observan acciones concretas en cuestiones como ampliar el nivel de conocimiento de los civiles en temas de Defensa, mejorar los niveles de confianza [21] entre los políticos y el personal de la (IC) y vencer el desconocimiento, la apatía y el miedo que la palabra inteligencia despierta en la sociedad. Esta es una cuestión clave para mejorar el control directo e indirecto y traer una mayor legitimidad para el esfuerzo fiscal que el Estado debe realizar para mantener las capacidades que requiere en el escenario estratégico que se viene cristalizando desde 2000 en virtud del Plan Colombia y del Plan Patriota. Solo así Colombia avanzará en el propósito de contar con un sistema de inteligencia eficaz y legítimo – condición necesaria para la democratización y la seguridad en el actual sistema internacional. Lamentablemente por ahora lo único que parece claro es la notable coincidencia entre el gobierno saliente de Uribe y el entrante de Juan Manuel Santos, no solo porque ambos han manifestado su interés de liquidar el DAS para crear una nueva agencia sino en la medida que ninguno ha dicho hasta ahora cómo lo van a hacer, cuándo y con qué.

REFERÊNCIAS

BORAZ, Steven & BRUNEAU, Thomas. (2006). Democracy and Effectiveness, publicado en Journal of Democracy [http://muse.jhu.edu/login?uri=/journals/journal_of_democracy/v017/17.3boraz.pdf]. Disponible: 05/09/2010.

[21] Un detective de la subdirección de operaciones del DAS declaró en 2009: "Acá se trabaja por blancos y objetivos que puedan ser una amenaza a la seguridad del Estado y del Presidente. Dentro de esos está la guerrilla, las bacrim (bandas criminales), algunos narcos. Pero dentro de esos blancos también están, y es obvio como parte de una de las funciones del DAS, controlar a algunos personajes e instituciones para mantener informada a la Presidencia. Por ejemplo, cómo no va a ser misión del DAS controlar a Petro, que es un ex guerrillero y es de la oposición. O a Piedad Córdoba, por sus vínculos con Chávez y la guerrilla" (El Espectador, 2009f).

BORAZ, Steven. (2008). Colombia: En PSI Handbook of Global Security and Inteligence, National Approaches, Volume 1. Praeger Security International Westport, Connecticut, London.

BRUNEAU, Thomas & DOMBROSKI, Kenneth. (2008). *Reforming Intelligence*: The Challenge of Control in New Dew Democracies. En: Global Politics of Defense Reform. Polgrave Macmillan.

CEPIK, Marco. (2003). *Espionagem e democracia*: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV.

_____. (2005). *Regime Político e Sistema de Inteligência no Brasil*: Legitimidade e Efetividade como desafios institucionais. [http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0011-52582005000100004&lng=en&nrm=iso]. Disponible: 05/09/2010.

CHIRI, Renzo. (2006). *Lineamientos para una política de defensa nacional*: Perú 2006-2011, publicado en RESDAL [http://www.resdal.org/libros/Archivo/libro-chiri.html]. Disponible: 05/09/2010.

COLÔMBIA, Departamento Administrativo de Seguridad. http://www.das.gov.co/

COLÔMBIA, Política de Defensa y Seguridad Democratica. Publicado en DNP [http://www.dnp.gov.co/PortalWeb/Portals/0/archivos/documentos/DIFP/Cap.%202%20Web.pdf]. Disponible: 09/08 2010.

Congreso de la Republica. Ley 1288 de 2009. [http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1288_2009.html]. Disponible: 09/08 2010.

DAHL, Robert. (2005). *Poliorquia Participação e Oposição*. São Paulo: Editora da Universidade de São Paulo.

GOMEZ, Andrés. (2009). *Servicios de Inteligencia y Democracia en America del Sur*: ¿Hacia una segunda generacion de reformas normativas? publicado en RESDAL http://www.resdal.org/producciones-miembros/trabajo-academico-gomez.pdf []. Disponible: 05/09/2010.

EL ESPECTADOR. 2009f "Petro señala que "chuzadas" del DAS son orden de Uribe [http://www.elespectador.com/articulo120242-petro-senala-chuzadas-del-das-son-orden-de-uribe]. Disponible 02/06/2010.

_____. 2010e "Liquidación del DAS, a punto de caerse en el Congreso" [http://www.elespectador.com/noticias/politica/articulo-203992-liquidacion-del-das-punto-de-caerse-el-congreso]. Disponible 02/06/2010.

_____. 2010d "Semana gana premio Latinoamericano de periodismo de investigación" [http://www.elespectador.com/articulo-222672-revista-a-gana-premio-latinoamericano-de-periodismo-de-investigacion]. Disponible 02/06/2010.

EL ESPECTADOR. 2010c "Chuzadas eran del interés de Uribe" [http://www.elespectador.com/noticias/judicial/articulo-214866-chuzadas-eran-de-interes-de-uribe-dice-ex-director-de-inteligencia]. Disponible 02/06/2010.

_____. (2009b) *En 2004 empezaron rastreos del DAS* [http://www.elespectador.com/impreso/articuloimpreso145453-2004-empezaron-rastreos-del-das]. Disponible 02/06/2010.

_____. 2010a a. "Los juegos del poder" [http://www.elespectador.com/impreso/judicial/articuloimpreso122558-los-juegos-de-poder-el-das]. Disponible 02/06/2010.

EL TIEMPO. 1999a "Crean Central De Inteligencia Antinarcóticos En Tres Esquinas Caquetá" 1999a [http://www.eltiempo.com/archivo/documento/MAM-952557]. Disponible 02/06/2010.

_____. 2009b "Hasta el año pasado se mantuvieron las "chuzadas" ilegales del DAS, confirmo la Fiscalía" [http://www.eltiempo.com/colombia/justicia/hasta-el-ano-pasado-se-mantuvieron-chuzadas-ilegales-del-das-confirmo-la-fiscalia_5299768-1#].Disponible 02/06/2010.

_____. 2010c "Si el gobierno ordenara espionajes ilegales tendría cárcel, empezando por el Presidente" [http://www.eltiempo.com/colombia/justicia/ARTICULO-WEB-PLANTILLA_NOTA_INTERIOR-7634773.html]. Disponible 08/09/2010.

_____. 2010d "Arrancó juicio a Mario Aranguren por caso de las interceptaciones ilegales" [http://www.eltiempo.com/colombia/justicia/arranca-juicio-a-mario-aranguren-por-caso-de-las-interceptaciones-ilegales_7888294-1]. Disponible 08/09/2010.

FUNDACIÓN Ideas para la Paz. Siguiendo el conflicto: hechos y análisis de la semana. Número 42/ 7 de abril de 2006. Boletín disponible en [www.ideaspaz.org/publicaciones.]. Disponible: 05/09/2010.

INFORME DEL DAS AL CONGRESO DE LA REPUBLICA DE COLOMBIA 2009-2010 "Inteligencia al servicio del país" [http://www.das.gov.co/]. Disponible: 05/09/2010.

JANE'S. (2009). Country Profiles: Colombia. Disponível em: www.janes.com.

LEAL BUITRAGO, Francisco & TOKATLIAN, Juan Manuel. (1994). Orden Mundial y Seguridad, Bogotá: TM Editores IEPRI.

PEARCE, Jenny. (1992). Colombia dentro del laberinto, Bogotá: Altamir Ediciones.

PORCH, Douglas. (2009). Taming a "Dysfunctional Beast"—Reform in Colombia's Departamento Administrativo de Securidad',International, publicado en Journal of Intelligence and CounterIntelligence [http://www.informaworld.com/smpp/title~content=t713723134]. Disponible: 09/08 2009.

REVISTA SEMANA. 2009a "¿Se acaba el DAS? [http://www.semana.com/noticias-nacion/acaba-das/128923.aspx" Disponible 02/08/2010.

REVISTA SEMANA. 2009b “El DAS sigue gravando” [http://www.semana.com/noticias-nacion/das-sigue-grabando/120991.aspx]. Disponible 02/06/2010.

_____. 2010c “Restructuración del DAS: ¿cirugía o eutanasia?” [http://www.semana.com/noticias-justicia/reestructuracion-del-das-cirugia-eutanasia/138734.aspx]. Disponible 02/06/2010.

SERRANO, Jorge. (2005). La comunidad de inteligencia colombiana. Publicado en PROJUSTICIA. Disponível em: http://projusticia.org.pe/site.php?plantilla=contenido&ncategoria1=109&ncategoria2=139&ncontenido=3242]. Último acesso: 09/08/2010.

Capítulo 4

INTELIGÊNCIA E SEGURANÇA REGIONAL NA ÁFRICA OCIDENTAL: O CASO DA NIGÉRIA

Mamadou Alpha Diallo

A África foi um dos palcos da Guerra Fria, na qual uma das principais armas ou ferramentas foi sem dúvida a atividade de inteligência. Esta, por sua vez, consiste na coleta, análise e disseminação de informação que auxilia na tomada de decisões. Vinte anos depois do fim da bipolaridade, a África volta a chamar atenção por interesses econômicos, políticos e sociais.

Nesse sentido, é sempre bem-vindo um estudo acadêmico sobre a África, principalmente na área de inteligência e a segurança, que até hoje é pouco explorada ou pouco conhecida no continente negro. Isso não quer dizer que não existam serviços de inteligência; ao contrário, há serviços de inteligência funcionando, que ajudaram os movimentos de independência na luta pela libertação, e que continuaram existindo após as independências, em suas várias formas. Todos os regimes africanos e movimentos de libertação tiveram uma forma de aparato de segurança – em vários casos considerados como ajuda externa.[1]

Assim sendo, este artigo tem como objetivo examinar o processo evolutivo das estruturas de inteligência da Nigéria, sua possível relação com a consolidação da democracia no país e o papel da República Federativa da Nigéria como líder das forças de segurança regional (ECOMOG). Para tanto, o artigo será dividido em três seções. Na primeira, tratarei da evolução política do país. Na segunda, analisarei mais a fundo o papel e a importância da Nigéria na construção do complexo regional de segurança no âmbito da CEDEAO. Por fim, será analisado o serviço de inteligência da Nigéria, com o objetivo de identificar o lugar que ele

[1] *The Journal of Modern African Studies*, 30, 4(1992), p. 585, Cambridge University Press.

ocupa dentro do aparato estatal do país, assim como seu peso e importância no funcionamento das instituições burocráticas.

4.1. Evolução Política da Nigéria

Com 120 milhões de habitantes, a Nigéria é a nação mais populosa da África: um mosaico de mais de 250 grupos étnicos e lingüísticos. Os três principais grupos étnicos são os Hausa-Fulani, no norte; os Iorubas, no sudoeste; e os Ibos no sudeste do país, que juntos contabilizam cerca de três quartos da população nigeriana. A superfície do país (923.768 km^2) é dotada de muitos recursos, tais como enormes jazidas de petróleo e gás, betume e demais recursos minerais como estanho, ferro, carvão, cal, nióbio, chumbo, zinco, bauxita, além de solos para cultivo. Os produtos agrícolas e de pecuária incluem cação, borracha, dendê, amendoim, milho, arroz, mandioca, inhame, carneiro, gado, madeira, etc. Segundo dados do governo nigeriano (2010), em termos de energia elétrica, o país possui 6.000MV de capacidade instalada de geração, que é grosseiramente inadequada. O país tem reservas comprovadas de gás e cerca de 8.000MV de energia hidrelétrica estão sendo planejados. O Produto Interno Bruto (PIB) foi estimado em 2008 em US$ 338,1 bilhões, e o crescimento real foi de 6,1%, no período por ano. Tradicionalmente, existem tensões sociais e econômicas entre o norte muçulmano e o sul, principalmente cristão.

Ciente das suas potencialidades, a Nigéria vem desempenhando o papel de líder no âmbito regional e continental nos últimos anos. Fato este que teria certamente mais impacto e credibilidade se o país tivesse resolvido seus problemas internos referentes principalmente à democracia ou simplesmente à forma de acesso ao poder. O problema de acesso à instância suprema do Estado é apontado como uma das principais causas de conflitos e de subdesenvolvimento na África. No fundo, a fragilidade do Estado africano vem da inexistência de um consenso universal sobre as estruturas e as regras de funcionamento da arena política, conforme Wade (2005). Ou seja, é preciso definir como ter acesso e direito ao uso dos meios de coerção do Estado nos países africanos em geral e, principalmente, na Nigéria, onde as forças armadas têm sido envolvidas em todos os processos políticos. Isto é devido, em parte, ao passado colonial.

Como bem lembra Fayemi (2002), na África, as forças armadas são descendentes diretos das forças coloniais, enraizados na visão imperial de manter a ordem. Neste sentido, o autor mencionado observa que as forças armadas nigerianas são um produto do colonialismo britânico, tendo sido inclusive consideradas parte das forças armadas britânicas depois da Segunda Guerra Mundial. Como tal, controlava as fronteiras dos territórios da Nigéria, da Costa de Marfim, da Gâmbia e de Serra Leoa e era vista como uma extensão do poder colonial devido às suas interações maiores com a metrópole, tanto lutando ao

lado das forças imperialistas, durante a Primeira Guerra Mundial, quanto contra ela, durante as Guerras de Libertação Nacional. Esta elite africana se vê como a principal e a mais bem preparada para assumir o destino dos Estados africanos independentes. Isso certamente ajuda a explicar a ingerência dos militares na política nigeriana depois da independência do país. Segundo Fayemi (2002), a longa interação entre militares das colônias com as forças da metrópole e o importante papel exercido por esses militares no campo dos aliados na Segunda Guerra Mundial criou uma rede que possibilitou aos africanos o acesso aos cargos políticos nos seus respectivos países depois da independência. Por isso, ainda conforme Fayemi (2002), entender o caráter colonial dos militares é um fator crucial para explicar o aumento dos seus instintos pretorianos pós-coloniais na África. De fato, as forças armadas na África são os descendentes diretos da força colonial, sustentados pelos governantes imperiais para manter a velha ordem.

No caso da Nigéria, após a independência, a nova liderança política era mista, e isso causou a indiferença desta elite sobre o crescimento da instituição militar como uma extensão da autoridade colonial. Na opinião de Fayemi (2002), essa ambivalência dos líderes políticos pós-independência sobre as forças armadas era compreensível, mas um pouco exagerada dada a sua estreita ligação com o poder metropolitano. Desconfiada das instituições militares, a elite política decide aderir aos acordos de defesa anglo-nigerianos, reforçando o controle colonial ou simplesmente, como afirma o autor acima citado, permitindo uma expansão do poder britânico após a independência, no início do processo de construção da atual República Federativa da Nigéria.

O país se torna uma federação de três regiões sob o comando de um governo civil entre 1960 e 1966. A revisão da Constituição em 1963 permitiu a posse do Dr. Azikiwe como o primeiro presidente da Nigéria, substituindo o Governador-Geral que representava a monarquia britânica. As rivalidades étnicas, o sectarismo e o desejo de autonomia dentro do sistema federal foram os principais problemas enfrentados pelo primeiro presidente, os quais levaram à formação de vários grupos e alianças políticas.[2]

Assim, o crescimento da luta política e a corrupção levou os jovens oficiais a fomentar um primeiro golpe militar em 1966, matando na ocasião o primeiro ministro Balewa e dois líderes regionais. Em seguida, a tentativa de separação da região do leste do país provocou certamente a mais dura guerra civil no país (Biafra), em 1967. O General Yacubu aproveita do crescimento da credibilidade dos militares após a guerra para legitimar a incorporação dos militares no projeto de construção do Estado. Contudo, conforme Fayemi (2002), embora a guerra tenha resgatado a legitimidade das instituições militares, também as fragmentou.

[2] Ver: "Nigeria: history and politics". Disponível em: <http:\\www.iss.co.za\\af\\profiles\\nigeria\\politics.html>.

A intervenção dos militares na política na Nigéria foi justificada como um projeto de erradicação da corrupção e reorganização do Estado, conforme Fayemi (2002). Mas os fatos provaram o contrário, pois o país entrou em uma crise étnica e regional que levou a Nigéria a enfrentar três anos de guerra civil. As clivagens étnicas e o regionalismo tornaram difícil o controle dos elementos das forças armadas e a estrutura de controle autoritária, preocupada com a segurança do regime, foi encorajada através da promoção das elites militares em todas as instâncias comuns. É importante ressaltar que esta promoção das elites militares visava, além de garantir a segurança do regime, a limitar a ação política dos nacionalistas que pretendiam construir o Estado nacional apelando ao glorioso passado não só da Nigéria, mas de toda África, como bem lembra Barry (2000).

No entanto, apesar de a independência abrir novas perspectivas aos povos africanos na década de 1960, a influência externa continua acompanhando e dividindo os africanos, principalmente na parte ocidental do continente, onde os objetivos contraditórios da unidade e da construção do Estado-Nação entraram em confronto direto – adiando o sonho do pan-africanismo e da integração regional. Estas iniciativas e tentativas de integração são retomadas a partir de 2002 com a criação da União Africana (UA), que, ao constatar que os problemas sociopolíticos, culturais e econômicos do continente deveriam ser enfrentados em conjunto, aposta desde então nas organizações sub-regionais como a CEDEAO, as quais dependem da atuação e do comprometimento dos países-membros – em geral e principalmente das potências mais robustas, como é o caso da Nigéria na África Ocidental.

Uma avaliação atualizada da situação dos países da África ocidental mostra que em virtude do tamanho geográfico, da abundância dos recursos e da força militar, a Nigéria é um dos países capazes de influenciar a paz e a segurança da região, assim como as prioridades de desenvolvimento da região, mesmo com os conflitos internos de cada um dos vizinhos e com seus aparatos de segurança distintos.[3] A África Ocidental, em certa medida, depende da atuação e do comprometimento da Nigéria devido aos fatos referidos anteriormente e que são resumidos no texto a seguir:

> A Nigéria por si só, em função da sua dimensão, reúne todas as vantagens e inconvenientes das outras regiões, com o handicap principal da desunião que caracteriza esse conjunto esquartejado entre as diferentes nacionalidades do Norte, do Leste e do Oeste. A configuração deste país reúne o leque de problemas da integração regional, dando conta da importância da gestão das fronteiras em relação a outros fatores culturais, políticos e econômicos (BARRY, 2000:78).

[3] Outros países são: Gana, Mali, Costa de Marfim e Senegal.

No caso da maioria dos países, é fundamental, para garantir a segurança doméstica, se preocupar com os problemas ligados aos conflitos tanto internos quanto externos, o que justifica a importância da construção de um aparato regional de segurança. Este aparato, por sua vez, dada a complexidade das novas ameaças, precisa da colaboração e da participação de todos os países que pertencem a uma dada região. Nessa ótica, supõe-se que a integração regional na África Ocidental será capaz de resolver os conflitos e colaborar para o desenvolvimento da região. Para isso, no entanto, é necessária a colaboração e o comprometimento de todos os membros da CEDEAO, e o papel de países como a Nigéria será fundamental nesta tarefa.

4.2. Segurança Regional na África Ocidental: O Papel da Nigéria

É importante esclarecer o que se entende por segurança, assim como definir ou situar geograficamente a África Ocidental para facilitar a compreensão do que vai ser tratado nesta parte do texto. Para tanto, julgamos necessário trazer um olhar retrospectivo sobre o conceito de segurança.

A evolução do conceito de segurança se explica certamente pela antiguidade do assunto no âmbito das políticas de Estado. Inicialmente, a segurança era relacionada à proteção de fronteira por uma força militar até que os desdobramentos da Primeira Guerra Mundial (1914-1918) nos campos político, militar, econômico e social provaram ao mundo que a defesa militar em si só não protege o Estado. Portanto, o conceito de segurança é mais amplo e não poderia ser restrito à área militar devido aos avanços registrados nas áreas de inovações tecnológicas, fruto da Revolução Industrial (RODRIGUES, 2007). Na década de 1940, o conceito de segurança, que era voltado para o Estado, passou a ser questionado por falta de eficácia e utilidade devido às alterações ocorridas no Sistema Internacional. Essas mudanças alteram o entendimento relativo à agenda de segurança, levando a uma revisão conceitual. Nessa ótica é importante notar que, no entanto, a conceituação atemporal da segurança aplicável a um dado contexto específico deve ser evitada. O conceito de segurança varia ao longo dos níveis de análise, visto que os problemas de segurança referem-se às relações políticas de amizade e inimizade que acompanham a escala dos objetos referentes ao longo dos diferentes níveis de análise.

Conforme Pagliai (2006), se durante a bipolaridade os problemas de segurança internacional estavam vinculados, sobretudo, às questões militares estratégicas, em função da temática desta confrontação, com o fim da Guerra Fria, novos temas, ameaças e novos atores passaram a configurar a agenda de segurança internacional. Logo, surge a necessidade da regionalização dos estudos da área de segurança internacional devido à velocidade das comunicações

e ao surgimento de novas tecnologias, como ressalta Rodrigues (2007). Essa regionalização dos estudos e da prática da segurança foi denominada como Complexos Regionais de Segurança, em que as chamadas superpotências (como Estados Unidos das Américas) e as potências regionais (em que se enquadra a Nigéria na África Ocidental) exercem influência (Buzan & Weaver, 2003). Os aprimoramentos dos avanços tecnológicos da Segunda Guerra Mundial assim como da Guerra Fria consolidaram a ampliação de conceito de segurança modificando significativamente o sistema internacional do século XX e o conceito de segurança internacional.

Nessa ótica, viu-se que o conceito de segurança é amplo tanto em termos geográficos, pois pode ser situado em nível nacional, regional ou internacional, como em termos de conteúdo, visto que vai além do setor restrito das forças armadas. Segundo Rodrigues (2007), a Grande Guerra e seus desdobramentos nos campos político, militar, econômico e social mostraram ao mundo que o conceito de segurança era mais amplo, e não poderia ficar restrito à área militar, pois, apenas defesa militar não protege mais o Estado. Esta nova concepção do conceito de segurança se deve ao uso das novas ferramentas de informação e de comunicação que foram desenvolvidas ao longo do tempo principalmente durante a Segunda Revolução Industrial. Levando em consideração estas mudanças tecnológicas, Rodrigues (2007) conclui que as mudanças nos conceitos sobre segurança internacional são consequência das modificações sofridas pelo sistema internacional no período pós-guerra. Essas mudanças conceituais se refletem por sua vez nas políticas de segurança e de defesa dos Estados ao redor do mundo.

A partir deste momento, a segurança nacional passa a ser uma questão não somente interna, pois, como mostra o caso dos conflitos africanos, o problema dos vizinhos é, por exemplo, igualmente uma ameaça para os que dividem as mesmas fronteiras. Do momento que se leva em conta as novas ameaças – como, terrorismo, tráfico de armas e de drogas, e as guerras civis – percebe-se que há realmente uma necessidade de gerenciar de forma conjunta esta questão que se torna cada vez mais complexa. Assim, após o fim da bipolaridade, os gestores da segurança, tanto no plano político quanto teórico e socioeconômico se deram conta que o assunto deve ser tratado regional e internacionalmente.

Segundo Cepik (2005), a necessidade de regionalização dos estudos da área de segurança internacional se deu após a Guerra Fria, devido à velocidade das comunicações, ao surgimento de novas tecnologias e à interdependência que exige o sistema internacional. Com o aumento cada vez maior da complexidade deste setor, surgiu o conceito de complexo regional de segurança, formulado por Barry Buzan em 1991 e cuja nova versão foi desenvolvida e apresentada

conjuntamente entre Buzan e Waever em 2003 sob o título de "teoria dos complexos regionais de segurança". Essa noção tem os Estados como objeto de referência. Assim, conforme os autores acima citados, a segurança regional deve ser composta de dois ou mais Estados de relações securitárias interdependentes, positiva ou negativamente; estes devem ser situados em uma mesma área geográfica, onde o padrão de segurança deve ser duradouro e profundo.

A África ocidental se enquadra nesta definição, pois a região conta atualmente com dezesseis países, dos quais quinze são membros da Comunidade Econômica dos Estados da África Ocidental (CEDEAO). Além de ser uma região homogênea em termos geográficos, a questão de segurança foi em várias ocasiões tratada de forma conjunta, apesar das hostilidades e atritos que marcaram a história regional, mesmo no período pré-colonial. Nessa época, a maior parte da região estava sob domínio de um único império (Gana, Songai, Mali, Gaabu, Futa Jalon, etc.), mas mesmo nos conflitos entre povos ou tribos da região, há vários relatos sobre cooperação para a garantia da segurança. Na atual região da África ocidental, violentos combates opuseram, entre 1840 e 1850, os Fulas do Futa Jalon, aliados dos marabout Malinkes e as populações animistas da floresta (atual golfo da Guiné), apoiadas pelos Bainunkês. No período colonial, a pacificação da região contou com a cooperação entre colonizadores (franceses e Ingleses) e os chefes tradicionais de um lado, e do outro, entre os próprios colonizadores. Podem ser consideradas medidas de segurança regional o acordo Franco-britânico, que tinha como objetivo capturar o líder local, Fodé Kaba, e pacificar a região que agrupa atualmente Gâmbia, Casamance e uma parte da Guiné Bissau, e o acordo luso-francês de 1886, que fixou a delimitação entre as duas colônias. Da mesma forma, o êxito dos estados teocráticos, do Futa Djalon, Futa-Toro e Boundou, é em parte resultado dos esforços feitos por seus líderes para estabelecerem relações de cooperação político-militar e, assim, garantir a segurança dos Estados e da população. O império de Futa Djalon era uma confederação de nove províncias, que, embora dirigida por pequeno número de grandes famílias aristocráticas, teve que estabelecer regras que limitavam o mandato a dois anos para cada família – o que ilustra a importância da integração regional na África Ocidental.

Na década de 1960, a tentativa de construção de um Estado federativo que agrupasse todos os territórios da África Ocidental Francês (AOF) tinha como preocupação evitar a fragmentação da região em países inviáveis no plano sociopolítico e econômico, o que levaria a uma instabilidade na região. Atualmente, a União Africana, em colaboração com as organizações regionais como a CEDEAO, trabalha na busca de respostas aos principais desafios da globalização enfrentados pela África. Nesta lógica, a questão da segurança na África em geral e, particularmente na África ocidental, vem sendo desenvolvida com prioridade na

busca de paz e, de bem-estar social, o que passa necessariamente pela resolução dos conflitos, pelo reforço da integração regional, pela boa governança e pelo respeito aos direitos humanos. Ou seja, para se conseguir a segurança na região, não basta resolver os conflitos, é preciso também levar em consideração outros fatores que causam incertezas à população.

No caso da África ocidental, isso tem um significado particularmente importante quando se pensa na segurança regional, pois, conforme um estudo do Instituto Dinamarquês de Direitos humanos (2007), os países da África Ocidental estão entre os mais pobres do mundo e registram um crescimento demográfico conjunto de mais de 3% ao ano.[4] Dessa forma, os quinze países que compõem a CEDEAO totalizam em torno de 257 milhões de habitantes sendo que 52,54% destes são nigerianos. Portanto, a construção de paz e segurança na África Ocidental, que, desde o fim da Guerra Fria, constitui uma das mais importantes zonas de conflito na África, necessita de uma participação especial da Nigéria, por ser o gigante da região tanto em termos físicos (geográficos) e socioeconômicos, quanto militares.

Segundo dados de Jane's (2009), as forças armadas nigerianas, estimadas em setenta mil (70.000) membros, divididas em suas várias brigadas (infantaria, guarda presidencial, defesa aérea, forças especiais etc.), são encarregadas de defender a integridade territorial do país, e de auxiliar a autoridade civil na manutenção da ordem interna, desempenhando um papel que, tradicionalmente é reservado para a polícia. Além disso, participam em operações de paz sob a bandeira dos organismos regionais e internacionais (ONU, UA, ECOMOG). Apesar dos problemas e insuficiências relativos aos conflitos internos e à consolidação da democracia, a Nigéria continua sendo o mais importante membro do sistema de operação de paz no plano regional e internacional do continente. Historicamente, a Nigéria é o país africano que mais fornece tropas para as forças da Organização das Nações Unidas (ONU).[5]

Em 2008, conforme dados de Jane's (2009), a Nigéria contribuiu com 2694 homens em diversas operações. Atualmente (2010), estima-se em 6 mil o número de soldados nigerianos engajados em operações de paz no mundo, sendo três mil e quinhentos (3500) soldados apenas no Sudão. Nessa ótica, Nigéria assume, ou pelo menos pretende assumir, um papel de maior importância na região, devido a todos os fatores já evocados, como mostra afirmação a seguir:

---

[4] *L'institut danois des droits de l'Homme*: Stratégie pour l'afrique de l'ouest 2007-2011.

[5] Artigo publicado pela *RFI* em 3/8/2010 com o título: «Le Nigeria menace de ne plus participer aux missions de paix de l'ONU». Disponível em: <http:\\www.rfi.fr\\afrique\\20100803>. Acesso em: 4/8/2010.

> The Federal Republic of Nigeria is the continent's most populous country. Thanks almost entirely to vast hydrocarbon reserves; it is also the continent's greatest oil producer, one of its top three destinations for foreign investment and source of 14 per cent of sub-Saharan Africa's economic output. (Jane's, 2009).

No entanto, o presidente do país ameaçou retirar suas tropas das forças da paz da ONU se a organização não modificar as regras de participação para proteger os soldados. Na opinião de Wase (2010), a Nigéria, através de seu atual presidente (Jonathan Goodluck), busca ser reconhecida como membro importante do sistema de segurança internacional e, para tanto, aproveita da sua posição de membro do conselho de segurança da ONU para pressionar a comunidade internacional. É importante salientar que a Nigéria é membro não-permanente do conselho de segurança das Nações Unidas desde Janeiro, por um mandato de um ano (2010-2011) e dirige as forças da paz da UA no Sudão, onde os africanos foram os primeiros a reagir ao drama do Darfur – comandados por Olesegun Obasanjo, então presidente da Nigéria, mas também da UA.

Esse engajamento é uma afirmação da liderança nigeriana na segurança regional devido não somente ao seu título de "gigante", mas também ao seu peso sócio-político e econômico. Um distúrbio ou uma crise interna no país pode afetar os vizinhos, devido à porosidade das fronteiras.

Nessa ótica, um documento sobre a proliferação de armas de pequenos portes elaborado pelos países membros da CEDEAO chama atenção sobre a extensão das fronteiras da Nigéria. A Nigéria divide 770 quilômetros de fronteira terrestre com a república do Benin, 1500 km com o Níger, 1700 km com Camarões e 90 km com o Chade, além dos 850 quilômetros de costa do lado do Oceano Atlântico (YACUBU, 1998). Em caso de instabilidade tanto na Nigéria quanto nos países da região, a população pode atravessar as fronteiras do país com facilidade para se refugiar em um dos países vizinhos, causando instabilidade regional. Neste sentido, pode-se afirmar que o progresso da situação política, econômica e social da África requer segurança – cuja chave de sucesso deve ser a resolução dos conflitos e garantia da segurança regional.

É nessa lógica que a União africana (UA), criada em 2002 em substituição à Organização da Unidade Africana (OUA), deu uma ênfase maior nas questões de segurança e do desenvolvimento. A Nigéria vem sendo ativa em todas estas novas iniciativas, ao lado de África do Sul, Líbia e de certa forma do Senegal. Este último atuou através do presidente Abdoulaye Wade em conjunto com os presidentes da Nigéria Olesugun Obasanjo e Thabo Mbeki da África do Sul no projeto da Nova Parceria pelo Desenvolvimento (NEPAD).[6]

[6] O papel da Nigéria na África em geral e particularmente da África ocidental se justifica tanto pela sua importância econômica, geográfica e social como pelo engajamento político das autoridades do país.

Essas novas iniciativas, nos níveis regional, continental e internacional em direção sobre a África, vêm fortalecendo a posição e a importância de países como a Nigéria para o alcance dos objetivos do milênio –, entre os quais estão a resolução dos conflitos, a erradicação da pobreza, a boa governança e a consolidação do Estado democrático. A resolução de conflitos se refere à identificação, à análise, e ao tratamento de suas causas. Ou seja, a resolução do conflito significa tratar definitivamente o conflito, eliminando suas causas, enquanto que o apaziguamento se refere a uma resolução de curto prazo, temporária.

A partir desses objetivos, percebe-se a importância do serviço da inteligência na Nigéria, que, de um lado, enfrenta problemas de segurança interna e, de outro, está localizada em uma região, onde são comuns os conflitos internos devido a uma variedade de forças com poder de coerção. Conforme Berghe (2008), há vários tipos de forças armadas na África, cada uma com um objetivo ou especialidade diferente, o que aumenta o risco de insegurança. Desde a época da colonização, conforme o autor acima citado, a própria existência destas forças oferece ameaças constantes de desordem aos governos que pretendem servir; se bem que no caso da Nigéria, do Senegal e do Gana, as forças armadas têm sido até certo ponto fiéis ao governo. Por exemplo, no Senegal, o exército apoiou Senghor duas vezes, nos momentos críticos. Em Gana e na Nigéria, as forças armadas também têm provado serem dignas de confiança.

Nesse ambiente, a segurança regional vem sendo tratada como prioridade desde 2001, quando a União Europeia (EU) e os países da África, do Caribe e do Pacífico (ACP), incluíram novas áreas (Paz, prevenção, resolução de conflitos, comércio de armas etc.) no diálogo político que reuniu as duas entidades em Cotonou (Benin). A cooperação entre EU e ACP, que teve início em 1975 com a assinatura da convenção do Lomé (Togo), tinha somente objetivos econômicos. No entanto, com o fim da Guerra Fria, esta cooperação foi ampliada, condicionando a ajuda externa aos países do ACP à boa governança e ao respeito aos direitos humanos. Portanto, o acordo de Cotonou, ao reconhecer que a estabilidade é provavelmente uma das mais importantes condições para qualquer processo de desenvolvimento, reforça a importância da criação de uma estrutura de segurança regional na África Ocidental, conforme ilustrado a seguir:

> A resolução de conflitos e a paz são uma parte importante do Acordo de Cotonou. As partes acordaram em perseguir uma política ativa, detalhada e integrada para a construção da paz, prevenção e resolução de conflitos no quadro da Parceria. Esta política fundar-se-á no princípio da apropriação social (TEKERE, 2001).

A criação do conselho da segurança da UA e a adoção do programa de trabalho sobre a Paz e segurança por todos os Estados em 2002 são iniciativas

que fizeram das lideranças africanas uma esperança para o continente, como bem destacou a Conferência África-União Europeia.

Na África, a Nigéria passa a ter um papel fundamental na consolidação da paz e da democracia, assim como na resolução dos conflitos regionais, onde ela lidera as forças de intervenção da CEDEAO (ECOMOG). Foi nesse sentido que o país foi induzido a um conflito com a Libéria em nome da manutenção da paz sob a bandeira da organização regional. Assim, a Nigéria passou a encabeçar todas as intervenções da CEDEAO, conduzindo a um cessar fogo no caso da Costa do Marfim. Além disso, a Nigéria participa ativamente das negociações, como foi o caso da Mauritânia em 2008. É um membro fundamental da União Africana, do NEPAD e também um dos únicos países africanos membros da Organização dos Países Exportadores de Petróleo (OPEP).

4.3. Os Serviços de Inteligência da Nigéria

Serviços de inteligência são órgãos do Poder Executivo que trabalham prioritariamente para os chefes de estados e de governos e, dependendo de cada ordenamento constitucional, para outras autoridades na administração pública e mesmo no parlamento (CEPIK, 2003:85).

Nessa ótica, pode-se perceber a importância do serviço da inteligência na construção e na consolidação do Estado-nação, principalmente no que tange ao Estado democrático de direito – que é, na luz da constituição brasileira de 1988, um Estado baseado no princípio da legalidade (art. 5º, II). Ou seja, aquele que busca a realização do bem-estar social sobre a égide da lei justa e que garante ampla participação do povo no processo político decisório. Os serviços de inteligência de qualquer país podem, por definição, contribuir para o aprimoramento dos processos decisórios dos *policymakers*, sobre assuntos tanto internos quanto externos, pois são organizações governamentais especializadas na coleta, análise e disseminação de informações sobre problemas e alvos relevantes para a política externa, as políticas de defesa nacional e para a segurança pública de um país (CEPIK, 2003). Na era da globalização e da regionalização, o serviço de inteligência ganha mais importância quando se trata principalmente da questão de segurança, que tem o desafio de lutar contra todas as formas de ameaças, não somente dos Estados, mas também da sociedade como um todo.

Conforme Gbanite (2001), a segurança nacional de um país, em conjunto com a política de inteligência, muitas vezes se torna o eixo do sucesso ou do fracasso da administração. Isso explica, conforme o autor, a continuidade das políticas de segurança tanto nos Estados Unidos da América quanto no Reino Unido, independentemente do partido político que está no poder. A palavra segurança se refere aqui à proteção, garantia de confiança, de certeza ou ausência

de medo; grosso modo a tudo que garante aos cidadãos uma vida livre e isenta de perigo. Dentro desse raciocínio, a palavra inteligência, significa a capacidade de adquirir e aplicar conhecimento; de ter a aptidão de refletir sobre informações, notícias chaves ou sigilosas ligadas à atividade de inimigos, como mostra o texto a seguir:

> The word "intelligence" is described as "the capacity to acquire and apply knowledge, the faculty of thought and reason-information; news, secret information especially about an enemy, and an agency engaged in seeking such information. (GBANITE, 2001).

Nessa lógica, percebe-se que o serviço de inteligência de um país pode abranger várias áreas de conhecimento, como pode também demandar a colaboração de diferentes setores do Estado, pois se trata de uma questão de segurança nacional, meio estratégico de tomada de decisão dos que governam o Estado. Segundo Ribeiro (2006), a atividade de inteligência é um instrumento que favorece a construção de poder, um dos elementos mais estratégicos que a direção do Estado tem em seu rol de atividades; portanto, ela envolve diferentes setores e agências. Nessa ótica, a assertiva a seguir, é bem esclarecedora:

> O perfil organizacional dos serviços de inteligência, desde o seu surgimento na Europa, durante o período absolutista, até a formação dos atuais sistemas nacionais de inteligência é composto por várias agências com diferentes missões: inteligência externa, militar, interna (ou de segurança) e policial. (CEPIK, 2003).

Para analisar o serviço de inteligência da Nigéria, é bom não perder de vista o perfil organizacional dos serviços de inteligência, pois o setor de segurança nigeriano é composto pelas Forças Armadas que, em 1990, totalizavam 94.500 membros, divididos em Exército (80.000), Força Aérea (5.000) e Marinha (9.500), conforme dados do governo do país publicados em 1991. A Polícia Nacional (Nigerian Police), no mesmo período, era estimada em 152 mil membros, organizada em sete áreas de comandos e dirigida pelo Nigeria Police Council (NPC), composto pelo presidente, um chefe de gabinete, o ministro de assuntos internos, e um inspetor geral de polícia. Já em 2006, segundo dados do Jane's (2008), as forças armadas da Nigéria contavam com 85 mil membros ativos, dos quais 67 mil pertenciam aos batalhões do Exército, oito mil da Marinha e 10 mil da Força Aérea. Ou seja, houve uma diminuição de 9,5 mil pessoas nas fileiras das forças de segurança do país. No entanto, houve uma modernização do setor.

Conforme o Global Security (2010), entre 1976 e 1986, o setor de segurança da Nigéria estava sob o comando de três principais órgãos do Estado: a Organização Nigeriana de Segurança (ONS), ligada à presidência da república, a Força Nacional da Polícia (FNP), comandada pelo Ministério da Administração Interna (MAI); e, as Forças Armadas (FA), ligadas ao Ministério da Defesa (MD).

Durante esta década, a ONS foi o único órgão responsável pelos serviços de inteligência interna e externa do Estado. Ou seja, a coleta, a análise de dados e informações visando a detectar, a prevenir os crimes contra o Estado, assim como a proteger matérias e informações sigilosas, são papéis exclusivos da Organização Nigeriana de Segurança, que também se encarrega da execução das medidas de segurança determinadas pelo presidente da República.

A partir dessas tarefas, pode-se observar a importância e o peso da ONS no setor de segurança nigeriano. Nesse caso, é fundamental para a ONS conquistar e preservar a confiança da sociedade nigeriana como um todo, tanto do governo quanto da sociedade civil, de forma a continuar exercendo legitimamente suas tarefas. Evidentemente, isso demanda, além de recursos humanos qualificados e ética profissional, meios materiais e logísticos suficientes para levar a cabo os objetivos da organização. Ora, em um país como a Nigéria, que desde a independência tem usado as armas como meio de escolher seus dirigentes, há motivos para duvidar de qualquer organização coercitiva do Estado, e não poderia ser diferente no caso da ONS.

Assim, no governo de Buhari (1983-1985), o serviço de inteligência foi acusado de realizar escutas telefônicas não autorizadas, detenção arbitrária de pessoas, prisões sem julgamento de inocentes etc. A ONS, que é uma organização que deveria garantir a segurança da população e da sociedade em geral contra possíveis ameaças internas e externas, se torna, ela mesma, uma ameaça para os cidadãos nigerianos e, conseqüentemente, perde a legitimidade e a confiança do povo, e principalmente dos que governam. A partir deste momento, a ONS passa de uma organização promotora de segurança para uma organização que ameaça a segurança nacional. Dito com outras palavras, houve um uso abusivo ou desproporcional das medidas e dispositivos na execução das tarefas de coleta e análise de informações destinadas a detectar as ameaças à segurança nigeriana. Neste caso, a Nigéria ilustra bem esta afirmação:

> As medidas de proteção devem guardar certa proporcionalidade em relação às ameaças percebidas contra a existência, efetividade e autonomia de quem - ou do que - está sendo protegido. Na ausência de proporcionalidade, a busca de segurança torna-se ela própria uma ameaça à efetividade, autonomia e, no limite, à própria existência do "objeto" da proteção (CEPIK, 2001).

Portanto, na falta de legitimidade da ONS, devido ao envolvimento de seus membros em abusos generalizados do devido processo legal, à uma crise econômica aguda, e ao aumento da corrupção, sua existência não é mais legítima. Considerando-se a importância do serviço da inteligência para o Estado, a saída foi a reforma geral do setor de segurança, o que, aliás, foi um dos destaques no primeiro discurso, pronunciado pelo General Ibrahim Babaguida como presidente da República Federativa da Nigéria em 1986.

Se até então não se tinha nenhuma informação oficial sobre a Organização do serviço de inteligência da Nigéria, um decreto publicado em 19 de junho de 1986 dissolve a ONS e reestrutura a Inteligência do país em três Organizações distintas, subordinadas ao Gabinete de Coordenação de Segurança Nacional (CNS), duas de natureza Civil e a terceira de natureza militar (Jane's, 2008). As duas primeiras são, respectivamente, o Serviço de Segurança do Estado (do inglês State Security Service, SSS), responsável pela Inteligência interna e a Agência Nacional de Inteligência (ANI), encarregada da inteligência e da contrainteligência externa do país. A direção de Inteligência Militar (DIM) foi responsabilizada pela coleta de informação ou inteligência militar de interesse do país no âmbito nacional e internacional. A partir desse momento, pode-se representar a estrutura de comando do Serviço de Inteligência da Nigéria da seguinte maneira:

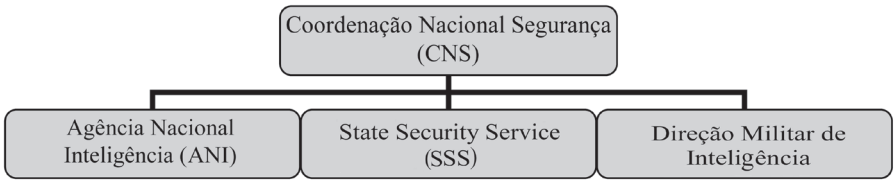


Figura 1. Organograma dos serviços de inteligência da Nigéria (1976-1986)

A reorganização do setor de segurança procurou distribuir as responsabilidades no intuito de racionalizar e despolitizar o setor, buscando a estabilidade da instituição e a eficácia dos serviços de segurança nacional. No entanto, a reforma certamente levou em consideração somente a estrutura do comando, esquecendo um dos fatores mais importante do setor: os meios materiais e humanos. Assim, os objetivos da reforma não foram alcançados, pois o setor de segurança continuou sendo ineficiente nas suas principais tarefas, que são coleta e análise de informações.

A incapacidade em combater as ameaças à segurança, tais como a operação encoberta os movimentos dissidentes e a violação das fronteiras, entre outros, indicou rapidamente os limites das novas organizações. Em 1988, o diretor da Agência da Inteligência da Defesa e o diretor adjunto do Serviço da Segurança do Estado foram acusados de participar na interpelação e no assassinato de civis e jornalistas que ameaçavam divulgar informações sigilosas a respeito de alguns membros do alto escalão do Estado, em 1986. Isso demonstra que o problema da segurança continua sendo uma das grandes preocupações do Estado nigeriano, pois a estabilidade política do país depende em parte do fortalecimento do setor de segurança.

A acusação de envolvimento de membros dos serviços de inteligência e de segurança no assassinato do presidente Mohamed Murtala leva as autoridades a reformular as estruturas organizacionais do setor de segurança. Primeiramente, os envolvidos são afastados, e substitutos são nomeados numa tentativa de resgatar a imagem da instituição. Assim, em 29 de dezembro de 1989, o vice-almirante Patrick S. Koshoni, que era chefe da Marinha nigeriana desde outubro de 1986, foi nomeado chefe da Comissão Nacional para a reestruturação da Segurança Interna. A reforma consistiu na abolição do CNS e, na subordinação direta do State Security Serviço (SSS) e da Agência Nacional de Inteligência (ANI) à Presidência da República, enquanto a Direção Militar de Inteligência foi subordinada ao Ministério das Forças Armadas. A partir desse momento, a nova estrutura ou novo organograma pode ser apresentado da seguinte forma:

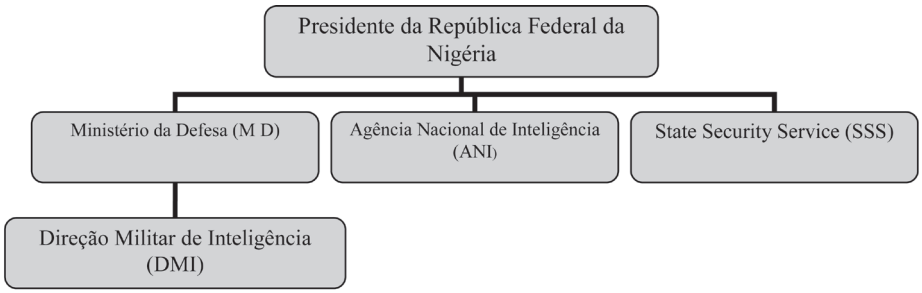


Figura 2. Novo organograma dos serviços de inteligência da Nigéria a partir de 1989.

A partir da reforma de 1989, como se observa na figura 2, o serviço de inteligência nigeriano é gerenciado por três centros de comandos independentes uns dos outros, porém todos subordinados ao presidente da república. Isso se explica certamente pelas persistentes e crônicas ameaças à segurança interna do país. As divergências internas foram agravadas por rápidas mudanças socioeconômicas e produziram problemas políticos e desordem civil que inviabilizaram todos os processos legais de gestão do Estado. Os longos períodos de ditadura militar, as violações dos direitos humanos, praticadas por forças de segurança descontroladas, entre outros, são fatos que podem servir de base para explicar a criação de órgãos de segurança diretamente controlados a partir da presidência da república, que busca modernizar e profissionalizar os serviços de segurança, incluindo: Serviço de Polícia (SP), as Organizações Paramilitares, (as forças alfandegárias), o serviço de imigração, o serviço penitenciário, o judiciário e o Serviço de Inteligência civil e militar. Esta reorganização descentraliza a administração dos serviços de segurança, visando à concentração do comando, principalmente dos serviços de segurança e de inteligência, na personalidade do

presidente da república, que continua como chefe supremo, conforme Fayemi (2002). A descentralização procurou criar um ambiente de complementaridade entre as forças armadas, os serviços de inteligência e as forças policiais nigerianas, que desempenham um papel importante na área de segurança interna do país. A respeito das forças de polícia, é importante lembrar que o Serviço de Inteligência é também conhecido como polícia secreta e, na Nigéria, as Forças de Polícia Nigerianas (FPN) foram as primeiras forças de segurança do país desde a época colonial.

Segundo dados de *Global Security* (2010), a polícia da Nigéria começou com a formação de trinta membros na colônia de Lagos em 1861. Em 1879, 1200 paramilitares foram formados e em 1896 foi estabelecida a polícia de Lagos. Uma força similar foi criada na costa do Níger (NCP) em Carbala, em 1894, sob o novo protetorado da costa do Níger, enquanto no norte o Royal Níger Company (RNC) tinha criado em 1888 sua polícia, a Royal Níger Company Police (RNCP). Quando os protetorados do norte e do sul da Nigéria foram proclamados, em 1900, parte da RNCP se tornou a Polícia do Norte da Nigéria e a polícia da Costa do Níger (NCP) se transformou em Polícia do Sul da Nigéria.

Apesar da união entre Norte e Sul em 1914, a união das duas polícias que formará a Polícia Federal Nigeriana será feita somente em 1930, e terá como sede Lagos, a atual capital do país. Durante o período colonial, a maioria das polícias estava associada aos governos locais. Em 1960, depois da independência, a Nigéria não tinha uma polícia unificada no âmbito da Federação. As forças policiais foram primeiramente regionais; depois foram unificadas para formar a Polícia Federal da Nigéria, como é conhecida atualmente, que passa a exercer um papel importante na gestão da segurança do país.

As Forças da Polícia Nigeriana (NPF) foram transformadas em polícia nacional pela seção 194 da constituição de 1979, com competência exclusiva em todo o território nacional. No entanto, há também uma disposição constitucional que menciona a criação de uma filial da NPF separada, que faria parte das forças armadas da federação. Esta filial teria como missão dar proteção aos portos, rodovias, ferrovias e aeroportos, e teria nos anos 1990 entre 1500 e 1200 membros. (GLOBAL SECURITY, 2010).

A NPF desempenhou várias funções, entre as quais a segurança interna – também chamada de segurança nacional – atuando no apoio a prisões, no controle da imigração, nos serviços aduaneiros e também nos serviços militares dentro e fora do país. Em meados dos anos 1980, foram anunciados planos para expandir as forças que chegaram, conforme estimativas, a 152 mil em 1983, apesar de algumas fontes estimarem entre 20 e 80 mil homens distribuídos entre aproximadamente 1300 postos de polícia em todo país. Estes, juntamente com os serviços de inteligência do Estado, cuidam da segurança interna e externa do país.

Nessa ótica, pode-se perceber a importância do serviço da inteligência na construção e na consolidação do Estado-nação, principalmente no que tange o Estado democrático de direito. Os serviços de inteligência de qualquer país oferecem por definição a garantia institucional da sobrevivência nacional. Ou seja, o serviço de inteligência é um elemento principal na formação do Estado moderno, visto que ele surgiu no contexto da afirmação dos Estados nacionais como forma predominantemente de estruturação da autoridade política moderna.[7]

Segundo Dombroski (2004), nas democracias modernas como Estados Unidos ou Reino Unido, o serviço de inteligência tem como proposta informar e subsidiar as decisões políticas. Na opinião desse autor, o papel essencial do serviço de inteligência é detectar ou identificar a capacidade e intenções das nações adversárias ou inimigas e tomar providências contra atritos potenciais. No que se refere aos países do Terceiro Mundo e, precisamente, aos países africanos marcados por uma longa história de golpes militares e de violência, além do passado colonial, os serviços de inteligência e de segurança têm um papel importante no desenvolvimento e na consolidação das instituições democráticas. Portanto, a principal preocupação da inteligência em qualquer país do continente africano deve ser a criação de um ambiente que garanta a estabilidade política onde todos os cidadãos sejam capazes de defender seus interesses legitimamente sem entrave ou medo – além da manutenção da segurança internacional e regional. Ou seja, fazer uso democrático das informações coletadas, organizadas ou analisadas, que é nada mais que o uso democrático da inteligência no sentido da definição ampla (CEPIK, 2003).

Por democracia, entende-se aqui o processo evolutivo no estabelecimento do Estado do direito em qualquer país, que oferece amplo espaço de ação a cada um dos três poderes.[8] No entanto, sabe- se que na África ao sul do Saara fala-se de democracia de fato somente na década de 1990, sendo que os trinta anos que seguiram as independências foram marcados pela era do partido único, como bem mostra Anna Maria Gentili (2005:2):

> Soon after independence in almost all sub Saharan Africa nation-States the main justification for the adoption of single party "democracies" derived from a conception of the society as one single constituency, united by the common history of oppression.

Segundo Barry (2000), a ideologia nacionalista que apelava para o glorioso passado da África foi paulatinamente substituída pela ideologia nacionalista de unanimidade baseada no partido único, que coincidia com o Estado. A questão nesta altura não é dizer se um sistema é melhor ou pior que outro, mas

[7] Ver *Espionagem e Democracia*, Cepik (2003:86).

[8] Russell G. Swenson y Susana C. Lemozy 2009: *Poder legislativo, poder executivo e poder judiciário*.

simplesmente chamar a atenção para o fato de que, nos dois sistemas, o que se defendia como interesse da "Nação" era na verdade o interesse de uma pequena elite. Isso nos remete ao surgimento das primeiras organizações permanentes e profissionais de inteligência na Europa moderna a partir do século XVI – conforme Cepik (2003:86), um contexto da afirmação dos Estados nacionais como forma predominante de estruturação da autoridade política moderna.

No continente africano, em geral e particularmente na Nigéria, esse processo de construção do Estado nacional aprisionou a história na dupla camisa de força da unanimidade e do silêncio, com o objetivo de apagar as diferenças e contradições na competição pela obtenção de poder e de riqueza (Barry, 2000:57). Quanto à suposta unanimidade, o autor Ahmadou Kourouma (1970) chama a atenção sobre prováveis problemas e dificuldades que os países africanos podem encontrar na consolidação ou construção do Estado-nação moderno. Segundo ele, não se juntam aves quando se tem medo do barulho de asas.[9] Ou seja, os que advogavam pelo partido único ou unanimidade o faziam somente para poder dominar e, no caso da Nigéria, como em tantos outros países, a luta pelo poder se traduziu por sucessivos golpes de Estados. É assim que uma ditadura chega ao comando do país em 1966, a qual terminará, por sua vez, nove anos depois por outro golpe, considerado pacífico. Murtala Ramat Mohammed, o novo governante, promete, em curto prazo, devolver o poder aos civis, mas seu assassinato em seguida prova, mais uma vez, a incapacidade das forças de segurança em garantir a continuidade do funcionamento das instituições.

Segundo Fayemi (2002), ao assumir o poder, Obasanjo prioriza a descentralização do poder e, por meio da adoção de uma nova constituição, em 1977, prevê a organização de eleições livres e democráticas em 1979. Porém, sabemos que, como bem lembra Anna Maria Gentili (2005:2), tanto na Nigéria quanto em outros países da África, somente a terceira onda democrática colocará no centro do debate a transição ao multipartidarismo, as eleições competitivas e constitucionais e as reformas institucionais. Estas reformas foram importantes para a organização dos serviços de inteligência e de segurança visto a importância da democracia na consolidação do Estado moderno.

As autoridades e elites do país sabiam da importância dessa reforma para garantir a segurança e o bom funcionamento das instituições, pondo fim aos golpes militares e assassinatos. Nesse processo, a inteligência é importante, tanto

[9] Traduzido do Francês: *on ne rassamble pas des oiseaux quand on craint le bruit des ailes* (Kourouma, 1970, p.153). Para esse autor, a atual situação política econômica e social do continente africano não é surpresa. Segundo ele, as independências tinham eliminado não só as organizações políticas tradicionais (Cheferies), mas também as culturas e tradições locais, substituindo-as por comitês de bairros com um presidente, que nada significavam para a sociedade.

para maximizar poder quanto para tornar o processo decisório mais racional e realista, conforme destacado na primeira utilidade do serviço de inteligência para os governos.[10]

Portanto, a questão de segurança é uma preocupação nacional em qualquer país e, na Nigéria não pode ser diferente. Nesse sentido, Gbanite (2001) pensa que é imperativo compreender como o cidadão desse país deve sentir-se a respeito da segurança e, se esta está entrelaçada com a inteligência, então a segurança da Nigéria e as agências de inteligência precisam melhorar seu desempenho e começar a trabalhar imediatamente antes que a democracia desuna os próprios nigerianos. A preocupação deste autor pode ser facilmente compreendida a partir de exemplos ou acontecimentos recentes no continente, onde a democratização se traduz ou se transforma em conflitos internos, como na Costa do Marfim. Nesse país, a abertura democrática que aconteceu depois da morte do primeiro presidente Félix Houphouet Boigny gerou um conflito qualificado de étnico; portanto, a democracia, em vez de unir o povo o desuniu, resultando num conflito interno devido a uma polarização étnica.

Conforme Roy Pateman (1992), os regimes africanos e os movimentos de libertação muitas vezes estabeleceram aparatos de segurança estatal com considerável assistência externa. Na Nigéria, houve a influência e o apoio externo à criação e ao fortalecimento do serviço secreto ou serviço de inteligência. Na opinião de Fayemi (2002), como em vários países africanos de colonização inglesa, as atividades de inteligência têm sido conduzidas pelo "Special Branch of Nigerian Police force", exceto o trabalho da inteligência militar. Ou seja, há no país uma inteligência militar enfraquecida pelo conflito de Biafra, no qual ela foi responsabilizada pelas falhas que impediram o Exército de concluir o conflito em quarenta e oito (48) horas como planejado. A partir de então, uma rede de polícia secreta se fortaleceu, quando o regime resolveu reorganizar a estruturas de coleta, análise e interpretação das informações. Tudo isso resultou, conforme esse autor, no reforço das operações encobertas em nível interno por parte da polícia secreta (Special Branch of Nigerian Police), que pode ser comparada com o SAP sul-africano (Special Branch of the South African Police). É importante destacar que as semelhanças entre os serviços de inteligência da Nigéria e da África do Sul não são por acaso, porque ambos sofrem influência inglesa.

Conforme Dombroski (2004), o serviço de inteligência e o departamento militar de inteligência são responsáveis pela coleta, análise e disseminação das informações assim como pela condução das operações de contrainteligência. No serviço de inteligência nigeriano, a imagem da inteligência britânica foi responsável pela segurança interna até a falha que levou ao golpe de 1976, quando foi assassinado o então presidente General Mohamed. A partir de então,

[10] Ver Cepik (2003:64).

a Nigéria iniciou uma reforma profunda do serviço de segurança na perspectiva de acompanhar o crescimento rápido do país, principalmente em termos populacionais e urbanos. A sociedade nigeriana tem sido objeto de transformação em vários aspectos ao longo de quase meio século de independência, como observa o chefe da policia nigeriano, que lamenta do fato de que a polícia como instituição não acompanhou estas transformações. Ou seja, as autoridades do país nos últimos anos vêm trabalhando para modernizar as força de segurança em geral.[11] A declaração da política geral do país prevê uma polícia capaz de lidar com desafios de uma nação moderna e cada vez mais urbana, além de tomar conhecimento da magnitude da segurança e do desenvolvimento. Estes são os desafios da nação e da polícia até 2020, afirma o chefe do Estado-Maior do país. Nessa lógica, este comunicado da autoridade afirma que a reforma e a reposição são necessárias para tornar as forças de segurança funcionais em toda a federação para, assim, cumprir bem seu mandato constitucional de eficaz manutenção da lei e da ordem. Conforme a mesma fonte, para o bom cumprimento desta tarefa, é preciso ampliar e diversificar a corporação, mas também dar condições melhores de trabalho e de bem-estar – que é uma das maneiras de evitar a corrupção ou a revolta das forças de segurança. Neste sentido, foi criado em 1992 "The Nigeria Police Welfare Insurance Scheme" para dar apoio e cobertura aos oficiais e soldados da polícia em exercício, assim como a seus familiares.

A história do setor de segurança, como se vê, é marcada por várias reformas (1966, 1976, 1986 etc.) que são provocadas por conflitos internos e por brigas pelo poder, devido a uma falta de regras claras de acesso ao poder – o qual, na maioria dos países africanos, é um caminho curto para a riqueza e para o bem-estar social. Nessa ótica, viu-se que todas as reformas do setor de segurança da Nigéria foram precedidas ou de uma intervenção militar na gestão do Estado (golpe do Estado), ou simplesmente de perda de credibilidade de uma das organizações dirigentes por uso abusivo do poder de coerção. Assim, entre 1976 e 1986, a concentração dos serviços de inteligência do país, sob o comando da Organização Nigeriana de Segurança (NSO), foi mal vista pelos outros órgãos do setor de segurança nacional, principalmente, pelo serviço da Inteligência militar. Isso acabou gerando um conflito interno, uma briga por recursos e poder entre os elementos de comando dos três setores que compõem o aparato de segurança nacional. Segundo Fayemi (2002), a briga por poder transformou o setor de segurança da Nigéria, durante o governo de Buhari Idiagbo, em um conjunto de elementos descontrolados, gerando uma perda de credibilidade e de confiança. Para conquistar a confiança e a credibilidade do povo, as organizações que governam o Estado devem trabalhar

[11] Disponível em <http:\\www.nigeriapolice.org\\police-annual-report\\128-overview-of-the-nigeria-police-force.html>. Acesso em: 22 set. 2010.

para a continuidade das instituições legais e praticar uma gestão que visa ao interesse coletivo da nação (FAYEMI, 2002).

A centralização do serviço de inteligência, através da criação do posto de Coordenador Nacional da Segurança (CNS), comandando os três setores de segurança nacional (Fig.1) em 1988, durante o governo do General Ibrahim Babaguida, foi justificada pela necessidade de se buscar conjuntamente o trabalho para o interesse nacional. Durante o período, o que se observa é uma concentração e uma fortificação do serviço de inteligência e de segurança do país, à procura de um controle real sobre a as forças de inteligência, mas também da restituição de credibilidade para as instituições. Segundo o autor, a criação de uma estrutura paralela pelos militares (Babaguida) assumiu uma grande importância neste contexto de falta de credibilidade das instituições no país.

Segundo Fayemi (2002), no início de seu governo, o presidente Obasanjo usa os agentes, que no passado foram responsáveis por sérias violações de direitos humanos, para ajudar o governo a entender o tamanho dos serviços de inteligência e a partir disso determinar que o serviço de inteligência deve agir com base na constituição e da lei. Assim, começa a exigir "accountability" sobre a ética e o Legislativo passa a ter poder de controle sobre o Executivo. Ou seja, a partir dos erros e abusos do passado, tenta-se instituir uma conduta ou comportamento democrático, que é fundamental para a ascensão do país como líder tanto regional quanto continental e para seu reconhecimento internacional.

A Nigéria, apesar de continuar enfrentando tensões étnicas e religiosas, como ilustram as eleições presidenciais de 2003 e de 2007, marcadas por irregularidades significativas e violência, atravessa atualmente o seu mais longo período de regime civil desde a independência. As eleições gerais de abril de 2007 marcaram a primeira transferência do poder de um governo civil para outro na história do país, simbolizando assim a primeira fase de democratização da Nigéria e, sua projeção como líder incontornável na construção tanto da União Africana, quanto da CEDEAO. Igualmente, a partir de então ela se afirma no plano Internacional como um parceiro de peso no continente africano.

4.4. Considerações Finais

Este trabalho procurou analisar o serviço de inteligência da Nigéria, um dos países mais importante da África ocidental não só pelo tamanho da sua população, mas também pelo papel que ele vem exercendo no continente africano em termos de integração, desenvolvimento e respeito aos direitos humanos. A primeira parte procurou trazer fatos históricos sem pretender abranger todo o assunto, e a segunda parte, o papel importante que a Nigéria vem exercendo no âmbito regional, principalmente nas forças de segurança e de manutenção da paz. Na terceira e última parte, foi analisado o serviço de

inteligência do país, destacando que ele é uma herança da metrópole, mas vem sendo modificado e melhorado, devido às diferentes fases de altos e baixos no exercício da sua principal função de coleta e análise de informações.

Apesar de tudo, considera-se que o serviço de inteligência e de segurança precisa ser aperfeiçoado, devido à importância do país na região e ao papel que as suas forças de seguranças vêm desempenhando na segurança regional, continental e, mesmo internacional, no âmbito das missões de paz da Organização das Nações Unidas (ONU). Para tanto, é importante a consolidação da democracia e do respeito aos direitos humanos no país, o que passa pelo fortalecimento e a consolidação da União Africana e da CEDEAO.

REFERÊNCIAS

AFRICA on Web. Disponível em: <www.africaonweb.com/pays/nigeria/>. Acesso em: 05/08/2010.

BARRY, Boubacar. (2000). *Senegâmbia*: o desafio da história regional. Rio de Janeiro, Centro de estudos Afro-Asiáticos/UCAM-SEPHIS, 2000.

BAYO, Adekson. (1981). *Nigeria in search of a Stable Civil-Military System*. Gower; Westview Press.

BERGHE, Pierre L. Van Den. (1964). o Papel Das Forças Armadas na África Contemporânea. Publicado em *África Report.*, Vol. 10, nº 3, Washinton, EUA.

CENTRO de Estudos de Comércio e Desenvolvimento, Zimbábue, 2001. Disponível em: <http://library.fes.de/pdf-files/bueros/angola/hosting/upd12_02cotonou4.pdf>. Acesso em: 18 ago. de 2010.

CEPIK, Marco. (2003). *Espionagem e Democracia*: agilidade e transparência como dilema na institucionalização de serviço de inteligência. Rio de janeiro: Editora FGV.

_____. (2005). Segurança na America do Sul: Traços estruturais e dinâmica conjuntural. *Analise de conjuntura* OPSA, nº 9.

CIA World Factbook: <www.cia.gov/library/publications/the-world-factbook/geos/ni.html>. Acesso em: 18/08/2010.

CLAPHAM, Christopher, HERBST Jeffery and MIls Greg. (2006). *Big African States*, University Press, Johannesburg.

COMUNIDADE ECONÔMICA DOS ESTADOS DA ÁFRICA OCIDENTAL (CEDEAO): <http://www.ecowas.int/>. Acesso em: 10/08/2010.

DOMBROSKI, Kenneth R. (2004). *Transforming Intelligence in South África*, Center for Civil-Military relations, Naval Postgraduate School.

EMBAIXADA DA NIGÉRIA NO BRASIL. <www.nigerianembassy-brazil.org>. Acesso em: 18/08/2010.

ESTADOS UNIDOS. Library of Congress. Country Study: Nigéria. Disponível em: <http://lcweb2.loc.gov/frd/cs/ngtoc.html>. Acesso em: 18/08/2010.

FAYEMI, J & MUSAH, A. (Eds). (1999). *Mercenaries*: An African Security Dilemma, Pluto Press, London.

FAYEMI, J. Civil-Military Relations and the Future of Democratic Consolidation in West Africa. *African Journal of Political Science* (AJPS, Special Issue on Security in Africa), 1998.

FAYEMI, J. Militarism and the future of democracie in Nigeria, 2002.

FERREIRA, Muniz. (1997). *A África Contemporânea*: Dilema e Possibilidades. Disponível em: <http://www.smec.salvador.ba.gov.br/site/documentos/espaco-virtual/espaco-diversidade/RELA%C3%87%C3%95ES%20%C3%89TNICAS/WEBARTIGOS/africa%20contemporanea.pdf>.

GLOBAL SECURITY. <www.globalsecurity.org>. Acesso em 18/08/2010.

GRAF, William D. (1985). The Nigerian New Year´s Coup of December 31, 1983: A Class Analysis. *Jornal of Black Studies*, vol. 16, nº 1, p. 21-45

HENDERSON, Rober. (1995). South African Intelligence under the Klerk. *Internacional Journal of Intelligence and Counterintelligenc*e, vol. 8, nº (spring), p36-56.

HERMAN, Michel. (2001). *Intelligence Services in the Information age*. London; FrankCass.

HERZOG, Jeffrey Owen. (2008). *Using Economic Intelligence to Achieve Regional Security Objectives*. Internacional Jornal of Intelligence and Counter Intelligence. ISSN: 0885-0607/print/1521-0561.

INFORPRESS: Agência de Notícias do Cabo Verde. <www.infopress.publ.cv>. Acesso em: 18/08/2010.

INSTITUT des Nations Unies pour la Recherche sur le desarmement (UNIDIR). Disponível em: <www.unindir.ch>, Acesso em: 18/08/2010.

INSTITUTE FOR SECURITY STUDIES (ISS): <www.iss.co.za>. Acesso em: 18/08/2010.

JANE'S. (2009). Country Profiles: Nigeria. Disponível em: <www.janes.com>.

JOHNSON, Loch & WIRTZ, James J. (2004). Strategic Intelligence: Windows into a secret world and, and Antropology. Los Angeless-CA: Roxbury Publishing.

MESSARI, Nizar. (2004). *Existe um novo cenário de segurança internacional*? Disponível em: <http://bibliotecavirtual.clacso.org.ar/ar/libros/relint/messari.pdf>. Acesso em: 22/07/2010.

NIGERIA. National Bureau of Statistics: <www.nigerianstat.gov.ng/>. Acesso em: 18/08/2010.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU): <www.onu.org>.

ORGANIZATION INTERNACIONALE DE LA FRANCOPHONIE (OIF): <www.francophonie.org>. Acesso em: 18/08/2010.

PAGLIAI Graciela de Conti. (2006). Segurança hemisférica: uma discussão sobre a validade e atualidade de seus mecanismos institucionais. *Rev. Bras. Polít. Int*. 49 (1): 26-42.

PATEMAN, Roy. (1992). Intelligence Agencies in África: a preliminary assessment. *The Journal of Modern African Stadies*, 30, 4, p. 569-585, Cambridge Univercity Press.

PORTEOUS, Tom. (2003). L´evolution des conflits en Afrique subsaharienne: *Politique Etrangére*, vol. 68, nº 2, p. 307-320.

RIBEIRO, Fabio Pereira. (2006). *Cooperação Estratégica em Inteligência Formação da Defesa Regional*: uma Contribuição dos Serviços de Inteligência. Disponível em: <www.usp.br/prolam/dowloads/2006_1_6.pdf>. Acesso em 18/08/2010.

RODRIGUES, Cláudio Marin. Novos conceitos de segurança internacional e seus reflexos na política de defesa nacional (CMG (RM1)). Disponível em: <http://www.egn.mar.mil.br/viEnee/palestras/claudio.pdf>. Acesso em: 21/07/2010.

SORJ, Bernardo. *Segurança, Segurança humana e América Latina*. Disponível em: <http://www.bernardosorj.com.br/pdf/Seguranca_humana_port.pdf>. Acesso em: 21/07/2010.

SWENSON, Russel G. & LEMOZY, Susana C. (2009). *El Marco de una Teoria Axiologica de la Intelgencia Nacional*. Nacional defense intelligence college, Washington, DC.

UNIÃO AFRICANA (UA): <http://www.africa-union.org>. Acesso em: 17/08/2010.

WADE, Abdoulaye. (2005). *Um destino para a África*. Editor Michel Lafon.

YACUBU, J, G. *Colaboration entre les force Armée et de securité dans la lutte contre la proliferation des armes legeres*, 2006. Disponível em: <http://www.unidir.org/pdf/articles/pdf-art1943.pdf>. Acesso em: 18/08/2010.

Capítulo 5

REFORMA DA INTELIGÊNCIA NA RDC: DIREITOS INDIVIDUAIS E CONSTRUÇÃO DO ESTADO

Igor Castellano da Silva

A República Democrática do Congo (RDC) encontra-se em uma situação crítica. Mesmo após o fim formal da Segunda Guerra do Congo (1998-2003), grupos armados continuam a operar no país, desafiando os princípios básicos da existência do Estado. No que tange ao seu sistema de inteligência, críticas a abusos cometidos aos direitos individuais de cidadãos congoleses têm se generalizado. Essas opiniões são reproduzidas pelos diversos discursos em prol da reforma dos serviços de inteligência no país, que se daria sob o guarda-chuva do processo de Reforma do Setor de Segurança (SSR) estabelecido atualmente nas forças policiais e militares do país. Todavia, este debate deve ser qualificado a partir de uma análise da trajetória de construção do Estado congolês no período pós-independência e do papel dos serviços de inteligência estatais na construção e na manutenção das atividades estatais básicas.

Este trabalho discute brevemente os fundamentos teóricos sobre o papel dos serviços de inteligência no processo de construção do Estado e discorre sobre as características particulares de formação do Estado africano e da RDC. Em seguida, apresenta a trajetória de formação da esfera coercitiva do Estado congolês no período pós-independência, salientando nesse processo a importância das forças de segurança, mormente dos serviços de inteligência. Por fim, o estudo se debruça sobre o problema da Reforma do Setor de Segurança, prospectando as vantagens e as possíveis desvantagens de sua adoção no serviço de inteligência atual da RDC.

A pergunta de pesquisa é "por que uma possível reforma no serviço de inteligência congolês (ANR) deve ser realizada com precaução?". Para além de uma resposta óbvia, este trabalho argumenta é que, apesar dos problemas à

segurança individual gerados pelos abusos aos direitos individuais no país, o serviço de inteligência congolês é uma das únicas forças relevantes de segurança estatal que ainda mantém o padrão histórico de suporte à esfera coercitiva interna estatal. Nesse sentido, mantém-se como uma das poucas bases de sustentação do Estado no Congo. Assim, uma possível reforma de suas estruturas deve ter a precaução de não dirimir as capacidades já relativamente reduzidas dessa organização.

Sugere-se, normativamente, que esta reforma priorize o estabelecimento de um mandato claro para a ANR e o maior controle democrático sobre a organização. Ademais, deve-se evitar alguns erros cometidos pelo processo de SSR nas Forças Armadas e policias do país; mais especificamente no que se refere à integração nas forças estatais de grupos insurgentes opositores ao governo. Estes erros estão relacionados à ausência de um projeto sustentável e financiável a médio e longo prazos, à falta de critérios adequados para a triagem de ex-combatentes, e à ausência de um processo de treinamento continuado e integrado das novas forças que faça com que elas adquiram capacidade e responsividade.

5.1. Construção do Estado e Serviços de Inteligência no Caso Africano

O processo de construção do Estado no caso Europeu foi descrito com propriedade por Charles Tilly (1996).[1] O autor demonstrou que a preparação para a guerra e a própria guerra construiu o Estado como o conhecemos hoje (TILLY, 1985; 1996). De maneira lógica e cronológica, a interação estratégica histórica entre cidades e Estados (e de ambos entre si) fez com que estes últimos fossem impelidos a intensificar (i) seus mecanismos coercitivos, (ii) a extração de recursos para financiar sua proteção e, posteriormente, (iii) a distribuição de direitos como formar de barganha com a sociedade nos casos em que o capital ofereceu um contraponto à sua dominação.

Todavia, a intensidade e as prioridades na construção dessas esferas do Estado dependeram em grande medida do peso e da distribuição de capital (cidades) e de coerção (Estados) em cada território. Territórios com grande intensidade de capital e quantidade reduzida de coerção traçaram uma trajetória de construção estatal capitalizada. Territórios com intensidade reduzida de capital e grande intensidade de coerção seguiram uma trajetória coercitiva. Por fim, Estados que conseguiram equilibrar mais propriamente coerção e capital, esboçaram uma trajetória de coerção-capitalizada. Tilly (1996) argumenta,

[1] Este trabalho adota o conceito weberiano de Estado – como uma organização política compulsória que controla uma área territorial onde a burocracia detém de maneira bem-sucedida a reivindicação ao monopólio do uso legítimo da força física na imposição de sua ordem (WEBER, 1991).

entretanto, que na Europa, os Estados tenderam a convergir posteriormente a este último formato, o que resultou no padrão generalizado do Estado nacional.

As diferentes trajetórias assumidas no processo de construção do Estado (coerção, capital e coerção capitalizada), como resultado de um processo de competição interestatal e de busca pela dominação de territórios e populações por parte de governantes, ajudam a entender os perfis doutrinários e organizacionais adotados pelos primeiros serviços de inteligência.[2] Segundo Cepik,

> A formação dos sistemas nacionais de inteligência acompanhou as lições mais gerais da delimitação de identidades nacionais, da construção do Estado (State-building), da institucionalização democrática, da utilização de sistemas de informação e de usos de meios de força na era moderna (CEPIK, 2003:90).

A partir de uma lógica de interação estratégica entre atores (governantes entre si e com a população), a origem destes serviços foi marcada por um lado informacional e outro coercitivo (CEPIK, 2003).[3] Assim, uma das raízes dos serviços de inteligência contemporâneos está no desenvolvimento histórico da inteligência interna (*security intelligence*) – a qual remonta ao policiamento político europeu do século XIX e a busca de informações e perseguição/repressão de adversários políticos do governo.

A evolução dos serviços de segurança e das polícias políticas para a estrutura de serviços de inteligência doméstica (interna) ocorreu apenas no Século XX. Todavia, pode-se afirmar que suas funções nunca deixaram de incluir, além da coleta de informações, algum tipo de atividade coercitiva interna. Pode-se inferir que, nos processos de construção estatal em que a lógica coercitiva do Estado foi predominante, o peso relativo do capital (sociedade) nunca foi suficiente para controlar efetivamente a atividade interna repressora desses serviços.

Ainda para este trabalho importa reter: (1) quais foram as esferas da capacidade estatal formadas ao longo do tempo no processo de construção do Estado; e (2) qual foi a trajetória predominante adotada por países do Terceiro Mundo, os quais experimentaram um processo de construção estatal deveras diferente do modelo Europeu.

---

[2] A definição de inteligência aqui adotada se diferencia, por um lado, da noção de inteligência como mera informação analisada; e, por outro, da percepção de inteligência como informação ou guerra secreta. Entende-se inteligência como uma informação específica que se caracteriza por um processo particular de aquisição, coleta, análise e disseminação (RANSOM, 1958), por ser relevante à segurança da nação (WILSON, 2005) e por possuir capacidade explicativa e/ou preditiva (CEPIK, 2003).

[3] Enquanto Giddens (1987) demonstra a importância do controle da informação pelo governo como parte da construção das estruturas do Estado, Tilly (1996) "enfatiza a função coercitiva em detrimento do papel informacional dos órgãos de inteligência" (CEPIK, 2003:89), ressaltando a função desses órgãos no estabelecimento da autoridade do Estado entre o centro e as fronteiras do território.

Com relação ao primeiro ponto, em sua análise sobre o Estado europeu, Tilly (1996) identifica atributos que foram sendo desenvolvidos na estrutura do Estado ao longo do tempo, de maneira não uniforme e não necessariamente planejada. A passagem dos Estados europeus "de vespas a locomotivas" seguiu a seguinte lógica:

> O mínimo de atividades essenciais de um Estado são três: criação do estado: atacando e controlando os competidores e desafiantes dentro do território reclamado pelo estado; prática da guerra: atacando os antagonistas fora do território já reclamado pelo estado; proteção: atacando e controlando os antagonistas dos principais aliados dos governantes, quer dentro quer fora do território reclamado do estado. Contudo, não dura muito um estado que negligencia uma quarta atividade crucial: extração: sacando de sua própria população os meios de criação do estado de prática da guerra e de proteção. Os estados extorquidores de tributos permanecem no mínimo restritos a esse conjunto indispensável de quatro atividades, intervindo nas vidas de seus súditos nominais especialmente para impor o poder da classe dirigente e para extrair rendas. Contudo, além de uma determinada escala, todos os estados acabam aventurando-se em três outros terrenos perigosos: aplicação de justiça: solução peremptória de disputas entre os membros da população; distribuição: intervenção na divisão dos bens entre os membros da população; produção: controle da criação e transformação de bens e serviços pelos membros da população (TILLY, 1996:158).

Dessa forma, pode-se entender que um Estado deve no mínimo possuir, além de um território, capacidades coercitivas fundamentais contra seus antagonistas externos (coerção externa) e internos (coerção interna). Como visto, além da (e, em geral, após a) esfera coercitiva, os Estados tenderiam a construir, tipologicamente, esferas extrativas, jurídicas, distributivas e produtivas.

Concernente ao segundo ponto supracitado, Tilly (1996: 283) evidencia que, no caso dos países descolonizados após a II Guerra Mundial, a trajetória padrão de construção do Estado seguida foi a coercitiva. Entretanto, mesmo esta coerção possuía características próprias: eram direcionadas para dentro do Estado (coerção interna).[4] Pode-se dizer ainda que esta especialização no controle interno de populações civis por parte dos Estados criados no século XX é resultado da ausência relativa de ameaças militares sérias do exterior vis-à-vis o interior. Isto decorre primordialmente do fato de estes Estados serem triplamente externos. Isto é, foram construídos (i) sob a forma de possessões coloniais de outros Estados; (ii) sob a influência de outra potência bem maior e

[4] Segundo Tilly, "em média, os novos participantes [do sistema de Estados] seguiam as trajetórias de intensa aplicação de coerção. As potências coloniais que abandonaram suas possessões deixaram atrás de si pouco capital acumulado, mas legaram como herança aos estados sucessores forças militares que haviam sido recrutadas entre as forças repressivas e moldadas a partir dessas mesmas forças que eles criaram para manter as suas administrações locais. Essas forças armadas, relativamente bem-equipadas e bem-treinadas, se especializaram, então, muito mais no controle das populações civis e no combate aos insurgentes do que nas guerras entre Estados" (TILLY, 1996: 283).

(iii) por um concerto de nações (como o das Nações Unidas). Essa característica estabeleceu sua existência como membros separados do sistema internacional de Estados (TILLY, 1996).

Em certa consonância com a percepção de Tilly sobre a externalidade do Estado no Terceiro Mundo, Jeffrey Herbst (2000) demonstra que a característica amistosa do sistema internacional na África, desde o período colonial, gerou poucos incentivos para o fortalecimento das estruturas estatais.[5] Do mesmo modo, as particularidades do sistema internacional no período pós-colonial contribuíram para a manutenção de Estados com pouca capacidade de estender o poder da capital à periferia. O sistema baseado nos pressupostos da Carta da ONU e da OUA (Organização da União Africana) congelava a possível modificação das estruturas herdadas do colonialismo, principalmente (i) pela condenação às guerras de conquista e (ii) pelo mecanismo de patronagem característico da Guerra Fria (proteção externa sempre que havia ameaças). O que Herbst sugere é que na África as esferas (atividades) do Estado foram construídas de forma incompleta.

Portanto, diferentemente da Europa, a combinação entre um ambiente internacional amistoso, a presença constante de ameaças internas e a herança de um Estado construído externamente fez com que, na África, a trajetória predominante de construção do Estado fosse a coercitiva interna. Pretende-se, a partir do estudo de caso da República Democrática do Congo (RDC), entender a colaboração dos serviços de inteligência para manutenção e reprodução deste ciclo.

5.2. A Coerção Interna e os Serviços de Inteligência na RDC

O Estado congolês do período pós-colonial foi amplamente influenciado pelas estruturas estatais implantadas nos períodos de domínio do Rei Leopoldo II da Bélgica (1885-1908) e da colonização direta belga (1908-1960). Nesses dois momentos, a máquina coercitiva do Estado esteve voltada para dentro: para a repressão, o massacre e a cooptação violenta do trabalho forçado das populações locais (HOCHSCHILD, 1999). Ao mesmo tempo, o ambiente externo se manteve relativamente estável, assim como na maior parte da África.

[5] A partir da delimitação de fronteiras, o sistema internacional na época colonial contribuiu para a estabilidade das divisões territoriais iniciadas na Conferência de Berlim. Isto, porque havia um baixo grau de conflitividade entre as grandes potências pelo domínio do continente africano. As disputas entre as potências imperialistas eram realizadas no campo diplomático, em detrimento de conflitos militares. Nesse sentido, devido à ausência da necessidade de se fortalecerem as estruturas do Estado para uma eventual defesa do território, os Estados coloniais africanos foram caracterizados em geral por um território comandado por uma cidade capital relativamente forte, assegurada por fronteiras distantes e internacionalmente legítimas, havendo um vácuo de poder nas regiões interioranas (HERBST, 2000).

Consequentemente, em maior ou menor grau esse padrão de desequilíbrio a favor da coerção interna se reproduziu nos diferentes períodos do Estado pós-colonial. Essa lógica foi ainda sustentada, pelo menos até o fim da Guerra Fria, pelo ambiente externo favorável construído com o apoio de parceiros ocidentais (França, EUA e Bélgica).

Igualmente, a ocorrência constante de guerras que envolveram grupos intraestatais foi um fator central que contribuiu para a reprodução desse modelo coercitivo interno. Pode-se citar aqui, principalmente, a Crise do Congo (1960-65), a Primeira Guerra do Congo (1996-97) e a Segunda Guerra do Congo (1998-2003). Cumpre entender que as características particulares destas guerras condicionaram as estruturas estatais dos regimes políticos que as sucederam. Ou seja, a Crise do Congo influenciou as estruturas estatais construídas no regime de Mobutu Sese Seko (1960-1997); a Primeira Guerra do Congo condicionou as atividades estatais no governo de Laurent Kabila (1997-2001); e a Segunda Guerra do Congo, interferiu nas estruturas presentes no governo de Joseph Kabila (2001-...). Em suma, o fato de estes conflitos terem englobado conflagrações civis provocou o direcionamento das estruturas estatais que as sucederam em direção à especialização na repressão interna, como forma de evitar que problemas semelhantes (de forças rivais ameaçando o poder central) se repetissem.

Todavia, é necessário salientar uma diferença importante entre o atual governo de J. Kabila e os anteriores, precisamente nesta relação entre guerra e construção de esferas do Estado. Ao contrário dos conflitos armados anteriores, a Segunda Guerra do Congo não foi definida militarmente, mas encerrada exclusivamente por um acordo formal de paz. Como consequência, o governo que a sucedeu (após 2003) esteve e está marcado não somente pela habitual incapacidade coercitiva externa, mas também pela ausência relativa de capacidades coercitivas internas.

Por outro lado, algumas forças de segurança do Estado atual conseguem amenizar a incapacidade coercitiva interna do Estado. Entre elas pode-se citar os serviços de inteligência governamentais.

Esta seção apresenta brevemente as características das forças de segurança responsáveis pela manutenção da lógica de coerção interna nos três governos supracitados. Mantém, contudo, foco especial nos serviços de inteligência governamental, em suas estruturas principais e no papel desempenhado para a capacidade coercitiva do Estado. Adicionalmente, serão apresentadas as forças de segurança presentes no imediato pós-independência (Crise do Congo), visando à compreensão do processo de adaptação das forças de segurança coloniais para aquelas do Estado independente.

O quadro abaixo sintetiza os principais serviços de inteligência do país no período pós-colonial. O papel destes serviços dentro das características gerais das forças de segurança do Estado serão descritos nas subseções a seguir.

Principais Serviços de Inteligência Congoleses no Pós-Independência			
Período	**Nome da Organização**	**Tempo de Operação**	**Principais Características**
Crise do Congo	*Sûreté Nationale* (SN)	Período colonial-1969	Ligações estreitas com os EUA; comandada pelo grupo Binza
Regime de Mobutu	*Centre Nationale de Documentation* (CND) *Agence Nationale de Documentation* (AND) *Service Nationale d'Inteligence e Protection* (SNIP)	1969-1980 1980-1990 1990-1997	Polícia política, repressão interna e pilhagem
	Service d'Action et de Renseignements Militaire (SARM)	1986-1997	Inteligência militar e repressão Interna
Regime de L. Kabila	*Agence Nationale de Renseignements* (ANR)	1997-2003	Base na inteligência da AFDL; prisões e perseguições a jornalistas e opositores políticos
	Détection Militaire des activités Anti-Patrie (DEMIAP)	1997-2003	Inteligência militar interior e exterior
Regime de J. Kabila	*Agence Nationale de Renseignements* (ANR)	2003 (mandato)-hoje	Repressão interna de jornalistas e opositores políticos
	Service de Renseignement Militaire (SRM) *Sécurité Militaire* (SM)	2003-hoje	Inteligência militar interior e exterior

5.3. Forças de Segurança e Inteligência na Crise do Congo (1960-1965)

O Estado congolês, no imediato pós-independência (30 de junho de 1960), foi marcado pela instabilidade, resultando no que se convencionou chamar de Crise do Congo (1960-1965).[6] Essa guerra civil generalizada resultou em aproximadamente 200 mil mortos e foi marcada pela incapacidade coercitiva estatal – que só pôde ser superada com a ajuda de combatentes externos: tropas da ONU, mercenários sul-africanos, cubanos e europeus (em especial belgas), e apoio logístico, tecnológico, técnico e financeiro dos EUA.

Com a independência formal do Congo e a instabilidade gerada pela brusca descolonização belga, o amotinamento de militares negros da Force Publique

[6] A Crise do Congo foi uma crise belga que resultou no colapso de sua principal colônia, o Congo-Leopoldville. O fenômeno representou uma crise política, econômica e principalmente de segurança (guerra civil) – se estendendo de 1960 a 1965. Entre os eventos principais estão um motim inicial de soldados do exército, que lutavam por maiores direitos frente aos seus superiores belgas; a secessão de duas províncias de central importância para a viabilidade do novo Estado Congolês, Katanga (1960-1963) e Kasai Sul (1960-1962); os dois golpes militares (1960 e 1965) realizados pelo Coronel Joseph Desiré Mobutu (depois Mobutu Sese Seko), ambos apoiados política e economicamente pela CIA; o estabelecimento em Stanleyville de um governo rival ao de Kinshasa, pelo lumumbista Antoine Gizenga; o assassinato, em 17 de janeiro de 1961, do líder nacionalista-progressista Patrice Lumumba (então primeiro-ministro) com conhecimento da CIA e cooperação belga, de militares congoleses e de forças de Katanga; e as duas tentativas revolucionárias principais implantadas a partir do final de 1963 em Kwilu (centro do país), por Pierre Mulele, e em toda a região leste e nordeste, pelo grupo CNL (Conselho Nacional de Libertação) – que contou com a presença de Che Guevara e 128 cubanos.

foi o estopim para a explosão da crise congolesa. [7] A situação exigiu uma atitude imediata do então primeiro-ministro Patrice Lumumba, que removeu mil oficiais europeus do Exército, reformou suas estruturas de comando e renomeou a Force Publique do Congo Belga como Exército Nacional Congolês (Armée Nationale Congolaise – ANC).[8] Apesar das rápidas modificações, a desintegração das forças armadas continuou e a ANC tornou-se "uma força armada apenas nominalmente, tendo *performances* precárias, e sendo inapta a manter a ordem estatal sem auxílio externo" (MEDITZ e MERRILL, 1993). No que tange às forças policiais, o novo Estado independente detinha serviços distintos: a Gendarmerie Nationale, a Polícia Territorial e a Polícia de Chefes Locais. A primeira fazia parte da ANC e era composta por agentes pertencentes às antigas Tropas de Serviço Territorial da Force Publique; a segunda, era administrada no nível provincial e marcada pelos laços locais; e a terceira, servia sob o controle de chefes locais, sem uma estrutura de comando nacional.

No que tange ao sistema de inteligência, o Congo recém-independente manteve sua agência nacional, a Sûreté Nationale (SN). A SN desempenhava na colônia belga atividades de polícia especial e de investigação – além de ser responsável pela proteção e a segurança estatal mediante o controle de imigração, a supervisão de estrangeiros residentes na colônia e a proteção de líderes do governo. Após a independência do país, a SN manteve suas funções básicas, sendo subordinada ao Ministério do Interior. Entretanto, em meados de 1961, seu primeiro diretor, Victor Nendaka, a transformou em uma organização semi-autônoma sob seu controle particular.

São escassas as fontes que tratam sobre a agência. Entretanto, pelos relatos de Lawrence Devlin (2007), Chefe da Estação da CIA no Congo entre 1960 e 1967, é possível perceber sua estreita ligação com a inteligência norte-americana.

---

[7] Poucas fontes tratam das forças de segurança do Estado congolês nesse período. Pelos dados disponíveis, pode-se dizer que elas foram herdeiras diretas da estrutura belga de segurança, principalmente, a Force Publique. Sobre esta basta salientar que englobava as funções de manutenção da ordem pública doméstica (Tropas de Serviço Territorial) e de proteção contra ameaças externas (Tropas de Guarnição).

[8] Com a generalização dos motins do exército, Lumumba operou uma rápida e limitada reforma nas forças de segurança. O processo de africanização foi representado principalmente por: (1) a promoção de Victor Lundula para General e sua indicação para o cargo de Comandante em Chefe das Forças Armadas; e (2) a promoção de Mobutu para o posto de coronel e sua indicação para Chefe do Estado-Maior do Exército. Contudo, essas duas promoções se mostraram equivocadas – devido à falta de qualificação de ambos, ao apego a relações pessoais tribais por parte de Mobutu e às estreitas conexões com os serviços de inteligência norte-americano e belga também no caso de Mobutu. Por outro lado, além de reduzir o monopólio belga no alto escalão das forças de segurança, Lumumba mantinha laços com o bloco soviético com o intuito a restabelecer a segurança interna do país. Apesar de pecar pela imparcialidade, e talvez pela falta de veracidade, Lawrence Devlin, então chefe da estação da CIA no Congo, afirma que assessores soviéticos trabalhavam diretamente com a agência de inteligência congolesa no período mais turbulento do governo Lumumba (DEVLIN, 2007: 28). Após sua queda, estes laços teriam sido imediatamente rompidos.

O fato de o aparato estatal ter derivado diretamente da estrutura colonial contribui para essa lógica – ocorrida mesmo no breve governo de Patrice Lumumba. [9] No período imediatamente posterior à independência, belgas ainda ocupavam as principais posições na Sûreté Nationale e só foram substituídos após o amotinamento do exército congolês. Nos poucos dias entre a independência e as reformas de Lumumba, sua posição neutralista não impedia que agentes belgas da Sûreté mantivessem contatos estreitos com a CIA.[10] Após a eliminação do primeiro-ministro, a relação entre CIA e SN pôde se estreitar – agora sem a necessidade de intermediação de agentes de origem belga.

Para isto, foi fundamental a ascensão de Victor Nedaka à direção da SN, como parte do movimento de fortalecimento do Grupo Binza.[11, 12] O momento chave para a consumação do fato foi o golpe de 14 de setembro do então Chefe do Estado-Maior do Exército Joseph Desiré Mobutu e a instalação de um governo de tecnocratas congoleses graduados (o Colégio de Comissários), com o financiamento da CIA. [13] Neste momento se iniciaria uma relação estreita entre CIA e SN – que tenderia a se intensificar gradualmente com o regime posterior

---

[9] Sobre o fenômeno, Westad ressalta que "there was also the suspicion quite held, in some cases – that the colonial bureaucracy still served two masters; that the officials who had been appointed by the old regime served as agents for the political and economic interests of the former metropolis" (WESTAD, 2006:90).

[10] Como exemplo há o caso relatado por Devlin (2007:14), que afirma ter recebido duas pistolas semi-automáticas de um belga, oficial de inteligência da SN.

[11] Victor Nedaka era um líder tribal da província Oriental (noroeste do país), que havia sido vice-presidente da ala de Lumumba do partido Moviment National Congolais (MNC-L). Posteriormente, Nendaka rompeu com o primeiro-ministro e cooperou com sua deposição. Um exemplo disso foi sua ida à Embaixada norte-americana para informar a um oficial da delegação que Lumumba estava próximo da URSS (DEVLIN, 2007:98).

[12] O Grupo Binza foi uma organização informal que teve papel de protagonista durante a Crise do Congo. Seu nome se refere ao próspero subúrbio de Leopoldville onde a maioria de seus membros vivia. Operou de maneiras variadas, seja como grupo de pressão, seja por influência pessoal de seus membros junto ao alto escalão da política congolesa. Dentre seus principais integrantes estavam Mobutu Sese Seko, Justin Bomboko (fundador do partido de diplomados universitários UNIMO, e posteriormente presidente do Colégio de Comissários Gerais de Mobutu e ministro das relações exteriores entre 1961 e 1963), Victor Nendaka (vice-presidente da ala lumumbista do partido MNC e posteriormente diretor do Serviço de Segurança Nacional - Sûreté Nationale) e Cyrille Adoula (líder trabalhista, senador e posteriormente primeiro-ministro). Principalmente durante o período do governo de Joseph Kasavubu (1961 a 1965), o grupo Binza foi "o poder atrás da presidência" (DEVLIN, 2007:99).

[13] Mobutu relatou ao chefe da Estação no Congo, Larry Devlin, seu plano de destituir Lumumba a partir de um golpe de Estado e estabelecer um governo de tecnocratas congoleses graduados durante o tempo necessário para criar um regime democrático. Mobutu pediu ajuda à CIA para executar seu plano. Devlin garantiu o reconhecimento do novo governo e o auxílio financeiro de 5 mil dólares, quantia que Mobutu daria aos seus oficiais do alto escalão para apoiarem o golpe. Mobutu prometeu declarar os embaixadores soviéticos e tchecos e a delegação da China comunista persona non grata (DEVLIN, 2007). Assim, o comandante liderou a ascensão da cúpula militar, que suspendeu o parlamento e a Constituição em 1960. O primeiro-ministro Lumumba e o presidente Kasa-Vubu foram declarados neutralizados. No entanto, Kasa-Vubu foi restituído no Gabinete, enquanto Lumumba foi posto em prisão domiciliar sob proteção das tropas da ONU.

de Mobutu (pós-1965) e se distenderia somente com o final da Guerra Fria. Uma passagem de Devlin corrobora com a assertiva:

> Although he [Nendaka] had no experience in intelligence, he proved to be a quick learner. He recognized that American support was essential to the success of the new government and started to cultivate the most important officials in our embassy as I began to focus on him. The result was that we eventually became close friends, and our friendship continued until his death in Brussels in 2002. (DEVLIN, 2007:98. Grifos meus).

A relação estreita entre a CIA a SN, intermediada pelo grupo Binza, possibilitou a influência direta dos EUA na política congolesa daquele período. Além das relações diplomáticas abertas e das pressões sobre as políticas da ONU e da Europa para o Congo (DEVLIN, 2007; GLEIJESES, 2003), outra forma de interferência foi o estabelecimento de operações encobertas. Estas tiveram de ser intensificadas com insurgência de grupos rebeldes após o assassinato de Lumumba – pelo qual a CIA era amplamente acusada.[14] Essa intervenção direta e indireta dos EUA na política congolesa foi um dos fatores que colaboraram para o segundo golpe do então Comandante-em-chefe da Forças Armadas Joseph Mobutu em 14 de novembro de 1965. Dessa vez, contudo, sua permanência foi prolongada.

5.4. Forças de Segurança e de Inteligência no Regime de Mobutu (1965-1997)

O regime centralizado de 32 anos do General Mobutu (1965-97) foi construído como resposta à Crise do Congo e caracterizado pelo foco na esfera coercitiva interna – enquanto que a externa se manteve inefetiva.[15, 16] Em termos

[14] Entre as dez OEs principais que os Estado Unidos realizaram no Congo entre 1960 e 1965 pode-se citar (i) o apoio e o financiamento ao Golpe de Estado de Mobutu de 14 de setembro de 1960; (ii) a polêmica ordem de assassinato de Patrice Lumumba; (iii) o suporte à neutralização de lumumbistas no novo governo de integração nacional de Cyrille Adoula; (iv) e o apoio cerrado dos EUA nas operações do governo congolês contra os rebeldes do país (DEVLIN, 2007; DE WITTE, 2001; CHURCH COMMITTEE; 2007).

[15] Um dos indicadores da especialização na coerção interna foi o aumento da repressão à sociedade em finais de 1970 e início dos anos 1980 (CALLLAGHY, 1984). Nesse caso, o fato mais marcante foi, em 1978, o massacre secreto de brancos que procuravam refúgio da região de Kolwezi, recém atacada por rebeldes de Katanga. A operação secreta serviu como uma isca para que se estabelecesse a intervenção de França, Bélgica e EUA na guerra de Shaba II. Na década de 1990, com a crise acentuada do regime e as pressões para a liberalização política, as repressões foram intensificadas. Pode-se citar o massacre de estudantes no campus da Universidade de Lubumbashi (maio de 1990), o massacre e sequestro de membros do então Haut Conseil de la République (parlamento provisório) (fevereiro de 1992), o ciclo de saques cometidos por militares mal pagos (1991-1993) e a limpeza étnica de grupos rivais ao presidente em Katanga e Kivu Norte (1992-94). Mobutu atuava politicamente como um caudilho (CALLLAGHY, 1984), ou como um senhor da guerra (RENO, 1998) – mantendo a dominação pelo braço armado e pelo controle dos recursos naturais.

[16] A incapacidade coercitiva externa do Estado de Mobutu foi quase absoluta, seguindo um padrão pós-colonial de inefetividade. As guerras de Shaba I (1977) e Shaba II (1978) foram indicativas desta incapacidade militar. Em ambas as guerras, a postura dos militares zairianos foi de falta de disciplina,

gerais, seu regime foi marcado (i) pelo domínio quase absoluto do Estado por parte do presidente, (ii) pela repressão interna, (iii) pela cooptação econômica de uma burguesia nascente mediante a concessão de posições administrativo-burocráticas, e (iv) pela busca de uma autenticidade africana (CALLLAGHY, 1984; NZONGOLA-NTALAJA, 2003; YOUNG e TURNER, 1985).

A estrutura das forças de segurança assemelhava-se, novamente, ao perfil colonial. Caracterizou-se por um exército onipresente e inflado, junto a uma polícia fraca (ICG, 2006). Dessa forma, o exército foi o responsável tanto pela coerção externa, praticamente inexistente, quanto pela interna, base da sustentação do regime.[17] Todavia a aliança de Mobutu com as forças de segurança (mormente o exército), feita com o intuito de garantir seu domínio sobre a sociedade, foi construída com muito cuidado. Mobutu assegurou a sua fidelização através da vigilância constante, principalmente nas promoções e nomeações de oficiais superiores e generais para postos de comando, a partir de laços políticos, étnicos e familiares (MEDITZ e MERRILL, 1993). Seu controle também esteve institucionalizado pela autoridade direta sobre o Conselho de Segurança Nacional (CSN) e o Ministério da Defesa.[18, 19] Ademais, supostamente por razões de segurança, Mobutu foi construindo desde 1977 um corpo militar

deserção, desobediência, covardia, rebelião e violação da segurança estatal (NZONGOLA-NTALAJA, 2003:153; LEOGRANDE, 1980). A sucessão de expurgos, a transformação do alto comando das Forças Armadas em uma fraternidade e a especialização na área paramilitar foram agravantes para a capacidade coercitiva externa do Estado congolês. Em 1993, as Forças Aérea e Naval eram apenas operacionais, devido a negligência em instituir treinamento, equipamento e logística adequados. De fato, a desestruturação do exército era total em meados dos anos 1990, quando os 70.000 militares de 1983 foram reduzidos para 20.000. (MCCALPIN, 2002:45). Isto contribuiu para a completa deserção das Forças Armadas do Zaire (FAZ) no contexto da Primeira Guerra do Congo (TURNER, 2007).

17 De acordo com Meditz e Merril, "[…] throughout its existence, the mission to protect Zaire against internal threats – as well as threats to Mobutu's rule – has been the military's primary task. The military's importance in propping up the Mobutu regime is amply demonstrated by the role military and security forces played in suppressing political opposition in the early 1990s. Mobutu has routinely deployed loyal military units to suppress popular demonstrations; to harass and intimidate political opponents and newspapers critical of his regime; to gain and retain control of key government institutions such as state-run radio and television facilities and the central bank; to incite ethnic violence; and to obstruct the operations of the transitional government, including blocking access by members of that government to their government offices" (1993:on-line).

18 Mobutu presidia o CSN, que era composto, além do presidente, pelo primeiro-ministro; pelos ministros da defesa e assuntos veteranos, das relações externas, do interior e segurança, e da justiça; pelos administradores gerais do SNIP (serviço de inteligência civil) e do SARM (serviço de inteligência militar); pelo assessor especial da presidência em assuntos de segurança; e pelos chefes do Estado-Maior das Forças Armadas e da Gendarmerie. Em maio de 1982, um Comitê de Segurança e um Secretariado foram estabelecidos internamente ao órgão. O CSN, e depois o CSE, encabeçavam todos as forças de segurança do Estado (MEDITZ e MERRILL, 1993).

19 Mobutu, além de presidente, assumiu a função de ministro da defesa e de assuntos veteranos desde o seu golpe em 1965 – cedendo a posição somente em 1990 – com o anúncio da abertura política. Seu controle sobre o Ministério da Defesa significava o controle sobre o Exército e as forças de segurança. Ademais, durante a crise de Shaba de 1977, Mobutu assumiu pessoalmente o cargo de Chefe do Estado-Maior das Forças Armadas (MEDITZ e MERRILL, 1993).

de elite: a Divisão Especial Presidencial (Division Spéciale Présidentielle - DSP). Esta, além do SARM (serviço de inteligência militar), servia como uma força pessoal do presidente.

As forças militares do regime de Mobutu eram compostas pelas Forças Armadas Zairianas (Forces Armées Zaïroises – FAZ), pela Gendamerie Nationale (polícia militar) e pelo Serviço de Inteligência Militar (Service d'Action et de Renseignement Militaire - SARM). A capacidade militar era desequilibrada. Enquanto o corpo logístico era completamente marginalizado, forças especiais, como a Divisão Especial Presidencial (Division Spéciale Présidentielle - DSP), eram bem treinadas e equipadas – devido, sobretudo, ao auxílio externo.[20] Em média, a capacidade ofensiva externa era praticamente inexistente e a defensiva, sobremaneira limitada. Ademais, a Gendarmerie Nationale (GN) contribuía pouco para a manutenção da lei e da ordem no Zaire, e estava afundada em bandidagens, assassinatos e extorsões. Este quadro era causado principalmente pelos baixos salários e mesmo pela falta de pagamentos. Já as forças policiais civis do regime de Mobutu eram, assim como o Exército, caracterizadas pelo foco na repressão interna. O presidente controlou de perto essas forças, principalmente a partir de 1984, quando optou por realizar uma descentralização do sistema policial, então centralizado na inflada GN. Assim, criou a Guarda Civil (Garde Civile – GC) como espelho da DSP, ou seja, fortemente leal ao presidente. A GC manteve-se nas regiões urbanas, enquanto que a GN permaneceu nas áreas rurais.

Em relação ao setor de inteligência governamental, somente em 1969 Mobutu passou a controlar efetivamente o serviço nacional de inteligência. Neste ano, a SN tornou-se o Centro Nacional de Documentação (Centre Nationale de Documentation - CND). Com a prerrogativa da escolha de sua diretoria, Mobutu garantia um controle estreito à organização. No início da década de 1970, foram introduzidas seções internas e externas dentro da agência – embora suas atividades fossem muito semelhantes: prisões, interrogações e detenções de indivíduos considerados uma ameaça ao regime. Já no início dos anos 1980, o nome do CND foi alterado para Agência Nacional de Documentação (Agence Nationale de Documentation - AND); e posteriormente, em agosto de 1990, a organização foi renomeada Serviço Nacional de Inteligência e Proteção (Service Nationale d'Inteligence e Protection - SNIP).

[20] Cumpre aqui ressaltar a importância da DSP. Suas missões principais eram: proteger a Presidência e outras hierarquias do poder; e realizar operações de repressão e luta contra o terrorismo e a guerrilha urbana. Esta última função levou suas tropas a serem particularmente temidas pela população civil. As características diferenciais da DSP faziam com que ela fosse, "indubitavelmente, a única força militar zairiana suficientemente leal e capaz de ser estabelecida no exterior" (MEDITZ e MERRILL, 1993:on-line. Tradução minha).

Como já observado, as atividades principais do serviço estavam relacionadas com a prioridade dada ao componente interno da segurança estatal (AGABA e PULKOL, 2009). A atuação do SNIP consistia no trabalho de corpos relativamente pequenos de agentes que obtinham informação por meio de uma rede de informantes e de outros órgãos do aparato do Estado. Todavia, o serviço era profundamente politizado, prevalecendo mais a função de intimidação a grupos políticos de oposição do que a atividade informacional. O SNIP realizava interrogações, prisões e abusos a "indivíduos ou grupos que estabelecessem desafios para a autoridade do regime" (AGABA e PULKOL, 2009:141). Principalmente nas décadas de 1980 e 1990, a inteligência congolesa aplicou em larga escala a repressão de ativistas políticos internos e a perseguição de grupos exilados na Europa.

> Given its relatively successful infiltration of the major arenas of political dissent such as universities and professional associations, it did achieve a high level of intimidation and was widely feared before 1990 (NZONGOLA-NTALAJA, 2003:155).

Nos anos 1990, houve na SNIP, assim como em outros órgãos do aparato de segurança, a intensificação de saques e pilhagem e a generalização de abusos cometidos por seus agentes. Uma das origens dessa inflexão está no fato de que em finais dos anos 1980, sob o comando Honoré Nganbanda Nzambo-ku-Atumba, o serviço de inteligência passou a se especializar em atividades paramilitares. Ademais, segundo Meditz e Merrill (1993), em 1990, alguns membros da SNIP passaram a fazer parte de uma força secreta de operações especiais, estabelecida dentro da GC: as Forças de Intervenções Especiais. O grupo tinha a tarefa de abduzir e intimidar dissidentes políticos. Chegou a ser chamada de Les Hiboux (Os Corujas) – mesmo apelido de uma subunidade especial do DSP. O nome vinha de suas temidas ações noturnas guiando Mitsubishi Pajero pretos com vidros escuros e espalhando terror pelas ruas de Kinshasa (NZONGOLA-NTALAJA, 2003).

Além de o serviço de inteligência civil se reportar diretamente ao presidente, auxiliava na centralização do poder em suas mãos na medida em que fiscalizava outros braços do poder estatal, como as Forças Armadas e policiais. Mobutu também confiava atividades de inteligência a redes de ligações particulares que serviam como forma de controle das informações que recebia dos serviços oficiais. Tratava-se de espiões particulares dentro das próprias forças de segurança (MEDITZ e MERRILL, 1993).

Outros órgãos do setor de segurança possuíam serviços de inteligência próprios. O braço de inteligência das FAZ, Serviço de Ação e Inteligência Militar (Service d'Action et de Renseignements Militaire - SARM), mantinha atividades usuais de inteligência militar, como vigilância interna e coleta de

inteligência entre civis e militares, além de atividades de repressão.[21] Não obteve a proeminência e a liberdade de ação do SNIP, mas conseguiu construir uma rede ampla e bem distribuída de informantes entre civis e militares. A Agência Nacional de Imigração (Agence Nationale d'Immigration - ANI) também possuía atividades de inteligência. Esta agência era responsável prioritariamente pela segurança de fronteiras e seus funcionários eram distribuídos nas onze províncias do país. Outras unidades de inteligência estavam estabelecidas na GC e na GN.

5.5. Forças de Segurança e Inteligência sob Laurent Kabila (1997-1998)

Mediante a vitória de suas forças (Alliance de Forces Democratique pour la Liberation du Congo-Zaire – AFDL) na Primeira Guerra do Congo, em 28 de maio de 1997, Laurent Kabila assumiu a administração congolesa com viés autocrático e a integração de ruandeses, ugandeses e Tutsi em seu governo.[22,23] Kabila mudou o nome do país e de suas províncias, além de assinar um decreto anulando o Ato de Transição de Mobutu de 1990 e tomando o controle do executivo, das forças militares e do poder legislativo – o que se manteria até a suposta criação de uma assembléia constituinte. Ademais, o novo presidente integrou seus apoiadores

[21] O SARM tinha sede em Kinshasa, onde estava seu QG com celas de detenção. Para certos usos, o SARM partilhava celas subterrâneas com a DSP. Seus recrutas vinham da circunscrição de Kinshasa da GN e de quadros da DSP. O serviço era dividido em um regimento de investigação (incluindo um Destacamento Especial de Investigação) e um regimento de "ação". Este último era temido pela eficácia e brutalidade de seus métodos (FR, 2006).

[22] A Primeira Guerra do Congo foi um conflito armado decorrente da crise econômica e política do Estado de Mobutu e do transbordamento dos conflitos de Ruanda e Burundi ao vizinho Zaire. A guerra, apesar de seu caráter civil, é aqui interpretada a partir de sua característica principal: a agressão de Ruanda, Uganda, Burundi e Angola ao território zairiano. Ou seja, trata-se de uma guerra interestal em forma de guerra civil (guerra mista). As decisões de estabelecer a invasão ocorreram pelo apoio de Mobutu aos grupos rivais dos governos de Ruanda, Burundi e Angola. Nos dois primeiros casos, destaca-se o patrocínio de Mobutu aos Hutu expulsos do território Ruandês – os quais haviam cometido o genocídio de 800.000 Tutsi e continuavam, desde 1995, a realizar ataques ao território de Ruanda e a Banyamulenge (Tutsi do Congo) em Kivu Sul a partir dos campos de refugiados no Zaire. No último caso, constata-se que Angola teve interesses muito particulares, e, mormente, internos, para entrar na Primeira Guerra do Congo. Tratava-se de capturar Savimbi, desmobilizar o exército secreto da UNITA (acreditava-se que 15.000 homens estavam em operação no Zaire) que voltou à guerra após as conciliações de 1994 e 1995, e quebrar suas redes comerciais de diamantes. Para legitimar a invasão, foi criado um grupo rebelde praticamente fantoche, sem base ideológica e heterogêneo: a Alliance de Forces Democratique pour la Liberation du Congo-Zaire (ADFL).

[23] As características da Primeira Guerra do Congo influenciaram a criação das estruturas do Estado de Laurent Kabila. A Primeira Guerra do Congo diferenciou-se da Crise do Congo por ter sido uma guerra mista (interestatal e civil) e pelo fato de que o Estado Congolês, ainda representado pela figura de Mobutu Sese Seko, foi derrotado. Ademais, a Primeira Guerra do Congo teve como característica principal a participação de Forças Armadas externas na composição das forças vitoriosas da AFDL. Como consequência, houve a grande dependência das tropas externas para a construção de um novo exército nacional. De acordo com Dunn, "once in power, Kabila continued to rely heavily on Rwandan assistance and protection" (2002:57).

externos da guerra (ruandeses e ugandeses) à estrutura administrativa do Estado (Gabinete e Forças Armadas). Como resultado, o Estado congolês comandado por L. Kabila foi pautado, por um lado, pela precária atividade coercitiva externa, mas, por outro, pela atividade coercitiva interna ao menos incipiente.[24, 25]

Apesar do rompimento simbólico com o regime de Mobutu, as forças de segurança de L. Kabila reproduziram a lógica do período anterior. Houve a manutenção das estruturas das forças de segurança e do controle pessoal do presidente sobre elas mediante nomeações para os cargos de comando. Além disso, Kabila manteve o controle presidencial sobre o Conselho de Segurança Nacional (após 1998, Conselho de Segurança do Estado – CSE). Outrossim, o núcleo das forças de elite se manteve mais fiel ao presidente do que às estruturas de segurança impessoais do Estado. Kabila, assim como Mobutu, confiou sua própria segurança e a do Estado, sobretudo, na unidade presidencial de elite (agora GSSP).

Por outro lado, suas tentativas de reformas foram desastrosas. Ao ascender ao poder, Kabila estabeleceu o General ruandês James Kaberebe como Chefe do Estado-Maior das Forças Armadas. Esta atitude foi uma agressão à soberania estatal, na medida em que o militar era um representante dos interesses estratégicos ruandeses. Ademais, a marginalização dos antigos soldados de Mobutu nas novas FAC (Forças Armadas Congolesas) – por meio de uma política de fome e de falta de tratamento médico – resultou na incapacidade militar para enfrentar as forças de Ruanda, Uganda e Burundi que invadiram novamente o país na Segunda Guerra do Congo (1998-2003).

Com relação às Forças Armadas, importa reter que as novas FAC foram compostas, principalmente por ex-soldados das FAZ precariamente motivados e por Kadogos inexperientes.[26, 27] Além disso, nas FAC predominou um sistema de redes pessoais e de patronagem, com o favorecimento de membros da comunidade Lubakat de Kabila (norte da província de Katanga), principalmente

---

[24] A esfera coercitiva externa do regime de L. Kabila esteve, na maior parte do tempo, dependente das tropas dos países vizinhos. Em meados de 1998, com o rompimento de L. Kabila com as forças externas, o país ficou absolutamente vulnerável a novas agressões externas – o que ficou claro com o início da Segunda Guerra do Congo (agosto/1998) – e, novamente, com o apoio externo de grupos internos ao país.

[25] O tempo de atuação das novas FAC (Forças Armadas Congolesas) e das outras forças de segurança não foi suficiente para identificar sua efetividade. Entretanto, o fato de as forças de segurança congolesas passarem a reprimir os rebeldes Tutsi no leste do país dá sinais de que uma esfera coercitiva interna era, pelo menos, incipiente.

[26] No que se refere aos ex-membros das FAZ, cumpre ressaltar que, ao ascender ao poder em maio de 1997, Kabila realizou rapidamente uma campanha de educação ideológica na base militar de Kitona para facilitar a sua integração nas novas FAC (Forças Armadas Congolesas). Esta campanha seria repetida em 1998, com uma grande operação de reintegração. É possível admitir com algum cuidado que aproximadamente dois terços do contingente das FAZ foram integrados nas FAC (FR, 2006).

[27] Estes se tratavam de uma coleção de soldados crianças que fizeram parte das forças de 40.000 homens da ADFL, junto aos Tigres de Katanga – até então exilados em Angola.

nas novas forças de elite, as GSSP.[28] No que concerne às forças policiais, em 1997 Kabila recriou em essência a Police Nationale Congolaise (PNC) (existente entre 1966 e 1972) – combinando a Garde Civile e a Gendamerie Nationale. Entretanto, durante o breve período de paz e a II Guerra do Congo, a polícia permaneceu pouco armada e completamente marginalizada.

Acerca dos serviços de inteligência do novo regime, interessa o fato de que a estrutura de inteligência da AFDL foi fundamental na ascensão de L. Kabila ao poder. Passava informações sobre os diversos órgãos das FAZ, suas reais capacidades operacionais, bem como os dados pessoais relativos aos seus oficiais de comando. No novo arcabouço de inteligência governamental, as estruturas da AFDL se mantiveram como base principal. A nova Agência Nacional de Inteligência (Agence Nationale de Renseignements - ANR), foi estabelecida em 1997 nos moldes da antiga AND (Agence Nationale de Documentation) e, como a anterior, foi colocada sob autoridade direta do presidente. Além de atividades de segurança estatal, cometia prisões e perseguições de jornalistas e opositores políticos.[29] Igualmente, o serviço de inteligência militar de Mobutu (SARM) foi dissolvido de imediato e substituído pela Detecção Militar de Atividades Anti-Pátria (Détection Militaire des activités Anti-Patrie – DEMIAP), de missão e objetivos similares. Em março de 1999, o órgão foi cindido em duas direções: Interior (localizada em Kinshasa no mesmo local da antiga SARM) e Exterior (localizada em Gombe).

Sobre a nova invasão de Ruanda, Uganda e Burundi ao Congo em 1998, não se sabe ao certo se foram os serviços de inteligência civis e militares que falharam em antevê-la ou o ciclo de decisão política que tardou em empreender uma reação.[30]

---

[28] A GSSP (Groupe spécial de sécurité présidentielle) manteve as tarefas da antiga DSP: um corpo de elite com funções principais de segurança presidencial. Somente o nome foi alterado, em finais de 1997. Além das políticas de favorecimento étnico por parte de L. Kabila, parte dos ex-membros da DSP foram integrados ao novo regime, mesmo aqueles que haviam fugido para o exterior. Indo de encontro ao movimento de integração de grupos estrangeiros nas estruturas do Estado, L. Kabila tinha interesse central em manter a GSSP como uma força coesa. Dessa forma, confiou inicialmente o comando do grupo ao seu filho, depois presidente, Joseph Kabila.

[29] Outras organizações possuíam atividades parecidas, como a Direction spéciale des investigations et recherches (DSIR), que se reportava diretamente ao CSE e atuava em colaboração com a Polícia de Intervenção Rápida (Police d'intervention rapide - PIR).

[30] A inserção dos ruandeses nas forças armadas chegou ao ponto de promover uma tentativa de golpe a Kabila em 1998 (ICG, 2006:3). Dessa forma, em julho do mesmo ano, Kabila realizou uma inflexão em seu governo, ordenando ruandeses e ugandeses saírem do país. A atitude foi a causa fundamental para a nova invasão – já que aqueles países haviam auxiliado a ascensão de Kabila para que este servisse como um fantoche do Estados vizinhos. Não obstante as tentativas de reestruturação das forças armadas no breve período do governo Kabila, sua debandada foi rápida na Segunda Guerra do Congo – deixando o Estado dependente do bloqueio regional operado, mormente, por Zimbábue, Angola e Namíbia.

5.6. Forças de Segurança e Serviço de Inteligência sob Joseph Kabila (2001)

O Estado congolês herdeiro da Segunda Guerra do Congo foi diretamente condicionado pelas características particulares deste conflito.[31] A dependência das forças armadas estrangeiras contribuiu, novamente, para a incapacidade do Estado em prover segurança externa para seus cidadãos. [32] No que tange à coerção interna, apesar de a Segunda Guerra do Congo ser considerada, em parte, uma guerra civil, a recorrente especialização das forças de segurança com relação à repressão interna não ocorreu. Mantiveram-se grupos armados que continuam atuando impunemente contra o governo nacional.[33]

Com relação às forças de segurança, Joseph Kabila conservou inicialmente as estruturas organizacionais do governo de seu pai (assassinado em janeiro de 2001), incluindo a cadeia hierárquica de comando e funções. Entretanto, no início de 2002 realizou mudanças no comando das organizações (titulares dos Estados-Maiores e comandantes das dez regiões militares) com o intuito de reiniciar o Diálogo Intercongolês [34] que previa a incorporação de diferentes grupos às novas

---

[31] A Segunda Guerra do Congo foi o conflito decorrente da quebra da aliança vencedora da Primeira Guerra do Congo. Com as inflexões nacionalistas de Kabila, a demora em resolver os problemas de inclusão social dos Banyamulenge no leste do país, e tolerância de Kabila com a continuidade de incursões Hutu ao território ruandês, a aliança Ruanda, Uganda e Burundi se refez – agora para destituir do poder quem eles haviam lá colocado (VISENTINI, 2010). Se na Primeira Guerra do Congo o apoio de um grupo supostamente revolucionário e autóctone foi a forma encontrada para legitimar a guerra de agressão, na Segunda Guerra do Congo a mesma estratégia de guerra proxy foi implantada. Ruanda e Uganda apoiaram o surgimento do grupo RCD-Goma; e Uganda do MLC e do RCD-K-ML (PRUNIER, 2009).

[32] Desde o fim dos conflitos, invasões de Ruanda e Uganda ao território congolês foram frequentes e só cessaram com a declaração de Angola em agosto de 2006 de que 30.000 tropas estavam preparadas na região de Cabinda para serem utilizadas contra qualquer invasão ruandesa (STRATFOR, 2006).

[33] Com relação aos grupos internos nacionais, em um primeiro momento, após o cessar fogo de 2003, houve a emergência do conflito na região de Ituri envolvendo etnias Lendu (FNI - Front des Nationalistes et Integrationnistes e outros) e Hema (UPC - Union des Patriotes Congolais, e outros), enquanto que grupos Mai Mai continuavam a lutar contra populações estrangeiras. Já em um segundo período, o grupo CNDP (Congresso Congrès National pour la Défense du Peuple) foi o foco das atenções. Houve novas ameaças a partir dos conflitos armados por direitos à agricultura e à pesca entre etnias Enyelle e Munzaya no final de 2009 e a criação da Aliança para Salvaguarda dos Acordos de Paz de Goma no início de 2010. No que tange aos grupos internos estrangeiros, os principais rebeldes armados, operantes desde a Segunda Guerra, são Hutu da milícia Interahamwe e ex-integrantes das Forças Armadas Ruandeses (FAR). A maior parte destes grupos organizou-se na FDLR (Forces Démocratiques de la Libération du Rwanda), que conta com 6.000 homens e situa-se atualmente na região leste do país. O segundo principal grupo de guerrilheiros estrangeiros que atua na RDC é o LRA (Lord's Resistance Army) – que opera no nordeste do país, tem como alvo central o governo de Museveni em Uganda e estima-se que tenha entre 500 e 3.000 combatentes (HRW, 2009; ISN, 2009).

[34] Em 10 de julho de 1999 foi firmado o Acordo de Lusaka, que previa o estabelecimento da paz e a saída de L. Kabila do poder através do processo eleitoral. O acordo foi fundamental para a criação da Missão da ONU no Congo (MONUC) em 30 de novembro de 1999. Entretanto, apesar de Kabila ter assinado o acordo, não realizou a saída conforme estipulado. Esta só pôde se concretizar com o seu assassinato em 16 de janeiro 2001. A subida de Joseph Kabila (filho de Laurent) 8 dias depois, articulada por Zimbábue e Angola, foi decisiva para o encerramento do conflito. As negociações em

forças de segurança do Estado e a desmobilização de ex-membros das FAZ que haviam se aliado aos grupos rebeldes.[35] Por outro lado, J. Kabila manteve uma posição de desconfiança frente às forças de segurança do Estado, principalmente devido ao fato de seu pai ter sido assassinado por um complô vindo de dentro destas estruturas. Destarte, blindou-se reforçando o poder e o tamanho da guarda presidencial (GSSP) e centralizando o comando da maior parte dos órgãos de segurança no escritório militar presidencial (Maison militaire).[36]

As forças militares da RDC foram reestruturadas, a partir do DIC e do Acordo Global e Todo-Inclusivo de Paz de 2002 (adotado em 2003), nas vésperas do lançamento do Governo de Transição (2003-2007). O princípio básico seguido foi a organização de Forças Armadas novas e integradas, as Forces Armées de la République Democratique du Congo (FARDC), inauguradas em setembro de 2003. A partir de sua formação, as FARDC foram divididas em três comandos preexistentes,[37] 10 regiões militares[38] e integradas com os cincos grupos insurgentes principais da Segunda Guerra do Congo.[39] Em essência, as tropas do governo e dos antigos grupos rebeldes continuaram controlando o território sob sua ocupação, mas agora com o envolvimento de outras facções e gradualmente se integrando às estruturas estatais (JANE'S, 2009).[40] Apesar

todo o ano de 2002 (Diálogo Inter-Congolês) abriram o caminho para o cessar-fogo. Acordos entre os países e grupos beligerantes nacionais congoleses (acordos de Sun City, de Pretoria e de Luanda), realizados no decorrer do ano, desembocaram no Acordo Global e Todo-Inclusivo de Paz, assinado na África do Sul em 2002 e adotado em 2003.

35 Com este precedente, o presidente se separou gradualmente de diversos ex-companheiros de seu falecido pai e estabeleceu uma renovação na maioria dos órgãos da segurança estatal. Institucionalmente, esse movimento foi possível a partir do Decreto Presidencial, publicado em 26 de abril de 2003, que provia a base legal para a integração nas forças de segurança do Estado dos braços armados das facções rebeldes signatárias do Acordo Global e Inclusivo de Paz e de ex-membros das FAZ que ainda não haviam sido integrados. Tratava-se do estabelecimento de um "novo período" – próprio da transição – o qual rompia com as políticas anteriores de L.Kabila.

36 Trata-se de um poder paralelo ao comando formal das forças de segurança "no matter what the formal hierarchy, the various civilian and military intelligence services and the Presidential Guard (GSSP) all answer to the Maison militaire" (ICG, 2006:14).

37 Há três comandos para as Forças: Leste (incluindo o nordeste), Sul (sul e oeste) e Central (Kinshasa e arredores).

38 As 10 regiões militares são: 1 - Bandundu; 2 - Bas-Congo; 3 - Équateur; 4 - Kasai-Occidental; 5 - Kasai-Oriental; 6 - Katanga; 7 - Maniema; 8 - Nord-Kivu; 9 - Orientale; 10 - Sud-Kivu.

39 Os cinco grupos eram: o RCD-Goma, entre 20 e 45 mil homens; o MLC, entre 10 e 20 mil homens; o RCD-K/ML, 5-15.000 tropas; o RCD-N, 10.000 homens; e os grupos tribais Mai-Mai, com entre 30 e 50 mil tropas. Posteriormente foram incluídos, a partir de um acordo de paz firmado em Dar es Salam em 2003, os grupos beligerantes nos conflitos armados da região de Ituri. Estes tinham 15 e 50 mil tropas. Ademais, as antigas FAC também tiveram de ser integradas nas novas FARDC. Suponha-se, possuíam uma força de 100-120.000 homens, apesar de alguns analistas argumentarem que metade dessas forças eram soldados "fantasmas" (JANE'S, 2009; WB, 2009; ICG, 2006).

40 A base institucional do processo de integração das Forças Armadas foi dada pela Estrutura Militar de Integração (Structure Militaire d'Intégration - SMI), estabelecida em 2004, a partir do lançamento do Programa Nacional de Desmobilização, Desarmamento e Reintegração (PNDDR). O comando das Forças também foi inicialmente repartido entre os grupos beligerantes principais; posteriormente, após a vitória nas eleições de 2006, J. Kabila estreitou seu controle sobre as FARDC.

de esforços de reforma, as forças terrestres estão atualmente infladas (151.251 homens) e mal treinadas, e as forças navais e aéreas encontram-se sucateadas – apesar de sua importância relativa às características geográficas do país. A antiga GSSP, agora Guarda Republicana (Garde Républicaine - GR), foge desta lógica, mantendo uma capacidade diferenciada. Entretanto, o procedimento geral de sua integração às FARDC tem sido demorado e seus principais elementos não são responsivos à estrutura de comando das FARDC, mas ao presidente Joseph Kabila.[41] Em relação às forças policiais, Joseph Kabila manteve as estruturas gerais do governo de seu pai. A Police Nationale Congolaise (PNC) continuou situada abaixo do Ministério do Interior, sendo chefiada por um Inspetor Geral e trabalhando junto aos governadores locais nomeados pelo presidente.[42]

No que concerne aos serviços de inteligência, a inteligência militar foi reorganizada após o início do Governo de Transição em 2003. Com base no Acordo Inclusivo de Paz, o Decreto-Lei de 18 de agosto de 2003 dissolveu o DEMIAP e estabeleceu suas funções no Estado-Maior de Inteligência Militar (Etat-Major général du Renseignement militaire - EMGRM). Nesse órgão, foram estabelecidos o Serviço de Inteligência Militar (Service de Renseignement Militaire – SRM) e a Sécurité Militaire (SM). Ambos foram divididos em exterior e interior, assumindo a maioria do pessoal do DEMIAP bem como suas instalações. Tanto a SRM quanto a SM foram afetadas pelo processo de integração dos ex-combatentes da Segunda Guerra do Congo. Isto porque foram incorporados os serviços especializados de segurança e inteligência dos grupos rebeldes, os quais se mantiveram estabelecidos nas mesmas regiões do país que anteriormente controlavam.

Por seu turno, a ANR se manteve como órgão civil responsável pela inteligência e a segurança do Estado, estabelecido sob a autoridade única do presidente da República. Ao contrário de todos os outros órgãos da segurança estatal da RDC, os quais passaram por um processo de integração de ex-combatentes rebeldes nas posições de base ao alto escalão de comando, "en ce qui concerne ses personnels, l'A.N.R. n'est donc pas concernée par la situation d'intégration de membres des ex-forces rebelles" (FR, 2006:29).[43] Criada no início

[41] A GR mantém as funções de controlar o acesso a aeroportos e de realizar serviços de segurança de fronteiras – bem como da segurança do Presidente e possui entre 6 e 15 mil homens (IiSS, 2010; AMNESTY, 2007).

[42] Em 2006, eram 38.000 homens divididos em três áreas: Unidades Especializadas (9.000 homens), subdivididas em Polícia de Intervenção Rápida e Unidade Policial Integrada; Forças Territoriais (20-25.000 homens), as quais são locais, descentralizadas e supervisionadas por um Inspetor Geral de Polícia; e os serviços especializados em investigadores criminais.

[43] Em agosto de 2003, uma série de decretos presidenciais fez com que todas as posições-chave em vários departamentos da transição – tanto no governo, na Assembléia Nacional, no Senado, e na administração local (nomeação dos governadores das onze províncias do país), quanto no Alto Comando do Exército, incluindo as dez regiões militares – fossem distribuídas nos termos do Acordo Global e Inclusivo. O caso da ANR tratava-se de uma compensação dessa divisão, haja vista que J. Kabila não estava disposto a deixar invadir seu "domínio reservado" (FR, 2006).

de 1997 por L. Kabila e herdeira do serviço de inteligência da AFDL, sua estrutura é regida pelo Decreto-Lei 003/2003 de 11 de janeiro de 2003. A agência possui a missão de assegurar a segurança interior e exterior do Estado[44]; é dirigida por um Administrador Geral e um Administrador Geral Adjunto; e está dividida em departamentos, direções centrais e provinciais, e estações exteriores (art. 5). O Admistrador Geral é assistido pelo Administrador Geral Adjunto e três administradores principais (chefes dos departamentos de segurança interior, de segurança exterior e de apoio).[45] Todos estes administradores são nomeados pelo presidente da República.

Outros órgãos de segurança que possuem divisões de inteligência são a Direção Geral de Migração (Direction générale de migration - DGM), responsável pelo controle de fronteiras (UK, 2009, USA, 2009); e a Direção de Informações Gerais e Serviços Especiais da Polícia (Direction des Renseignements Généraux et Services Spéciaux de la Police - DRGS) – divisão da PNC especializada pela inteligência interna (FIDH, 2009). Tanto a ANR quanto a DRGS, além da GR, são acusadas de perpetuação da repressão interna do regime (Ibidem). Entretanto, é necessário perceber que a ANR é certamente um dos únicos órgãos coercitivos de relevância do Estado que mantém alguma capacidade coercitiva interna, já que a tarefa coercitiva externa é quase inexistente no Estado.

Entre 2002 e 2009, foram 19 casos divulgados, além dos inúmeros omitidos, de prisões praticadas por membros da ANR (OMCT, 2006; UN, 2007a e 2007b; FIDH, 2009). A maioria dos presos foi liberada, em geral, em até dois dias.[46] Grande parte deles eram suspeitos de complô contra o presidente e de tentativas de fomentar golpes de Estado; tudo isto, no contexto dos traumas decorrentes do assassinato de L. Kabila e do temor de um novo atentado. Não obstante as justificativas, diversos casos envolveram a perseguição a opositores políticos[47], a

[44] Suas atribuições principais são: coleta, centralização, interpretação, exploração e difusão de informações relevantes à segurança interna e externa do Estado; busca e constatação de infrações à segurança do Estado; fiscalização de pessoas ou grupos suspeitos de atividades contra a segurança do Estado; e proteção do ambiente político (RDC, 2003).

[45] O Département de Sécurité Intérieure (DSI) é dotado de uma administração central que compreende uma direção de informações gerais, uma direção de operações, uma direção de contra-espionagem, uma direção de estudos e pesquisas, uma direção de identificação e uma direção técnica. O Département de Sécurité Extérieure (DSE) é dotado de uma administração central que compreende uma direção de operações e planificação, uma direção de ações, uma direção de pesquisa e estudos e uma direção técnica. Por fim, Département d'appui é responsável pelo apoio logístico aos outros departamentos descentralizados nas províncias e possui uma direção de serviços gerais, uma direção médica, uma academia de inteligência e segurança e um centro de telecomunicações, informática e documentação.

[46] Entretanto, acumulam-se casos de pessoas presas por meses – apesar de a lei prever um máximo de 48 horas de custódia (FIDH, 2009).

[47] "Most of the violations committed by the ANR were violations of the right to liberty, including political arrests during the electoral campaign. These violations constituted 59% of all cases involving the ANR and investigated by the UNHRO in the reporting period. These arrests were often accompanied by the violation of the right to physical integrity (41% of the violations)" (UN, 2007a:10).

violação de direitos individuais,[48] a exploração de recursos naturais do Estado[49] – em uma situação clara de falta de controle dos agentes[50] (UN, 2007a e 2007b).

A extensão de suas atividades, ao ponto de chegar às de uma polícia política, vai ao encontro do mecanismo histórico das forças de segurança do Congo: a incapacidade de prover segurança interna por parte das forças policiais é compensada com órgãos não especializados na tarefa. No regime de Mobutu, as FAZ e as forças especiais realizavam as principais tarefas de coerção interna. Já no regime de J. Kabila parecem ser os serviços de inteligência e as forças especiais que mantêm o pouco que há desta parte da esfera coercitiva.[51]

Todavia, esta realidade não deve ser motivo para barrar a busca de meios mais eficazes de controle das atividades da ANR, em busca de um direcionamento mais adequado das suas capacidades coercitivas, evitando os abusos aos direitos individuais. As características precárias da PNC e das FARDC estão relacionadas aos processos de integração de ex-combatentes às forças de segurança do Estado e de Reforma do Setor de Segurança. A análise desses processos pode trazer ensinamentos relevantes para a formulação de um projeto sustentável de reforma das forças de inteligência congolesas.

5.7. Reforma da Inteligência: A Experiência das Forças Armadas e Policiais

Atualmente há uma pressão generalizada da sociedade civil e de analistas especializados para que seja realizada a reforma do serviço de inteligência congolês como parte mais ampla do processo atual de Reforma do Setor de

[48] Em 15 de maio de 2007, 15 agentes da ANR e seis soldados das FARDC atacaram a vila de Kadimbu, (Katanga) – realizando torturas e violações sexuais. Dois agentes da ANR e quatro soldados foram presos e processados por crimes contra a humanidade. "ANR agents have also been implicated in politically motivated human rights violations, particularly of opposition members, journalists and human rights defenders." (UN, 2007b:8).

[49] Em escala reduzida em relação a membros das FARDC e da PNC, agentes da ANR também estão ligados a extorsões com o pretexto de coletar taxas de mineradores e da população em geral. Estas extorsões são geralmente relacionadas a violências e prisões (UN, 2007b).

[50] A falta de treinamento e de sensibilidade com relação aos direitos individuais deve ser qualificada, devido ao fato de que, em uma situação de guerra, como na prática se vive na RDC, qualquer tipo de oposição é vista com temeridade. A despeito da falta de comprometimento com os direitos humanos, o que se deve em grande parte pela falta de controle e de um mandato eficaz, percebe-se que a ANR possui capacidades coercitivas efetivas mesmo em províncias distantes da capital Kinshasa.

[51] As FARDC possuem falta de treinamento, disciplina e são incapazes de realizar, sozinhas, o desarmamento de grupos internos e externos operantes dentro do país. A PNC é mal treinada, não tem equipamentos e é impotente na promoção da segurança pública sem o auxílio externo – como se pôde observar nas eleições presidenciais de 2006. Isto ocorre mesmo após estas forças terem passado por um processo de reforma e de integração de ex-combatentes. Por seu turno, a ANR parece ser "the most professional of the different security services" (UK, 2009:39).

Segurança (SSR).[52] A perpetração de abusos contra os direitos individuais por parte da ANR sustenta a base dos argumentos. Todavia, há limites práticos para que a reforma sugerida não venha a desestabilizar ainda mais as estruturas precárias do Estado congolês.

Haja vista a quantidade e a intensidade de reformas pelas quais as instituições da RDC passaram na última década, pode-se trabalhar com dois pressupostos: (1) o Estado congolês já foi deveras conivente frente às pressões internacionais para reformas que, em muitos casos, eram um afronte à própria soberania estatal; e (2) todas as reformas incentivadas pela comunidade internacional e adotadas pelo Estado congolês estão aquém dos resultados esperados, devido às próprias deficiências intrínsecas dos modelos prescritos e à falta de comprometimento por parte de doadores e governo.

Portanto, questiona-se sobre a possível reforma da inteligência: "qual seria o resultado provável de uma reforma do setor?"; e "até que ponto estas reformas reduziriam, além da autonomia, as próprias capacidades dessa organização no papel de coerção interna?". Uma das respostas mais plausíveis para estes questionamentos assume que tudo dependerá, mormente, do tipo e do grau das reformas. A principal questão é a adoção ou não de um processo de integração das forças combatentes nacionais dentro das estruturas da ANR, assim como no caso das FARDC e da PNC.

Se a posição for negativa (reforma sem integração) trata-se de uma reforma do serviço de inteligência nos padrões comuns atuais. A RAND publicou em 2005 o trabalho mais popular sobre o tema (HANNAH ET alli, 2005), citado como bibliografia básica no documento do governo britânico, e de sua GFN-SSR, A Beginner's Guide to Security Sector Reform (SSR) (UK, 2007). Os autores assumem que o processo ideal de reforma dos serviços de inteligência deveria envolver: a formulação de mandatos claros;[53] a coordenação, a fiscalização e a

[52] O conceito de Reforma do Setor de Segurança (SSR) bebe na fonte da noção de segurança humana. Surgiu em fins dos anos de 1990 mediante o papel proeminente do Departamento de Desenvolvimento Internacional do Reino Unido (DfID, sigla em inglês) (BENDIX e STANLEY, 2008). Nos últimos 15 anos, o conceito tem evoluído por meio de diferentes formulações, como a do Conselho de Segurança da ONU, a da Grã-Bretanha e a da OCDE. Importa que os vários conceitos combinam na percepção normativa de que a RSS deve se dar de maneira holística e equilibrada (sem prioridades), estabelecendo a necessidade do controle democrático e do enxugamento dos gastos das estruturas militares (FONTOURA, 2008).

[53] Um mandato claro serve como primeiro passo para que os serviços de inteligência ajam em conformidade com a legislação doméstica, especialmente quando se trata da qualificação ou da restrição de direitos constitucionais dos cidadãos devido a interesses de segurança do Estado. Ademais, uma base legal auxilia nos reforço de valores democráticos, dá legitimidade às ações dos serviços de inteligência, possibilita a disciplina de agentes e facilita a busca por justiça por parte de vítimas de abusos de poder (HANNAH et alli, 2005).

accountability centrais;[54] a fiscalização jurídica;[55] e a fiscalização e a *accountability* parlamentares.[56] O ciclo de reformas buscaria um padrão mais equilibrado entre agilidade e transparência, conforme proposição de Cepik (2003).

Dentre os exemplos destacados de reformas da inteligência em países em desenvolvimento, pode-se citar o caso da África do Sul, que estabeleceu (1) um mandato para o serviço de inteligência com claras demarcações territoriais entre serviços de inteligência doméstica, criminal e militar; e (2) o controle central baseado no Comitê de Coordenação da Inteligência Nacional (National Intelligence Co-ordinating Committee), acompanhado por Inspetores Gerais que fiscalizam os diretores de cada serviço. O caso da Argentina também é relevante, no sentido de que estabeleceu (1) um mandato claro que mantém uma única agência para inteligência exterior e doméstica; e (2) mecanismos de fiscalização judicial em que juízes são convocados a autorizar mandados de vigilância emitidos pelos serviços de inteligência. Entretanto, nenhum dos casos se mostrou realmente efetivo na prática (HANNAH ET alli, 2005) – o que traz incertezas com relação a resultados no curto-prazo.

No caso congolês, tratar-se-ia inicialmente de estabelecer um mandato mais claro e detalhado para a ANR – superando-se o marco do Decreto-Lei nº 003/2003 –, além de delimitar melhor atividades de inteligência militar, civil, interior e exterior entre os diferentes serviços. Em seguida, importa o estabelecimento de um controle central sobre os serviços, mormente a criação de comitês parlamentares de fiscalização e de bases jurídicas para o julgamento de casos de abusos aos direitos individuais constitucionais.

Por outro lado, se a reforma da inteligência passar por um processo de integração das forças combatentes na Segunda Guerra do Congo e mesmo nos conflitos armados pós-2003 (reforma com integração), o alcance de seu sucesso parece ser ainda mais incerto. A integração de forças internas que desafiam o poder do Estado e o monopólio dos meios de coerção pode gerar (1) uma redução

---

[54] A coordenação e a fiscalização centrais dizem respeito ao comando centralizado das agências nacionais, evitando sobreposição de atividades e a reprodução de rivalidades. O accountability central é a subordinação dos serviços de inteligência ao controle de líderes democraticamente eleitos – o que sugere reformas no próprio tipo de governo no caso de regimes autocráticos ou parcialmente poliárquicos (HANNAH et alli, 2005). A inovação institucional geralmente envolve o estabelecimento de um Inspetor-Geral – com funções de auditoria.

[55] A fiscalização judicial serve como base para estabelecer limites entre a proteção individual de direitos e a coleta de informações necessárias – regulando as atividades de inteligência quando direitos individuais são usurpados mediante meios intrusivos ou buscas encobertas (HANNAH et alli, 2005).

[56] A fiscalização e o accountability parlamentares servem como forma de aprimorar a legitimidade e o controle democrático sobre os serviços de inteligência. Assim, incentiva-se o estabelecimento de serviços comprometidos com objetivos mais amplos do que os interesses políticos dos chefes de governo e de Estado. Geralmente concretizam-se no estabelecimento de comissões parlamentares. Cumpre lembrar que estas não deixam de envolver riscos ao segredo das informações e de uma politização exagerada dos temas de segurança.

imediata das pressões de forças opositoras ao poder central e (2) benefícios técnicos, logísticos e de pessoal com a incorporação das estruturas de inteligência dos diferentes grupos rebeldes. De maneira oposta, pode implicar em maiores complicações para a engenharia institucional dos serviços de inteligência estatais – além dos problemas intrínsecos à adoção de arranjos de *power-sharing*[57] em situações pós-conflitos civis que não foram definidos militarmente.[58]

Finalmente, a opção entre integração e não-integração produz resultados diferenciados no que diz respeito às capacidades coercitivas do Estado. A opção por um processo de reforma sem integração em princípio resultaria no maior controle central sobre o pessoal e a maior coesão dos serviços (mais responsivos aos intentos do presidente) – ao mesmo tempo em que não aumentariam os incentivos para a cooptação pacífica de grupos armados rivais ao Estado. Por seu turno, a opção pela integração pode gerar desafios adicionais ao estabelecimento de esferas coercitivas eficientes. Os casos da PNC e das FARDC são educativos neste sentido.

A reforma das forças policiais começou em 2003 sem um plano estratégico, permanecendo a realização de iniciativas *ad hoc*. Estes processos envolveram o suporte da União Européia (EUPOL); da França, de Angola, da África do Sul, da Grã-Bretanha, e a ONU (MONUC Police) (ICG, 2006). Ademais, o caso da reforma das forças policiais também é exemplo de como um plano de integração de forças beligerantes pode vir ao fracasso logo no início de seu estabelecimento. O plano de integração nacional das forças policiais adotado no Governo Transnacional foi

[57] A teoria consociativa, foca no modelo de democracia consensual – também chamado de regime *power-sharing*, proporcionalista ou consensualista. Trata-se de uma abordagem que mede os efeitos de diferentes tipos institucionais na democracia. Mais especificamente, os contrastes entre regimes *power-sharing* e *power-concentrating*. Os primeiros se caracterizam por conter regras institucionais formais que abrem espaço a um grande número de elites políticas no processo decisório, enquanto que os segundos permitem a inclusão de uma amplitude pequena de atores. Cumpre salientar que democracias consociativas (*power-sharing*) ou majoritárias (*power-concentrating*) são modelos ideais. No mundo real, a maioria das poliarquias é híbrida e se situa em um *continuum* dos dois polos. Pode-se medir a intensidade de um arranjo *power-sharing* pelo número adotado de dimensões que se aproximam do modelo ideal. Além de Lijphart (1969), outros autores foram pioneiros ao tratar do conceito de consociativismo, como Lehmbruch (1967), Steiner (1974), Daalder (1974), McRae (1974). Para abordagens atuais, ver Tsebelis (2002), Lijphart (2008) e Norris (2008).

[58] Donald Horowitz (1993) argumenta que regimes de *power-sharing* institucionalizam clivagens étnicas, reforçando tensões ao invés de acomodar e administrar diferenças. Para Jack Snyder (2000), soluções para conflitos étnicos que tratam identidades pré-democráticas como fixas podem cristalizar identidades nacionais exclusivas e inimigas, bem como divisões já existentes no país. No que concerne às críticas a arranjos de *power-sharing* em sociedades vindas de conflitos civis, afirma-se que arranjos de *power-sharing* impostos por poderes externos são menos prováveis de durar e gerar acordos de paz duráveis (COLLIER, 2005). Na África, ademais, esforços ocidentais para construir acordos de paz de *power-sharing* podem encorajar líderes rebeldes à insurgência em busca de inclusão em acordos semelhantes (TULL & MEHLER, 2005).

abolido em 2004, devido às complicações intrínsecas ao processo,[59] mantendo-se a integração somente nas forças especiais.[60]

Mesmo limitada, a integração das ex-forças combatentes gerou problemas como: a insuficiência de recursos governamentais devido ao aumento do gasto público decorrente da integração das forças[61] e a corrupção em larga escala.[62] Mesmo com alguns sucessos em Kinshasa,[63] as forças policiais permanecem incapazes de prover segurança à população e ao Estado; sua tarefa acaba sendo cumprida com o auxílio de outras forças, como as FARDC. Por outro lado, a tentativa ineficaz das Forças Armadas em compensar nas tarefas policiais desvia seu foco principal de dar cabo aos conflitos armados do leste (LRA e FDLR).

Por seu turno, a SSR das FARDC foi iniciada imediatamente no lançamento do Governo de Transição, com o intuito de sustentar o processo de integração dos ex-grupos beligerantes. A base principal para a reforma ocorreu a partir de auxílios bilaterais. Bélgica e Holanda proveram fundos para a melhora de centros de reagrupamento das FARDC, enquanto que Bélgica, Angola, África do Sul e, posteriormente, a MONUC auxiliaram com treinamento militar (BOSHOFF, 2008; WOLTERS e BOSHOFF, 2006; JANE'S, 2009). Já o processo de integração das forças militares teve duas fases principais. Na primeira fase (2004-2006) a integração iniciou-se como parte de um programa conjunto (Tronc Comum) que englobava, de um lado, a Desmobilização, o Desarmamento e a Reintegração (DDR) de ex-combatentes que quisessem ingressar na vida civil;[64] e, de outro, a integração nas Forças Armadas dos combatentes que preferissem seguir a carreira militar.[65] Como resultado foram desmobilizados 180 mil combatentes, dos quais 130 mil foram reintegrados à vida civil e 50 mil às FARDC. O objetivo principal da primeira fase era desmobilizar os combatentes da Segunda Guerra do Congo e estabelecer a segurança interna para as eleições de 2006. Com os requisitos

---

59 "The integration process proved so complicated, transport so difficult and housing so scarce, however, that in October 2004 the Joint Commission on Security Reform, in which Congolese authorities and donors meet, abandoned national integration and decided to proceed at a local level" (ICG, 2006:6).
60 "Unlike the army, there has been no nationwide integration of the police. There was an effort to integrate the various factions into the specialized units, but not the territorial police. For the latter, the existing police were maintained, and training was decentralized to the provincial level" (ICG, 2006:7).
61 Há pouco envolvimento de doadores na reforma policial (poucos equipamentos e treinamentos limitados).
62 A integração e a falta de comprometimento dos ex-grupos rebeldes com o governo central fazem com que salários não sejam devidamente passados pela cadeia de comando, sendo assim desviados.
63 Em junho de 2005, houve o controle de levantes em Kinshasa devido ao adiamento das eleições. Nesta data foram enviados 2.500 homens da Polícia de Intervenção Rápida e 1.000 da Unidade de Polícia Integrada.
64 O DDR no Congo teve como base legal o Programa Nacional de DDR (PNDDR); como base executora a Comissão Nacional de DDR (CONADER); e como principal mecanismo financiador o fundo Emergency Demobilization and Reintegration Project (EDRP) do Banco Mundial.
65 A integração das Forças Armadas foi administrada pela Structure Militaire d'Intégration (SMI) e financiada pelo governo congolês e por doações bilaterais.

longe de serem alcançados (ainda faltava desmobilizar 70 mil soldados das FAC e 19 mil rebeldes), o processo foi encerrado com o novo mandato de J. Kabila em 2007. Sua segunda fase foi iniciada apenas em 2008, no auge dos conflitos no leste com o CNDP e grupos Mai-Mai. Desta vez houve uma aceleração do processo de integração dos grupos rebeldes nas FARDC, principalmente após o acordo de paz assinado em março de 2009 com o CNDP.

Os pontos negativos do processo são diversos. A integração foi feita sem controle dos que ingressavam nas FARDC ou na PNC; como, por exemplo, a verificação de antecedentes criminais, de violações de direitos humanos ou de perpetração de crimes de guerra (BOSHOFF, 2010). As FARDC foram criadas com base em um acordo de paz vago com relação aos detalhes e à distribuição de poderes no novo exército[66] e sem um critério de distribuição que prezasse pela qualidade das forças.[67] A integração também atrasa, pois, com receio de perder sua força militar, líderes de grupos rebeldes em processo de desmobilização relutam em enviar suas melhores tropas para as novas forças integradas. Por outro lado, estes mesmos líderes lucram com o descontrole do processo de integração e o aumento no número de soldados fantasmas.[68] Se a SSR poderia ser uma esperança para a superação desse quadro, ela falha na falta de coordenação entre doadores internacionais[69] e nos constrangimentos internacionais que bloqueiam que recursos multilaterais sejam direcionados a programas de reestruturação militar.[70] Enquanto doadores apoiam o MONUC com mais de

[66] O DIC falhou em definir princípios e mecanismos adequados para a integração das várias facções combatentes em um exército nacional unificado. Os grupos buscaram manter estruturas de comando suficientemente fracas para que nenhuma facção pudesse sozinha controlá-las – o que resultou em múltiplas estruturas de poder concorrentes. A prioridade foi neutralizar o impacto das milícias e de encerrar o conflito – ao invés de estabelecer as bases para criar forças de segurança genuínas.

[67] O sistema de cotas para a alocação no exército fez com que oficiais qualificados fossem demitidos enquanto que oficiais não-treinados ou treinados em 45 dias adquirissem um cargo. Enquanto que ex-oficiais da FAZ levaram 20 anos para atingir o posto de general, um cidadão armado Mai-Mai chega a este posto em 1 ano.

[68] Os comandantes das ex-forças combatentes inflam seus números e garantem pagamentos para soldados fantasmas (de seus próprios bolsos). Não há números certos do novo exército e o CSE aloca pagamento para um número geralmente superior ao real. Em 2006, a metade dos USD 8 milhões direcionados mensalmente para salários ia para soldados fantasmas (ICG, 2006).

[69] A falta de coordenação entre doadores se deve principalmente às disputas pela liderança do processo. ONU e EUSEC competem, mas não conseguem cooptar efetivamente doadores como Angola, China e África do Sul (BOSHOFF, 2010). A falta de coordenação permite que o Ministério de Defesa duplique pedidos para o mesmo projeto. Outro problema da falta de coordenação entre parceiros bilaterais ocorre no caso do treinamento das forças integradas. Diferentes programas bilaterais de treinamento, pouco coordenados, produzem batalhões heterogêneos e com reduzida interoperatividade.

[70] O Banco Mundial, que coordena o maior fundo de DDR para a RDC, proíbe a utilização de seus recursos para o pagamento de militares ou para a reestruturação de forças armadas. O dispêndio tem de ficar a cargo do governo congolês ou de doadores bilaterais. Relativamente, há muito dinheiro para as pessoas que deixam o exército, mas pouco para os que permanecem em serviço. Assim: "80 per cent of ex-combatants choose demobilization over army integration. As a consequence, brigades have had to be downsized from 3,500 to approximately 2,200" (ICG, 2006:25).

USD 1 bilhão anuais, recusam a possibilidade de fornecer equipamentos básicos para as brigadas integradas e recursos para que se possa oferecer condições decentes de vida e trabalho aos militares. Somente a Bélgica respondeu aos apelos congoleses de fornecimento de melhorias logísticas e de equipamentos. Dessa maneira, sem o suporte logístico do MONUC, as unidades militares congolesas continuam inefetivas.

Apesar das experiências de saldo negativo das FARDC e da PNC, cumpre ressaltar que qualquer opção adotada de reforma pode ter consequências diversas. Dessa forma, ressalta-se que não há sucesso ou fracasso garantido para as diferentes opções disponíveis para a reforma da inteligência congolesa. Sugere-se, apenas, o cuidado redobrado para que esta reforma não contribua para o agravamento da incapacidade coercitiva interna do Estado congolês. Esta precaução poderia se concretizar no estabelecimento de uma reforma da inteligência que priorizasse: (1) um mandato mais claro para a ANR; (2) mecanismos de maior controle democrático e jurídico, principalmente em casos de apreensão a suspeitos de ameaças à segurança estatal; (3) a não-integração ou a integração lenta, gradual e segura de forças congolesas combatentes nos conflitos civis do país. É importante entender que esta integração só deve ocorrer caso haja um projeto bem estruturado, coordenado e amplamente financiado que tenha condições de realizar uma triagem adequada dos combatentes a serem integrados (sem registro de crimes de guerra e abusos a populações civis) e que ofereça treinamento adequado e contínuo a forças integradas. De outro modo, o Estado congolês estará apenas reduzindo ainda mais a sua já escassa capacidade coercitiva interna.

5.8. Considerações Finais

Este trabalho tratou sobre a relação dos serviços de inteligência com o processo de construção do Estado. Analisou o tema no caso africano e congolês, focou nas esferas do Estado desenvolvidas prioritariamente pela trajetória de construção do Estado adotada como padrão (coerção interna), e evidenciou o papel das forças de segurança e dos serviços de inteligência na manutenção desse legado. Pôde-se perceber que o serviço de inteligência na RDC foi historicamente um dos elementos colaboradores para o desenvolvimento da trajetória coercitiva do Estado (nos termos de Charles Tilly). Trata-se, entretanto, de uma coerção voltada para dentro – assim como no caso dos Estados surgidos no século XX.

Todavia, a situação atual da RDC se diferencia desta trajetória padrão, na medida em que o Estado perdeu a maior parte de sua capacidade coercitiva externa e, atualmente, interna – devido, principalmente, à falta de definição militar da Segunda Guerra do Congo e à precariedade das condições das forças

de segurança. Por outro lado, o serviço de inteligência civil do país parece fugir a esta lógica atual, cumprindo o seu papel histórico na coerção interna.

Essa realidade, entretanto, não descarta a necessidade de se estabelecer mecanismos de fiscalização mais eficazes e algum controle democrático sobre os serviços de inteligência atuais. Trata-se de expedientes fundamentais para a redução nos casos de abuso cometidos por agentes e oficiais de inteligência. Entretanto, a adoção desses mecanismos de reforma deve levar em conta, no momento de se definir ao tipo e grau das reformas, os avanços e retrocessos experimentados pelo processo de reforma de organizações como as Forças armadas (FARDC) e policiais (PNC).

A integração de ex-combatentes da Segunda Guerra do Congo nas estruturas das FARDC e da PNC gerou problemas no comando das forças, aprofundando a corrupção em larga escala e o aumento dos gastos do governo. Por outro lado, os processos amplos de SSR são atrasados pela falta de coordenação entre doadores e pelas barreiras internacionais para doações direcionadas a programas ligados a assuntos militares. São estas e outras lições que se deve levar em conta ao projetar um plano de reforma da inteligência para a República Democrática do Congo.

REFERÊNCIAS

AGABA, Andrew; PULKOL, David (2009). "The General Performance and Systems of Intelligence Bodies in the Great Lakes Region". In: SANDY, Africa (Ed.). *Changinng Intelligence Dynamics in Africa*. Londres: GFN-SSR e ASSN, pp. 125-154.

AMNESTY (2007). *Democratic Republic of Cong*o: Disarmament, Demobilization and Reintegration (DDR) and Reform of the Army. Amnesty International. AFR 62/001/2007, 25 January. [http://www.amnesty.org/en/library/asset/AFR62/001/2007/en/bc0c5b7e-d3c4-11dd-8743-d305bea2b2c7/afr620012007en.pdf]. Disponibilidade: 26/09/2011.

BENDIX, Daniel; STANLEY, Ruth (2008). "Security Sector Reform in Africa: The Promise and the Practice of a New Donor Approach". *African Centre for the Constructive Resolution of Disputes. Occasional Paper Series*, vol. 3, nº 2, 2008.

BOSHOFF, Henri (2008). "Security sector reform in the Democratic Republic of Congo: The status of military reform". *Institute for Security Studies: African Security Review* 17.2.

CALLLAGHY, Thomas M. (1984). *The State-Society Struggle*: Zaire in Comparative Perspective. New York: Columbia University Press.

CEPIK, Marco A. C. (2003). *Espionagem e Democracia*: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV.

CHURCH COMMITTEE (2007). "APPENDIX F - The CIA Assassination Plot in the Congo, 1960–61". In: JOHNSON, Loch H. (Ed.). Strategic Intelligence (vol. 3).

Covert Action: Behind the Veils of Secret Foreign Policy. Westport: Praeger Security International, p. 177-191.

COLLIER, Paul; SAMBANIS, Nicholas (Eds.) (2005). *Understanding Civil War*. Washington DC: The World Bank.

DAALDER, Hans (1974). 'The consociational democracy theme. *World Politics*, 26: 604-21.

DE WITTE, Ludo. (2001). *The Assassination of Lumumba*. New York and London: Verso Ed. Verso.

DEVLIN, Larry. (2007). *Chief of Station*, Congo: fighting the cold war in a hot zone. New York: PublicAffairs.

DUNN, Kevin C. (2002). "A Survival Guide to Kinshasa: Lessons of the Father, Passed Down to the Son". In: CLARK, John F. (Ed.). *The African Stakes of Congo War*. New York: Palgrave Macmillan.

FIDH (2009). *République démocratique du Congo* : La dérive autoritaire du regime. Fédération internationale des ligues des droits de l'Homme, n°526f, Juillet [www.fidh.org/IMG/pdf/RDC526fr2009.pdf]. Disponibilidade: 20/08/2010.

FONTOURA, (2008). *Convertendo espadas em espadas*: a ONU e a reforma das Forças Armadas do Timor-Leste. Dissertação de Mestrado. Rio de Janeiro: PUCRJ, PPG-RI.

FR (2006). RDC : les différentes forces en armes depuis 1997. République Française, Commission des Recours de Refugies, CRR-Centre d'information géopolitique. 31 janvier.

GIDDENS, Anthony (1987). *The Nation-State and Violence*. Berkeley: University of California Press.

GLEIJESES, Piero (2003). *Conflicting Missions*: Havana, Washington, and Africa, 1959–1976. Chapel Hill: The University of North Carolina.

HANNAH, Greg; O'BRIEN, Kevin; RATHMELL, Andrew (2005). *Intelligence and Security Legislation for Security Sector Reform*. Technical Report Prepared for the United Kingdom's Security Sector Development Advisory, RAND Europe.

HERBST, Jeffery (2000). *States and Power in Africa*. Princeton: Comparative Lessons in Authority and Control. Princeton: Princeton University Press.

HOCHSCHILD, Adam (1999). *O Fantasma do Rei Leopoldo*: uma história de cobiça, terror e heroísmo na África colonial. São Paulo: Companhia das Letras.

HOROWITZ, Donald L. (1993). "Democracy in Divided Societies". *Journal of Democracy*, 4:18-38.

Human Rights Watch (HRW) (2009). "Question and Answers - Dossier for Hillary Clinton's Visit". 10 August. Publicado em HRW [http://www.hrw.org/en/news/2009/08/10/faq-drc-human-rights-watch-dossier-hillary-clinton-s-visit]. Disponibilidade: 16/07/2010.

IISS (2006). The Military Balance. International Institute for Strategic Studies. London: Routledge.

_____. (2007). The Military Balance. International Institute for Strategic Studies. London: Routledge.

IISS (2008). The Military Balance. International Institute for Strategic Studies. London: Routledge.

_____. (2010). The Military Balance. International Institute for Strategic Studies. London: Routledge.

International Crisis Group (ICG) (2006). Security Sector Reform in the Congo. Africa Report Nº104 – 13 February [http://www.crisisgroup.org/en/regions/africa/central-africa/dr-congo/104-security-sector-reform-in-the-congo.aspx]. Disponibilidade: 20/08/2010.

ISN (2009). Africa: Resisting the Lord's Army. International Security Network. 3 Sep 2009 [http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?lng=en&id=105498]. Disponibilidade: 16/08/2010.

JANE'S (2009). JANE'S World Armies: Democratic Republic of Congo. Acervo do Núcleo de Estratégia e Relações Internacionais (NERINT), Compilação de 2009.

LEHMBRUCH, Gerhard (1967). *Proporzdemokratie*. Politisches System und politische Kultur in der Schweiz und Osterreich. Tubingen: Mohr.

LeoGRANDE, William. (1980). Cuba's Policy in Africa, 1959-1980. Policy Papers in International Affairs, nº 13. Berkeley: University of California.

LIJPHART, Arend (1969). 'Consociational democracy.', World Politics 21: 207-25.

_____. (2008). *Modelos de democracia*. Desempenho e padrões de governo em 36 países. Rio de Janeiro, Civilização Brasileira, 2ª ed.

McCALPIN, Jermaine (2002). "Historicity of a Crisis". In: CLARK, John F. (Ed.). *The African Stakes of Congo War*. New York: Palgrave Macmillan.

MCRAE, Kenneth (ed.) (1974). *Consociational Democracy*: Conflict Accommodation in Segmented Societies. Toronto: McClelland and Stewart.

MEDITZ, Sandra W.; MERRILL, Tim (1993). Zaire: a country study. Washington: Federal Research Division, Library of Congress [http://www.country-data.com/frd/cs/zrtoc.html#zr0212]. Disponibilidade: 20/08/2010.

NORRIS, Pippa (2008). *Driving Democracy*. New York: Cambridge University Press.

NZONGOLA-NTALAJA, Georges (2003). *The Congo from Leopold to Kabila*: A People's History. London and New York: Zed Books.

OMCT (2006). Examen du troisième rapport périodique de la République Démocratique du Congo. Organisation Mondiale contre la Torture. Comité des Droits de l'Homme 86e session, Mars 2006. [http://www.omct.org/files/2005/09/3065/loi_hrc_drcmars_2006.pdf]. Disponibilidade: 26/09/2011.

PRUNIER, Gérard (2009). *Africa's Worls War*. Congo, the Rwandan Genocide and the Making of a Continental Catastrophe. New York: Oxford University Press.

RANSOM, Harry (1958). Central Intelligence and National Security. London: Oxford University Press.

RDC (2003). Décret-Loi nº 003-2003 portant création et organisation de l'Agence nationale de renseignements. 11 janvier [http://www.leganet.cd/Legislation/Droit%20Public/Ordre/DL.11.01.2003.htm]. Disponibilidade: 20/08/2010.

RENO, William (1998). Warlord Politics and African States. Boulder: Lynne Rienner.

SNYDER, Jack (2000). *From Voting to Violence*: Democratization and Nationalist Conflict. New York: W.W. Norton.

_____. (2000). *From Voting to Violence*: Democratization and Nationalist Conflict. New York: W.W. Norton.

STEINER, Jurg (1974). *Amicable Agreement versus Majority Rule*: Conflict Resolution in Switzerland. Chapel Hill: University of North Carolina Press

STRAFOR (2006). *Angola*: Ready to Intervene in the DRC for Kabila 18 de agosto. Publicado em STRATFOR [http://www.stratfor.com/memberships/41075/angola_ready_intervene_drc_kabila]. Disponibilidade: 16/07/2010.

TILLY, Charles (1985). "War Making and State Making as Organized Crime". In: EVANS, Peter; RUESCHMEYER, Dietrich; SKOCPOL, Theda (Eds.). *Bringing the State Back In*. Cambridge: Cambridge University Press.

TILLY, Charles (1996). *Coerção, capital e estados europeus*. São Paulo: Edusp.

TSEBELIS, George (2002). *Veto Players*. How Political Institutions Work. Princeton, NJ: Princeton University Press.

TULL, Denis; MEHLER, Andreas (2005). The hidden costs of power-sharing: reproducing insurgent violence in Africa, *African Affairs*, 104, 416, p. 375-98.

TURNER, Thomas (2007). *Congo Wars*: conflict, myth and reality. London: Zed Books.

Twentieth Century Atlas (TCA) (2010). Death Tolls for the Major Wars and Atrocities of the Twentieth Century. [http://users.erols.com/mwhite28/warstat2.htm]. Disponibilidade: 16/07/2010.

UK (2007). A Beginner's Guide to Security Sector Reform. GFN-SSR Global Facilitation Network for Security Sector Reform. OECD.

UK (2009). Country of Origin Information Report: The Democratic Republic of Congo. United Kingdom Border Agency: Country of Origin Information Service. 30 June.

UN (2007a). The Human Rights Situation in the Democratic Republic of Congo (DRC): During the period of July to December 2006. Human Rights Division, Office of the United Nations, High Commissioner for Human Rights. MONUC Report: 8 February 2007

UN (2007b). The Human Rights Situation in the Democratic Republic of Congo (DRC) During the period January to June 2007. Human Rights Division, Office of the United Nations, High Commissioner for Human Rights. MONUC Report: 27 September 2007.

USA (2009). 2009 Human Rights Report: Democratic Republic of the Congo. Bureau of Democracy, Human Rights, and Labor, 2009 Country Reports on Human Rights Practices. Washington: Department of the State, March 11 [http://www.state.gov/g/drl/rls/hrrpt/2009/af/135947.htm]. Disponibilidade: 20/08/2010.

VISENTINI, P. F. (2007). "A África Independente e a Guerra Fria". VISENTINI, Paulo Fagundes; RIBEIRO, Luis Dario; PEREIRA, Analucia Danilevicz. *Breve História da África*. Porto Alegre: Leitura XXI.

_____. (2010). A *África Moderna*. Porto Alegre: Leitura XXI, 2010.

WALTERS, Stephanie; BOSHOFF, Henri (2006). Slow military reform and the transition process in the Democratic Republic of the Congo. Institute for Security Studies: *African Security Review*, 15.2.

WB (2009). DDR in the Democratic Republic of Congo Program Update. World Bank, September [www.mdrp.org/PDFs/DRC_Program_Update.pdf Disponibilidade: 20/08/2010.

WB (2009). DDR in the Democratic Republic of Congo: Program Update. World Bank Multi-Country Demobilization and Reintegration Program (MDRP), September. [http://www.mdrp.org/PDFs/DRC_Program_Update.pdf]. Disponibilidade: 26/09/2011.

WEBER, Max (1991). *Economia e sociedade*: fundamentos da sociologia compreensiva. Vol. 1. Brasília: UnB.

WESTAD, Odd Arne (2006). *The Global Cold War*: Third world interventions and the making of our times. Cambridge, Cambridge University Press.

WILSON, P. (2005). "The Contribution of Intelligence Services to Security Sector Reform". Conflict, Security and Development, 5:1 April.

_____. (2005), 'The contribution of intelligence services to security sector reform', Conflict, Security and Development, Volume 5, Number 1, pp. 87-107(21).

YOUNG, Crawford; TURNER, Thomas (1985). *The Rise and Decline of the Zairian State*. Madison: The University of Wisconsin Press.

PARTE II

DESAFIOS CONTEMPORÂNEOS

Capítulo 6

INTELIGÊNCIA E OPERAÇÕES DE PAZ DA ONU NO PÓS-GUERRA FRIA

Nathaly Silva Xavier

A Organização das Nações Unidas coordena, atualmente, dezessete operações de paz espalhadas pelo mundo, envolvendo civis e militares de mais de cem países: uma na América, oito na África e oito na Ásia.[1] A importância dessas operações para o sistema internacional, tendo em vista tanto os reflexos na política externa dos países integrantes da missão quanto daqueles que, por algum motivo, têm interesses no desenvolvimento/retrocesso do conflito, bem como os impactos na região em questão, é, praticamente, incontestável. Assim como em grande parte dos objetos de estudo no campo das relações internacionais, muitos são os vieses e as perspectivas que podem ser adotadas para analisar essas operações de paz, desde análises mais jurídicas, que consideram os aspectos normativos do problema, até investigações mais políticas, centradas nas causas e consequências da intervenção. Nesse trabalho, por nos concentrarmos em uma questão específica das operações de paz, a saber, o uso da inteligência, faremos uma abordagem mais conceitual e técnica, não entrando especificamente nos aspectos mais políticos de contextualização, tampouco nos detendo em análises mais profundas de casos específicos.

A investigação do papel da inteligência nas relações entre os Estados, por sua vez, é de grande valia para a compreensão do desenvolvimento do sistema internacional, especialmente nas análises históricas.[2] A utilização da inteligência por organismos internacionais, nesse caso, a Organização das Nações Unidas, todavia, nem sempre é considerada nas análises sobre o tema. Essa lacuna é fruto de uma problemática maior, que envolve a própria utilização da inteligência

[1] Dados segundo sítio da ONU, acessado em 22/11/2009.

[2] Embora a ONU não utilize o termo inteligência nos seus documentos e relatórios, entendemos que esse é o termo mais adequado e que, portanto, será empregado ao longo do trabalho, mesmo quando nos documentos o termo original seja informação.

nessas organizações. Tal restrição deve-se, em grande medida, ao temor dos Estados em relação à delegação de parte de sua soberania, o que reflete, como veremos mais adiante, na baixa institucionalização das atividades de inteligência em organizações internacionais, restringindo, assim, as fontes de análise para a academia.

As dificuldades para o desenvolvimento de pesquisas sobre o emprego de atividades de inteligência nas organizações internacionais, contudo, não impede que elas sejam feitas. Nosso intuito é, então, ainda que trabalhando com restrições bibliográficas e considerando que grande parte da produção que é feita traz uma visão bastante centrada nos Estados Unidos, desenvolver uma breve síntese sobre a relação entre as atividades de inteligência e as operações de paz conduzidas pela Organização das Nações Unidas, visando a contribuir para a área de estudos.

Partimos do pressuposto de que houve mudanças significativas no perfil das operações de paz conduzidas pelas Nações Unidas com o final da Guerra Fria, e que tal mudança também refletiu na importância e necessidade da utilização da inteligência nessas missões. O objetivo do trabalho é avaliar a evolução das atividades de inteligência desenvolvidas na Organização das Nações Unidas para as operações de manutenção da paz a partir da década de noventa. Para isso, analisaremos tanto as funções quanto os órgãos e departamentos envolvidos, além de tratar brevemente de alguns casos empíricos. Valer-nos-emos, principalmente, de uma revisão da bibliografia e da investigação de documentos e relatórios produzidos pela Organização das Nações Unidas.

O artigo está dividido em quatro seções, além das considerações iniciais e finais. A primeira parte é dedicada a uma conceituação preliminar sobre as definições de inteligência e operações de paz, com o intuito de delimitar de maneira mais precisa o objeto de estudo. Na segunda parte, analisaremos as principais funções que as atividades de inteligência podem desenvolver nas operações de paz, em especial, aquelas que a diferenciam da inteligência tradicionais. A terceira parte versará sobre as atividades de inteligência desenvolvidas no âmbito da Organização das Nações Unidas, abordando tanto a estrutura institucional envolvida, quanto as principais fontes utilizadas. Por fim, trataremos brevemente de alguns exemplos empíricos, quais sejam, o da Bósnia, o da Somália e o do Haiti, visando a ilustrar o desenvolvimento da inteligência nas operações de paz das Nações Unidas.

6.1. Conceituação das Atividades de Inteligência e a ONU

A análise de temas que envolvem inteligência já é bastante delicada, tendo em vista que há divergências sobre esse conceito. Relacionar inteligência com operações de paz multiplica essa dificuldade, pois também em relação a

essa definição não há um consenso. Faz-se necessário, então, iniciarmos nosso trabalho por uma definição mais clara dos nossos objetos de estudo, ou seja, o que entendemos por inteligência e por operações de paz.

A atividade de inteligência envolve diversas ações e, consequentemente, é de difícil conceituação. Grande parte das tentativas de definição do conceito ou adotam um abordagem ampla demais, englobando qualquer tipo de coleta e interpretação de informações, ou restringem excessivamente, considerando inteligência apenas as atividades de espionagem. Em uma tentativa de fugir dessa dicotomia, Cepik (2003) considera a dupla dimensão do conceito de inteligência, a operacional e a analítica. Nas palavras do autor:

> Enquanto a primeira dimensão destaca os meios especiais utilizados para coletar informações sem a cooperação e/ou conhecimento de um adversário, essa segunda dimensão é analítica e diz basicamente que a inteligência se diferencia da mera informação por sua capacidade explicativa e/ou preditiva (CEPIK, 2003:28).

Consoante o autor, podemos avançar nessa definição, diferenciando, nessas duas dimensões, o que separa uma atividade de inteligência das demais. No que tange à dimensão operacional, podemos identificar uma atividade de inteligência através do grau de intervenção humana necessário para a análise e disseminação, e da vulnerabilidade das fontes de informação em relação às contramedidas. Em relação à dimensão analítica, a diferença está nos objetivos da análise: as análises de inteligência visam a aumentar o conhecimento sobre o inimigo e sobre questões específicas que dizem respeito à segurança estatal e nacional. (CEPIK, 2003).

Partindo dessa definição inicial, entendemos inteligência com uma atividade acessória, que otimiza a tomada de decisão. Assim, como lembra Warner (2009), a atividade de inteligência fornece uma "vantagem decisória", ou seja, é um recurso utilizado pelo agente decisório que pode melhorar a sua capacidade de percepção da situação em questão. No caso das operações de paz, podemos considerar a inteligência como um fator de auxílio para as forças de paz tanto no conhecimento da situação da região a ser ocupada, quanto na antecipação de acontecimentos que podem oferecer risco às tropas.

A definição de operações de paz, mais especificamente daquelas comandadas pela Organização das Nações Unidas (ONU), também é controversa. A própria Carta da ONU não prevê explicitamente a criação de missões de paz. O estabelecimento de operações de paz pelo Conselho de Segurança da ONU é baseado nos denominados implied powers, ou poderes implícitos, e ancora-se no Artigo 24 da Carta da ONU, que destina ao Conselho a função de principal responsável pela manutenção da paz e da segurança internacionais, bem como no Artigo 42, que versa sobre utilização de forças aéreas, terrestres e navais dos

Membros das Nações Unidas com o fim de manter ou restabelecer a paz e a segurança internacionais.[3]

Tendo em vista a ausência de um fundamento jurídico específico, a definição de operação de paz torna-se mais complexa. Inicialmente, é preciso distinguir os diversos tipos de operações desenvolvidas pela ONU com o intuito de estabelecer e/ou manter a paz. Em um documento de 2008, conhecido como "Capstone Doctrine", o Departamento de Operações de Paz da ONU (DPKO) estabelece os princípios e diretrizes que guiam as missões de paz conduzidas pela Organização. Nele, são diferenciados cinco tipos operações: de prevenção de conflito (*conflict prevention*), de promoção da paz (*peacemaking*), de manutenção da paz (*peacekeeping*), de imposição da paz (*peace enforcement*) e de construção da paz (*peacebulding*). Embora bastante semelhantes, essas ações diferem-se, especialmente, pelo momento em que são implantadas. Enquanto as operações de promoção e de imposição da paz dão-se, principalmente, quando o conflito ainda está ocorrendo, as operações de manutenção e construção da paz iniciam-se após o final do conflito. Evidentemente, as missões não ocorrem de maneira linear, tampouco o início de uma pressupõe o fim de outra; ao contrário, é bastante comum que elas coexistam, especialmente no caso das operações de construção e manutenção da paz.

O presente trabalho visa a analisar as operações de manutenção da paz, definidas como ações com o intuito de preservar a paz, ainda que frágil, após o confronto já ter sido cessado, e auxiliar as forças de promoção da paz na implementação de acordos. Tais operações podem envolver o uso da força no nível tático, principalmente em situações nas quais o Estado não consegue garantir a segurança e a ordem pública. (ONU, 2008).

O final da Guerra Fria traz grandes alterações para o sistema internacional, e esse novo contexto reflete-se no papel das operações de paz.[4] Os principais conflitos passam a ser internos e não mais internacionais, e as missões de paz da ONU ganham um caráter multidimensional.[5] Para Charters (1999), algumas características específicas diferenciam a "segunda geração" de operações de paz, em contraste com as tradicionais. Em primeiro lugar, nem sempre a paz

[3] Os *implied powers* são prerrogativas que não estão previstas de maneira explícita na Carta da ONU, mas que podem ser extraídas da interpretação do texto literal. A Corte Internacional de Justiça reconheceu a doutrina dos implied powers em 1949, quando da decisão do caso "Reparation", estabelecendo que a ONU poderia valer-se de poderes que, ainda que não conferidos explicitamente, fossem necessários para garantia da manutenção dos seus princípios e deveres.

[4] A partir de agora, utilizaremos o termo "operações de paz" para nos referirmos às operações de manutenção de paz. Para citar outras operações, nos valeremos do termo completo.

[5] Segundo Jakobsen (2000), o pós-Guerra Fria trouxe a necessidade da ONU atuar na "zona cinzenta", avançando em operações que não contam com o consentimento total das partes e que situam-se entre as operações de manutenção de paz e as de imposição da paz.

já está estabelecida.[6] Em segundo, não há, em todos os casos, o consentimento das partes para a presença das forças internacionais. Deriva, em certa medida, dessa segunda característica, a não concordância de algumas forças políticas com a neutralidade das forças de paz, e a consequente oposição a sua presença; surge, então, a necessidade das forças de paz de utilizarem a força não só para restabelecer a paz, mas também para sua autoproteção.[7] Uma quarta característica é a manutenção das missões de paz por um longo período, mesmo após o estabelecimento supostamente definitivo da paz. Por fim, as operações de paz de "Segunda Geração" diferenciam-se das tradicionais pela composição múltipla, que inclui membros de organizações não-governamentais (ONGs), observadores civis, e mediadores, não se restringindo às forças exclusivamente militares.

São as operações de paz desenvolvidas no pós-Guerra Fria, ou operações de "Segunda Geração", que serão nosso objeto de estudo nesse trabalho. Essas missões, segundo a ONU (2008:23), têm como funções centrais:

- criar um ambiente estável e seguro enquanto fortalece a capacidade do Estado de prover segurança, de acordo com o Estado de direito e os direitos humanos;
- facilitar o processo político pela promoção do diálogo e da reconciliação e sustentar o estabelecimento de instituições de governança legítimas e efetivas;
- fornecer uma estrutura para que toda a ONU e demais atores internacionais exerçam suas atividades no país de forma coerente e coordenada.

Tendo por base esse contexto, analisaremos, então, o papel da inteligência nessas operações comandadas pela ONU, verificando em que medida essas atividades de inteligência podem auxiliar no cumprimento mais efetivo de tais funções.

6.2. O Papel da Inteligência nas Operações de Paz

As dificuldades do emprego da inteligência nas operações de paz da ONU podem ser sintetizadas em três grandes problemas. O primeiro, e o mais debatido, é o dilema entre a ética da instituição, devido aos meios questionáveis pela qual as informações são obtidas, e o cumprimento de seus fins pacíficos, o que pode ser garantido com o uso dessas informações. Tal fato é agravado pela

[6] Nesse caso, a diferenciação apresentada no documento da ONU, minimizaria esse contraste, já que as operações de manutenção da paz são, muitas vezes, desenvolvidas com as de construção da paz.
[7] Boyd (1996) afirma que os principais motivadores, e também o principal destino dos recursos, do uso de inteligência nas operações de paz são as questões de segurança dos *peacekeepers*.

inexistência, na esfera do direito internacional, de algum tipo de regulamentação acerca da legalidade e da legitimidade da atividade de inteligência no âmbito internacional. Um segundo problema, comum às atividades de inteligência estatais, é a gestão do componente de inteligência nas atividades de comando, controle e comunicação, o C³I.[8] Por fim, temos a característica plural das forças de paz; por serem forças integradas por diferentes nacionais, unem contingentes treinados das mais diversas formas, o que agrava o problema de comando e controle citado anteriormente.

O papel da inteligência nas operações de paz, nada obstante as dificuldades já apresentadas, torna-se ainda mais relevante no pós-Guerra Fria; de acordo com Dorn (1999), o espectro de atividades mais amplo dessas operações aumenta também a necessidade da atuação em segredo, como no caso de inspeções surpresa para a verificação de armamentos e de interceptação de atividades clandestinas. Smith (1994) compartilha a posição de Dorn (1999), afirmando que o uso da inteligência nas operações de paz não só pode ser decisivo para o sucesso da missão, mas também para garantir a segurança dos agentes da ONU. Willians (1993) ainda ressalta que a inteligência permite uma monitoração mais efetiva das áreas problemáticas e do cumprimento dos acordos.

Em um primeiro momento, faz-se necessário ressaltar que as atividades de inteligência nas operações de paz têm algumas características específicas, que as diferenciam das atividades de inteligência tradicionais. A utilização de inteligência humana (HUMINT) de maneira bastante expressiva, em uma proporção maior comparativamente, por exemplo, à coleta de imagens ou interceptação de sinais é um fator que caracteriza a inteligência nas operações de paz (BOYD, 1996; BOATNER, 2000). Outro fator de diferenciação é a defesa do compartilhamento das informações, o que, no nível da disseminação, contrasta com o segredo e as classificações bastante restritas dos documentos de inteligência nacionais; temos, ainda, a finalidade coletiva das atividades de inteligência nas operações de paz, uma vez que se trata de um problema internacional (SMITH, 1994).[9]

É possível dividir as atividades de inteligência em três grandes grupos, o estratégico, o operacional, e o tático. No nível estratégico, a inteligência serve a diversos fins: a identificação e compreensão da situação política, militar e sócio-econômica da região, incluindo as forças e as causas do conflito; o conhecimento geográfico da área e da infra-estrutura (estradas, portos, hospitais, etc.); e os objetivos da comunidade internacional (SMITH, 1994; CHARTERS, 1999).

[8] Os problemas do C³I são tratados por George Orr, no trabalho Combat Operations C³I: Fundamentals and Interactions. Maxwell Air Force Base, Alabama: Air University Press,1983.

[9] Dorn (1999) afirma que um dos problemas do segredo na ONU não é propriamente a classificação, que existe (restrito, confidencial, secreto e top secret), mas sim os procedimentos de desclassificação, às vezes excessivamente criteriosos, outras vezes muito frágeis.

As atividades no nível estratégico são desempenhadas nos escritórios da ONU em Nova Iorque, especialmente nos órgãos ligados à Secretaria Geral e ao Conselho de Segurança (JOHNSTON, 2003). São essas informações, segundo Williams (1993), que condicionam a eficiência das decisões tomadas pelas forças da ONU, inclusive nos níveis mais altos; nesse caso, o Conselho de Segurança. Evidentemente, a obtenção dessas informações atende diretamente às funções centrais das operações de paz citadas anteriormente.

O nível operacional está bastante interligado com o nível estratégico, e, portanto, compartilha algumas atividades. Entre as principais ações no nível operacional estão: o conhecimento das forças do conflito, incluindo seus objetivos e sua capacidade militar; a disposição das populações vulneráveis; e a função e presença de atores internacionais na região, como ONGs e diplomatas (CHARTERS, 1999). O nível operacional desenvolve-se, essencialmente, na estrutura das operações de paz em cada região. De acordo com Johnston (2003), é nesse nível que estão as maiores fraquezas da ONU, já que a falta de estruturas permanentes torna o uso das atividades de inteligência dependente da definição de prioridades do comando da missão em questão. Esse problema foi minimizado com a criação das Células de Análise de Missões Conjuntas (JMACs), como veremos mais adiante. A utilização da inteligência no nível operacional, assim, está mais relacionada com a terceira das funções das operações de paz.

Se no nível estratégico as atividades de inteligência podem, e devem, ser iniciadas antes das operações de paz, no que tange o nível tático, a inteligência está mais relacionada à ação das tropas propriamente dita e tem um caráter mais contemporâneo à presença da ONU na região. São desenvolvidas, nesse nível, ações que visam a identificar possíveis atos de insurgentes, venda de armamentos e drogas, bem como o desenvolvimento de rivalidades locais, sejam elas estritamente políticas ou envolvam também questões militares (CHARTERS, 1999). É bastante comum que nesse nível, não se perceba uma maior necessidade de desenvolvimento de inteligência própria das Nações Unidas, já que as próprias tropas, cedidas pelos países membros, geralmente contam com unidades de inteligência (JOHNSTON, 2003). Ainda no nível tático, a inteligência garante uma maior segurança das tropas, o que não só é vital para o sucesso da operação, mas também garante maior confiança nas ações da Organização. Isso pode refletir em maior participação dos países com o envio de contingente (WILLIAMS, 1993). Identificamos, desta forma, uma relação entre as atividades de inteligência no nível tático com a primeira função das operações de paz.

Estabelecidas as principais funções que as atividades de inteligência podem desenvolver em operações de paz conduzidas pela ONU, fica bastante

clara a importância da sua utilização. Não nos parece, assim, que o emprego da inteligência nas missões da ONU possa simplesmente ser descartado devido ao dilema apresentado no início do trabalho. Surge, então, uma nova questão: como e em que medida a ONU já utiliza a inteligência nas suas operações de paz?

6.3. As Demais Atividades de Inteligência no Âmbito da ONU

São diversos os órgãos do Sistema ONU que, em maior ou menor medida, estão envolvidos nos diversos tipos de operações de paz e nas atividades de coleta e análise de informações. Entre eles, os quatro principais, todos diretamente subordinados à Secretaria Geral, são: o já citado Departamento de Operações de Paz (DPKO); o Departamento de Suporte (DFS); o Departamento de Assuntos Políticos (DPA); e o Escritório para Coordenação de Questões Humanitárias (OCHA).

Inicialmente, é importante destacar que as operações de paz, a despeito de terem necessidades informacionais específicas, compartilham, segundo Ekpe (2007), duas grandes características comuns, as quais geram a necessidade de dados específicos para o planejamento da missão: o impacto da ONU como uma terceira parte no processo político em desenvolvimento na região; e os riscos aos quais os "capacetes azuis" submetem-se. Dentro do DPKO, dois órgãos nos interessam em especial, o Situation Centre e o Escritório de Assuntos Militares (OMA). O marco no uso de inteligência nas operações de paz da ONU é a criação do Situation Centre em 1993. Segundo Charters (1999), o Situation Centre surge em um contexto de aumento das críticas em relação às operações de paz da ONU, inclusive por parte dos participantes das missões, como foi o caso do comandante da missão na Bósnia (UNPROFOR). O Situation Centre, segundo a Organização, é fruto da própria expansão do espectro de atividade das operações de paz, o que gerou maior necessidade de um fluxo constante de informações.

O Situation Centre possui seis grandes funções: (1) Atuar como um ponto de contato entre os escritórios da ONU e as missões de paz espalhadas pelo mundo, mantendo comunicação em tempo integral, vinte e quatro horas por dia, sete dias por semana; (2) Monitorar as áreas nas quais estão presentes as missões, especialmente situações que podem significar algum risco para as tropas da ONU; (3) Coletar e analisar informações, recebendo relatórios diários das operações de paz e emitindo, com a mesma frequência, relatórios para os escritórios da ONU sobre a situação das missões; (4) Notificar os Estados Membros sobre problemas com seus nacionais presentes nas operações; (5) Gerenciar a resolução de crises iniciadas em território de operações, coordenando o trabalho da "Célula de Crise"; (6) Controlar, juntamente com os comandos das operações, os possíveis problemas de segurança para o contingente em missão.

O Situation Centre conta com uma célula de pesquisa e informação que se ocupa, basicamente, de processar, de maneira sistemática, as informações oriundas das missões, juntamente com aquelas obtidas por outras fontes (SMITH, 1994). Faz parte do Situation Centre, ainda, um Centro de Crise, responsável pelo gerenciamento no caso da necessidade de implementação de uma missão de emergência (EKPE, 2007).

O OMA tem uma estrutura bastante extensa, e antes da reestruturação sofrida pelo DPKO em 2007 era a Divisão Militar. Dentre as estruturas internas, nos interessa em especial o Escritório do Consultor Militar e, notadamente, o seu Serviço de Planejamento Militar (MPS). O MPS, por sua vez, tem como função central a implementação dos aspectos militares de operações de paz. Para isso, faz o trabalho de coleta e análise de informações, em especial de zonas de conflito que podem ser alvos potenciais de futuras operações de paz. Sua atuação é maior no setor operacional e tático, com a produção de planos operacionais para a missão em campo (EKPE, 2007).

O DFS foi criado em março de 2007 em um processo de reestruturação do DPKO. Esse novo departamento acumulou funções antes exercidas pelo Escritório de Suporte de Missão do DPKO e pelo Departamento de Gerenciamento. Assim como acontece nos serviços de inteligência nacional, os setores de Suporte e Planejamento, via de regra, também desenvolvem atividades de inteligência. Mesmo sendo um Departamento independente, o DFS trabalha em forte cooperação com o DPKO, especialmente no que tange à Divisão de Suporte Logístico (ONU, 2007). A criação do DFS pode significar um avanço na produção de inteligência pela ONU, especialmente no setor operacional. Já a Divisão de Suporte Logístico conta com o Serviço de Suporte Operacional, o qual desenvolve funções como planejamento de operações e o estabelecimento de diretrizes sobre procedimentos e conceitos concernentes às atividades de suporte nas operações de paz.

O DPA tem a função de informar a Secretaria Geral sobre supostas ameaças à paz e à segurança; ele é dividido geograficamente, contando com quatro divisões: duas para África, uma para Ásia e uma para América e Europa. Além das divisões geográficas, atualmente, o DPA também possui uma divisão para a Palestina e uma unidade para a descolonização. Vale ressaltar que as atividades do DPA, como lembra Ekpe (2007), se alteram ao longo do tempo, de acordo com as mudanças no sistema internacional. Após 1991, os principais temas com os quais o DPA ocupa-se são a diplomacia preventiva e o terrorismo. Devido a esse enfoque, muitas vezes as missões do DPA em determinadas regiões são seguidas pelo estabelecimento de uma operação de paz, como foi o caso do Sudão.

O OCHA é responsável, entre outras coisas, por estabelecer e coordenar operações de ajuda humanitária emergenciais. Para isso, ele conta com o Sistema de Alerta Humanitário Antecipado (HEWS), que, através da análise de indicadores e da avaliação de tendências, mantém uma grande base de informações sobre a situação em regiões sensíveis, aumentando, assim, a eficiência da ONU na detecção de crises humanitárias. O HEWS possui uma unidade de suporte com um sistema de informação geográfica e de informações de campo, e compartilha informações relevantes com outros departamentos da ONU, como o DPKO (EKPE, 2007). O OCHA também possui um departamento de informações e um de análise política, subordinados ao Escritório de Nova Iorque.

Fora do âmbito da Secretaria Geral, cabe ainda destacar as denominadas Missões de Reconhecimento (Fact-Finding Missions). As Missões de Reconhecimento são "atividades designadas para obter conhecimentos detalhados de fatos relevantes de qualquer disputa ou situação, dos quais os órgãos competentes da ONU necessitem para exercer efetivamente suas funções em relação à manutenção da paz e da segurança internacional".[10] (ONU, 1991: 290-1). Segundo Ekpe (2007), as Missões de Reconhecimento, dependendo dos seus objetivos, podem fornecer uma vasta gama de informações, como a natureza do conflito, o nível de escalada militar e as condições socioeconômicas da região. Nada obstante tais operações sejam de grande utilidade como fornecedoras de informações que auxiliam no processo de tomada de decisão dos órgãos da ONU, deve-se destacar o fato de que elas só são desenvolvidas com o consentimento do Estado. Essa necessidade de consentimento, e o fato de ser uma missão aberta, podem, em certa medida, dificultar a coleta de informações ou, até mesmo, em uma situação extrema, impedir a realização da missão por proibição do Estado em questão. Ainda assim, as Missões de Reconhecimento constituem uma importante fonte de geração de inteligência para as operações de paz da ONU.

Depois da criação do Situation Centre em 1993, ocorrida no âmbito das reformas nas operações de paz originadas pelo documento "Uma Agenda para Paz" (1992) de Boutros Boutros-Ghali, uma nova reestruturação da gestão das operações de paz ocorreu em 2000, por meio do que ficou conhecido como Brahimi Report.[11] O Brahimi Report faz recomendações expressas no que concerne à utilização de inteligência, tanto nos níveis estratégico e tático, quanto no operacional (MACEDA, 2007). Segundo Chesterman (2009), tal documento abordou os problemas de inteligência em dois sentidos: primeiro, ao declarar a necessidade de utilização de inteligência em operações de paz para defender-se

[10] As Missões de Reconhecimento podem ser requisitadas tanto pela Secretaria Geral quanto pelo Conselho de Segurança e pela Assembleia Geral, ancoradas na função compartilhada pelos três órgãos, e estabelecida na Carta, de manter a segurança e a paz internacionais.

[11] O documento é um Report do Secretário Geral para a Assembleia Geral e o Conselho de Segurança.

de "desafiadores violentos"; segundo, ao reconhecer a ausência de um sistema e de um corpo profissional capaz de gerenciar as informações sobre a zona de conflito, dando conta do ciclo de inteligência (coletar, analisar, disseminar). Além de outras considerações e recomendações sobre o DPKO, como a utilização dos recursos mais modernos de sistemas de informação, que deveriam ser empregados no planejamento e implementação das missões, o Report também trata de algumas reformas nos demais órgãos envolvidos nas operações de paz, tratados anteriormente, como o DPA e o OCHA (ONU, 2000).

É no contexto dessas reformas e ampliações do DPKO, frutos do Brahimi Report, que são instituídas as Células de Análise de Missões Conjuntas (JMACs).[12] As JMACs são estruturas *ad hoc*, criadas dentro da estrutura específica da operação de paz, que visam a preencher a lacuna da inteligência no nível operacional, que, como vimos anteriormente, é um dos mais problemáticos nas atividades da ONU. As JMACs possuem equipes que acompanham o caráter multidimensional das operações de "segunda geração", incluindo especialistas das mais diversas áreas, como direitos humanos, desenvolvimento socioeconômico e segurança (SHETLER-JONES, 2008). Essas células remetem-se diretamente ao Representante Especial do Secretário-Geral na missão, produzindo relatórios e outros subsídios para o comando da missão. Assim, as JMACs são responsáveis por todo o ciclo de inteligência desenvolvido no âmbito da operação de paz, acumulando as funções de coleta, coordenação, análise e disseminação das informações civis e militares da missão, garantindo um maior suporte para o processo de tomada de decisão (MACEDA, 2007).

De maneira mais específica, consoante Maceda (2007:53), tais Células têm as seguintes funções: (1) prover análises relevantes e atuais para o Representante Especial do Secretário-Geral e sua equipe; (2) monitorar, em conjunto com as células de operação e informação de segurança, ameaças e perigos iminentes; (3) estabelecer um ponto focal para toda a informação; (4) coletar informações e criar uma base de dados permanente; (5) prover análises de eventos e seus desenvolvimentos, no curto e no longo prazo, em resposta às necessidades do Representante Especial e demais membros da missão; (6) prover análises de riscos e ameaças, bem como aconselhar para a minimização do risco; (7) produzir documentos e avaliações orais e disseminá-los como julgar apropriado; (8) fazer a ligação com outras operações de paz próximas, objetivando uma maior coordenação e compartilhamento de informações relevantes; (9) coordenar encontros e grupos de trabalho para estimular o input de informações para todos os componentes da missão, assim como outros órgãos da ONU;

[12] A recomendação do Report era a criação de uma Secretaria de Análise Estratégica e Cooperação, no âmbito do Comitê Executivo para Paz e Segurança (ECPS). A criação, contudo, falhou por motivos políticos, em especial a preocupação de alguns países com o fato de a ONU desenvolver um serviço próprio de inteligência (MACEDA, 2007; CHESTERMAN, 2009).

(10) integrar análises e estimativas de ameaças produzidas pelas células de operação e informação de segurança.

Consoante Shetler-Jones (2008), as JMACs contribuem para uma integração mais eficiente das missões, tanto no planejamento das operações, quanto no comando da missão e na coleta de informações. No nível do planejamento, as JMACs, por serem constituídas de equipes multidisciplinares, podem promover uma harmonização das percepções, unindo as visões de trabalho em um núcleo mais condensado. As possíveis contribuições para o comando da missão são uma questão mais delicada, já que irá depender fortemente da postura do Representante Especial do Secretário-Geral em relação à própria JMACs. É preciso que o Representante Especial atue de forma conjunta com a coordenação da Célula, em um processo de deliberação que vise a uma definição mais precisa dos temas e problemas centrais da operação em questão. Os avanços no setor da coleta que as JMACs podem representar são mais evidentes, se levarmos em consideração que o processo de coleta de informações efetuado pelo *staff* da Célula, como vimos anteriormente nas suas funções, pode envolver a participação de outros órgãos e departamentos da ONU, tanto requisitando informações, quanto compartilhando-as.

Considerando as operações de paz em desenvolvimento atualmente, existem JMACs em nove das dezessete missões, um número bastante expressivo se considerarmos que a implantação das Células é um fenômeno relativamente recente (SHETLER-JONES, 2008). Segundo Maceda (2007), o sucesso considerável da implantação das JMACs deu-se não só pela necessidade latente de um desenvolvimento da atividade de inteligência no nível operacional, como também pela percepção dos Estados de que elas não afetam as suas soberanias, já que suas atuações são restritas às áreas das missões.

Estabelecidos os órgãos responsáveis pela inteligência na ONU, cabe, ainda, uma breve investigação das principais fontes. Vale fazer a ressalva de que, por julgarmos que facilitaria a compreensão, ao apresentarmos primeiro os órgãos da ONU e as suas atuações, e após as fontes de inteligência, invertemos o ciclo de inteligência, tratando antes do processo de análise e disseminação e, em seguida, do processo de coleta e processamento. Da mesma forma que dividimos as funções de inteligência em três níveis, também é possível utilizar essa divisão para analisar a maior ou menor importância de determinadas fontes em cada nível de inteligência. Fazendo uma releitura da divisão efetuada por Charters (1999), podemos identificar oito grandes grupos de fontes, as quais têm sua relevância variada de acordo com o nível de inteligência: as fontes abertas (OSINT); as fontes humanas (HUMINT); as fontes de imagens (IMINT); as fontes de sinais (SIGINT); o reconhecimento pessoal; as forças de operações especiais; os postos de observação e patrulhamento; e os oficiais de ligação.

No nível estratégico prevalecem as OSINT, HUMINT, IMINT e o reconhecimento pessoal. São de grande utilidade, portanto, as informações coletadas da imprensa, de agências governamentais e não governamentais e da academia; os relatórios diplomáticos e dos próprios órgãos da ONU; os relatos de pessoas que presenciaram a situação, como refugiados e correspondentes jornalísticos; as imagens da região obtidas por satélites e fotografias aéreas; e as já citadas missões de reconhecimento (CHARTERS, 1999). No tocante ao nível operacional, são de maior relevância o HUMINT, com destaque na coleta de informações com a população local, sejam civis, militares ou membros do governo; o IMINT, no monitoramento de zonas de cessar fogo e a localização de populações deslocadas; o SIGINT, na detecção antecipada de possíveis ataques, através da interceptação dos sinais; e forças de operações especiais, que, na verdade, não desempenham funções de inteligência específica, mas auxiliam e fornecem meios para o desenvolvimento, principalmente, do HUMINT e do SIGINT (CHARTERS, 1999). Por fim, no nível tático, são de maior importância o IMINT, para o fornecimento de mapas e fotografias; os patrulhamentos; os postos de observação; os oficiais de ligação e todas as ações que visem a um maior conhecimento da área (CHARTERS, 1999).

É necessário lembrar que, à exceção de OSINT, que, por definição são fontes abertas, os outros tipos de informação variam em um espectro acerca da forma de coleta, de permitidas (ou "área branca") a proibidas (ou "área negra"), passando pela denominada "área cinzenta". Dessa forma, as informações coletadas pela ONU situam-se na "área branca", ou seja, são obtidas por funcionários identificados, por informantes não pagos, e assim por diante. Segundo Dorn (1999), todavia, mesmo na "área branca" a ONU possui restrições, atuando sempre com a autorização prévia do Estado. Como já citamos anteriormente, isso está relacionado com um dos principais problemas da utilização de inteligência pelas Nações Unidas: o dilema da ética. Para Smith (1994), a utilização, quase que exclusivamente, de fontes abertas é mais uma característica que diferencia a inteligência nas operações de paz daquela desenvolvida pelos Estados.

Feita essa análise sucinta de como as atividades de inteligência são desenvolvidas no âmbito das operações de paz da ONU, é possível perceber que, apesar de ainda serem um tanto precárias e pouco institucionalizadas, ocorreram avanços significativos ao longo das últimas duas décadas. Para uma melhor compreensão da importância da inteligência nas missões de paz, julgamos relevante tratar brevemente de alguns casos específicos de operações de paz desenvolvidas pela ONU no período do pós-Guerra Fria.

6.4. Algumas Experiências Anteriores e a MINUSTAH

A relação entre supostas falhas de inteligência e crises nas operações de paz é bastante discutida e alguns episódios são sempre lembrados como evidências do problema da falta de utilização de inteligência nas missões de paz. O massacre em Ruanda em 1994 é um deles: uma fonte confidencial informou o então comandante da força de paz no país de que ocorreriam ataques, mas a ONU não autorizou a ação preventiva por se tratar de informações obtidas de forma clandestina (CHARTERS, 1999). Esse não é, entretanto, o único caso a ser destacado. As operações de paz na Bósnia, na Somália e no Haiti são de grande valia para o estudo da inteligência nesses tipos de missões, como veremos a seguir.

A Força de Proteção das Nações Unidas (UNPROFOR) iniciou suas atividades em 1992, como uma força humanitária na Croácia, mas já no ano seguinte foi expandida para a Bósnia. A situação de grande complexidade fez a ONU ampliar a sua atuação e o mandato da missão foi alterado mais de doze vezes (CHARTERS, 1999). A UNPROFOR, segundo Maceda (2007), demonstra a mudança no perfil das operações de paz, que passam a atuar em um espectro bem mais amplo e possuem funções também mais abrangentes que as anteriores.

A UNPROFOR possuía um escritório central em Zagreb, que coordenava a atuação dos comandos setoriais que eram responsáveis por determinadas regiões. No comando em Zagreb foi estabelecida uma seção de "informação militar", que desenvolvia atividades de inteligência, ainda que de maneira bastante precária, já que seus trabalhos se resumiam quase que exclusivamente à compilação dos relatórios das unidades regionais, produzindo um informativo diário (JOHNSTON, 2003). A ausência de uma estrutura única e eficiente de inteligência propiciou a utilização de estruturas *ad hoc*, compostas pelas próprias forças nacionais que integraram a missão (CHARTERS, 1999; JOHNSTON, 2003; MACEDA, 2007). Essa substituição da inteligência que deveria ser produzida pelas Nações Unidas pelas inteligências nacionais, contudo, não resolve o problema, já que, por ser composta por diferentes nacionais e, tendo cada país suas próprias fontes, métodos e critérios de classificação, muitas das informações obtidas não eram compartilhadas; não existia, portanto, uma inteligência única dentro da missão. Dorn (1999) afirma, por exemplo, que um peacekeeper canadense recebeu imagens de um satélite norte-americano, mas não foi autorizado a compartilhá-las com seu comandante, porque era um oficial francês.

O episódio do ataque à área de Srebrenica, na Bósnia, em 1995 – um local que, supostamente, era uma zona de segurança controlada pela ONU – evidencia a deficiência da inteligência produzida na UNPROFOR. Na ocasião, mais de seis mil bósnios muçulmanos foram mortos por sérvios, em uma ação totalmente desconhecida pelos oficiais alemães que compunham a missão nessa região.

Mais do que uma falha de inteligência, o ataque em Srebrenica evidenciou problemas no sistema de informação da missão, já que os pedidos de reforços não chegaram ao escritório da ONU em Sarajevo e as notícias dos primeiros ataques levaram mais de um dia para serem recebidas no comando central da operação em Zagreb. A ONU reconheceu a falha, mas nenhuma medida concreta foi tomada para evitar novas ações semelhantes. (MACEDA, 2007).

A presença das forças de paz da ONU na Somália iniciou-se em 1992, com uma operação frustrada que durou menos de um ano, a Operação das Nações Unidas na Somália (UNOSOM). Imediatamente após seu encerramento, foi iniciada a UNOSOM II, que permaneceu até 1995. Consoante Maceda (2007), a operação na Somália é um marco nas operações de paz conduzidas pela ONU, haja vista que foi estabelecida com base nos marcos do Capítulo VII da Carta, o que significa que ela não é baseada no amplo consenso das partes e não limita o uso da força exclusivamente para autodefesa.[13] Essas características, segundo o autor, aumentam as necessidades do uso da inteligência, o que corrobora as ideias apresentadas anteriormente sobre a crescente importância das atividades de inteligência nas operações de paz de "segunda geração".

A UNOSOM possuía um Escritório de Gerenciamento de Informações, que contava com um efetivo expressivo, mas suas atividades foram suplantadas pela atuação da inteligência norte-americana, uma vez que os EUA lideravam a Força Tarefa Unificada das Nações Unidas (UNITAF) no país. De acordo com Dorn (1999), o componente de inteligência estava fortemente presente na UNOSOM, especialmente a HUMINT, tendo em vista que a população local colaborava significativamente com o fornecimento de informações; há registros, inclusive, do pagamento de informantes e agentes. Além disso, a UNOSOM foi a primeira missão na qual foi utilizado o Sistema de Suporte de Inteligência Destacável Conjunta (JDISS), fornecido pelos EUA ao Situation Centre, que possibilitava a transferência de informações em um curto espaço de tempo, entre as missões e os escritórios centrais da ONU (CHARTERS, 1999). No âmbito da UNITAF, os EUA também criaram o Elemento de Suporte de Inteligência (ISE), mas este fornecia informações somente para as tropas norte-americanas. Maceda (2007) afirma que o não compartilhamento de informações era oriundo de problemas em ambos os lados: os EUA não confiavam nos sistemas de segurança de informação da ONU; a ONU, por sua vez, além da sua restrição habitual à inteligência militar, também não queria ser vista como um organismo manipulado pelos EUA. Embora existisse alguma inteligência tática e operacional na UNOSOM, ainda que não fosse uma inteligência produzida pelo staff da ONU, fica clara a lacuna no nível estratégico, com a ausência da formulação de um plano anterior ao início da operação.

[13] Se considerarmos as definições mais recentes apresentadas pela ONU, poderíamos enquadrar a UNASOM como uma missão também de imposição da paz, e não somente de manutenção.

A Missão das Nações Unidas para Estabilização do Haiti (MINUSTAH) foi estabelecida em abril de 2004 pela Resolução 1542 do Conselho de Segurança da ONU e teve seu mandato estendido duas vezes: em 2006, após as eleições de René Préval; e em 2009, para, principalmente, auxiliar na condução do processo eleitoral de 2010.[14] A situação no Haiti quando da implantação da MINUSTAH era de crise: problemas de forte corrupção no governo central, intensa disputa política e caos na segurança com o país sob o controle de gangues armadas (MAGUIRE, 2009). Nesse contexto, a prioridade número um das forças de paz era o restabelecimento da segurança, o que foi conseguido com relativa rapidez em grande parte do país, exceto na capital Porto Príncipe. As ações para conter as gangues na capital do Haiti, em especial na região de Cité Soleil, a favela mais populosa de Porto Príncipe e também a principal base dos líderes das gangues, iniciaram-se em dezembro de 2006, baseadas em um amplo planejamento respaldado pela inteligência produzida na MINUSTAH. (DORN, 2009).

A MINUSTAH, foi uma das operações de paz da ONU pioneiras no uso de inteligência de forma sistemática, juntamente com a missão no Kosovo (UNMIK) (DORN, 2009). A MINUSTAH conta com uma JMAC bem como com braços de inteligência nos escritórios centrais da missão e nos batalhões dos contingentes nacionais.[15] A JMAC valeu-se de informantes locais, inclusive informantes pagos, e de um vasto planejamento sobre a situação da região a ser tomada, incluindo o posicionamento e os hábitos detalhados dos líderes das gangues. Enfatiza-se, assim, mais uma vez, a importância da HUMINT e da IMINT nas operações de paz da ONU. Outro fator destacado por Dorn (2009) é o uso de operações noturnas, o que maximiza o fator surpresa, ao mesmo tempo em que minimiza o número de possíveis vítimas civis. A operação de paz no Haiti, assim, significou um grande avanço no uso da inteligência pela ONU; nas palavras de Dziedzic e Perito (2008:8, tradução livre):

> A JMAC da MINUSTAH estabeleceu um padrão de ouro para o suporte de inteligência para planejamento e execução de operações armadas para defesa e imposição do mandato. [...] A base para o sucesso da JMAC foi uma rigorosa administração e avaliação de fontes, juntamente com um esforço sistemático para reunir todas as fontes de informação disponíveis para a missão.

[14] A MINUSTAH foi antecedida por uma Força Multinacional (MNF-H), autorizada pelo Conselho de Segurança e liderada pelos EUA, que permaneceu no país nos dois meses anteriores à criação da MINUSTAH (DORN, 2009). Além disso, outras operações de paz já tinham sido estabelecidas no Haiti em períodos anteriores: a Missão das Nações Unidas no Haiti (UNMIH), 1993-1996; a Missão de Suporte das Nações Unidas no Haiti (UNSMIH), 1996-1997; a Missão de Transição das Nações Unidas no Haiti (UNTMIH), 1997; e a Missão de Polícia Civil das Nações Unidas no Haiti (MIPONUH), 1997-2000.

[15] A estrutura da JMAC contava com três principais componentes: uma unidade de análise estratégica, uma unidade de suporte de planejamento e de análise operacional, e uma unidade de análise de coleta (DORN, 2009).

Essa breve descrição destas operações evidencia as dificuldades, a baixa institucionalização e a falta de coordenação no uso da inteligência nas missões de paz implantadas pelas Nações Unidas no período do pós-Guerra Fria. O ataque em Srebrenica, no caso da UNPROFOR, sustenta, de maneira praticamente incontestável, a necessidade imperativa da utilização da inteligência nas operações de paz como forma de garantir a segurança das tropas envolvidas e de evitar a morte de civis. A atuação das forças na Somália, por sua vez, evidencia, entre outras coisas, o uso das inteligências nacionais para suprir a ausência de órgãos de inteligência institucionalizados na ONU, o que agrava o problema de controle e comando presente nas operações que envolvem tropas de mais de uma nacionalidade. O caso do Haiti, em contrapartida, demonstra os avanços significativos ocorridos no uso de inteligência pela ONU e o papel decisivo que esta teve no sucesso da pacificação de Porto Príncipe.

6.5. Considerações Finais

As operações de paz no pós-Guerra Fria desenvolveram, como vimos anteriormente, novas funções, adaptando-se ao novo contexto no qual se dão os conflitos, segundo Charters (1999), caracterizado pela complexidade política, pelo fanatismo, pelas participação de civis no conflito armado, pela novas táticas e pela indefinição da zona de conflito. A união dessas características dos conflitos no pós-Guerra Fria com o novo espectro de atuação das missões de paz torna a utilização de inteligência uma necessidade ainda maior, já que, em última instância, as operações de paz, nessas novas circunstâncias, constituem guerras de fato e, portanto, demandam os mesmos inputs de informação e inteligência que aquelas.

A necessidade do uso da inteligência nas operações de paz da ONU, todavia, não foi um estímulo suficiente para que houvesse um desenvolvimento de capacidades próprias dentro da instituição e de uma institucionalização das atividades já existentes. A pressão dos países membros, preocupados com a manutenção das suas soberanias, e o próprio dilema da ONU de utilizar ou não a inteligência por questões éticas, frearam maiores avanços. Ainda assim, alguns progressos pontuais foram feitos, destacando-se a criação do Situation Centre e a regulamentação das Células de Análise de Missões Conjuntas.

As debilidades no nível operacional, contudo, ainda são evidentes. Isso se reflete também nos níveis estratégico e tático, tendo em vista que é o nível operacional que mantém a ligação entre os outros dois. A prevalência de estruturas ad hoc dificulta a criação de um padrão de conduta, deixando o estabelecimento/uso de atividades de inteligência nas operações dependente do comando daquela missão em específico. Essas dificuldades de implantação e condução de atividades de inteligência nas operações de paz levam os países

envolvidos na missão a utilizar seus próprios serviços de inteligência o que, por vezes, dificulta os problemas já existentes de comando e controle presentes nessas operações, além de se tornar mais um empecilho para a institucionalização de serviços de inteligência permanentes próprios das Nações Unidas.

Os exemplos empíricos evidenciam o que foi demonstrado ao longo de trabalho. Tanto no caso da Bósnia quanto no da Somália, as deficiências no fornecimento de informações, que poderiam ser supridas com a institucionalização de atividades de inteligência, ocasionaram erros e falhas na atuação das missões nas regiões em questão.

O caso do Haiti, embora possa ser entendido como um sucesso e um grande avanço no emprego da inteligência nas operações de paz, não pode ser generalizado, já que se tratou, muito mais de uma atividade de polícia do que militar, o que implica demandas e práticas de inteligência diferentes.

Ficam, portanto, duas grandes conclusões: a primeira, de que de fato o pós-Guerra Fria trouxe novas demandas para as operações de paz e que essas demandas aumentaram a necessidade do uso da inteligência nessas missões; em segundo, as evoluções no uso da inteligência pelas Nações Unidas a partir da década de 1990, embora tenham ocorrido, ainda estão muito aquém do necessário.

REFERÊNCIAS

BOATNER, Helene (2000). Sharing and using intelligence in International Organizations: some guidelines. *National Security and the Future*, v.1, n. 1.

BOYD, Herchel A (1996). Joint intelligence in support of peace operations. *Naval War College*, 14 June.

CEPIK, Marco A. C (2003). *Espionagem e Democracia*: agilidade e transparência como dilemas na institucionalização de serviços de inteligência. Rio de Janeiro: Editora FGV.

CHARTERS, David (1999). Out of the Closet: Intelligence Support for Post-Modernist Peacekeeping. In: DORN, Walter & CHARTERS, David. Intelligence in Peacekeeping. The Pearson Center Papers, n. 4.

CHESTERMAN, Simon. Intelligence Cooperation in International Operations: Peacekeeping, Weapons Inspections, and the Apprehension and Prosecution of War Criminals. New York University School of Law, New York University Public Law and Legal Theory Working Papers, 2009.

DORN, Walter (1999). The Cloak and the Blue-Beret: the limits of intelligence-gathering in UN Peacekeeping. In: DORN,Walter & CHARTERS, David. *Intelligence in Peacekeeping*. The Pearson Center Papers, n. 4.

_____. (2009). Intelligence-led Peacekeeping: The United Nation Stabilization Mission in Haiti (MINUSTAH), 2006-07. *Intelligence and National Security*, v. 24, n. 6, p. 805-35, December 2009.

DZIEDZIC, Michael; PERITO, Robert M. (2008). *Haiti*: Confronting the Gangs of Port-au-Prince. Special Report, United States Institute for Peace, Washington DC.

EKPE, Bassey (2007). The intelligence assets of the UN: Sources, Methods and implications. *International Journal of Intelligence and Counter-intelligence*, n. 20.

JOHNSTON, Paul (2003). No Cloak and Dagger Required: Intelligence Support to UN Peacekeeping. In: JONG, Bend; PIATJE, Wies; STEELE, Robert D. *Peacekeeping Intelligence*: Emerging Concepts for the Future. Oakton: OSS International Press.

JAKOBSEN, Peter V (2000). The Emerging Consensus on Grey Area Peace Operations Doctrine: Will it last and enhance operational effectiveness? *International Peacekeeping*, v.7, n. 3.

MACEDA, Steven (2007). Dysfunction Junction: Intelligence, Peacekeeping and UN. Naval Postgraduate School, Thesis.

MAGUIRE, Robert (2009). *What Role for the United Nations in Haiti*? Peace Briefing, United States Institute for Peace, Washington DC.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (1945). Carta das Nações Unidas. Disponível em <http://www.onu-brasil.org.br/documentos_carta.php>. Acesso: em: 12/11/2009.

_____. (1991). Declaration on Fact-Finding by the United Nations in the Field of the Maintenance of International Peace and Security. General Assembly, A/RES/46/59, 9 December 1991.

_____. (2000). Report of the Panel on United Nations Peace Operations (Brahmi Report. General Assembly, A/55/305-S/2000/809, 21 August 2000.

_____. (2007). Declaration on Strengthening of the Capacity of the Organization in Peacekeeping Operations. General Assembly, A/RES/61/256, 22 March 2007.

_____. (2008). United Nations Peacekeeping Operations: Principles and Guidelines. "Capstone Doctrine". Department of Peacekeeping Operations.

SHETLER-JONES, Philip (2008). Intelligence in integrated UN peacekeeping missions: the joint mission analysis centre. *International Peacekeeping*, v. 15, n. 4.

SMITH, Hugh (1994). Intelligence and UN peacekeeping. *Survival*, v. 36, n. 3.

UNITED NATIONS PEACEKEEPING (<http://www.un.org/en/peacekeeping/>).

WARNER, Michael (2009). Building a theory of intelligence systems. In: TREVERTON, Gregory & AGRELL, Wilhelm. National Intelligence Systems: current research and future prospects. Cambridge – MA: Cambridge University Press.

WILLIANS, Charlles (1993). *Intelligence support to UN Peacekeeping Operations*. Washington DC, The Industrial College of the Armed Forces, Executive Research Project, S81.

Capítulo 7

PROPAGANDA: OPERAÇÃO PSICOLÓGICA OU OPERAÇÃO ENCOBERTA?

Marília Bortoluzzi Severo

A utilização dos meios de comunicação para propagar uma percepção sobre um determinado assunto constitui a função primordial dos instrumentos de propaganda, sejam eles sonoros, escritos ou audiovisuais. Para fins de esclarecimento, as técnicas de propaganda são estabelecidas aqui como uma forma específica de comunicação, com o objetivo determinado de persuadir, influenciar ou moldar a percepção de um público-alvo.

O presente estudo buscará examinar a natureza das técnicas de propaganda utilizadas pelos agentes estatais em situações de conflito e tentará situar tais estratégias no contexto das atividades de inteligência. A idéia é mostrar que os mecanismos de propaganda constituem um ramo específico das operações de defesa e estão correlacionadas aos servidores de inteligência, de acordo com o conceito do termo inteligência aqui proposto. Por esse raciocínio, esses instrumentos não fazem parte do arcabouço de operações informacionais do tipo operação psicológica, mas sim constituem uma modalidade de operação encoberta. Essa é a hipótese que rege a lógica deste trabalho. A perspectiva do estudo é, portanto, puramente conceitual – considerações a respeito das vantagens e deficiências desse tipo de estratégia não serão perquiridos aqui.

Partindo-se da premissa que a engrenagem das técnicas de propaganda sugere uma atividade específica de inteligência, o presente trabalho será dividido em quatro seções explicativas. A primeira seção apresentará as considerações conceituais a respeito dos termos inteligência, operações encobertas e informações operacionais, e traçará as respectivas conexões entre estes fenômenos. Na segunda seção, serão tratados os aspectos conceituais sobre as técnicas de propaganda, seus objetivos e seus limites. A terceira seção, por sua vez, se encarrega de desfazer a confusão a respeito da diferenciação

entre as estratégias de propaganda e as operações psicológicas informacionais. Já a quarta seção estabelecerá a natureza da propaganda como uma forma de operação encoberta, e trará esclarecimentos sobre a tipologia dessas operações e a sua eficiência como técnica de inteligência. Por fim, as considerações finais elencarão as principais conclusões sobre o assunto.

7.1. Inteligência, Operações Encobertas e Operações Informacionais

O termo inteligência não é de fácil definição e gera uma acalorada discussão, devido à importância das atividades de inteligência como instrumento para a defesa e a segurança dos Estados nacionais. Não obstante o debate, é possível identificar na literatura especializada duas tendências sobre o conceito de inteligência, ambas refletindo os elementos ou funções dessa atividade. A necessidade de se definir, inicialmente, o conceito utilizado neste trabalho encontra-se justamente no fato de que essas definições divergem quanto ao que classificam como inteligência.

A definição mais usual é dada por Sims (2009:04) ao dizer que inteligência é a informação coletada, organizada e analisada em benefício dos atores ou tomadores de decisão. Disso decorre que qualquer atividade que envolva a coleta, organização ou análise de informação em um contexto de defesa e proteção da ordem pública pode ser classificada como atividade de inteligência governamental. Essa definição enfoca dois aspectos essenciais na caracterização do termo: as funções da inteligência e os seus propósitos, isto é, a quem ela serve. Atividade de inteligência, sem dúvida, necessita ter o propósito de servir os tomadores de decisão de política pública para que possam formar sua opinião e tomar suas decisões da forma mais fundamentada possível.

Essa tendência conceitual também pode ser vista em Cepik (2003b:249), que coloca a atividade de inteligência como "a coleta de informações sem o consentimento, a cooperação ou mesmo o conhecimento por parte dos alvos da ação", somada à dimensão explicativa ou preditiva da atividade de inteligência (CEPIK, 2003a:28), que é consubstanciada pela análise e processamento da informação. Esse conceito, numa tentativa de localizar a inteligência entre as noções de informação e espionagem, tem como mérito somar essas duas noções e ao mesmo tempo delimitá-las para constituir uma idéia de aquisição de informação fundamentada com vistas à produção de decisões de políticas de defesa e de segurança.

Entretanto, a perspectiva de inteligência até agora tratada deixa de considerar como aspecto fundamental desse tipo de atividade a dimensão de disseminação da informação como componente do conceito. Ora, se uma

informação é coletada e analisada, é necessário disseminá-la para que, como o próprio conceito de Sims estabelece, o tomador de decisão decida suas políticas de forma fundamentada. O que se propõe nesse estudo é a consideração da disseminação da informação em uma dimensão mais ampla, não apenas com o propósito de informar os atores governamentais, mas também com o objetivo de influenciar ou moldar as atitudes e decisões dos mais variados atores envolvidos no jogo político.[1] Esses atores podem ser classificados por uma perspectiva interna, relacionada ao contexto político interno de um Estado, isto é, sua sociedade civil, organizações não governamentais e afins, e por um viés externo, focado nos atores externos ao Estado, que podem, contudo, ser relacionados a ele: o governo e a sociedade de um Estado inimigo, organizações internacionais, etc.

Por essa linha de raciocínio, a definição de inteligência que melhor se enquadra ao escopo deste estudo é a de Godson (1995:01), que define inteligência como a informação adquirida, explorada e protegida pelas atividades de organizações especificamente estabelecidas para esse propósito. O termo a ser desmembrado aqui é o da informação explorada: deve a informação tanto ser analisada como utilizada para os fins a que se destinam os serviços de inteligência. Lembrando, que a missão da inteligência é também garantir a segurança e a defesa do Estado nacional e da ordem pública, não se pode deixar de considerar a atividade de exploração de informação na perspectiva de sua disseminação para auxiliar operações que objetivam assegurar a segurança estatal (BRUNEAU e BORAZ, 2007:07).

É dentro dessa lógica que boa parte da literatura especializada considera as atividades de inteligência como compostas por quatro elementos: coleta, análise, contra-espionagem e operações encobertas. Os dois primeiros, coleta e análise de informações, decorrem diretamente de qualquer conceito que se dê para a noção de inteligência. A contraespionagem resulta da necessidade de proteção da informação coletada e analisada, e é consubstanciada pelo esforço em proteger os segredos governamentais de outros Estados ou organizações (BRUNEAU e BORAZ, 2007:09).[2] As operações encobertas , por sua vez, são os esforços de um governo ou grupo no sentido de influenciar eventos em um território sem revelar o seu envolvimento (GODSON, 1995:02).[3]

---

[1] No sentido contrário: ver Herman (2001:44-47).

[2] Para maiores esclarecimentos sobre contraespionagem e sua relação com contrainteligência e segurança informacional, ver Cepik (2003a) e Godson (1995).

[3] O termo operações encobertas (CA ou *covert actions*, em inglês) é comumente utilizado para as atividades desse tipo exercidas pelas agências governamentais dos Estados Unidos. Na Inglaterra, são chamadas de operações políticas especiais (*special political actions*), e na União Soviética, eram chamadas de medidas ativas (Cepik, 2003a). De acordo com o *Dicionário Militar do Departamento* de *Defesa dos Estados Unidos* (JCS U.S., 2009) seriam operações planejadas e executadas de maneira a ocultar a identidade ou permitir a negação plausível do seu executor. Para fins de simplificação, as atividades aqui tratadas serão tratadas genericamente como operações encobertas.

Importante lembrar que, para alguns autores, os instrumentos de operações encobertas são, na realidade, ferramentas de implementação de políticas, muito mais do que estratégias de inteligência propriamente ditas (CEPIK, 2003b:260). Elas teriam sido colocadas sob a responsabilidade dos serviços de inteligência mais por uma opção histórica e estrutural, em razão das capacidades materiais e humanas desse tipo de serviço, do que por uma questão de semântica. Outros autores colocam as ações encobertas como uma espécie de atividade associada à inteligência, considerando-se o parco orçamento e material humano da Central Intelligence Agency (CIA) norte-americana relacionado a essas operações (HERMAN, 2001:54).[4, 5]

Não é esse o entendimento em que se apoia este estudo. É bem verdade que, como preceitua Anderson (1998:404), ações encobertas constituem um elemento integral na busca dos interesses e metas de política externa, através do emprego de meios secretos para alcançar o que não poderia ser obtido abertamente. No entanto, operações encobertas possuem um nítido viés de inteligência na medida em que, em geral, ocupam-se da disseminação de informações com propósito específico, sejam elas verdadeiras ou falsas, e são executadas com a finalidade máxima de salvaguardar os interesses estatais de um determinado ente, em termos de defesa e segurança, ainda que indiretamente. Nesse sentido, corrobora-se o entendimento de Godson (1995), ao estabelecer esse tipo de instrumento como um elemento primordial das atividades de inteligência. Com isso, ações do tipo atividades paramilitares, apoio a golpes de Estado, distorção de informações, fornecimento de assistência secreta a governos e demais operações destinadas a manipular aspectos relevantes e produzir uma influência favorável aos interesses do executor da operação são consideradas como atividades de inteligência.

Nesse ponto, precisamente, é necessário compreender um fenômeno que não faz parte, diretamente, das atividades de inteligência, e muitas vezes é confundido com algumas espécies de operações encobertas: são as operações informacionais (IO ou information operations). As operações informacionais são definidas pelo Dicionário Militar do Departamento de Defesa dos Estados Unidos como "o emprego integrado das capacidades essenciais de guerra eletrônica, operações de redes de computadores, operações psicológicas, dissimulação militar, e operações de segurança, para influenciar, desorganizar, corromper ou usurpar um processo de decisão" (PAUL, 2008:02). É importante

[4] Para Herman, a essência ocidental de inteligência consiste no fornecimento de informações e previsões para uma tomada de ação, e não propriamente na ação em si (2001:56). Daí a sua noção restritiva da atividade de inteligência não abarcar as operações encobertas.

[5] Com razão, Wettering (2003:561) comenta que muito da capacidade da CIA concernente às operações encobertas tem desaparecido com o passar do tempo, e que grande parte de sua metodologia foi transmitida para organizações abertas que recebem financiamento público.

observar que apenas os esforços do Departamento de Defesa norte-americano podem ser considerados como operações informacionais, decorrendo disso a principal característica que as diferencia das atividades realizadas pelos serviços de inteligência.

A correlação da atividade de inteligência com as operações informacionais está no fato de que o produto da primeira comumente serve como embasamento para a execução da última. No entanto, ao se considerar uma perspectiva mais ampla de inteligência, é possível confundir facilmente algumas operações informacionais com operações encobertas, precipuamente em função de seus objetivos semelhantes – influenciar ou manipular eventos e processos de tomadas de decisão. Tal confusão, porém, é desfeita no momento em que se salienta que aqueles esforços do governo em termos gerais de informação que não são realizados pelo Departamento de Defesa dos Estados Unidos (e assim analogicamente para os demais Estados) não são considerados operações informacionais – e aí entram as atividades de inteligência.

Em realidade, a compreensão do tema se torna mais fácil ao se visualizar uma classificação taxionômica da questão: considerando-se a informação como um dos principais requisitos para uma ação, sua classe enquadra os gêneros de atividades do tipo inteligência (coleta, análise e disseminação de informação) e do tipo operação informacional (emprego de determinadas informações pelo Departamento de Defesa para influenciar um evento). No gênero inteligência, pode-se encontrar como espécie as operações encobertas, no sentido de disseminação de informações por agências de inteligência com o objetivo de influenciar um evento sem a revelação da autoria.

Como se percebe, os fins a que se destinam as operações encobertas e as operações informacionais são os mesmos – ambos constituem-se em estratégias para influenciar um ator político na defesa dos interesses governamentais e da segurança e defesa do Estado. A diferença entre esses dois fenômenos, mais do que conceitual, está no "como" se faz e no "quem" realiza tais operações. Essa distinção é importante para a compreensão do tópico a seguir.

7.2. Uma Impressão Positiva das Técnicas de Propaganda

A propaganda é um dos meios de comunicação mais antigos no mundo: existem relatos de que a propaganda estatal pró-Roma e pró-catolicismo teria sido um dos motores da expansão do Império Romano. Avançando no tempo, as técnicas de propaganda evoluiram durante a Segunda Guerra Mundial, onde eram utilizadas como armas de guerra tanto pelos Aliados como pelo Eixo. Hitler acreditava que as técnicas de manipulação de informação teriam sido as responsáveis pelo senso de derrotismo adquirido pelo exército alemão na

Primeira Guerra Mundial. De fato, atualmente tem-se como bem-sucedidas as operações de propaganda realizadas pelos Aliados nas duas guerras mundiais.

Com este *boom*, essas operações passaram a ser atividades recorrentes dos agentes governamentais especialmente dos Estados Unidos e da União Soviética, e desempenharam um papel central no período da Guerra Fria. Tanto os norte-americanos como os soviéticos utilizaram amplamente a propaganda durante esse período. Filmes, jornais, programas de televisão e de rádio foram utilizados para influenciar os governos e populações inimigos e até mesmo seus próprios cidadãos. Os mais citados exemplos referem-se às rádios Voz da América, Free Europe e Liberty como as estações que mais difundiam informações tendenciosas em notícias e programas de entretenimento a favor do bloco capitalista.

Um dos casos mais recentes de utilização da propaganda como forma de manipulação foi na última Guerra do Iraque, em 2003, quando os governos dos Estados Unidos e do Reino Unido utilizaram o argumento de que o Iraque teria armas de destruição em massa para justificar e legitimar a sua invasão. Documentos falsos e forjados alegaram suposta transferência de urânio do Níger para o Iraque, e essa evidência baseou toda a justificativa de contenção do "Eixo do mal", termo criado pelo então presidente George W. Bush. As duas superpotências recorreram a essa desculpa sobre o programa nuclear do Iraque porque se tornou óbvio que estavam perdendo a batalha pela opinião pública internacional.

A propaganda, aplicada à sociedade, influi diretamente no comportamento humano e é destinada às atitudes, emoções e opiniões de grupos determinados, para moldar suas percepções, o que leva a um elemento constitutivo primordial: a persuasão. Sem esta capacidade, a técnica de propaganda não possuirá a efetividade necessária para atingir o público-alvo da ação. Com isso, o estudo das formas de comunicação e de como elas influem nos mapas cognitivos dos indivíduos torna-se imprescindível.

A literatura especializada concorda em afirmar que outro elemento essencial para a caracterização da propaganda é a sua intenção, isto é, a sua meta principal. Os governos não enganam ou mentem deliberadamente para seu público ou para um agente externo, seja ele um Estado, uma organização ou uma população sem motivação. O fim último de qualquer tipo de informação não-verdadeira é sempre o interesse da defesa e da segurança nacional. Até porque propaganda não consiste apenas em disseminar uma verdade ou uma mentira; mais que isso, é uma tentativa de modelação de mapas cognitivos, e requer, acima de tudo, a credibilidade da fonte de informação. Isso garante que os Estados não utilizarão indistintamente e de forma deliberada as estratégias de propaganda.

Através dos exemplos citados, é possível identificar claramente o objetivo primordial das técnicas de propaganda: influenciar as ações e ideas

de um determinado alvo, normalmente inimigo, em favor de seus próprios interesses. Definido isso, é necessário agora examinar as técnicas mais comuns de propaganda no contexto das atividades de informação e inteligência, para a seguir elaborar um conceito de propaganda que se enquadre nos termos propostos por este estudo.

As ações de propaganda nas quais se pode identificar o responsável por sua emissão são chamadas de propagandas brancas (*white* propaganda) ou claras (*overt* propaganda). São aquelas disseminadas através de pronunciamentos oficiais do governo, da produção de centros acadêmicos e mesmo dos meios de mídia, em que a fonte da informação encontra-se bem determinada, e são geralmente verdadeiras. As formas de persuasão contidas nesse tipo de propaganda, via de regra, são mais sutis e visam ao estabelecimento ou manutenção de apoio popular para o ator que a emite.[6]

A propaganda é do tipo cinza (*gray* propaganda) quando esconde sua fonte do público inespecífico, mas não dos observadores sofisticados (GODSON, 1995:152). Essas informações propagadas podem ser verdadeiras ou intencionalmente falsas. Quando a fonte da informação é falsa ou oculta, e a própria informação é falsa, diz-se que a propaganda é negra (*black* propaganda). As técnicas de propaganda nas quais o responsável pela disseminação da informação resta desconhecido enquadram-se nessa categoria e são conhecidas como estratégias de desinformação (*disinformation*).[7]

Seja em razão da utilização histórica da propaganda como informação equivocada, seja em função da falta de confiança nas fontes disseminadoras, o fato é que a propaganda, como técnica, sofre de um grande descrédito e até de uma visão negativa por parte da população. O desconhecimento acerca do conceito científico de propaganda faz com que o termo seja carregado normalmente com uma conotação pessimista de fraude e manipulação insidiosa. Por esse motivo, Paul (2008:09) acredita que a maioria dos responsáveis por uma atividade, tanto de diplomacia, inteligência ou operação informacional, prefere não denominar nenhuma parte dessa atividade como propaganda.[8]

---

[6] É bem conhecido o caráter discreto e formal dos pronunciamentos oficiais do governo norte-americano – a população sabe o que o governo está fazendo mais através da mídia do que por sua própria voz. Entretanto, fora dos Estados Unidos, o governo se sente livre para levar a sua mensagem diretamente para as populações estrangeiras, vide o caso dos folhetos de propaganda que caíam do céu durante a Guerra do Golfo.

[7] Tal termo provavelmente é de origem alemã, e foi adotado pela espionagem soviética como um conceito profissional para descrever operações de inteligência secreta destinadas a enganar o adversário (BITTMAN, 1990:249). Atualmente, é tido como operações intencionalmente distorcidas, ao contrário do conceito de misinformation, que significa apenas informação incorreta, sem a intenção de distorção.

[8] O autor ainda brinda o leitor com uma colocação interessante feita pelo Coronel Jack Summe, do Grupo de Operações Psicológicas do Exército dos Estados Unidos, que teria dito que a sua atividade "é chamada de informação e a do inimigo é chamada propaganda" (PAUL, 2008:09).

O termo propaganda, na literatura acadêmica sobre meios de comunicação, indica uma forma propositada e sistemática de persuasão que objetiva influenciar as emoções, atitudes, opiniões e ações de um público-alvo através da transmissão controlada de informação (que pode ou não ser verdadeira) por meio de canais diretos e de mídia (NELSON, 1996). Já o Departamento de Defesa norte-americano (JCS U.S., 2009) conceitua como propaganda qualquer forma de comunicação em prol dos objetivos nacionais destinada a influenciar as opiniões, emoções, atitudes ou comportamentos de qualquer grupo, a fim de beneficiar o executor da estratégia, direta ou indiretamente.

A partir desses conceitos, é possível elaborar uma definição técnica de propaganda como as estratégias de comunicação realizadas pelos governos nacionais, destinadas a persuadir e influenciar um alvo contrário ou sua própria população, com o fim último de estabelecer juízos de valor positivos em relação ao responsável pela manobra e negativos em relação ao seu opositor. O peso da guerra transmitida pela televisão no imaginário popular, por exemplo, é uma das estratégias mais eficientes de transformação de um conflito em um espetáculo teatral, visto que as imagens são armas poderosas. Ainda, esse conceito não se confunde com o de informação, que abarca um leque mais amplo de instrumentos e não inclui o propósito específico de persuadir ou influenciar, a despeito do que defende Paul (2008:10).[9]

Percebe-se, por todo o exposto, que as técnicas de propaganda, quando utilizadas no contexto político, em uma perspectiva de conflito, possuem como meta principal influenciar as atitudes e o comportamento de um ator que esteja em oposição ao patrocinador da técnica, ou seja, o seu inimigo. Tal intento constitui a função final tanto das operações informacionais, que podem ser da espécie operações psicológicas, como pode ser uma técnica de operação encoberta. Como definir a sua natureza? Este é o tema que será tratado nos próximos tópicos.

7.3. Operações Psicológicas: Mais uma Forma de Propaganda?

As operações informacionais, como estratégias de segurança e defesa nacional, estão assentadas sobre cinco pilares, isto é, cinco princípios de ação: operações psicológicas (PSYOP), dissimulação militar (MILDEC), operações de segurança (OPSEC), guerra eletrônica (EW) e operações de redes de computadores (CNO). Essas são as estratégias desenhadas pelo Dicionário Militar do Departamento de Defesa dos Estados Unidos como operações de informação,

[9] Para Paul, o conceito de informação requer necessariamente um propósito – informar algo "para quê". Não é possível concordar com tal argumento, na medida em que se acredita que uma informação, por si só, pode ser isenta de valor; a sua valoração depende da perspectiva de análise que se dá a ela. Daí a importância da etapa de análise no ciclo de inteligência.

que ficam a cargo de um setor específico dentro desse departamento. Nesse momento, o que interessa é lançar um olhar sobre a primeira modalidade de ação.

O Dicionário Militar do Departamento de Defesa dos Estados Unidos define PSYOP como operações planejadas para transmitir informações selecionadas e indicadores, a fim de influenciar emoções, motivos, raciocínio objetivo e o comportamento de governos estrangeiros, organizações, grupos ou indivíduos (BOWDISH, 1999). Essa definição, no entanto, oferece um sério problema: o conceito é bastante amplo e sem limites teóricos. Isso permite abraçar qualquer espécie de operação, o que pode causar uma confusão conceitual, como se verá a seguir.

Por outro lado, Narula (2004:187) descreve as operações psicológicas como o uso planejado de todas as formas de comunicação e informação e outras ações psicológicas, incluindo ações políticas, militares, econômicas e ideológicas, com o objetivo de influenciar as opiniões, emoções, atitudes e comportamentos de grupos hostis e não-hostis, tanto estrangeiros e nacionais, como meio de apoiar a realização dos objetivos nacionais. Aqui, o problema refere-se à possibilidade de utilização de tais operações em direção à população nacional.

Tal intento foi limitado legalmente nos Estados Unidos pelo Smith-Mundt Act de 1948, alterado em 1972 e 1998, o qual proibia a Agência de Informação dos Estados Unidos (USIA) de disseminar informações para o público doméstico. Essa agência não existe mais, entretanto, a expressão ainda é interpretada como uma proibição dirigida ao governo norte-americano de utilizar informações e operações psicológicas dirigidas a públicos estrangeiros para o público nacional (SEGELL, 2009:94). A questão, contudo, não se torna mais fácil: com a natureza global da mídia contemporânea, como delimitar as fronteiras entre o público doméstico e o estrangeiro? O problema permanece sem respostas.

Assim, em função das questões expostas, sugere-se uma conceituação mais singela das operações psicológicas, como sendo ações realizadas pelo Departamento de Defesa destinadas a afetar atitudes e comportamentos de um alvo estrangeiro, em apoio aos objetivos nacionais. O termo é recente – data do século XX – mas a sua utilização como estratégia de guerra para vencer conflitos é bem antiga, e confunde-se com a própria história da propaganda. Em realidade, as ações de guerra psicológica eram uma forma de propaganda, realizada pelo Departamento de Defesa dos Estados Unidos. Após a Segunda Guerra Mundial, no entanto, várias competências nesse sentido foram repassadas a agências governamentais, como a CIA, restando apenas um nicho determinado de operações a cargo das atividades militares específicas.

O papel essencial da credibilidade aqui também é importante; prova-se isso pelo consenso geral de que armas de persuasão são muito mais efetivas se baseadas na verdade. Até porque, muitas vezes, o dano causado à credibilidade da

fonte que dissemina uma mentira é tão grande que limita a sua posterior utilização como fonte. A confiança depositada na fonte não está em jogo quando a técnica utilizada é negra ou cinza, isto é, quando a fonte está escondida. No entanto, é preciso lembrar que grande parte das operações psicológicas são do tipo claras, onde a fonte é facilmente identificável, e mesmo aquelas que não as são, mais cedo ou mais tarde, acabam se tornando conhecidas pelo público.

Basta ver a questão da utilização indiscriminada de técnicas de propaganda e dissimulação na invasão ao Iraque pelos Estados Unidos em 2003 para compreender a questão da legitimidade. O declínio do poder hegemônico norte-americano somente se acentuou com as desaventuras da guerra contra o Iraque, que tiveram um impacto corrosivo na imagem internacional do país. Como Wallerstein (2002: 68) afirma, nos últimos duzentos anos, os Estados Unidos adquiriram uma quantidade considerável de crédito em termos de ideologia. Atualmente, porém, o país está a gastar esse crédito ainda mais depressa do que gastava o seu excedente de ouro na década de 1960.

As operações psicológicas são o núcleo central das operações informacionais contemporâneas, pois desempenham cinco importantes papéis: influenciam populações estrangeiras, assessoram o comandante militar, produzem informações públicas, servem como apoio à voz do comandante, e contra-atacam as informações inimigas (PAUL, 2008:58). Ainda, podem ser realizadas em três níveis: estratégico, operacional e tático, de acordo com as dimensões de planejamento da ação. Requerem um cuidadoso monitoramento, já que podem acarretar resultados indesejáveis, visto que se trata de um instrumento de caráter subjetivo.

Alguns autores enquadram as técnicas de propaganda como operações psicológicas, em função de seus propósitos em absoluto semelhantes. A partir dos elementos expostos, no entanto, é possível distinguir claramente as operações psicológicas das operações de propaganda. Em primeiro lugar, quando o Departamento de Defesa de um Estado realiza uma operação de manipulação e disseminação de informação, com fonte conhecida ou não, ela é uma operação psicológica, e tem como público-alvo determinado uma população ou governo estrangeiro. Requerem uma disciplina específica de operação militar, e possuem como objetivo também auxiliar o comandante no processo decisório.

Quando, no entanto, agências de inteligência manipulam e disseminam informações, com fonte conhecida ou não, elas são operações do tipo encobertas, na medida em que se ocupam centralmente do processo de disseminação de informação e podem atingir mesmo o público doméstico. Essas operações realizadas por atores estatais requerem a aprovação presidencial. Ressalte-se que mesmo atores não-estatais podem se encarregar dessa técnica de propaganda, que hoje se encontra cada vez menos centralizada nesses atores – movimentos

políticos, rebeldes, e mesmo as causas sociais podem bancar atualmente um espaço nos meios de comunicação de massa.

Outra diferenciação importante é que as operações psicológicas são consideradas um acessório em relação ao esforço de vencer um conflito, e não uma precondição às decisões de comando. As operações encobertas, como parte das atividades de inteligência, transpiram a essência informativa dos serviços típicos dessa área, já que tem por espírito servir aos tomadores de decisão para que tomem decisões fundamentadas. Com isso, o caráter de não obrigatoriedade, mas de essencialidade das operações encobertas, sobreleva-se às operações psicológicas.

A verdade é, contudo, que tudo se resolve em termos do que se define por propaganda, conforme preceitua Paul (2008). As operações psicológicas utilizam, sim, propaganda, mas em termos de instrumento, e não de estratégia. A propaganda, como planejamento e artifício para enganar o adversário, é própria das atividades de inteligência do tipo operações encobertas. É sobre esse tipo de atividade que tratará o tópico a seguir.

7.4. A Propaganda como Operação Encoberta

As operações encobertas constituem um tema quase que místico em razão do encanto que a mídia direcionou, no século XX, aos atos de espionagem e serviços secretos, através de filmes, livros e afins. São compostas de uma gama variada de técnicas e recursos, como agentes secretos, operações paramilitares, golpes de Estado, suporte financeiro e propagandas encobertas. É praticamente impossível pensar em uma atividade de espionagem e não relacioná-la diretamente a agências como a CIA e a KGB e às suas atuações durante a Guerra Fria.

No período pós-Guerra Fria, a importância das estratégias de operações encobertas no cenário internacional atual continua sendo inquestionável, em razão do dilema de segurança presente nas relações internacionais. Explique-se: em um sistema internacional anárquico, um Estado pode armar-se para proteger-se de eventuais ameaças de outros Estados. Entretanto, outros Estados podem ver isso como uma ameaça, com o que também passarão a investir em armamentos. Essa situação gera uma corrida armamentista que pode levar à guerra, e nesse caso as operações encobertas podem servir como um instrumento dessa corrida, como uma arma ofensiva não-convencional, como explica Anderson:

> In other words, one country's covert action operation may threaten the security of either the target state or another state that views its interests as threatened by such activity. It may then spark a counter-covert action against the initial sponsoring state, and perhaps an increasing spiral of covert activity. This, too,

> could eventually lead to war if a state chooses to take the game to that level (ANDERSON, 1998: 405).[10]

A importância das operações encobertas sob a ótica do dilema de segurança internacional, ademais, está ligada ao fato de que este dilema decorre de um fator que Silva e Gonçalves (2005) chamam de "comunicação imperfeita". Ora, sendo a comunicação entre dois Estados imperfeita, a compreensão das intenções de cada um pode tornar-se equivocada, e com isso gerar o supracitado dilema. Como os autores explicam, "a impossibilidade de avaliar seguramente os interesses de cada Estado leva à prevalência da lógica de que a ação preventiva é essencial (SILVA e GONÇALVES, 2005:50). Nesse sentido, ações encobertas, principalmente quando descobertas, podem causar uma espécie de mal-entendido na interpretação dos interesses de um Estado em relação ao outro, e gerar uma corrida de operações deste tipo.

Ressaltada a importância das operações encobertas, vale lembrar que a propaganda é a técnica mais comum de operação encoberta, conforme Bittman (1990:251). A maior parte da literatura especializada sobre o assunto trata meramente de casos bem ou mal sucedidos de operações encobertas, mas carece de rigor metodológico e conceitual. Com isso, o próprio enquadramento das atividades de propaganda dentro das operações encobertas torna-se uma tarefa penosa.

O conceito de operação encoberta como já visto, envolve a utilização de certos instrumentos de forma a não se identificar o responsável, com o propósito de influenciar um determinado grupo-alvo. Stempel (2007:125) traz a brilhante definição de Richelson:

> Operação encoberta é formalmente referida nas Ordens Executivas como "atividades especiais''. Talvez a descrição mais abrangente seja a do Dr. Jeffrey T. Richelson: Ações encobertas, também conhecidas como "atividades especiais", incluem qualquer operação destinada a influenciar os governos estrangeiros, pessoas ou eventos em apoio aos objetivos de política externa do governo patrocinador, mantendo secreta a responsabilidade pela operação. Considerando que, na coleta clandestina, a ênfase é em manter a atividade secreta, na ação encoberta a ênfase é em manter o segredo do patrocínio.

Delimitado o espectro de ação das operações encobertas, resta saber agora como e porque se defende a classificação das estratégias de propaganda como uma espécie de ação encoberta. Lembrando as tipologias variantes da

[10] Em outro momento, o autor continua: "If covert action is a trigger for the security dilemma, it might be possible to predict and generalize regarding the expected reaction in the international system from a given covert operation. Even if the actual covert operation is unsuccessful in its immediate goals, it may still generate a reaction among other states. This makes covert action as a whole an important factor in international relations, and worthy of greater, and more serious attention than it has garnered in the past" (ANDERSON, 1998:422). Essa passagem explica bem a importância das operações encobertas nas relações internacionais contemporâneas.

propaganda – brancas, cinzas ou negras, salienta-se de início que a utilização de propaganda branca é própria de ações abertas (*overt* propaganda), e comumente são utilizadas nas operações psicológicas. A propaganda encoberta (*covert* propaganda) é uma estratégia de operação encoberta, e pode ter a fonte completamente secreta (*black*) ou parcialmente escondida (*gray*).

As operações encobertas levantam uma série de questões em relação a sua eficácia, mormente à utilização de técnicas de propaganda. É possível destacar vários pontos negativos, como os danos ocasionados à política externa por causa dessas operações; a necessidade de compreensão cultural para se ter sucesso ao manipular outras culturas; o fato de que a combinação entre poder e segredo sugere corrupção (BLOOMFIELD JR., 1990); o fato de não constituírem um mecanismo de resolução de crises; e os limites obscuros entre os resultados das operações militares em comparação às encobertas (STEMPEL, 2007). Outros advogam em favor dessas operações, salientando a sua utilidade se integradas em um conjunto de política externa coerente e se mantida a coordenação entre as agências governamentais (GODSON, 1995). Além disso, existem casos em que o resultado esperado não pode ser obtido por formas abertas de ação, o que requer a utilização de uma operação secreta.

Apesar dos pesares, as operações encobertas são atividades essenciais para os serviços de inteligência em momentos de crise, tanto por sua dimensão informativa quanto pela dimensão persuasiva. E são justamente essas duas dimensões que explicam a necessidade de se compreender as técnicas de propaganda como operações encobertas. Inteligência é, sobretudo, aliar informação à estratégia. E, na perspectiva das ações encobertas como elemento de inteligência, que forma mais característica existe disso do que a propaganda, uma informação estrategicamente montada e posicionada para a obtenção dos interesses nacionais?

Propaganda, por fim, como estratégia de ação, faz parte do rol de capacidades que compõem as operações encobertas. Pode-se dizer, de qualquer modo, que as operações informacionais, do tipo psicológicas, incluem um elemento de propaganda, sem dúvida. Porém, nesse caso, ela deve ser vista muito mais como instrumento que como estratégia, isto é, mais como meio de operação psicológica do que como fim.

7.5. Conclusão

Com o presente texto, buscou-se um esforço metodológico no sentido de delimitar os conceitos de propaganda, operações encobertas e operações psicológicas, devido à utilização indiscriminada desses termos na literatura especializada. Partiu-se do conceito inicial de inteligência e da interpretação do mesmo, para enquadrar as operações encobertas como um componente essencial

dessa atividade. Posteriormente, foi feita a conexão entre esses fenômenos e as operações informacionais, típicas do Departamento de Defesa dos Estados Unidos.

Após, seguiu-se uma tentativa de teorizar a respeito do significado da palavra propaganda, e de suas dimensões como técnica e estratégia. Foram utilizados exemplos de formas de propaganda durante épocas de conflito para que se pudesse retirar os elementos primordiais dessa estrutura: a persuasão e o propósito.

Ao final, as duas últimas seções debateram os conceitos de operações psicológicas, muito confundido com as estratégias de propagandas encobertas, e as operações encobertas em si, com o escopo de demonstrar a diferença na utilização do termo propaganda em cada uma dessas atividades.

Não obstante o esforço deste trabalho, a questão permanece em aberto. Se a atividade de inteligência for considerada em uma perspectiva restritiva, as operações encobertas serão vistas no máximo como atividades associadas, e o enquadramento da propaganda como estratégia de inteligência de disseminação de informação fica comprometido. Mas, como em tudo na ciência, essa é apenas uma questão de ponto de vista.

REFERÊNCIAS

ANDERSON, Elizabeth E. (1998). The security dilemma and covert action: The Truman years. *International Journal of Intelligence and CounterIntelligence*, 11:4, 403-427.

BETTS, Richard K. (1978). Analysis, War, and Decision: Why Intelligence Failures Are inevitable. *World Politics*, vol. 31, n. 1, p. 61-89.

BITTMAN, Ladislav. (1990). The use of disinformation by democracies. *International Journal of Intelligence and CounterIntelligence*, 4:2, 243-261.

BLOOMFIELD JR., Lincoln P. (1990). The legitimacy of covert action: Sorting out the moral responsibilities. *International Journal of Intelligence and CounterIntelligence*, 4:4, 525-537.

BOWDISH, Randall G. (1999). Information-Age Psychological Operations. *Military Review*, December/February 1999, p. 28-36.

BRUNEAU, Thomas C. & BORAZ, Steven C. (2007). *Reforming intelligence*: obstacles to democratic control and effecttiveness. Austin - TX, University of Texas Press.

CEPIK, Marco. (2003a), *Espionagem e Democracia*: agilidade e transparência como dilemas na institucionalização de serviços de Inteligência. Rio de Janeiro: RJ, Editora FGV.

_____. (2003b). Inteligência e políticas públicas: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*, vol. 2 Winter 2002/2003.

GODSON, Roy. (1995). *Dirty Tricks or Trump Cards*: U.S. Counterintelligence and Covert Action. Washington – D.C., Brassey's.

HERMAN, Michael. (2001). *Intelligence services in the information age*. London, FrankCass.

JCS U.S. DOD *Dictionary of Military and Associated Terms*. Disponível em: <http://www.dtic.mil/doctrine/dod_dictionary/index.html>. Acesso em: 02 dez. 2009.

JOHNSON, Loch K. (1992). On Drawing a Bright Line for Covert Operations. *The American Journal of International Law*, vol. 86, n. 2, p. 284-309.

NARULA, Sunil. (2004). Psychological Operations (PSYOPs): A Conceptual Overview. *Strategic Analysis*, vol. 28, n. 1, Jan-Mar.

NELSON, Richard Alan. (1996). *A Chronology and Glossary of Propaganda in the United States*. Westport, Connecticut, GreenWood Press.

PAUL, Christopher. (2008). *Information Operations*: doctrine and practice. Westport, Connecticut, Praeger Security International.

RAMSON, Harry Howe. (1980) Being Intelligent about Secret Intelligence Agencies. *The American Political Science Review*, vol. 74, n. 1, p. 141-148.

SEGELL, Glen M. (2009), Creating Intelligence: Information Operations in Iraq. *International Journal of Intelligence and CounterIntelligence*, 22:1, 89-109.

SILVA, Guilherme A.; GONÇALVES, Williams. (2005), *Dicionário de relações internacionais*. Barueri, SP: Manole.

SIMS, Jennifer. (2009). A theory of intelligence and international politics. In: TREVERTON, G.; AGRELL, W. *National Intelligence Systems*: current research and future prospects. Cambridge - MA, Cambridge University Press, p. 58-92.

STEMPEL, John D. (2007). Covert Action and Diplomacy. International Journal of Intelligence and CounterIntelligence, 20:1, 122-135.

WALLERSTEIN, Immanuell. (2002). The Eagle has Crash Landed. *Foreign Policy*, July–August: 60-80.

WETTERING, Frederick L. (2003). Covert Action: The Disappearing of C. *International Journal of Intelligence and CounterIntelligence*, 16:4, 561-572.

WHITE, Ed. (2002). The Value of Conspiracy Theory. *American Literary History*, vol. 14.1, p. 1-31.

Capítulo 8

INTELIGÊNCIA E DISSUASÃO: IMINT E LEGITIMAÇÃO

Fabrício Schiavo Ávila

A inteligência militar, no nível estratégico, está sofrendo uma profunda alteração. Desde o início do século XXI, o advento da digitalização trouxe novas perspectivas para a aquisição de informações estratégicas. O termo digitalização ainda não encontra uma definição satisfatória porque estamos vivendo o processo, mas poderíamos conceituá-lo como o impacto das plataformas da informática nos sistemas de armamentos. Esse fenômeno compreende uma profunda modificação nos meios de condução dos conflitos. O impacto desse fenômeno não está desvinculado de uma dimensão prosaica, tampouco dos meios de aquisição de informações que servem para a condução de conflitos.

Concomitantemente, na esfera estratégica, a dissuasão não perdeu sua importância, pelo contrário, sofisticou-se.[1] Nesse sentido, existem quatro conceitos auxiliares. Em primeiro lugar, a dissuasão (deterrence) consiste na ameaça de emprego de armas nucleares como resposta a um ataque nuclear. (GRAY, 2003: 13). Atualmente, a China amplia e moderniza seus arsenais nucleares, frente a uma ameaça de ataque preventivo dos Estados Unidos da América.[2]

---

[1] *Deterence*, *dissuasion* e *compellence* ainda não possuem uma tradução na língua portuguesa. Devido a esse motivo, os termos não serão traduzidos. Da mesma forma, dissuasão será mantido como *deterrence*.

[2] Na língua inglesa, *preemptive* é um adjetivo relacionado com o substantivo *preemption*, que pode ser traduzido por preempção. O *Dicionário Houaiss da língua portuguesa* não registra a palavra "preemptivo", mas registra preempção com os seguintes significados: compra antecipada, precedência na compra ou, em informática, quando sistemas multitarefa alteram a condição de processamento de uma instrução de um programa para outro. Como preempção e preemption provêm do vocábulo latino praemptione ('prae' – antes e 'emptione' – compra), o sentido da diferença estabelecida no vocabulário inglês entre prevenção e preempção reside em um hiato temporal significativo. Enquanto a prevenção lida com a antecipação de média e longa duração, a preempção lida com eventos que são de curto prazo ou iminentes.

Em segundo lugar, a *deterence* é a capacidade de impedir um ataque convencional, aumentando a quantidade de armas nucleares no arsenal. Originalmente, esse conceito foi desenvolvido pela França do pós-Segunda Guerra Mundial, frente ao receio de um ataque da Alemanha. Atualmente, a Coréia do Norte empreende um programa de construção e teste de artefatos nucleares para impedir um possível ataque sul-coreano em seu território.

A tentativa de coagir a vontade do outro é a *compellence*, a forma mais branda de política dissuasória. O Irã está sendo forçado a abrir seu programa nuclear para as inspeções estrangeiras. Todavia, a *dissuasion* é a forma mais violenta desse tipo de política. Corresponde ao desarme estratégico de um oponente. A primeira experiência histórica foi a destruição do reator iraquiano de Osirak, pela Força Aérea Israelense, em 1983. (GRAY, 2003:16) A invasão do Iraque em 2003 demonstrou os efeitos nefastos da implementação dessa política. Os arsenais desses países foram vigiados por plataformas espaciais. A busca da informação para a tomada de decisão leva os países a buscar, na vigilância espacial, suporte para essa decisão.

As informações, no nível estratégico, compreendem uma dimensão da segurança do Estado em que o limite entre a informação para a decisão e a guerra silenciosa fica muito tênue. Localização de bases aéreas, reatores nucleares, depósito de armas, entre outros, assumem uma grande vulnerabilidade em tempos de guerra. Ao mesmo tempo, a digitalização dos armamentos proporcionou o surgimento de uma série de artefatos bélicos e plataformas de vigilância cuja manufatura está no alcance dos países em desenvolvimento.

A horizontalização de capacidades com o baixo custo dos armamentos está mudando a polarização no sistema internacional inexoravelmente.[3] Talvez nenhum país do mundo tenha a capacidade de investimento dos norte-americanos em tecnologias do espaço. Entretanto, alguns países do mundo, neste momento, podem adquirir certa capacidade IMINT e SIGINT de maneira assimétrica. No outro extremo, capacidades que são assimétricas, nos padrões europeus e norte-americanos, adquirem um caráter estratégico nas nações em desenvolvimento. Nesse sentido, a dissuasão do século XXI passa pela busca de informação na esfera estratégica, principalmente, na vigilância IMINT da tríade de armas estratégicas do adversário.[4] Este trabalho pretende discutir a relação entre a legitimação de políticas de dissuasão e a capacidade de coleta de

[3] Horizontalização de capacidades é a popularização de plataformas de combate, antes restritas a poucos países.

[4] Tríade estratégica compreende mísseis estratégicos armados de ogivas nucleares de alcance intercontinental (ICBMs), submarinos de propulsão nuclear armados de mísseis estratégicos de alcance intercontinental (SLBMs) e bombardeiros de alcance intercontinental armados de bombas ou mísseis nucleares.

informações visuais através de plataformas espaciais. [5] A IMINT e a necessidade do Comando do Espaço estão ligados, intrinsecamente. [6] Contudo, a discussão teórico-metodológica será conduzida na conclusão deste trabalho.

8.1. Deterrence e a Estabilidade Estratégica

Na grande estratégia, os Estados Unidos ainda são líderes e precursores de novas tecnologias.[7] Contudo, os Estados Unidos não estão imunes das querelas sobre a digitalização. A abundância de recursos materiais e humanos pode dificultar a adaptabilidade da sua organização burocrática para a nova realidade da digitalização. Neste sentido, o conceito da administração do espaço sideral é pautado pela Geopolítica de Mahan.[8] O espaço sideral surge como uma nova dimensão da esfera estratégica. Nesse sentido, os artefatos comissionados do espaço possuem o mesmo papel das belonaves. Assim como no mar, a função primordial desses armamentos é a manutenção de linhas de comunicação, que difere da lógica das forças terrestres (captura e manutenção de posições em territórios).

Os Estados Unidos estão muito preocupados com a militarização do espaço exterior, ainda mais depois do teste ASAT chinês.[9] Vários países investem maciçamente em plataformas. A digitalização proporciona o emprego de tecnologias em outros níveis. Por exemplo, UAVs iranianos, de uso tático, para reconhecimento no Golfo Pérsico, possuem emprego estratégico.

Desde a década de 1960, os Estados Unidos da América, assim como os russos, lançaram-se na conquista e consolidação de plataformas no espaço exterior. O acesso a diferentes formas de aquisição de imagens começou o processo de profissionalização de um novo ramo da inteligência, a IMINT.

A IMINT, ou a aquisição de dados a partir de imagens, começou com sobrevoos de aviões, em missões arriscadas, na aquisição de imagens. A derrubada do piloto norte-americano Gary Powers em 1960 e, concomitantemente, o processo da crise dos mísseis em Cuba, mostrou o valor das imagens adquiridas por satélites. Essas plataformas espaciais foram eficientes por dois motivos

---

[5] Legitimação é o enquadramento de valores para legitimar uma disciplina, de acordo com a ideologia vigente de uma classe dominante (BONAVIDES, 2007:121). Contudo, a legitimação está voltada para o público interno de um Estado porque, no Sistema Internacional, vigora a Anarquia (ausência de um poder superior organizador) (WALTZ, 1979).

[6] Comando do Espaço refere-se à capacidade de uma nação em possuir uma rede de comando e controle no espaço sideral, análogo à capacidade das marinhas no domínio do mar.

[7] Grande estratégia consiste na organização das forças produtivas e de defesa de um país para a obtenção de fins políticos definidos. Talvez, o programa de modernização chinesa, nas quatro grandes áreas, ilustre esse conceito (NARIZNY:2007).

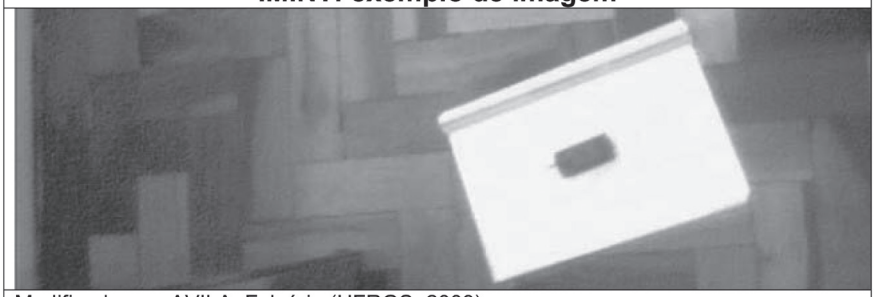
[8] Alfred Tayer Mahan escreveu no contexto do poder naval do final do século XIX. O espaço sideral é análogo aos oceanos e suas plataformas corresponderiam aos navios de guerra (COSTA, 2008:68-78).

[9] ASAT - Anti-Satelllite Weapon. O teste chinês foi em janeiro de 2007. Dois satélites obsoletos colidiram em órbita.

principais: não violavam os espaços aéreos e não causavam constrangimentos diplomáticos pela baixa de pilotos.

Artesanalmente, um modelo de imagem adquirida em combate pode ser produzido:

IMINT: exemplo de imagem



Modificado por: AVILA, Fabrício (UFRGS, 2009)

O modelo acima foi produzido de forma artesanal para a ilustração da inteligência por imagens. Um modelo de um carro de combate norte-americano M-1 Abrams, na escala 1:113, encontra-se em uma folha de tamanho A4. Em uma altura real de 1,5m, foi tirada uma foto de uma webcam, com uma objetiva de 3mm de diâmetro. Na escala do tanque, 1,5 corresponderia a 170m, aproximadamente. Isso corresponderia a uma altitude de operação de um UAV.[10] A foto produzida possui a escala de 1:6cm, aproximadamente. Mesmo sem o zoom, a foto possuiria uma escala dezoito vezes maior que a do modelo do blindado. Esse pequeno exemplo mostra as armadilhas de escala a que os analistas são submetidos. Por isso, os países investem nessa área, formando instituições de inteligência voltadas para a interpretação das informações obtidas por diversos sensores. Neste sentido, os investimentos na área de inteligência são fundamentais.

Os problemas da IMINT, na área da estratégia, possuem diversas dimensões. Isso pode ser aprofundado, principalmente, com a chegada ao poder de Barack Obama que, de acordo com o orçamento de defesa, pretende lançar uma guerra de baixa intensidade para amenizar os problemas no Afeganistão e Iraque, comportamento análogo à administração do presidente Kennedy. (FREEDMAN, 2000). Para isso, anunciou a retirada do escudo antimíssil na Europa e aproximou-se da Rússia.[11]

Todavia, a Ásia oferece-nos a perspectiva da consolidação inexorável de um sistema internacional multipolar. Desde o colapso do sistema soviético em 1991, a China desponta como a grande potência que pode concorrer com a superioridade

[10] UAV – Umanned Aerial Vehicle. Veículo Aéreo não Tripulado.

[11] Notícia veiculada nos meios de comunicação. Porém, a exatidão dos termos do acordo e seu alcance estratégico ainda permanecem incógnitos.

norte-americana. Esta seção do trabalho apresenta dois pontos concomitantes. Se, de um lado, os norte-americanos se utilizam de suas plataforma espaciais para a vigilância IMINT da China, os chineses empreendem a consolidação de um Comando do Espaço.

Todavia, politicamente, a inteligência por imagens pode cooperar para a implementação de estratégias. O advento de programas como o Google Earth e sua utilização pela mídia, pode aumentar a percepção de ameaças, principalmente pelos países que mais resistiram à unipolaridade no sistema internacional. Nesse contexto, a China surge como uma nova rival dos Estados Unidos da América.

A modernização militar chinesa ainda constitui uma questão em aberto. As suposições sobre a defesa chinesa estão sendo pesquisadas, mas os trabalhos apontam para direções diferentes.

A dimensão que se apresenta mais obtusa refere-se à delimitação de uso de obras de defesa que podem apresentar emprego duplo na esfera estratégica, como por exemplo, proteção contra ICBMs, e nas operações, estoque estratégico.[12] A figura abaixo mostra que, em Lop Nur, existe um túnel cuja função ainda não é especificada. Neste sentido, os problemas vinculam-se a uma análise primária das imagens obtidas pelos satélites. Essa imagem foi obtida em 2007, gratuitamente, pelo programa Google Earth.

O problema da hipótese oriunda da utilização de um túnel, na China, ainda merece um cuidado descritivo mais apropriado. Cientistas podem se enganar caso as fontes de imagens não sejam contrastadas com outros tipos de aquisição de informações. (KRISTENSEN, NORRIS & McKENZIE, 2006: 125) Neste sentido, não se pode afirmar que a localização de um túnel, em Lop Nur, esteja intrinsecamente ligada à questão de defesa contra armas estratégicas.

China: entrada de túneis

Modificado por: AVILA, Fabrício (UFRGS, 2009)

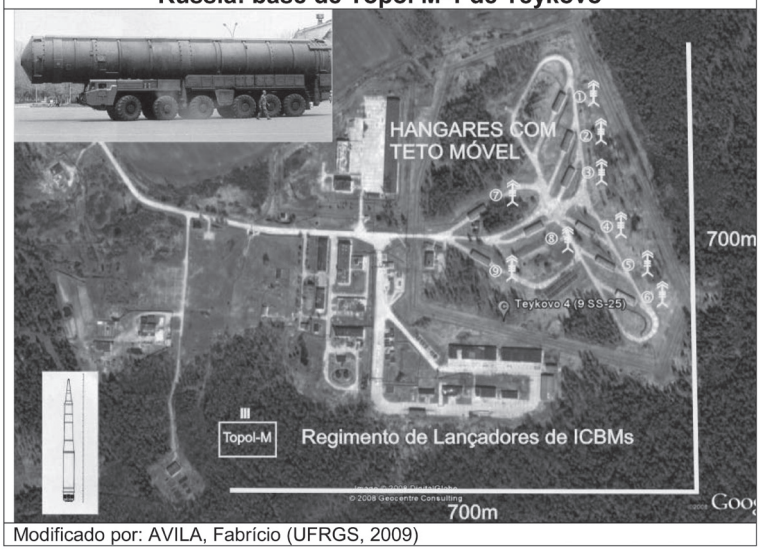
[12] ICBM – Inter-Continental Ballistic Missile. Míssil Balístico Intercontinental.

Essa hipótese deveria ser complementada com outras fontes, coletadas ou por meio de sinais eletrônicos (SIGINT), ou outro tipo de fonte, ostensiva ou não. A imagem acima obtida apresenta uma defasagem temporal. Plataformas de vigilância, em tempo real, podem ser uma grande fonte de informação, porque o fluxo de veículos poderia denunciar o papel da utilização da caverna. Nesse sentido, a identificação dessas máquinas militares pode sofrer problemas, pois a camuflagem de instalações e veículos é amplamente utilizada. Outrossim, quando a camuflagem não é possível, vários países utilizam-se de reproduções de modelos de blindados, na escala real. Geralmente, sendo de plástico, madeira ou papelão, confundem os sistemas óticos de reconhecimento e em caso de conflito, ocasionam o desperdício de munição.

Ainda dentro do conceito clássico de dissuasão, a Rússia desponta como o outro país desafiante da unipolaridade. A figura abaixo mostra a disposição das bases de ICBMs Topol M-1. (KRISTENSEN, NORRIS & McKENZIE, 2006).

A figura abaixo mostra um arranjo físico de uma instalação de mísseis estratégicos. Nesse sentido, pode ser mostrada a disposição de subunidades de combate. Esse tipo de imagem mostrou que essa base possui realmente um papel estratégico para os russos. A presença dos tetos telescópicos, de manutenção dos mísseis, denuncia seu emprego, sendo que, no ambiente russo, as considerações de profundidade do território existem em uma escala que não pode ser comparada a nenhuma outra nação. Contudo, os radares da OTAN, instalados na República Tcheca são mais distantes que o território da Geórgia. Essa hipótese pode ilustrar o tipo de reação que as forças armadas russas tiveram no episódio do conflito entre os dois países.

Rússia: base de Topol M-1 de Teykovo



Modificado por: AVILA, Fabrício (UFRGS, 2009)

Esta seção tentou demonstrar, dentro do conceito clássico de dissuasão, os limites da construção de ameaça e de reconhecimento de forças. Assim como os chineses, os russos também poderiam colocar seus mísseis em um túnel para a proteção. Contudo, não poderíamos saber dos detalhes dos armamentos estratégicos envolvidos na inteligência estratégica sem a ajuda de outras plataformas de coleta de informações. Esse fato, porém, não diminui a importância das imagens na qualidade da informação.

8.2. *Deterence* e Prevenção de Conflitos

A Coreia do Norte ainda possui uma das maiores forças convencionais do mundo.[13] Esse contingente é um reflexo do Estado de Guerra permanente da Península Coreana desde a metade do século XX. Contudo, os últimos anos têm despertado na comunidade internacional a percepção da Coreia do Norte como uma ameaça crível, com o teste de mísseis e a construção de artefatos nucleares. Novamente, a vigilância espacial IMINT do inventário do arsenal norte-coreano está no cerne da construção da ameaça do país frente aos países vizinhos. A figura abaixo mostra o complexo de Musudan-ri, de lançamento de mísseis de médio alcance.

Coreia do Norte: complexo de Musudan-ri

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Essa seria a localidade que materializa a política de dissuasão estratégica do deterence.[14] A Coreia do Norte pretende fazer frente a um ataque convencional preventivo de desarme de japoneses e sul-coreanos. O país desafiou os Estados

[13] Compreende cerca de um milhão de homens em serviço ativo, quase cinco milhões de reservistas e quase noventa mil comandos. (IISS, 2008: 387b)

[14] *Deterence* consiste em prevenir que um Estado utilize suas forças armadas convencionais. (FREEDMAN, 2003:303) Esse conceito, originalmente, foi formulado pela França, temerosa de um ataque alemão.

Unidos da América no contexto da unipolaridade no sistema internacional, o que levou a administração de George W. Bush a classificar o país como parte do "Eixo do Mal".[15] Entretanto, a ameaça construída sobre Coreia do Norte precisa de certos ajustes, pois, por exemplo, os mísseis testados pelo país apresentam graves defeitos e os artefatos nucleares testados carecem de estudos.

Outro exemplo apresenta-se, na figura abaixo, que mostra o reator norte-coreano de Yongbyon:

Coreia do Norte: Reator de Yongbyon

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Geralmente, mede-se a possível produção de energia de um reator nuclear, de acordo com o corpo de água, onde é despejada a água oriunda da fissão nuclear. Nesse sentido, o reator norte-coreano tem sua produção estimada em 5 MWh.[16] Comparativamente, a figura adiante mostra o possível reator nuclear localizado em Asquelon, Israel.

Esse suposto reator nuclear está camuflado como uma usina termelétrica ordinária.[17] Contudo, a aplicação de uma lente térmica, utilizando o programa Corel Draw 14, mostra uma grande quantidade de água em altas temperaturas. As usinas nucleares necessitam de grandes quantidades de água para resfriarem

[15] Eixo do Mal era a denominação dada a países desafiantes da unipolaridade estadunidense no Sistema Internacional e compreendia Líbia, Iraque, Irã e Coreia do Norte. Habilmente, a Líbia desarmou-se e o Iraque foi invadido em 2002. Os outros dois países continuam na mesma situação.

[16] Refere-se a um milhão de Watts produzidos em uma hora.

[17] Usina termelétrica consiste na geração de energia elétrica através da combustão de carvão ou gás natural. Tecnicamente, as usinas nucleares são um tipo de usina termelétrica que obtém energia elétrica a partir da fissão do urânio.

seus reatores. Nesse sentido, essa usina seria estratégica para Israel porque forneceria energia elétrica e água potável dessalinizada para a sua população.

Israel: reator nuclear de Asquelon

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Novamente, a decisão estratégica da Coreia do Norte de recorrer à política de *deterence* remete a uma construção de ameaça que corrobora a hipótese de guerra preventiva na Península Coreana. Outrossim, esta seção mostrou que a comparação entre imagens também consiste em uma técnica de apropriação de informação estratégica a partir de imagens.

8.3. *Compellence* e Apoio Político

A República Islâmica do Irã enfrenta, desde 1979, a construção de uma ameaça no sistema internacional. Iranianos e norte-coreanos foram classificados pelos norte-americanos como parte do "Eixo do Mal". Geograficamente, o país possui a oeste a presença dos Estados Unidos no território de seu inimigo histórico, o Iraque. Ao mesmo tempo, a leste, os norte-americanos estão presentes no Afeganistão e no Paquistão. O governo do Irã produz uma tentativa de esboçar uma independência energética com a construção de novas usinas elétricas nucleares e, no suporte direto, está a construção e implementação de novos armamentos no inventário.

Os iranianos estão sofrendo a estratégia estadunidense da compellence, ou seja, estão sendo compelidos a aceitar um comportamento imposto. (GRAY, 2003:13). Atualmente, o país está sendo forçado a abrir suas instalações nucleares para a inspeção internacional.[18] Nesse sentido, o debate insere-se no objeto das imagens vinculadas nos meios de comunicação de massa e na discussão a respeito

[18] O presente trabalho foi escrito em novembro de 2009.

da real ameaça para o sistema internacional. Este capítulo pretende demonstrar a importância da IMINT para a complementação das pesquisas sobre inventários.[19]

A figura abaixo suscitou grande debate na prospecção de itens militares nas imagens de satélite obtidas de fontes gratuitas. Esses veículos são caminhões no Norte da base aérea iraniana de Shiraz.

Irã: postos de comando móveis.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Inicialmente, pensou-se que esses caminhões eram veículos de reabastecimento de aeronaves. Contudo, a partir da verificação das dimensões dos veículos, como largura e comprimento, a afirmação foi descartada. A hipótese mais aceita é que esses veículos seriam postos móveis de comando e controle, ou seja, caminhões dotados de aparelhos eletrônicos que serviriam tanto para a comunicação com blindados e aeronaves como para auxílio na guiagem dos mísseis. Os iranianos adotariam esse tipo de veículo para que sua cadeia C4ISR não sofresse abalo em caso de combate aéreo. [20] Contudo, esta hipótese ainda se constitui muito frágil para receber qualquer afirmação mais peremptória.

Outra imagem que contrasta com os inventários disponíveis encontra-se em Shiraz, como mostra a figura abaixo:

Irã: aeronave AWACS.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

[19] Os inventários disponíveis são os Military Balance do International Institute for Strategic Studies de Londres, no período de 2003-2008.

[20] C4ISR compreende o comando das tropas em combate.

O avião na imagem supra mostra a existência no Irã de aviões do tipo AWACS.[21] Esses aviões de reconhecimento estratégico dariam ao país uma grande capacidade de defesa, o que justificaria a conservação da incógnita dessa arma dos inventários. Porém, seu tipo e origem não podem ser confirmados com certeza. Esse avião poderia ter origem no transporte da Força Aérea Iraquiana antes da Guerra do Golfo de 1991.[22] Outra investigação aponta para o repasse de armamentos oriundos da Rússia, o que seria mais plausível porque iranianos e russos compartilham fluxos econômicos pelo Mar Cáspio. O colapso do Irã privaria os russos de atingir uma saída crível para o Oceano Índico. Outrossim, os inventários do Irã mostram que o país continua diversificando as fontes de aquisição de material bélico.

Os iranianos aprenderam, com os embargos econômicos sofridos após 1979, a diversificar fontes e a manufaturar veículos.[23] Pelas reduzidas dimensões dos hangares, esse local deve ser um local de montagem e manutenção de aviões de transporte, como o Iran-140, um avião de transporte médio, bimotor. Pelas dimensões do país, esse tipo de avião deve possuir uma pequena necessidade de pistas para decolagem, sendo o veículo ideal para o transporte de tropas pelo interior.[24] A Força Aérea Iraniana possui quarenta (40) aeronaves desse tipo. (IISS, 2008:224a)

A figura abaixo mostra uma seção de manufatura da base iraniana de Shiraz.

Irã: manufatura de aviões.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

[21] AWACS – Airborne Warning and Control System.

[22] A Força Aérea Iraquiana foi enviada para o Irã antes da operação de guerra norte-americana Tempestade no Deserto de 1991. No inventário da Força Aérea do Irã ainda existem MiG-29s (A e UB), Mirages F-1E, Su-25Ks, Su-24MKs. (IISS, 2008: 244a)

[23] 1979 foi o ano do começo da Revolução Islâmica, liderada pelo aiatolá Ruhollah Khomeini. (FERRO, 2008: 146-167)

[24] A área do Irã é de 1.648.195 km².

Esta seção tentou mostrar que existe uma relação entre a política de dissuasão de *compellence* e a implementação da coerção no Sistema Internacional. Os ambientes de monitoramento consistem no respaldo da legitimação do uso da força frente à opinião pública do seu próprio território. Esse tipo de política torna-se sensível no tocante à escalada do conflito, na qual questões de inteligência poderiam ser a base de outras ações. A próxima seção refere-se a essa questão, ao abordar a experiência estadunidense na derrubada de Saddam Hussein, no Iraque.

8.4. *Dissuasion* e a Ameaça do Ataque Preemptivo

Desde 1991, com o fim da Segunda Guerra do Golfo, o Iraque estava sob pressão de desarmamento estratégico dos Estados Unidos.[25] A materialização desse fato foi a criação da Zona de Exclusão Aérea.[26] Nesse sentido, o Iraque foi forçado a não se rearmar e a não constituir uma ameaça. A secretária de Estado norte-americana, no governo de George Bush, anunciou o conceito de dissuasion: consiste na eliminação da ameaça, antes mesmo de sua formação. Ou seja, o advento da polaridade no sistema internacional implicaria no desarmamento estratégico dos países, mesmo que esses atores possuíssem somente armas convencionais. A relação entre a posse de armas de destruição em massa (WMD) e o governo do Iraque não foi estabelecida até hoje.[27] Contudo, permanece a dúvida a respeito de até que ponto a ameaça construída carrega a legitimidade de uma ação militar.

Conforme citado na seção acima, ainda permanece o mistério sobre as aeronaves da Força Aérea Iraquiana. A figura abaixo ilustra um problema:

Iraque: quatro aviões destruídos.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

[25] A Primeira Guerra do Golfo foi a Guerra Irã-Iraque, de 1980 até 1988. A Segunda Guerra do Golfo foi a invasão do Kuwait pelo Iraque e sua derrota pelos Estados Unidos da América e sua Coalizão (1990-1991) e a Terceira Guerra do Golfo começa com a invasão do Iraque pelos Estados Unidos da América em 2002.

[26] Desde 1991, o Iraque possuía as zonas de exclusão aérea, que compreendiam a área acima do paralelo 36°N (curdos) e abaixo dos 32°N (minoria xiita).

[27] WMD – Weapons Mass Destruction.

Nesse sentido, apesar da imagem desses aviões ter sido realizada após a invasão de 2002, não há como saber se esses aviões não haviam sido destruídos ainda na guerra de 1991. Pelas imagens, os aviões parecem ser do tipo Mirage F-1. Esse tipo de imagem serviria para reforçar o impacto da guerra no atrito, e é um tipo de reconhecimento é muito antigo. As unidades de artilharia do exército possuíam organicamente, no período da Segunda Guerra Mundial, uma unidade de controle de danos de alvos. Como exemplo, a artilharia divisionária da Força Aérea Brasileira possuía a Primeira Esquadrilha de Ligação e Observação, constituída de aviões leves. A adoção de plataformas de coleta espaciais não substitui o reconhecimento tático oferecido por aeronaves de combate. Contudo, a digitalização tem proporcionado cada vez mais a utilização de UAVs para esse tipo de missão. Sem piloto, a economia de combustível e o preço de fabricação fazem dessa arma um meio muito eficiente de aquisição de imagens.

Outra utilização das imagens em um conflito refere-se ao andamento do controle do processo de gestão do território ocupado. A imagem abaixo mostra um exemplo:

Iraque: instalações petrolíferas sabotadas.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Na Guerra de 1991, foi notório o desastre ecológico provocado pelas tropas iraquianas em retirada. Todavia, a maioria dos contingentes da resistência iraquiana era oriunda do exército. Não pode ser esquecido um contingente de um milhão de homens em 1991. A área de fotografia mostra o sul do Iraque, que estava sob controle britânico desde 2002. A imagem mostra a sabotagem de uma de quatro refinarias que faziam a ligação do Kuwait e do Iraque, além de destacar a dificuldade da utilização da reconstrução de um país.

Validando esse argumento, a inteligência a partir de imagens não serviria para o monitoramento de conflitos. Cabul, a capital do Afeganistão, oferece-nos uma perspectiva de emprego civil de plataformas de imagem. As fotos de satélites, obtidas a partir de 2001, mostram que, em seis anos, a cidade triplicou de tamanho. (BATSON, 2008:23) Esse emprego possuiria finalidades civis de reconstrução e planejamento urbano e atenderia às necessidades militares de combate à insurgência, indiretamente. Novamente, reafirma-se que somente a IMINT não bastaria para a política. O trabalho deveria ser acompanhado

da consulta a fontes locais e pesquisas demográficas para o controle do fluxo populacional durante o conflito.

A figura abaixo mostra a incapacidade dos países da coalizão, notadamente os Estados Unidos da América, em reerguer o país ocupado. Entretanto, as imagens utilizadas na construção de uma ameaça não mostram o relativo fracasso da contenção da resistência iraquiana e na reconstrução do país. Até hoje, ainda não foram provadas as vinculações entre o regime de Saddam Hussein e a fabricação e manutenção de armas WMD.

Iraque: poços de petróleo inutilizados.

Modificado por: AVILA, Fabrício (UFRGS, 2009)

Os problemas da utilização de imagens ainda não conseguem obter uma parcialidade técnica. A sofisticação de plataformas e a sua popularização, oriunda da digitalização, mostram um fluxo de informações que ainda não conseguimos mensurar. Não obstante, essa seção tentou mostrar que a dissuasion ainda apresenta problemas quanto a sua legitimação. Para a opinião pública norte-americana, e mundial talvez, a dissuasion passou para a História como uma agressão gratuita, não como um reflexo da balança de poder unipolar do pós-Guerra Fria.[28]

A IMINT é insuficiente para esse tipo de política. Seus argumentos e trabalhos de coleta de informações podem garantir legitimação a um ataque cirúrgico, contra um alvo limitado, como o reator iraquiano de Osirak em 1983. Entretanto, sua legitimação precisaria de mais plataformas de coleta de informações estratégicas para um conflito prolongado. O exemplo histórico

[28] Balança de Poder são as condições de equilíbrio de poder entre Estados-chave do Sistema Internacional (PAUL, WIRTZ e FORTMANN, 2004:03)

da invasão norte-americana do Iraque em 2002 mostrou que um número insuficiente de informações destrói os argumentos para a preparação de uma hipótese de guerra. Os Estados Unidos da América estão em dois conflitos, Afeganistão e Iraque, simultaneamente, cujo envolvimento está sendo mais oneroso que no Vietnã, proporcionalmente. Já são sete anos de insurgências de uma guerra convencional de dois meses.

8.5. Conclusão

A IMINT constitui-se na dimensão da inteligência que mais influencia a política. Seu alcance deve-se ao impacto da fácil assimilação frente ao homem comum. Desde a Guerra do Vietnã, a opinião pública ficou muito perplexa frente aos horrores da guerra. A legitimação sofreu um colapso e o apoio do homem comum desapareceu no esforço de guerra. Entretanto, o contexto no Sistema Internacional era da bipolaridade e a política era da deterrence, a dissuasão clássica.

Na hipótese de guerra contra o Iraque, em 2002, dentro da política de dissuasion, a situação apresentava-se diferente. As imagens foram utilizadas para a sustentabilidade do esforço de guerra estadunidense, dentro da busca do apoio da comunidade internacional no esforço de guerra. Contudo, as imagens foram suficientes para o apoio inicial da guerra, mas se tornaram frágeis frente ao desenvolvimento do conflito.

A conclusão principal desse estudo pode ser enunciada na tabela abaixo:

Relação entre a necessidade de técnicas para legitimação das políticas de dissuasão				
Dissuasão/Técnicas	IMINT	SIGINT	ELINT	OSINT (inventários)
Deterrence	X			
Deterence	X	X		
Compellence	X	X	X	
Dissuasion	X	X	X	X

É exigida mais tecnologia de obtenção de informações para a legitimação do uso da força. A dissuasão baseia-se em hipóteses de conflito, insofismavelmente. Reafirmo que as imagens apresentam grande impacto para o homem comum na compreensão do conflito. O argumento continua com a preocupação desse trabalho ao mostrar a construção da percepção da ameaça. Quanto mais é exigido

o uso da força, acompanhado da perda de soberania, mais se necessita de coleta de informações para a sua legitimação.

Nesse sentido, cada capítulo tentou ilustrar a fragilidade das hipóteses de guerra, baseadas na construção de ameaças, a partir da IMINT. A China não é uma ameaça crível porque sua atitude é defensiva, dentro do exemplo da política de deterrence. Seus arsenais nucleares são comparativamente muito inferiores, em quantidade, aos arsenais norte-americanos.[29] A única ameaça real dos chineses constitui uma capacidade de segundo ataque frente a um ataque nuclear estadunidense. (BLAIR e YALI, 2006:51-78) Essa resposta impacta a balança de poder no sistema internacional, dentro da conjuntura de utilização de alta tecnologia para fazer frente à assimetria quantitativa. Todavia, a IMINT já é suficiente para a deterrence, porque os custos políticos são proibitivos em uma guerra nuclear.

A Coreia do Norte não é ameaça porque seus mísseis são ineficientes.[30] Dentro do contexto do *deterence*, a utilização de maiores plataformas se faz presente, porque o impacto na balança de poder regional de um ator que faz uso de bombas atômicas para desencorajar ataques convencionais deixa o sistema internacional mais instável. Por esse motivo, a IMINT necessita de ELINT para a monitoração de testes atômicos realizados.

Igualmente, dentro do contexto da *compellence*, o Irã não é ameaça porque possui um PIB de 600 bilhões de dólares, menos que os gastos norte--americanos em defesa (IISS, 2008) Contudo, além da IMINT e ELINT, a pesquisa sobre os inventários se faz necessária, pois o motivo se encontra na construção de ameaça a partir da posse de artefatos WMD. A maior proteção dos iranianos é a imobilidade da comunidade internacional frente a uma nova hipótese de guerra preventiva, como mostrou o ano de 2002.

Finalmente, dento da política de dissuasion, o Iraque não era ameaça porque o país já estava derrotado e repartido desde 1991. Sua Força Aérea foi dada ao Irã no início da década de 1990. Sua Marinha não existia mais e seu Exército estava reduzido a um terço. Dentro da conjuntura da unipolaridade do Sistema Internacional, os estadunidenses destruíram um Estado que, ineficazmente, garantia uma estabilidade naquele país. São sete anos de uma intervenção que se revelou desastrosa e onerosa em termos econômicos e, principalmente, políticos.

---

[29] Em 2008, os chineses possuíam cerca de 50 ICBMs. (IISS, 2008:376a) Essa transição corresponde ao programa de modernização que desestabilizou seu arsenal, quantitativamente. Entretanto, os novos mísseis estratégicos garantirão um papel preponderante da China no Sistema Internacional.

[30] O único míssil que os norte-coreanos possuem, realmente eficaz, é o míssil Scud, do qual eles têm aproximadamente 200 unidades, em 30 veículos eretores-lançadores (TEL) (IISS, 2008:388a). Os mísseis testados sobre o Mar do Japão são tentativas de agregação de estágios nessa arma, cujos resultados são duvidosos. Suas armas nucleares ainda produzem controvérsias sobre rendimento. A WMD que é notória de utilização pelo país são as armas químicas. Os estoques são desconhecidos, mas cada divisão possui uma companhia especializada em armas químicas.

A conclusão aponta para a necessidade de um maior estudo entre a relação intrínseca das imagens na legitimação de políticas dissuasórias que possuem impacto direto nas balanças de poder. A combinação da utilização de *softwares* de imagem, internet e televisão pode contribuir para uma rapidez muito maior da construção da percepção de ameaça. Como demonstrou a intervenção no Iraque, em 2002, os efeitos podem ser nefastos no sistema internacional, principalmente porque uma legitimação frágil pode colapsar o apoio às políticas estratégicas dos Estados envolvidos nos conflitos. No outro extremo, a digitalização de plataformas de coleta de imagens está proporcionando, a países de baixa polaridade, um recurso estratégico de longo alcance.[31] A conjuntura mostra o advento de novas tecnologias que poderão conduzir o Sistema Internacional às novas políticas de dissuasão.

REFERÊNCIAS

ADELMAN, Kenneth & AUGUSTINE, Norman. (2005). The Defense Revolution: Intelligent Downsizing of America's Military. San Francisco: Institute for Contemporary studies Press, 1990. In.: BEASON, Doug. The *E-Bomb*: how America's new direct energy weapons will change the way future wars will be fought. Cambridge, Da Capo Press, p. 33.

ARON, Raymond. (1986a). *Paz e Guerra entre as Nações*. Brasília: Editora UnB, 928 p. 2ª edição.

ARON, Raymond. (1985). *Estudos Políticos*. Brasília: Editora UnB, 562 p.

ARON, Raymond. (1986b). *Pensar a guerra,* Clausewitz: A Era Europeia. (Tomo I). Brasília: Editora UnB, 415 p.

BATSON, Douglas E. (2008). *Registering the Human Terrain*: a valuation of cadastre. Washington: NDIC Press.

BLAIR, Bruce & YALI, Chen. (2006). The Fallacy of Nuclear Primacy. China Security, p. 51-78.

BONAVIDES, Paulo. (2007). *Ciência Política*. (14ª edição) São Paulo: Malheiros Editores.

BUZAN, Barry & WÆVER, Ole. (2003). *Regions and Powers*: the structure of International Security. Cambridge-UK: Cambridge University Press. 564 p.

CLAUSEWITZ, Carl von. (2003). *Da guerra*. São Paulo: Martins Fontes.

CORDESMAN, Anthony H. (2007). *Iran, Israel, and Nuclear War*. Washington: CSIS. (on-line) http://www.csis/burke (01/12/2007).

COSTA, Wanderley. (2008). *Geografia Política e Geopolítica*: discursos sobre o território e o poder. (2ª ed.) São Paulo: Editora da Universidade de São Paulo.

DUNNINGAN, James F. (1993). *How To Make War*: A Comprehensive Guide To Modern Warfare in The 21st Century, (Fourth Edition). New York: Quill, 659 p.

[31] Polaridade refere-se à capacidade do país em causar impacto no Sistema Internacional (WALTZ, 1979).

FARIA, Luiz. (2004). *A Chave do Tamanho*: desenvolvimento econômico e perspectivas do Mercosul. Porto Alegre: Editora da UFRGS/FEE.

FERRO, Marc. (2008). *O Choque do Islã*. Rio de Janeiro: Bilblioteca do Exército Editora.

FREEDMAN, Lawrence. (2000). *Kennedy's Wars*: Oxford: Berlin, Cuba, Laos and Vietnam. Oxford University Press.

FREEDMAN, Lawrence. (2003). *The Evolution of Nuclear Strategy,* (3ª edição). Nova York, Palgrave MacMillan.

GLASSTONE, Samuel, e DOLAN, Philip. (1977). *The Effects of Nuclear Weapons*, 3ª edição. Washington: U.S. Government Printing Office. 644 p. (on-line) http://www.princeton.edu/~globsec/publications/effects/effects.shtml (06/06/2007).

GRAY, Colin. (2003). Maintaing Effective Deterrence. ISS. p. 13-16.

IAEA. (1970). Nuclear Non-Proliferation Treaty (NPT). Genebra.

IISS. (2003). The Military Balance. Londres: Routledge.

IISS. (2004). The Military Balance. Londres: Routledge.

IISS. (2005). The Military Balance. Londres: Routledge.

IISS. (2006). The Military Balance. Londres: Routledge.

IISS. (2007). The Military Balance. Londres: Routledge.

IISS. (2008). The Military Balance. Londres: Routledge.

KELLEY, Patrick A. (2008). *Imperial Secrets*: remmaping the mind of empire. Washington: NDIC Press.

KHALSA, Sundri K. (2004). *Terrorism Forecasting*: a web-based methodology. Washington: Joint Military Intelligence College.

KRISTENSEN, NORRIS & McKENZIE. (2006). *Chinese Nuclear Forces and U.S. Nuclear War Planning*. Washington: FAS & NRDC.

KRISTENSEN, Hans. (2005). *US Nuclear Weapons in Europe*: a Review of Post-War Policy, Force Levels, War Planing. Natural Resources Defense Council.

LIMA, M. e HIRST, M. (Orgs.) (2009). *Brasil, Índia e África do Sul*: desafios e oportunidades para novas parcerias. São Paulo: Paz e Terra.

MEARSHEIMER, John J. (2001). *The tragedy of great power politics*. W.W. Norton.

NARIZNY, Kevin. (2007). *The Political Economy of Grand Strategy*. Ithaca: Cornell University Press.

NDIC. (2006). International Intelligence Forum, 2006: Latin America. Washington: NDIC Press.

NDIC. (2009). Democratización de la Función de Inteligencia: el nexo de la cultura nacional y la inteligencia estratégica. Washington: NDIC Press.

NDIC. (2006). Intelligence + Technology = intelligence on target. Washington: NDIC Press.

NDIC. (2007). Intelligence Strategy: new challenges and opportunities. Washington: NDIC Press.

PAUL, T., WIRTZ, J. e FORTMANN, N. (2004). *Balance of Power*: Theory and Pratice in the 21º Century. Stanford: Stanford University Press.

PIKE, John. (2009). *Nuclear Posture Review*: extract from the 1995 Annual Defense Report. http://www.globalsecurity.org/wmd/library/policy/dod/95_npr.htm (16/04/2009).

PROENÇA Jr., Domício. DINIZ, Eugênio. RAZA, Salvador Ghelfi. (1999). *Guia de Estudos de Estratégia*. Rio de Janeiro: Jorge Zahar Editor Ltda, 186 p.

SAFRANCHUK, Ivan. (2006). *Beyond MAD*. China Security, p. 90-98.

SAGAN, Scott and WALTZ, Kenneth. (1995). *The Spread of Nuclear Weapons*: a debate. New York, W.W. Norton & Company.

SIMONOV, Vladímir. (2007). *Rusia está por abandonar el Tratado sobre Fuerzas Convencionales en Europa RIA Novosti*. 27/04/2007. (On-line) http://sp.rian.ru/analysis/20070427/64547287.html (28/04/2007).

SPRINZ, Detlef F. & WOLINSKY-NAHMIAS, Yael. [Ed.]. (2004). *Models, Numbers & Cases*: methods for studying international relations. Michigan, The University of Michigan Press.

The Official Web Site of The City of Los Angeles. (on-line) http://cityplanning.lacity.org/DRU/Locl/LocPfl.cfm?geo=cp&loc=Arl&yrx=06 (16/02/2008).

TILLY, Charles. *Coerção, Capital e Estados Europeus*: 990-1992. (1996). São Paulo, EdUSP, 357 p.

_____. (2003). *The Politics of Collective Violence*. Cambridge-UK, Cambridge University Press.

USA. Cia World Factbook. (2009). https://www.cia.gov/library/publications/the-world-factbook/fields/2026.html?countryName=Paraguay&coutryCode=pa&regionCode-sa&#pa (03/08/2009).

US FAA. Aeronautical Information Manual (on-line) http://www.faa.gov/airports_airtraffic/air_traffic/publications/atpubs/aim/Chap1/aim0101.html#1-1-2 (19/02/2008).

VAN EVERA, Stephen. (1997). *Guide to methods for students of Political Science*. Ithaca-NY, Cornell University Press.

VIZENTINI, Paulo G. F. (1990). *Da Guerra Fria à Crise* (1945-1990): as relações internacionais contemporâneas. Porto Alegre, Ed. UFRGS.

WALTZ, Kenneth. (1979). *Theory of International Politics*. New York, McGraw-Hill.

WALTZ, Kenneth. (2000). *Structural Realism after the Cold War*. International Security, vol. 25, n. 1, p. 5-41.

Capítulo 9

TEORIA DOS JOGOS E INTELIGÊNCIA

Marcos Carra

A Teoria dos Jogos tem como objetivo indicar, num ambiente de conflito e incerteza, qual é a estratégica ótima a ser adotada pelos jogadores a fim de eles poderem maximizar seus ganhos. Isso é feito por meio da matemática como ferramenta básica, aliada a dois dogmas: (i) os jogadores procuraram maximizar seus ganhos; e (ii) os jogadores sempre agem de forma racional.

A partir disso, torna-se clara a importância da Teoria dos Jogos para a Inteligência, se esta é entendida como toda a informação coletada, organizada ou analisada para atender a demanda de um tomador de decisões (Jennifer Sims apud Cepik, 2002: 2-3), uma vez que, nos assuntos de defesa, a Teoria dos Jogos permite vislumbrar os possíveis movimentos dos adversários em infindáveis situações – tais como operações de combate, manobras navais, jogos de guerra convencionais, prognósticos de guerra nuclear e assim por diante. Porém, a teoria é apenas um instrumento analítico, que processa informações retiradas do mundo real e por isso sua aplicação não é isenta de problemas, os quais podem reduzir e até mesmo invalidar os resultados obtidos.

Assim, o objetivo aqui é apresentar e analisar quais são esses problemas. Nossa hipótese é que enquanto alguns problemas têm origem na própria atividade de inteligência outros têm origem na Teoria dos Jogos. Os fundamentos teóricos serão dados pela própria Teoria dos Jogos. A metodologia será a de articular a atividade de Inteligência com a Teoria dos Jogos, ressaltando quais são esses problemas.

Este trabalho está dividido em seis partes. A primeira é esta introdução, a segunda composta de um breve histórico da Teoria dos Jogos; na terceira, apresentaremos alguns conceitos básicos da Teoria dos Jogos; na quarta parte analisaremos as implicações da utilização da Teoria dos Jogos para a Inteligência; na quinta parte apresentaremos as conclusões e na parte final apresentaremos as referências bibliográficas.

9.1. As Origens da Teoria dos Jogos

A rigor, os conceitos principais da Teoria dos Jogos não são novos. Eles foram desenvolvidos ao longo do tempo a partir de esforços de vários matemáticos oriundos de diversos países. O primeiro problema em que se reconheceu a aplicabilidade da Teoria dos Jogos foi encontrado no Talmud, uma compilação de leis e tradições babilônicas datado de 500 a.C. Ele é chamado de "problema do contrato de casamento", no qual aparentemente são feitas recomendações contraditórias sobre como três esposas devem receber a herança do marido. Se ele morrer deixando uma herança de 100, o Talmud recomenda a divisão por igual. Se ele morrer deixando 200, o Talmud recomenda uma divisão 50/75/75. Se ele morrer deixando 300, o Talmud recomenda uma divisão 50/100/150. Após anos de intenso debate, em 1985, os estudiosos concluíram que o Talmud antecipa a moderna teoria dos jogos cooperativos, sendo que cada solução corresponde ao núcleo de um jogo bem definido.

No entanto, o ponto de partida para a sistematização da Teoria dos Jogos esteve na preocupação em torno da possibilidade de se vencer/perder nos denominados "jogos de azar" (dados, cartas etc.), pois eles inspiraram o nascimento da teoria da probabilidade, um dos componentes fundamentais da Teoria dos Jogos. Nesse sentido, as primeiras tentativas de formalizar matematicamente as possibilidades inerentes aos jogos de azar foram feitas em 1494 pelo italiano Luca Pacioli (1445/1517) e posteriormente pelo italiano Girolamo Cardano (1501/1576); porém, esses estudos não passaram do estágio especulativo. O assunto foi retomado numa carta datada de 24 de agosto de 1654, na qual o matemático francês Pierre de Fermat (1601/1665) questiona o filósofo francês Blaise Pascal (1623/1662) sobre como deveria ser dividido um total de 64 pistolas de um jogo de dados interrompido. A solução desse problema permitiu dar um tratamento matemático formal à teoria das probabilidades.

Com o intuito de resolver um problema semelhante, em correspondência datada de 13 de novembro de 1713 dirigida ao matemático suíço Nicolas Bernoulli (1687/1759), o nobre inglês James Waldegrave (1684/1741) analisa um jogo de cartas chamado "le Her" e fornece uma solução que atualmente é denominada de "equilíbrio de estratégia mista". Em 1730, o matemático suíço Daniel Bernoulli (1700/1782) concebeu a noção de que, tendo em vista o comportamento dos jogadores, haveria uma medida subjetiva de satisfação que explicaria a reação das pessoas em situações de risco, nos termos de maximização de sua utilidade. Outra noção fundamental para a Teoria dos Jogos foi apresentada pelo inglês Thomas Bayes (1702/1761) que, num trabalho póstumo datado de 1764, apresentou a probabilidade de um evento ocorrer a partir de uma informação dada. Finalmente, outro conceito chave para a Teoria dos Jogos foi desenvolvido pelo matemático francês Antoine Augustin Cournot (1801/1877) que, ao analisar o duopólio, formalizou um conceito específico de equilíbrio.

Com base nessas noções, surgiram as primeiras soluções parciais da Teoria dos Jogos. Em 1913, o matemático alemão Ernst Zermelo (1871/1953) publicou o primeiro teorema matemático da teoria, no qual afirma que, num jogo de xadrez estritamente determinado, pelo menos um dos jogadores tem uma estratégia que lhe dará o empate ou a vitória. Porém, a solução era parcial porque o teorema só resolvia problemas nos quais havia informação perfeita e soma zero (em que só um ganhador vence). Em 1927, o matemático francês Emile Borel (1871/1956) publicou uma série de quatro artigos onde esboçou o teorema minimax, demonstrando que sempre há uma solução racional para um conflito entre dois indivíduos. Igualmente, a solução de Borel era parcial, visto que se limitava a prever o comportamento de duas pessoas que tivessem até cinco opções de estratégias a sua escolha.

Os problemas deixados em aberto por Borel chamaram a atenção do matemático húngaro John Von Neumann (1903/1957) que, em 1928, publicou o artigo "Zur Theorie der Gesellschaftsspiele".[1] Nesse trabalho, o autor, utilizando a topologia e a análise funcional, demonstrou que todo jogo finito de soma zero com duas pessoas possui uma solução em estratégias mistas. Ocorre, porém, que a solução dada por Neumann tinha dois limites: 1) era extremamente complexa, mas foi simplificada em 1937 quando ele ofereceu nova demonstração baseada no teorema do ponto fixo de Brouwer; e 2) Neumann considerava apenas os jogos com dois jogadores.

Ainda em 1928, o economista alemão Oskar Morgenstern (1902/1977) publicou o livro *Wirtschaftsprognose: Eine Untersuchung ihrer Voraussetzungen und Möglichkeite,* no qual discute qual deveria ser a unidade de análise econômica: o indivíduo ou a interação social.[2] Morgenstern demonstra que a maximização depende da interação entre os indivíduos e indiretamente do meio no qual os indivíduos interagem, concluindo que a racionalidade dos indivíduos é relativa e, em sendo assim, sua maximização não será plena.

Posteriormente, Von Neumann e Morgenstern uniriam forças. Em 1944, publicaram aquela que é considerada a obra fundadora da Teoria dos Jogos: *The Theory of Games and Economics Behavior.* Nela, os autores afirmam que o comportamento da economia depende da interação entre produtores e consumidores, uma vez que ele afeta a elaboração de estratégias e as decisões desses agentes. Logo, a Teoria dos Jogos foi utilizada na economia e na matemática aplicada para descobrir qual o melhor comportamento a ser adotado pelos participantes em jogos que dependiam de habilidade e de sorte. Apesar desses avanços, Borel contestou os resultados de Von Neumann e Morgenstern afirmando que é difícil encontrar jogadas ótimas em jogos reais e, se encontradas, as pessoas deixariam de jogar.

---

1 Sobre a Teoria dos Jogos de Estratégia.

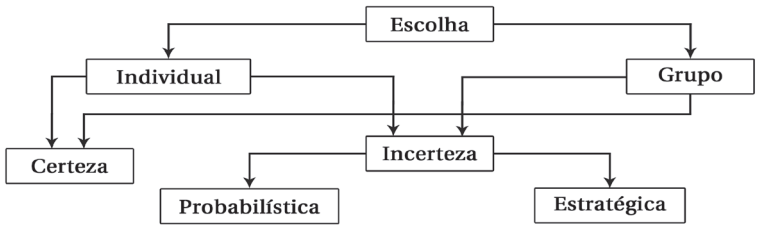
2 Implicações Quantitativas do Comportamento do Máximo.

As imperfeições da teoria foram reduzidas nos anos seguintes, a começar com os trabalhos do matemático norte-americano John Forbes Nash Jr. (1928). Em 1949, na tese *Non Cooperative Games*, Nash provou a existência de ao menos um ponto de equilíbrio em jogos de estratégias para múltiplos jogadores. Contudo, para que o equilíbrio ocorra é necessário que os jogadores se comportem racionalmente e não exista acordo prévio entre eles. Ainda em 1949, no artigo "The Bargaining Problem", Nash resolveu o problema da barganha, atualmente conhecido como "barganha de Nash". Em 1950, o autor publicou o artigo "Equilibrium Points in N-Person Games", ampliando a Teoria dos Jogos para mais de dois jogadores, superando assim as limitações de Neumann. Finalmente, em 1953, no artigo "Two-Person Cooperative Games", Nash provou a existência de um equilíbrio de estratégias mistas para jogos não-cooperativos, denominado equilíbrio de Nash. Assim, Nash fixou um dos fundamentos da teoria: a possibilidade de vencer sem a necessidade de derrotar o adversário.

Existia ainda uma última limitação para a Teoria dos Jogos: até então, todos os teóricos pressupunham que os jogadores utilizavam informação completa. Todavia, em 1965 o economista alemão Reinhard Selten introduziu seu conceito de "equilíbrio de jogo imperfeito", que refinou o Equilíbrio de Nash, e em 1967 o economista húngaro John Harsanyi (1920/2000) publicou a obra *Games with Incomplete Information Played by "Bayesian" Players, I-III. Part I. The Basic Model*, no qual introduziu as noções de "informação completa" e de "informação incompleta". Esses aperfeiçoamentos expandiram o campo de aplicação da Teoria dos Jogos para as mais diversas áreas, como biologia, economia, matemática aplicada, política, psicologia, sociologia e, como veremos, inteligência.

9.2. Os Fundamentos da Teoria dos Jogos

Como vimos na introdução, o objetivo da Teoria dos Jogos é indicar qual é a estratégica ótima a ser escolhida sob incerteza. Nesse sentido, ela é uma ferramenta auxiliar para a tomada de decisões. Decidir significa fazer uma escolha. Escolher significa selecionar um item de um conjunto de opções. Assim, a Teoria dos Jogos é parte integrante da Teoria das Decisões, tal como se pode ver na figura 1:



Fonte: Barrichelo, 2009

Figura 1: Organograma da Teoria das Decisões

A figura mostra que uma escolha pode ser feita de duas formas: 1) individual**:** quando apenas um indivíduo é o responsável por tomar a decisão; ou, 2) em grupo: quando mais de uma pessoa é responsável por tomar a decisão. Ambas as escolhas podem ser feitas sob duas formas: ou sob certeza: quando o conjunto de opções é finito, com preferências e consequências bem definidas, ou sob incerteza: quando o conjunto de opções é finito, porém as preferências e consequências não são bem definidas. Finalmente, as escolhas sob incerteza podem ser de outros dois tipos ainda: 1) sob incerteza probabilística: que ocorre quando há certo grau de probabilidade de um evento ocorrer; e, 2) sob incerteza estratégica: que ocorre quando o resultado de uma decisão depende da decisão de outrem.

Especificamente, um jogo tem seis elementos básicos:

1. Há um número finito de jogadores g_i, que formam o conjunto G, tal que $G = \{g_1, g_2,..., g_n\}$;
2. As decisões dos jogadores g_i são feitas de forma racional;
3. Cada jogador g_i – G possui um conjunto de estratégias Si, tal que $Si = \{s_{i1}, s_{i2},..., s_{imi}\}$. O conjunto de estratégias tem duas características: 1) é finito; 2) não é um valor estático, podendo ser encaixado em dois tipos: a) Estratégia Pura: é definida como aquela em que não existe aleatoriedade e cada jogador possui probabilidade igual a 1; e b) Estratégia Mista: é quando um jogador escolhe as ações baseado numa distribuição de probabilidade;
4. Cada jogador g_i – G possui uma estratégia de jogo s_{iji}, tal que $s = (s_{1j1}, s_{2j2},..., s_{njn})$, sendo que todos os perfis de estratégia formam o produto cartesiano, que apresenta todas as situações possíveis do jogo:

$$S = \prod_{i=1}^{n} S_i = S_1 \times S_2 \times \ldots \times S_n,$$

5. Cada jogador g_i – G possui uma função utilidade u_i: $S \rightarrow R$, tal que $u_i(s)$ representa o "ganho" ou "payoff" de cada jogador g_i para cada estratégia s – S adotada.

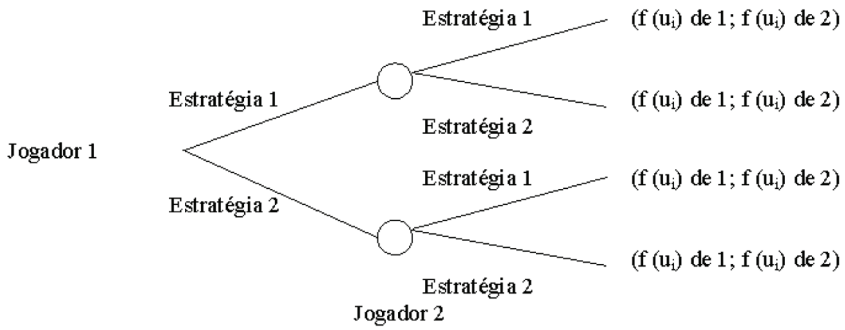
Normalmente os *payoffs* dos jogadores podem ser representados de duas formas. A primeira delas é a chamada "matriz de payoffs", mais utilizada para jogos simultâneos, ou seja, para jogos em que os jogadores atuam ao mesmo tempo. A forma da matriz está ilustrada na figura 2:

		Jogador 2	
		Estratégia A	Estratégia B
Jogador 1	Estratégia A	(f(ui) de 1; f(ui) de 2)	(f(ui) de 1; f(ui) de 2)
	Estratégia B	(f(ui) de 1; f(ui) de 2)	(f(ui) de 1; f(ui) de 2)

Fonte: Elaboração própria.

Figura 2: A Matriz de Payoffs

A segunda forma de representar os *payoffs* dos jogadores se dá por meio de uma "árvore de probabilidades", mais utilizada para jogos não-simultâneos. A forma da árvore matriz está ilustrada na figura 3:



Fonte: Elaboração própria.

Figura 3: A Árvore de Probabilidades

Em ambos os casos, os ganhos f (u_i) são representados por valores numéricos indicando quanto os jogadores 1 e 2 receberão conforme a estratégia A ou B adotada.

6. Cada jogador g_i – G possui um conjunto de preferências para cada situação no jogo. Neste caso, existem duas estratégias principais: 1) Estratégia Dominante: ocorre quando um jogador faz o melhor, independente da ação do outro jogador; e, 2) Estratégia Dominada: ocorre quando um jogador não toma determinada decisão, qualquer que seja a decisão do outro jogador. Dificilmente esta estratégia é adotada, pois oferece *payoff* menor.

Conforme Barrichelo (2009), a Teoria dos Jogos pode apresentar os seguintes formatos, sendo possível encontrar um ou mais de um deles no mesmo jogo:

1. **Jogos com um jogador:** são jogos em que há apenas um jogador (como quebra-cabeças), nos quais se procura resolver um problema, mas não há competição;

2. **Jogos com dois jogadores:** são jogos em que há dois e apenas dois jogadores;
3. **Jogos com n-jogadores:** são jogos em que há mais de dois jogadores;
4. **Jogos de Soma Zero:** são aqueles em que a soma dos payoffs dos jogadores é zero, ou seja, um jogador só pode ganhar se o outro perder. Assim temos:

$$\text{Ganho do jogador I} = - \text{Ganho do jogador II, ou}$$

$$f(u_i) \text{ de } 1 = -f(u_i) \text{ de } 2$$

Dessa forma, temos um jogo de soma zero, porque $f(u_i)$ de $1 + f(u_i)$ de $2 = 0$.

5. **Jogos de Soma Não-zero:** são aqueles em que um jogador pode vencer sem o outro perder;
6. **Jogos Randomizados:** são jogos que incluem aleatoriedade de acordo com uma distribuição de probabilidades, como jogos de cartas, dados, etc.;
7. **Jogos Não-Randomizados:** são jogos que não incluem aleatoriedade e nos quais se aplica a estratégia pura, como o xadrez, damas, etc.;
8. **Jogos de Informação Completa (ou Jogos Não-Bayesianos):** são aqueles em que todas as informações são conhecidas de forma que não há incerteza;
9. **Jogos de Informação Incompleta (ou Jogos Bayesianos):** são aqueles em que nem todas as informações são conhecidas de forma que há incerteza;
10. **Jogos Cooperativos:** é aquele em que os jogadores podem fazer acordos prévios;
11. **Jogos Não-Cooperativos:** é aquele em que os jogadores não fazem acordos prévios;
12. **Jogos Simultâneos:** são aqueles em que os jogadores atuam ao mesmo tempo;
13. **Jogos Não-Simultâneos:** são aqueles em que um jogador faz a sua jogada antes do outro.

Ainda conforme Barrichelo (2009), existem as mais variadas aplicações para a Teoria dos Jogos, sendo as principais: 1) Jogos Empírico/Históricos: estuda o comportamento de jogadores no mundo real; 2) Jogos Comportamentais: utiliza pesquisas laboratoriais para analisar o comportamento de jogadores; 3) Jogos Evolucionários: estuda jogos guiados por princípios como imitação e sobrevivência dos mais ajustados; 4) Jogos Algoritmos/Artificiais: estuda assuntos de complexidade computacional, comportamental e de informação em jogos feitos por jogadores humanos ou computadores; 5) Epistemologia

Interativa: estuda a construção do conhecimento da Teoria dos Jogos, incluindo o conhecimento do conhecimento; 6) Jogos Combinatórios: lida com assuntos matemáticos particulares aos jogos; 7) Estudos Neurológicos: estudas as atividades psicológicas observadas durante o jogo; 8) Jogos Econômicos: usa as ferramentas acima para ganhar insights nas interações estratégicas/econômicas e a performance de sistemas econômicos; 9) Jogos Políticos: usa as ferramentas acima para ganhar insights nos comportamentos políticos/estratégicos e a performance de sistemas políticos e sociais; e 10) Engenharia de Jogos: usa o conhecimento teórico e comportamental na construção de jogos no mundo real e suas estratégias.

Afinal, cada jogo tem um conjunto de soluções possíveis, sendo os principais deles:

1. Teorema Minimax: provado por John Von Neumann. Segundo este teorema, há sempre uma solução racional para um conflito entre dois indivíduos cujos interesses são completamente opostos, ou seja, o que é ganho pelo um lado é perdido pelo outro. Porém, o Teorema Minimax se aplica apenas para situações em que há soma zero, ou seja, quando o ganho de um jogador é traduzido em perda do outro jogador.

2. Teorema Maximin: também provado por John Von Neumann. Segundo ele, o objetivo dos jogadores é do maximizar seus ganhos mínimos. Dessa forma, cada jogador deve escolher os menores ganhos em cada linha e depois o maior ganho entre eles.

3. O Equilíbrio de Nash: provado por John Nash Jr. John Von Neumann e Oskar Morgenstern haviam resolvido apenas os jogos não-cooperativos de soma zero, mas Nash foi capaz de generalizar esta resolução para qualquer jogo não cooperativo, com n pessoas, de soma zero ou não, no qual cada jogador dispõe de um número finito de estratégias puras e tem, pelo menos, um conjunto de estratégias de equilíbrio. Um conjunto de estratégias constitui um equilíbrio de Nash se a escolha de cada jogador for ótima dada a escolha de todos os outros jogadores, o qual implica em não arrependimento.

9.3. Aplicando a Teoria dos Jogos na Inteligência

Esta parte está dividida em duas. Na primeira parte, faremos uma breve introdução sobre a aplicação da Teoria dos Jogos na Inteligência. Na segunda parte, apresentaremos uma perspectiva ampla da aplicação da teoria na Inteligência, destacando os principais problemas apresentados por essa abordagem.

9.3.1 As primeiras aplicações na área de inteligência

Desde a mais alta antiguidade, a humanidade realiza a simulação dos efeitos da adoção de uma determinada estratégia na guerra. Nogueira (2009) informa que esta preocupação teria surgido na Mesopotâmia por volta de 3.600 a.C. Depois, por volta de 500 a.C., Sun Tzu teria criado um jogo conhecido como "Wei Hai" (Cerco) que, por sua vez, teria inspirado o jogo japonês "Go". Na mesma época, surgia na Índia o jogo conhecido como "Chaturanga". Similares ao xadrez, todos esses jogos guardavam relações com os assuntos militares. Em 1664, Christofer Weikhmann desenvolveu o chamado "Jogo do Rei" e, durante o reinado de Luís XV (1715/74) na França, surgiram os primeiros jogos de combate simulados. Em Portugal, em 1719, foi desenvolvido o "Novo Jogo da Marinha", dedicado ao Príncipe Herdeiro, que buscava incutir uma mentalidade marítima nos herdeiros do trono, garantindo a manutenção dos interesses políticos da metrópole. Porém, apenas em 1824, apareceu na Prússia o "Kriegspiel" um verdadeiro Jogo de Guerra, utilizado para treinar jovens comandantes.

No início do século XX, a simulação de combates passou a ser explorada com regularidade e metodologia, mas foi apenas durante a Segunda Guerra Mundial que seu uso foi intensificado. Neste sentido, logo ficou evidente que a Teoria dos Jogos, a despeito das suas limitações, era um poderoso instrumento de análise com ampla aplicação na Inteligência. O pioneirismo da aplicação nessa área caberia ao próprio Von Neumann (que tinha particular interesse nesses assuntos): no início do conflito, ele logrou desenvolver um modelo de conflito, deduzindo que os aliados venceriam. Durante a guerra, Von Neumann expandiu as aplicações da Teoria dos Jogos para prever as melhores estratégias em operações pontuais, como no Projeto Manhattan e no desembarque da Normandia.[3] Findo o conflito, rapidamente a Teoria dos Jogos foi aplicada tanto nos EUA como na URSS para formular estratégias de guerra. Em 1948, Von Neumann tornou-se consultor da Rand Coporation , onde utilizou a Teoria dos Jogos para examinar as possíveis estratégias a serem adotadas na guerra nuclear, prevendo a interação entre EUA e URSS como um jogo de soma zero.

Scheve (2008) comenta que ao conceber a interação entre EUA e URSS como um jogo de soma zero, Von Neumann admitia a hipótese de que venceria o primeiro a fazer uso das armas nucleares numa guerra, influenciando na formulação das estratégias a serem adotadas e fixando, durante a administração Eisenhower (1952/60), a percepção de que as armas nucleares tinham o mesmo

[3] É bem conhecido o caráter discreto e formal dos pronunciamentos oficiais do governo norte-americano – a população sabe o que o governo está fazendo mais através da mídia do que por sua própria voz. Entretanto, fora dos Estados Unidos, o governo se sente livre para levar a sua mensagem diretamente para as populações estrangeiras, vide o caso dos folhetos de propaganda que caíam do céu durante a Guerra do Golfo.

status das armas convencionais. Porém, em 1960 o matemático Thomas Schelling publicou a obra *"The Strategy of Conflict"*, na qual utilizou uma Teoria dos Jogos já enriquecida por John Nash, para demonstrar que em caso de ataque nuclear a aniquilação dos EUA e URSS estaria assegurada – o que desaconselhava um ataque deste tipo. Ele também demonstrou que a retaliação era mais eficiente, propondo que os EUA desenvolvessem uma variedade de respostas nesse sentido. A constatação de que nenhuma superpotência poderia obter a vitória através da agressão nuclear originou o conceito de "Destruição Mútua Assegurada" (**Mutual Assured Destruction, MAD**) e demonstrou que os contendores apresentavam vulnerabilidades. Entretanto, ficou claro também que cada superpotência estava preocupada apenas com os seus interesses. Por conta disso, cada uma deveria limitar os riscos adotando uma estratégia dominante.

Segundo Scheve (op. cit.), a atmosfera do período era tensa e até mesmo uma atitude defensiva poderia ser interpretada como provocação, de forma que qualquer falha de comunicação poderia levar a resultados catastróficos. Isso levou as superpotências a formular inúmeras questões, como, por exemplo: se for construído um escudo antimísseis, o ato poderá ser um erro estratégico capaz de levar a guerra nuclear? Os governantes consultaram os matemáticos especializados em Teoria dos Jogos para obter uma resposta. E a resposta continuava a indicar que a melhor opção era seguir as recomendações formuladas por Thomas Schelling. Assim, ambas as superpotências investiram na construção de silos, de forças aéreas e de submarinos de alcance global com o objetivo de aumentar a possibilidade de sobrevivência a um eventual primeiro ataque e diminuir a capacidade de retaliação do outro. Porém, quando a corrida armamentista passou a comprometer o desempenho econômico das superpotências ambas começaram a promover encontros visando a aumentar o controle de armas e o desarmamento.

Estes encontros podem ser vistos como jogos repetitivos, uma vez que cada reunião aumentava a compreensão mútua, a confiança e a cooperação entre EUA e URSS, permitindo-lhes renovar a cooperação e punir a defecção, de forma que paulatinamente as superpotências adotaram uma postura menos agressiva. Segundo Szalai (2008), tão importante quanto as estratégias que ajudou a elaborar, foi o fato de que, durante o período da Guerra Fria, a Teoria dos Jogos tornou-se o fundamento da política de defesa dos EUA, de forma que o próprio *mainstream* assumia que havia certa simbiose entre ambas.

Ainda segundo Szalai (op. cit.), nos anos recentes, a Teoria dos Jogos continua a ser amplamente utilizada nos assuntos de defesa. Após 11 de setembro de 2001, ela começou a ser aplicada mais incisivamente para prever as ações antiterrorismo.

9.3.2 O quadro atual: problemas e perspectivas

Para compreender como a Teoria dos Jogos se relaciona com a Inteligência devemos ter em conta o lugar que ela ocupa nesta última. Segundo Handel (1989), o trabalho de inteligência possui três níveis distintos e cada um deles afeta o nível subsequente: 1) a aquisição de informações; 2) a análise das informações; e, 3) a aceitação ou não de uma prescrição elaborada com base na análise das informações. Vejamos como a Teoria dos Jogos se encaixa nesses níveis.

Nível 1: A Aquisição de Informações

O primeiro nível é a aquisição de informações. Nesse caso, segundo Cepik (op. cit.) os meios de coleta são bastante especializados, sendo os principais:

1. Humint (Human Intelligence): tem como fonte os seres humanos. Aqui se incluem tanto o terreno da espionagem propriamente dita quanto uma variedade de fontes não clandestinas, tais como a interrogação de prisioneiros de guerra, entrevistas de viajantes ocasionais, relatórios diplomáticos ou de adidos militares, contatos comerciais etc.

2. Sigint (Signals Intelligence): tem como fonte os sinais. Aqui se incluem interceptação, decodificação, tradução e análise das comunicações por uma terceira parte além do emissor e do pretenso receptor. Além do acesso direto ao conteúdo das mensagens (cifrado/codificado ou não), essa área inclui também a interceptação de diferentes tipos de sinais eletrônicos emitidos por aparelhos civis e militares (radares, transmissores etc.).

3. Imint (Imagery Intelligence): tem como fonte as imagens. Aqui se incluem as imagens fotográficas analógicas e digitais obtidas através de plataformas aerotransportadas e espaciais. Nesse caso, também se incluem as imagens produzidas utilizando outras porções do espectro eletromagnético invisíveis ao olho humano (próximas de infravermelho, termais, radar). Atualmente, sensores multiespectrais e hiperespectrais são capazes de produzir imagens através de bandas eletromagnéticas diversas que permitem detectar forma, densidade, temperatura, movimento e composição química dos objetos.

4. Masint (Measurement and Signature Intelligence): tem como fonte as informações sobre características singulares (as assinaturas) de sistemas de armas, aeronaves, embarcações e radares, além de monitorar dados geofísicos (acústicos, sísmicos e magnéticos), radiações nucleares, composição físico-química de materiais e uma variedade de fontes para a montagem de bancos de dados, análise e posterior emprego tático, estratégico e diplomático. No caso de países com programas aeroespaciais avançados, também são empregados sistemas terrestres e espaciais para a vigilância das atividades aeroespaciais de outros países.

5. Osint (Open Sources Intelligence): tem como fonte os documentos oficiais obtidos por vias legais, por meio da observação direta e não clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia (jornais, rádio e televisão), da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido. Quanto mais abertos os regimes políticos e mais flexíveis os controles sobre a circulação de informações, maior a quantidade de inteligência obtida a partir de programas de osint.

A atividade de coleta absorve entre 80/90% dos investimentos governamentais na área de inteligência nos países centrais do sistema internacional. A maioria desses recursos é dedicada às plataformas, sensores e sistemas tecnológicos de coleta e processamento de informações. Porém, o volume de dados brutos e informações primárias coletadas é muito maior do que os relatórios recebidos pelos usuários finais, os responsáveis pela tomada de decisões e pela implementação de políticas. Segundo uma estimativa da década de 1980, somente 10% das informações coletadas chega a sair dos muros dos sistemas de inteligência.

É aqui que começam os problemas para a aplicação da Teoria dos Jogos porque o material a ser analisado obrigatoriamente advirá de uma dessas fontes e o ideal é que este material fosse o mais abrangente, confiável e completo possível para não comprometer a análise. Porém, por conta do avanço tecnológico, as agências pré-analisam volumes crescentes de informações (imagens, sinais, material em língua estrangeira etc.). Uma consequência desse fenômeno é que alguns tipos de informações, especialmente as mais efêmeras e de uso diplomático ou militar imediato, chegam aos usuários finais sem passar pela análise.

Nível 2: A Análise das Informações

Realizada a coleta entramos no segundo nível, que é o da análise das informações, cujo objetivo é processar a informação coletada para gerar conhecimento, passível de aplicação. Nessa fase, para Handel (op. cit.), o primeiro problema está no fato de que nos serviços de inteligência há grande dificuldade de separar a informação correta da incorreta, ou, conforme o jargão da área de inteligência, separar os sinais dos ruídos. Para o autor, é virtualmente impossível distinguir uma da outra, o que dificulta sua classificação e consequente descarte. A análise e a evolução do processo são complicadas pela natureza contraditória das informações, que desafiam a simples análise quantitativa. Muitas das informações coletadas não são puras por si só porque, em última análise, o critério para sua seleção depende de fatos etnocêntricos, sentimentos humanos, ideias

e conceitos, os quais não podem ser automatizados. Aqui já surge um primeiro problema para a análise quantitativa, visto que muitas vezes a máquina não pode substituir a experiência humana. Para Handel, como há grande dificuldade de diferenciar as informações corretas das incorretas, é necessário tratar ambas em bases similares. Assim, o que de fato existe para o autor são os ruídos e a tentativa de separá-los dos sinais é agravada pelo fato de que a coleção de informação adicional também contribui para aumentar o nível de ruído do sistema. Isso aumenta a quantidade de dados coletados, tornando mais difícil de filtrar, organizar e processar as informações a tempo de serem utilizadas.

No caso da análise, é necessário considerar que por sua própria natureza, a Teoria dos Jogos realiza uma forçosa simplificação do trato das questões sociais, que é cristalizada na forma matemática. Isso implica na construção artificial das situações estudadas. Fato é que quanto maior a quantidade de informações corretas, melhor será a construção do modelo matemático, menor a incerteza envolvida e mais precisos os resultados. Porém, como nas questões de inteligência existem ruídos e não sinais, que, diga-se, podem ser ampliados pela atividade de contrainteligência, a maior quantidade de informações equivocadas poderá gerar um modelo matemático errado, que produzirá conclusões erradas.[4]

O segundo problema está na própria matematização, uma vez que, como foi dito acima, só é possível utilizar a Teoria dos Jogos depois de converter as informações em números, pouco importando se essas informações sejam sinais ou ruídos, se estão erradas ou não, se são completas ou não: só é possível trabalhá-las sob a forma de números. Para melhor compreender as implicações dessa conversão montemos um exemplo numérico:

1. um evento com dois jogadores, 1 e 2;
2. os jogadores 1 e 2 têm as opções estratégicas A e B a sua disposição;
3. o jogador 1 tem as seguintes funções numéricas de utilidade:
   - em caso de 1 adotar a estratégia A e 2 adotar a estratégia A, temos: (f (u_i) de 1 = 5;
   - em caso de 1 adotar a estratégia A e 2 adotar a estratégia B, temos: (f (u_i) de 1 = 3;
   - em caso de 1 adotar a estratégia B e 2 adotar a estratégia A, temos: (f (u_i) de 1 = 7;
   - em caso de 1 adotar a estratégia B e 2 adotar a estratégia B, temos: (f (u_i) de 1 = 4;
4. o jogador 2 tem as seguintes funções numéricas de utilidade:

[4] A contrainteligência tem por objetivo neutralizar as ações de Inteligência ou de espionagem de terceiros. As ações de contrainteligência buscam detetar o invasor, neutralizar sua atuação, recuperar ou mesmo contra-atacar por meio da produção de desinformação.

- em caso de 1 adotar a estratégia A e 2 adotar a estratégia A, temos: (f (u_i) de 1 = 2;
- em caso de 1 adotar a estratégia A e 2 adotar a estratégia B, temos: (f (u_i) de 1 = 8;
- em caso de 1 adotar a estratégia B e 2 adotar a estratégia A, temos: (f (u_i) de 1 = 6;
- em caso de 1 adotar a estratégia B e 2 adotar a estratégia B, temos: (f (u_i) de 1 = 4;

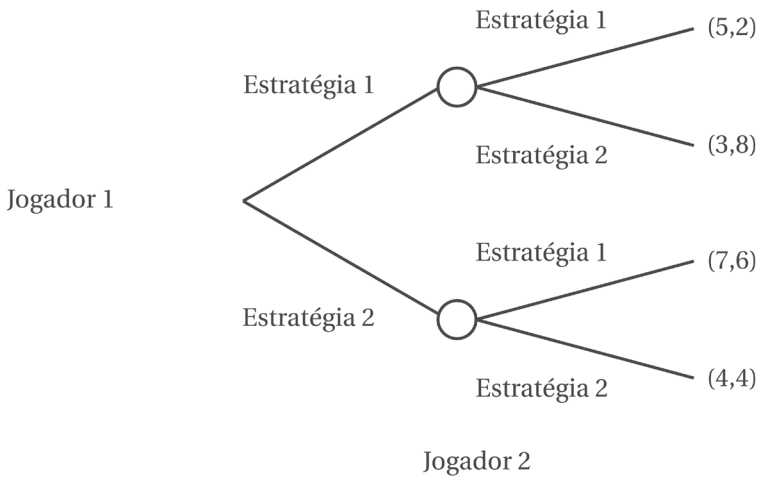
5. As figuras 4 e 5 mostram a configuração das utilidades na matriz de *payoffs* e na árvore de probabilidades respectivamente:

		Jogador 2	
		Estratégia A	Estratégia B
Jogador 1	Estratégia A	(5,2)	(3,8)
	Estratégia B	(7,6))	(4,4)

Fonte: Elaboração própria.

Figura 4: A Matriz de Payoffs

A mesma distribuição tem a seguinte configuração numa "árvore de probabilidades":



Fonte: Elaboração própria.

Figura 5: A Árvore de Probabilidades

Segundo o exemplo pode-se concluir que:

1. o jogador 1 obtêm maior ganho quando adota a estratégia A e o jogador 2 a estratégia B;
2. o jogador 2 obtém o maior ganho quando adota a estratégia B e o jogador 1 a estratégia A;
3. ambos obtêm o menor ganho quando o jogador 1 adota a estratégia B e 2 a estratégia A;
4. ambos obtêm o mesmo ganho quando o jogador 1 adota a estratégia B e 2 a estratégia B. Neste caso provavelmente encontraremos uma situação que representa o Equilíbrio de Nash.

Nessa situação hipotética, o pensamento racional diz que o jogador 1 é estimulado a adotar a estratégia A se o jogador 2 escolher a estratégia A; e que o jogador 2 é estimulado a escolher a estratégia B se o jogador 1 escolher a estratégia A. Ao mesmo tempo, ambos tenderão a descartar as outras opções por apresentar baixo ganho ou por levar a um impasse.

O exemplo acima demonstra a elegância, objetividade e simplicidade da aplicação da matemática na Teoria dos Jogos. Contudo, o problema está em montar a matriz de *payoffs*, tarefa que, segundo Nogueira (op. cit.), deve obedecer a três princípios:

1. O princípio da especificidade, que se refere à definição dos resultados desejados. Neste caso, segundo Abrantes (2004), a execução dos objetivos estratégicos, no tempo e no espaço, implica táticas que devem ser coerentes com os fins estratégicos. Considerando a complexidade das situações envolvidas, é difícil crer que aquele que tem a iniciativa do jogo possa assegurar uma articulação satisfatória das táticas dos adversários, com as diferentes etapas da sua própria estratégia. Para agravar isto, se um jogo é indeterminado, existem muitas variáveis intervenientes – o que torna difícil aplicar a teoria para mais de dois jogadores.
2. O princípio da homogeneidade, que se refere à seleção de jogadores familiarizados com os aspectos que influenciam suas decisões. Isto significa que, a montagem do jogo envolve uma determinada situação, na qual o analista já deve ter certa experiência na seleção dos dados.
3. O princípio da casualidade, que se refere à incerteza sobre um evento acontecer ou não.

Esses princípios demonstram que a montagem da matriz de *payoffs* não pode ser feita de forma aleatória: exige método, que por sua vez deve ser seguido para dar coerência e sentido aos dados, evitando que os resultados destoem das informações introduzidas sob a forma de números.

Conforme Barrichelo (op. cit), outro problema da matematização advém de um aspecto já mencionado e possível também de ser vislumbrado tanto a partir da leitura atenta desses princípios como da análise da própria matriz de *payoffs* e/ou da árvore de probabilidades, qual seja, a Teoria dos Jogos funciona melhor com dados quantitativos. É relativamente fácil obter um número capaz de expressar informações objetivas, como número de tropas, tanques, ogivas nucleares etc. Porém, é extremamente difícil obter um número capaz de expressar informações qualitativas como o caráter dos jogadores, quais as motivações que moldam suas estratégias, quais as suas vantagens e desvantagens, quais são suas opções estratégicas de curto e longo prazos e quais os custos e benefícios de cada combinação de estratégias.

Os problemas da matematização não param aí. Segundo Abrantes (op. cit.), mesmo sendo possível reduzir a um número todos os aspectos quantitativos e qualitativos, isso não basta: é necessário saber se existe correlação entre as preferências dos jogadores, ou seja, se existe a probabilidade da preferência de um jogador afetar a preferência do outro jogador. Em assim sendo, se esta relação assume grandeza infinitesimal, ou seja, se for muito baixa, os dados não se prestarão para uma análise sólida e conclusiva.

Outro problema da matematização é o fato de que a montagem da matriz de *payoffs* é concluída com os testes de validação, por meio dos quais, com o suporte da Teoria das Probabilidades, procura-se determinar qual o valor numérico deve ser atribuído a cada jogador em função de cada estratégia. Aqui tem papel fundamental a variância, ou seja, conhecer a dispersão dos valores para saber o quanto os dados destoam de um valor numérico esperado. Quando se admite uma variância mais abrangente do que a realmente existente, os resultados tendem a se aglomerar em torno de um mesmo valor fixo, demonstrando que as preferências dos jogadores pouco variam, não importando a estratégia adotada. Ao contrário, quando se admite uma variância menos abrangente do que a realmente existente, os resultados tendem a se dispersar, demonstrando que os jogadores não têm preferências definidas, não importando a estratégia adotada. Tais dificuldades provam o quanto é vital selecionar uma faixa de variância aceitável, pois um erro pode inutilizar completamente os resultados de um jogo. Se não é possível encontrar uma faixa de variância adequada ou se algum tipo de erro persiste, é necessário abandonar a Teoria dos Jogos e optar por outro instrumento analítico.

Como se vê, a matematização é uma tarefa complexa, visto que quantificar as informações é uma tarefa extremamente difícil, pois não bastasse a necessidade de se obter informação abundante e precisa, também é necessário enquadrar as informações qualitativas, tentar encontrar dois fenômenos que tenham correlação significativa (o que pode excluir muita informação da análise) e montar o jogo de forma que os resultados não se revelem absurdos, invalidando o resultado – o que requer certa experiência prática prévia.

O terceiro problema diz respeito à maximização dos ganhos, um dos axiomas da Teoria dos Jogos. A teoria supõe que todo jogador é um maximizador racional dos seus próprios objetivos, quando, na verdade, ele é incapaz de fazer os cálculos apropriados ou age de forma aleatória. Se esse axioma não se confirma ou é atenuado de alguma forma, toda a análise e consequente prescrição podem revelar-se erradas. Esse risco é reduzido à medida que mais e mais jogadores reconhecem a importância da interação estratégica e pensam através de suas escolhas estratégicas, ou obtêm aconselhamento especializado sobre o assunto – o que ajuda a manter os erros a um mínimo possível, eliminando aqueles que podem surgir a partir do pensamento lógico defeituoso sobre a interação estratégica. Mesmo assim, algum risco residual sempre permanece.

Finalmente, o quarto problema diz respeito ao próprio axioma do pensamento racional, pilar básico da Teoria dos Jogos. Desde que passou a ser aplicado nas ciências sociais, esse dogma é contestado pelos filósofos contrários à tendência de impregnar as ciências sociais com a formalização matemática. Inicialmente, os críticos contestavam o poder explicativo do pensamento racional na esfera econômica, argumentando que *a priori* os agentes reais não agem de forma puramente racional e deviam ser consideradas as questões necessárias ao convívio social como gostos, simpatias, relações pessoais e assim por diante. Outros filósofos atacavam a idéia do ambiente competitivo, nem sempre presente no cotidiano. Um terceiro grupo de filósofos atacava o próprio dogma do livre-mercado, considerando-o uma fonte de patologias sociais que desequilibravam as sociedades modernas. Porém, as críticas mais incisivas ao pensamento racional começaram a ser feitas em 1953 pelo economista francês Maurice F. Charles Allais (1911) que, utilizando os jogos de azar, conduziu uma série de experiências para testar a intensidade da preferência de um sujeito por um determinado objeto. Os testes empíricos mostraram que: 1) as preferências dos agentes não podiam ser ordenadas numa escala sequencial de utilidade; 2) havia dificuldade em definir preferências, ou seja, os agentes desistiam de uma escolha não necessariamente porque haviam optado por outra; 3) havia forte componente de irracionalidade nas escolhas, em geral, quanto maior era o ganho esperado, maior a aversão ao risco e quanto maior a perda esperada, maior a tendência ao risco; e, 4) existiam arranjos diferentes que conduziam aos mesmos resultados.

Esses testes demonstraram a importância da subjetividade, que ganha contornos ainda mais decisivos quando se trata da Inteligência, dadas as dificuldades de se obter informações precisas, a quantidade dos fatores a considerar e os impactos de uma possível decisão equivocada. Nem mesmo esta constatação é nova: o próprio Carl Von Clausewitz já questionava a eficiência do pensamento exclusivamente racional para orientar a guerra.

Handel (op. cit.) comenta que o analista de inteligência deve considerar vários aspectos não-racionais quando realiza seu trabalho, sendo o primeiro o

de diferenciar as intenções das capacidades. Apesar de parecer coisa bastante simples, a qualidade, a avaliação e a corroboração da informação são processos intrincados e envolvem vários passos no qual um único erro de julgamento pode resultar numa cadeia de erros que causa uma séria distorção analítica. Aqui talvez o maior problema esteja em diferenciar um do outro, sendo mais fácil obter informações sobre as capacidades do que sobre as intenções, uma vez que estas são mais fáceis de ocultar, pois podem estar na cabeça do(s) líder(es), além de seres suscetíveis a mudanças em qualquer instante.[5, 6] A interação entre intenções e capacidades pode ser vista na figura 6:

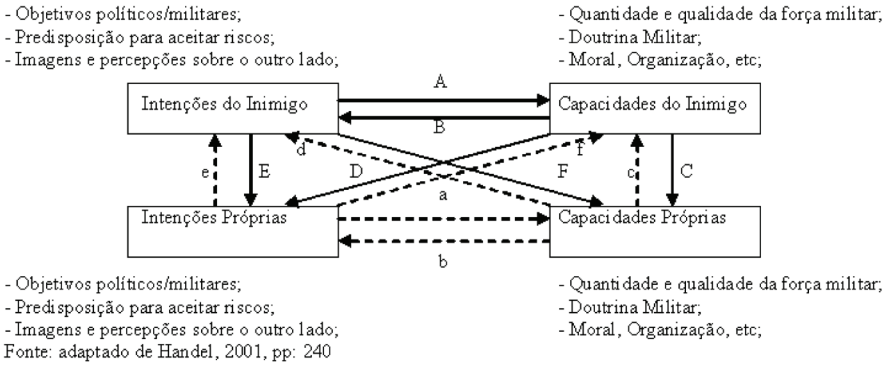


Figura 6: A Interação entre Intenções e Capacidades

A longo prazo, as intenções ofensivas se tornam perceptíveis quando uma nação investe em sua capacidade de ataque (flecha A), a qual, por sua vez, é interpretada como sendo intenção agressiva (flecha B). O processo pode ser complicado pelo fato de um adversário poder afirmar que ele precisa ampliar suas capacidades para se equiparar ao outro (flecha C), ou afirmar que aumenta suas capacidades em resposta à percepção das intenções hostis de outros (flecha D). Ademais, um adversário pode afirmar que ele tem sua própria intenção (flecha E) e percebe uma oportunidade em utilizar suas próprias capacidades para desferir um ataque preventivo (flecha F). Isso pode ampliar o antagonismo, e em casos extremos pode iniciar uma guerra preventiva. A descrição da evolução do processo indica que cada um deve não apenas ver o outro através da sua compreensão, mas também compreender como ele reage ao diferenciar intenções e capacidades. Um reflexo similar deve ocorre do lado inverso (flechas a, b, c, d, e, f).

[5] As informações sobre as capacidades podem ser materiais (tipos de armas e suas especificidades) ou imateriais (organização das tropas, moral, doutrina militar etc).

[6] As informações sobre as intenções podem ser obtidas a partir da análise de memórias, discursos, conversas nos círculos íntimos etc.

Para complicar o processo, não existe correlação direta entre a capacidade e as intenções: um país pode ter o poderio militar e mesmo assim decidir não fazer a guerra. Finalmente, a avaliação do processo exige a exata coordenação e tempo para a análise. Assim, é necessário analisar as intenções por dois motivos: 1) um adversário pode decidir atacar mesmo sendo fraco; 2) a guerra pode ser iniciada se há intenção de fazê-la.

O segundo aspecto apontado por Handel é a existência do risco, uma vez que assumindo o comportamento racional, o analista de inteligência pode predizer que uma operação com elevados riscos e ganhos incertos não deve ser implementada e vice-versa. Mas nem sempre isto é verdadeiro, pois deve-se considerar que: 1) algumas culturas estão mais predispostas a aceitar riscos que outras; 2) algumas vezes o analista desconhece fatores que o adversário considera como risco; 3) os ganhos de ataque surpresa podem compensar os riscos; 4) a existência do engodo: ao atacar sob condição de alto risco, o agressor pode induzir o agredido a acreditar no contrário, ou seja, o agressor assumiu que o risco para atacar é baixo e pode assumir riscos ainda maiores no futuro.

O terceiro aspecto apontado por Handel é o etnocentrismo, uma vez que dada a natureza do trabalho de inteligência, toda a análise deve estar inevitavelmente embasada em conceitos preexistentes, como, por exemplo, as intenções e doutrinas militares do adversário. Os conceitos, sistemas de crenças, teorias e imagens compõe uma estrutura para a assimilação de informações antagônicas que podem ser: velhas ou novas, detalhadas ou genéricas, rígidas ou flexíveis, estáticas ou dinâmicas. Se, ao longo do tempo, um conceito é bem sucedido em fornecer uma base para a interpretação e predição, e sua aplicação é fundamental para o sistema de crenças de um país, menor será a possibilidade de suas premissas serem questionadas. Mas, uma vez que algumas áreas da atividade política permanecem imutáveis em situações antagonistas, seu verdadeiro sucesso está no fato dele não incorrer em situações que o levam a autonegação. Se, entretanto, um conceito não é fundado em crenças arraigadas e tem um sucesso limitado, então é maior a possibilidade dele sofrer mudanças. Cada tipo ideal tem seus pontos fracos e fortes. Um conceito rígido fornece continuidade e fundamentação sólida para quem age, mas o perigo é que ele pode ignorar as evidências contrárias. Ademais, o conceito pode estar obsoleto, pondo em risco as políticas e estratégias. Em contraste, um conceito flexível não fornece bases bastante sólidas para ações ou planejamento a longo prazo, e como está em constante mudança, pode trazer confusão e paralisia.

Em termos genéricos, os erros de percepção decorrem da projeção da sua própria cultura, crenças ideológicas, doutrinas militares e expectativas sobre o adversário, ou seja, cada sociedade molda os fatos de acordo com as próprias esperanças. Neste sentido, os estudos antropológicos, culturais e psicossociais

levam à mesma conclusão: as percepções humanas são etnocêntricas e cada qual vê o mundo externo através dos filtros dos próprios sistemas de crenças e preconceitos – o que na maioria dos casos o leva a subestimar a capacidade do oponente. A correção desse problema está em eliminar a visão etnocêntrica, sendo a melhor solução a de "conhecer profundamente o inimigo", ou seja, conhecer sua cultura, língua, ideologia e assim por diante. Mais original é a sugestão de se conhecer a própria cultura, com o objetivo de predizer: 1) como o adversário reage ou percebe o observador; e 2) como alguém em seu próprio ambiente tem propensão a perceber a outra sociedade. Apesar da originalidade, essa visão é impraticável por que: 1) às inteligências frequentemente faltam os recursos necessários para analisar as intenções dos adversários, deixando de lado o estudo da própria sociedade; 2) o estudo da própria sociedade envolve visões e valores subjetivos e assim contribui para a politização da comunidade de inteligência; e, 3) da mesma forma que no estudo de outras sociedades, distorções de percepção também levam a análises equivocadas no estudo da sociedade do analista.

Um quarto aspecto apontado por Handel é que existe o risco dos analistas tenderem a esperar sempre o pior do inimigo. É uma medida custosa, visto que envolve o contínuo monitoramento das atividades do inimigo, o que os torna cautelosos e pessimistas. Isso ainda é exacerbado por falhas graves, como a incapacidade de antecipar a Inteligência. Este é o resultado da adoção do "pior caso", que assume que a atitude mais prudente é esperar sempre o pior do outro. O custo desta postura é obvio: 1) exige mobilização a cada vez que o outro lado de move; 2) eleva o nível de tensão ao máximo; 3) é uma saída fácil para a responsabilidade analítica e reduz a qualidade da análise; 4) aumenta o número de alertas falsos, o que reduz sua credibilidade.

O quinto aspecto apontado por Handel está no fato de se manter constante prontidão, elevando o número de alarmes falsos. Neste caso, as organizações de inteligência assumem que vários alarmes falsos podem ser justificados; contudo, mesmo sendo conhecida a causa do alarme, a inteligência pode encontrar dificuldade em explicar porque um ataque não ocorreu. Existem três razões para isso: 1) o inimigo não planeja atacar primeiro. Isto acontece porque a inteligência falhou devido à falta de informações, à análise incorreta ou ao baixo limiar da mobilização; 2) o inimigo decide atacar, mas cancela por uma razão qualquer: climatológico, condições políticas adversas, insatisfação com os planos de ataque, problemas com a doutrina militar ou elevado nível de mobilização do lado adverso; 3) o inimigo está preparado para atacar, mas os possíveis agredidos mobilizam-se ao receber os primeiros sinais. Ademais, a interpretação do alerta pode ser contraditória: um alerta isolado em meio a uma série deles ou em meio a um prolongado período de alerta que não é

seguido por uma guerra tem impacto negativo sobre as decisões futuras; um alerta falso compromete a credibilidade da inteligência; um prolongado período de alertas pode fazer baixar a atenção.

Finalmente, o último aspecto apontado por Handel é a existência dos próprios erros inerentes à condição humana. Para neutralizar os efeitos do elemento humano no processo analítico de inteligência, é desenvolvida uma detalhada lista de Indicadores e Avisos (I&W em inglês). Essencialmente, o propósito deste método é auxiliar na seleção de material relevante em meio à quantidade de informação ambígua e conflitiva disponível numa situação de crise. Para isto, o analista precisa apenas responder três questões: 1) se é necessária; 2) se não é ambígua; 3) se pode ser monitorada. Entre os avisos, temos: as manobras de larga escala, a intensificação/redução das comunicações a cabo, a partida de conselheiros militares, a distribuição de munição entre as tropas, a mobilização das reservas de unidade etc.

Concluindo, Handel aponta nove paradoxos que envolvem a tarefa de análise:

1. como resultado da grande dificuldade de diferenciar entre sinais e ruídos, ambos devem ser tratados como incertos, de forma que tudo o que existe são ruídos;
2. quanto maior o risco de uma operação, menor há a possibilidade dela ser adotada;
3. um ambiente internacional silencioso pode funcionar como um aviso de fundo, ocultando a preparação para a guerra;
4. quanto maiores a credibilidade e a reputação de uma agência de inteligência, menos suas conclusões são questionadas. Assim sendo, há o risco de confiar demais em suas conclusões;
5. a predição de um ataque iminente leva à contemporização que, em troca, leva o inimigo a cancelar seus planos;
6. quanto maior a quantidade de informação coletada, mais difícil é realizar a filtragem, organização e processamento dos dados;
7. quanto maior a quantidade de informação coletada, maior a quantidade de ruído coletada;
8. quanto maior o número de alertas, menor a crença neles;
9. a ampliação da sensibilidade dos sistemas reduz o risco de surpresa, mas aumenta o número de alarmes falsos.

Dessa forma, percebe-se que qualquer aplicação da Teoria dos Jogos na Inteligência não é uma tarefa simples. Ela envolve inúmeros problemas, sendo o primeiro dentre estes o de separar a informação correta da incorreta. Esse

problema resulta no segundo: a matematização, uma vez que, em função dos problemas de captação e separação inerentes à Inteligência, a montagem da matriz de *payoffs* deve contemplar grande quantidade de informação incompleta, randomização, presença de n-jogadores e jogos cujo resultado final normalmente difere da soma zero. Finalmente, não se pode ignorar a presença de fortíssimo componente psicológico não racional que faz parte do horizonte dos agentes responsáveis pela análise.

Recentemente, uma tentativa de minimizar os problemas apresentados pela Teoria dos Jogos foi proposta por meio da utilização da Teoria dos Fractais, ou Teoria dos Sistemas Complexos. Essa teoria se propõe a explicar, através dos sistemas de equações não-lineares, os fenômenos que apresentam pouca informação, alta incerteza e elevada aleatoriedade.

Nível 3: A Aceitação de uma Prescrição

Concluída a análise, a Teoria dos Jogos pode auxiliar os tomadores de decisão de três formas principais: 1) fornecer uma explicação: a Teoria dos Jogos pode explicar as opções adotadas em casos que requerem a interação dos "tomadores de decisão"; 2) realizar uma previsão: é possível utilizar a Teoria dos Jogos para prever as ações que os "tomadores de decisão" adotam em cada caso, bem como quais serão os possíveis resultados; e, 3) fornecer uma prescrição: é possível dizer a um tomador de decisão, numa determinada situação, quais as estratégias que provavelmente irão produzir os melhores resultados. Concentremo-nos neste último aspecto visto que a aceitação da prescrição é o último dos níveis na cadeia da inteligência, mesmo porque *a priori* não existem explicações nem previsões certas e erradas, sendo possível avaliar o sucesso de ambas após várias interações.

Para Handel (op. cit.), nada garante que os relatórios de inteligência terão qualquer impacto sobre a tomada de decisões. Um ponto de partida importante para a discussão sobre o ciclo da inteligência é ter claro que as análises e produtos de inteligência são apenas um dos diversos fluxos informacionais que influenciam o processo de tomada de decisões e seus relatórios podem ser mais ou menos importantes para certas decisões governamentais.

A dificuldade está em convencer os militares e líderes políticos a fazer o melhor uso da informação e da análise correspondente, uma vez que três grandes problemas afetam a aceitação de uma prescrição. O primeiro deles é a questão política, uma vez que quando estão em jogo assuntos de defesa é necessário contemplar uma miríade de interesses (individuais, coletivos, civis, militares etc.), que interferem nas decisões. Aqueles que discordam dos objetivos ou estratégias selecionadas e sentem que as decisões não contemplam seus interesses podem modificar ou subverter as decisões. Na verdade, planos operacionais são

escolhidos através de um processo político e não necessariamente da escolha racional, representando assim o produto do consenso que reflete a influência relativa dos diferentes indivíduos e organizações. A influência desses grupos pode ser enorme, definindo questões operacionais, escolhas estratégicas e militares, seleção e aquisição de sistemas de armas, recomendação e análise de informações e até mesmo na decisão de concluir uma guerra.

O segundo problema diz respeito à tecnologia, visto que a adoção de novas categorias de armas combinada com o aperfeiçoamento dos meios de comunicação e transporte reduziram acentuadamente o tempo disponível para tomar decisões, intensificando a pressão psicológica sobre os responsáveis por elas. Essas mudanças também alteraram a balança entre o controle militar e político da guerra, o relacionamento entre os agentes econômicos, e complicaram a definição do campo de combate, onde foi eliminada a distinção entre civis e combatentes. Ao mesmo tempo, a tecnologia moderna levou a uma paradoxal intermediação entre os elementos racionais e não racionais da guerra. O rápido processo de introdução de armas criou um viés não necessariamente racional, que depende da inspiração e imaginação. Em contraste, o desenvolvimento científico de cada sistema de armas e a comparação de sistemas de armas são predominantemente racionais. A impossibilidade de testar toda arma nova em condições reais de combate invariavelmente limita a habilidade dos militares de estabelecer doutrinas que correspondam à capacidade das armas. Por conta disso, muitos cenários de combates futuros dependem de fatores baseados na experiência, lições aprendidas com outros países e os interesses políticos e de organizações.

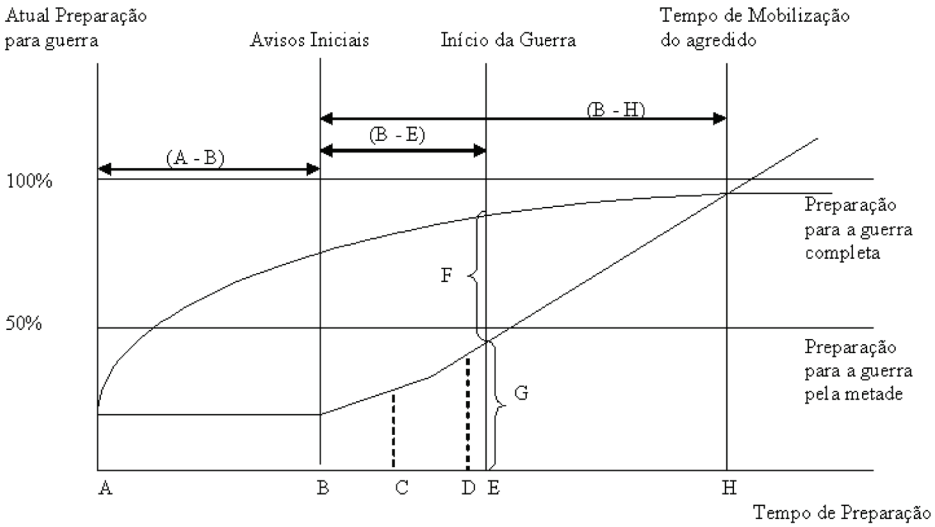
Um terceiro problema está no relacionamento entre os líderes e os agentes de inteligência. Nesse caso, tudo depende de quanto os líderes têm a mente aberta e encorajam crítica e precisão. Em tese, os líderes de uma democracia normalmente estão mais inclinados a considerar opiniões quando comparados com os líderes de um sistema autoritário. Isso acontece porque, nos países autoritários, a ascensão ao topo é obtida por meio da luta pelo poder, na qual os hábitos de cooperação são menos arraigados. Líderes de países autoritários normalmente têm pouca tolerância com ideias que desviam das linhas gerais, pois eles veem as críticas como um perigoso elemento para a ideologia existente. É claro que os padrões não são rígidos e não há remédio para estes problemas, porém duas sugestões cabem aqui: 1) devotar mais tempo para a educação dos líderes nesses assuntos antes deles ascenderem ao poder; e, 2) as organizações se prepararem, aprendendo como trabalhar com o líder.

Cada líder é sempre influenciado pelos seus conselheiros próximos, cuja interação com ele pode ter importância decisiva. A efetivação do seu relacionamento pode ser influenciada pelo caráter da comunidade de

inteligência. Há um relacionamento positivo ou negativo entre eles? Eles têm temperamento, caráter ou ambição complementares? Eles podem cooperar e respeitar um ao outro? Eles dividem uma ideologia comum ou uma experiência social e profissional comum? Para responder estas questões, nós também devemos conhecer como é o conselheiro de inteligência. Ele é um homem de absoluta integridade? Ele põe seu profissionalismo acima de tudo? Ele ascendeu à sua posição por suas conexões políticas ou pela sua capacidade profissional? Ele está preparado para aceitar quando sua posição profissional é ignorada ou não é aceita? É enorme a combinação de fatores que afetam o relacionamento entre o líder e conselheiro de inteligência. Isto leva a algumas observações: 1) o grau de afinidade entre o líder e seus conselheiros é de grande importância; se este relacionamento for ruim a efetividade da comunidade de inteligência diminui consideravelmente; 2) ter um bom tino político é de importância crítica para o líder da comunidade de inteligência. Entretanto, o analista pode carecer dessa qualidade, uma vez que, em tese, ele é treinado para ser objetivo e lidar com a verdade – o que torna difícil ter ao mesmo tempo um conselheiro de inteligência que aja politicamente com sutileza e tato; 3) a experiência demonstra que os líderes escolhem diretores de inteligência que comungam do mesmo ponto de vista político, reduzindo assim a possibilidade deste último oferecer alternativas; 4) não há dúvida que as melhores estimativas de inteligência aparecem quando o líder político e o seu conselheiro têm posições contraditórias, porém também é claro que em função disso, as relações tendem a se deteriorar mais cedo ou mais tarde. O resultado é que, a longo prazo, o líder tenderá a ignorar as estimativas produzidas pela inteligência.

Essa tensão entre a capacidade de cooperação entre os líderes políticos e seus conselheiros de inteligência, de um lado, e a necessidade para apresentar um objetivo com estimativas, de outro, não é uma solução simples no mundo real da política e da inteligência. O ideal pede um líder de mente aberta, que procure um conselheiro com sensibilidade política, o qual, por sua vez, comungue das inclinações políticas do líder, mas tenha coragem suficiente para apresentar estimativas realistas.

Observa-se, assim, que as atividades de coleta de material, análise de material e aceitação de uma prescrição, formuladas pelos analistas, afetam as opções de resposta nas mais diferentes situações, mas são especialmente graves para a decisão suprema: a da mobilização, que, segundo Handel, é a recomendação mais crítica que a organização de inteligência deve tomar. Nesse caso, um atraso não fica impune. Se há demora em qualquer nível, poderá haver atraso na resposta, sendo o impacto da demora melhor ilustrado pela figura 7:



- Ponto A: o agressor inicia a preparação para a guerra;
- Ponto B: o ameaçado percebe os primeiros avisos, mas a probabilidade de guerra ainda é incerta;
- Ponto C: fase de incerteza, com lenta preparação para a guerra;
- Ponto D: o ameaçado acelera seus preparativos, ante a crescente probabilidade de acontecer a guerra;
- Ponto E: inicia a guerra, o ameaçado vira agredido, mas sua preparação está incompleta;
- Ponto F: o hiato de tempo na resposta entre ataque e defesa, que favorece o agressor;
- Ponto G: a mobilização do agredido está completa;
- Ponto H: a preparação do agredido está completa;
- Intervalo A - B: representa o período de tempo em que o atacante tem a liderança;
- Intervalo B - E: representa o atual tempo de advertência do ameaçado;
- Intervalo B - H: representa o tempo que o agredido necessita para completar sua preparação;
- O intervalo B - H menos o intervalo B - E: representa o impacto do tempo de ataque.

Fonte: adaptado de Handel, 2001, pp: 238

Figura 7: Informação e Velocidade de Resposta

Pela figura, é possível ver que existe certo hiato de tempo (A - B) prévio à tomada de conhecimento do plano de ataque pelos serviços de inteligência do ameaçado. No tempo que o ameaçado começa a considerar a possibilidade de ataque (ponto B), o agressor estará bem à frente com seus preparativos de guerra. Mesmo assim, contudo, o ameaçado não está convencido que será atacado e, portanto, ele não ordena a mobilização total (ponto C). Enquanto o agressor continua os seus preparativos, o ameaçado gradualmente se convence da gravidade da situação e começa sua mobilização (ponto D). Uma vez preparado, o agressor lança o ataque (ponto E). Porém, existe uma lacuna de tempo entre os preparativos dos dois adversários, representado pelos avisos recebidos pelo ameaçado e sua mobilização (ponto F), estando este em certo estágio de preparação antes do ataque (ponto G). Enquanto o ameaçado está no ponto (B – E), ele precisa de mais tempo (B – H) para completar sua mobilização.

Toda a mobilização envolve grandes custos políticos, militares, materiais e psicológicos. Porém, se as análises de inteligência estiverem corretas e suas prescrições forem acatadas, elas podem salvar milhares de vidas e aumentar a chance de sobrevivência do Estado. Se as conclusões estiverem erradas ou se há demora em aceitar as prescrições, elas podem desencadear uma cadeia de eventos que possivelmente resultarão em guerra.

9.4. Conclusão

Como ficou demonstrado com este trabalho, a Teoria dos Jogos é um poderoso instrumento a ser utilizado pela inteligência. Todavia, ela apresenta problemas de aplicação que não podem ser desconsiderados, uma vez que podem não apenas reduzir, mas até mesmo invalidar os resultados obtidos. Os problemas começam com a própria dificuldade de selecionar a fonte das informações, tendo em vista a grande disponibilidade de meios de coletas à disposição dos serviços de inteligência, bem como a abundância de material fornecido por eles. Mas, observe-se que o problema não está exatamente na abundância dos dados, mas em sua abrangência, confiabilidade e completude.

O segundo problema está em obter informações corretas para a análise, o que é muito difícil na área de Inteligência, uma vez que estudiosos da área como Handel assumem *a priori* que não existe informação isenta de ruídos, o que implica na obrigatoriedade de se trabalhar com informação imperfeita.

Um terceiro problema está no reducionismo matemático que, em teoria, permite enquadrar em um número todas as situações sociais possíveis, facilitando assim sobremaneira a análise e permitindo atingir conclusões bem definidas. Porém, na prática, é extremamente difícil realiza esta tarefa, dada a quantidade de variáveis apresentadas por uma situação real, o que é especialmente verdadeiro no caso da Inteligência, em função da dificuldade de se obter informações, da quantidade de fatores a serem consideradas e da possibilidade bastante elevada de haver muita informação errada. Isto eleva drasticamente a incerteza e pode invalidar completamente as conclusões obtidas através da aplicação da Teoria dos Jogos.

Um quarto problema diz respeito ao dogma da maximização dos ganhos, no qual a própria experiência prática e a dificuldade de medi-lo mostram que se trata mais de uma premissa teórica destinada a permitir a análise matemática do que de um fator constante no mundo real. Na prática, quando uma interação envolve mais de um agente, todos os participantes têm dificuldade em saber o quanto estão maximizando os seus ganhos.

O quinto problema diz respeito a outro dogma da Teoria dos Jogos: o pensamento racional, que sempre foi utilizado como um fundamento balizador

para a análise, a despeito das contestações e problemas epistemológicos que apresenta quando utilizado em qualquer campo das ciências humanas. Não bastasse isto, como vimos, na Inteligência existem inúmeros fatores não racionais que devem ser considerados tendo em vista a desinformação, a tensão psicológica, as desconfianças, o temor do inimigo e até mesmo os preconceitos etnográficos a que são submetidos os agentes que atuam nesta área, de forma que sua análise nem sempre leva em conta o pensamento racional puro.

Finalmente, a Teoria dos Jogos pode ser extremamente importante quando contribui para a elaboração de cenários e fornece prescrições, porém, ela não é auto-executável, ou seja, ela nada decide, sendo apenas um instrumento auxiliar para tomada de decisões. Estas estão a cargo de agentes que podem ter suas próprias motivações para adotar determinada decisão, independentemente das conclusões obtidas através da aplicação da Teoria dos Jogos.

Apesar desses problemas devemos nos perguntar por que a Teoria dos Jogos é tão longeva e tão importante para a Inteligência. Isto se deve aos motivos que levaram a sua concepção e aperfeiçoamento ao longo da história: a despeito de todos os seus limitadores, através da Teoria dos Jogos é possível ter uma melhor compreensão da natureza do jogo, uma melhor percepção das motivações dos rivais, uma melhor compreensão do entendimento das ações e reações dos competidores antes de desenvolver e implementar sua própria estratégia, ou seja, ela pode afinal orientar os agentes sobre qual a melhor decisão tomar.

REFERÊNCIAS

ABRANTES, Maria Luísa. (2004). *Teoria dos Jogos e Oligopólio*. Disponível em: <www.caaei.org/anexos/33.pdf>. Acesso em: 20 out. 2009.

ALLINGHAN, Michael. (2006). *Choice Theory.* Oxford. Oxford University Press.

ALMEIDA, Alecsandra Neri de. (2006) Teoria dos Jogos: As Origens e os Fundamentos da Teoria dos Jogos. *UNIMESP.* p. 8.

ALVARES, Lilian. *Contra-Inteligência*. Disponível em: <www.cinform.ufba.br/v_anais/.../org_brasil_de_informacao.ppt>. Acesso em: 20 nov. 2009.

BARRETO, Larissa Santana; BORTOLOSSI, Humberto José; GARBUGIO, Gilmar; SANTOS, Polyane Alves & SARTINI, Brígida Alexandre. (2004). Uma Introdução a Teoria dos Jogos. *II Bienal da Sociedade Brasileira de Matemática*. UFB. 25 a 29 de outubro de 2004, p 67.

BARRICHELO, Fernando. *Teoria dos Jogos*. Disponível em: <http://www.teoriadosjogos.net/index.asp>. Acesso em: 5 nov. 2009.

DIÃO, Rui. (1995). *A Ciência dos Sistemas Complexos. Técnica.* n. 1, mar/05. p 14.

CEPIK, Marco. (2002). Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação. *Security and Defense Studies Review*, vol. 2 n. 2, Winter.

HANDEL, Michael I. (1989). *War, Strategy, and Intelligence*. London FrankCass.

HERMAN, Michael. (2001). *Intelligence services in the information age*. London: FrankCass.

Game Theory: Is there an ideal strategy for winning the war on terrorism. Disponível em: <http://members.cox.net/mathmistakes/game_theory.htm>. Acesso em: 19 nov. 2009.

GILL, Peter & PHYTHIAN, Mark. (2006). *Intelligence in an unsecure world*. Cambridge. Polity Press.

GLERIARO, Iram; MATSUSHITA, Raul & SILVA, Sérgio. (2004). Sistemas complexos, criticalidade e leis de potência. *Revista Brasileira de Ensino de Física* v. 26, n. 2, p 99-108. Disponível em: <sbfisica.org.br>. Acesso em: 21 out. 2009.

"Inteligência" Seminário Internacional de Inteligência (2007). São Paulo, Rio de Janeiro, Curitiba. Disponível em: <www.cendotec.org.br/pdf/dossierinteligencia.pdf>. Acesso em: 15 out. 2009.

MONTEIRO, Claudia Servilha. (2009). A Decisão Racional na Teoria dos Jogos. Disponível em: <www.conpedi.org/manaus/arquivos/anais/.../claudia_servilha_monteiro.pdf>. Acesso em: 20 out. 2009.

NOGUEIRA, Marcio de Andrade. *A Teoria dos Jogos no Desenvolvimento de Estratégias que Atendam à Estratégia Nacional de Defesa*. Disponível em: <www.abed-defesa.org/page4/page5/page27/.../page45.html>. Acesso em: 10 nov. 2009.

SZALAI, Andras. (2008) Rational Choice Theory in Early Cold War US Defense Policy – The Role of 'Defense Rationalist' Anual Doctoral Conference. Corvinus University. Disponível em: <web.ceu.hu/polsci/ADC/2008/papers/AndrasSzalai.pdf>. Acesso em: 20 nov. 2009.

SCHEVE, Tom. *How Game Theory Works*. (2008). Disponível em: <HowStuffWorks.com. <http://science.howstuffworks.com/game-theory.htm>. Acesso em: 20 nov. 2009.

SILVA, Antônio Rogério da. *Teoria dos Jogos e da Cooperação para Filósofos*. Disponível em: <http://www.scribd.com/explore>. Acesso em: nov. 2009.

Capítulo 10

ANÁLISES DE INTELIGÊNCIA: AMBIENTE, PERCEPÇÃO, EMOÇÃO E NEUROCIÊNCIA[1]

Christiano Cruz Ambros

O objetivo deste capítulo é identificar e expor ao leitor os principais vieses cognitivos e emocionais que afetam o processamento humano de informações e, consequentemente, os resultados das análises de Inteligência Governamental. Mais do que abordar profunda e exaustivamente o processo cognitivo humano – o que seria necessário para realmente compreender as nuances do fenômeno dos vieses cognitivos – este artigo se propõe a ser um estudo preliminar aos interessados no assunto. Nosso propósito foi sintetizar de forma sistemática algumas das relevantes pesquisas já feitas neste campo da ciência, que vem sendo chamado de "errologia", em um intuito eminentemente didático e introdutório.

A análise de Inteligência é o coração da atividade de Inteligência. A análise é aqui definida como o processo de sintetizar e avaliar um cenário ou uma solução utilizando-se de evidências vindas de fontes de informações variadas, complexas e extensas. Segundo Javier Jordán (2011:1), "a análise de inteligência consiste em um processo de avaliar e transformar informações brutas em descrições, explicações e conclusões destinadas aos consumidores de inteligência.[2] A natureza peculiar e complexa da análise de inteligência não consegue incorporar plenamente nenhum tipo de fórmula preestabelecida a dominar o ofício, evidenciando que não pode ser reduzida a métodos rígidos e

[1] O presente artigo é uma versão revisada do quarto capítulo da monografia de conclusão de curso do autor em Relações Internacionais na Universidade Federal do Rio Grande do Sul (UFRGS), sob orientação do Prof. Dr. Marco Cepik. A monografia completa, *Inteligência Governamental e Tomada de Decisão em Política Externa*: Aspectos Cognitivos e Modelos de Personalidade, está disponível em: <http:\\www.lume.ufrgs.br\\handle\\10183\\28393>.

[2] Disponível em: <http://wdb.ugr.es/~gesyp/analisis-inteligencia acessado a 02/04/2011>. Tradução nossa.

infalíveis. Neste contexto, vieses cognitivos são uma grande ameaça para uma análise de inteligência bem-sucedida.

Mark Lowentall (2008:306-310) procura descrever certos padrões para uma boa análise, desenvolvendo mais uma normativa de cuidados a se ter no processo de análise do que propriamente justificando um método analítico padrão. A robustez empírica e metodológica típica dos trabalhos científicos é difícil de ser alcançada pela análise de inteligência, e, por isso, as certezas, que são tão desejadas pelos tomadores de decisão a quem os analistas servem, são de difícil acesso. Como coloca Jordán (2011:2):

> Esto es así porque la inteligencia está orientada a asesorar y a reducir la incertidumbre em procesos de toma de decisiones que siguen unos ritmos temporales marcados por los acontecimientos, y que no pueden esperar a que al analista sea capaz de explicar de forma exhaustiva y empiricamente fundada objetos de estudio que, em muchos casos, consisten o se contemplan em escenarios futuros y, por tanto, inaccesibles a la experiencia.

Considerando a falta de uma metodologia rígida (ainda que haja muitas ferramentas de análise e métodos disponíveis aos analistas), a incerteza e informação incompleta típica dos contextos analisados pela inteligência, conjugadas a um ambiente de pressão e escassez de tempo, acabam por fazer com que o resultado final da análise dependa de maneira bastante forte do critério e do bom senso do analista. Assim, a análise de inteligência fica mais predisposta aos possíveis erros advindos de vieses cognitivos do analista.

Segundo Lowenthall (2008), a maior parte das falhas sofridas pela comunidade de inteligência norte-americana durante a década de 1990 esteve relacionada à análise. As lições, desafios e dilemas que enfrenta a Inteligência Governamental ocidental, em especial a norte-americana, a partir dos ataques terroristas de 11/9 e da Guerra do Iraque são, "em determinado grau, simplesmente exemplos contemporâneos de problemas que surgem, em partes, das limitações inerentes da cognição humana." (PHYTHIAN, 2009:67, tradução nossa).

Os erros em Análises de Inteligência podem ter suas origens em diferentes causas: falsas presunções, escassez de tempo, orientação ao consenso entre os analistas, disfunções organizacionais, interpretações interessadas etc. (JORDAN, 2011). Neste artigo nos concentraremos, principalmente, na descrição das origens psicológicas dos erros relacionados a vieses cognitivos. Segundo Heuer (1999:111-112, tradução nossa), "vieses cognitivos são erros mentais causados por nossas estratégias simplificadas de processamento de informações. [...] um viés cognitivo não é resultado de uma predisposição emocional ou intelectual para determinado julgamento, mas sim de um processo mental subconsciente de processamento de informações".

Hallinan (2010:16) afirma que "todos somos atormentados por certas inclinações e tendências sistêmicas na maneira como vemos, lembramos e percebemos o mundo a nossa volta, e essas influências e esses pendores para a parcialidade nos deixam propensos a cometer certos tipos de erros". O estudo sistemático dos erros reproduzíveis no raciocínio humano, e o que esses erros revelam sobre processos mentais subconscientes, é conhecido como o campo de heurísticas e vieses na Psicologia Cognitiva. Nos Estudos de Inteligência, o 11/9 acelerou o processo iniciado durante a década de noventa de revisão dos pilares básicos da análise na atividade de inteligência governamental. O estudo dos vieses e heurísticas aplicados à análise de inteligência se fortaleceu "na medida em que a análise de inteligência passou de ser um ofício para se tornar uma disciplina, e o corpo de conhecimento compartilhado que a sustentava cresceu, assim, a atenção quanto à dimensão desses problemas e de suas possíveis soluções se espraiaram" (PHYTHIAN, 2009:67, tradução nossa).

Na década de 1990, estudos de caso sobre agências de inteligência e seu desempenho analítico já indicavam que analistas e gestores não prestavam a devida atenção ao fenômeno dos vieses cognitivos (DAVIS, 1992). Confiar que se possa reduzir a zero os erros de análise é sensivelmente uma aspiração ilusória (JORDAN, 2011), mas estamos convencidos de que é possível melhorar os resultados dos relatórios de análise se o analista conhecer o seu próprio processo mental e estiver advertido dos erros que pode cometer.

Portanto, este artigo irá sistematizar as principais categorias de vieses cognitivos e explorará as possíveis influências emocionais do indivíduo na análise de inteligência. A primeira sessão descreve o ambiente em que a análise de inteligência ocorre e as restrições que sua natureza impõe ao funcionamento da atividade. A sessão seguinte expõe as considerações mais relevantes sobre a função da heurística e dos modelos mentais no processamento de informação e trata dos vieses cognitivos a que os analistas estão suscetíveis. Finalmente, a última sessão aborda a influência da emoção na avaliação de situações e o papel da neurociência em encontrar explicações sobre o funcionamento do cérebro quanto ao processamento de informações e tomada de decisão.

10.1. O Ambiente da Análise de Inteligência

Grande parte das decisões na área de inteligência governamental e muitas análises de inteligência precisam ser feitas em um espaço de tempo relativamente curto, sob estresse e ambiguidade de informação. As características do ambiente influem na estratégia da tomada de decisão que os oficiais gerenciais fazem e nas suas últimas escolhas, assim como também afetam a maneira como o analista de inteligência vai perceber, processar e sintetizar determinadas informações. O denominador comum dos fatores do ambiente que mediam o esquema das

decisões estratégicas centra-se nas demandas cognitivas impostas pela tarefa decisória (MINTZ & DeROUEN, 2010:30), assim como pela demanda por análises de inteligência. Quanto mais pesada for a demanda (por exemplo, quanto mais ambígua e estranha ao indivíduo a informação for), mais provavelmente o tomador de decisão e o analista empregarão simplificações heurísticas ou atalhos cognitivos.

Os ambientes de tomada de decisão e de análise estão geralmente em estado de fluxo, no qual crises de segurança nacional ou de política externa são marcadas de alguma forma por uma situação caótica em que a informação é apresentada e recebida pelo decisor de maneira ainda mais complexa e variada (MINTZ & DeROUEN, 2010:30). Especificamente, incerteza, estresse, familiaridade ou falta dela sobre determinada tarefa, risco e percepção de ameaça, e *accountability* sobre os resultados da decisão ou da análise: tudo isso afeta as estratégias de decisão, escolha e análise.

O constrangimento de tempo é um fator muito presente no ambiente de tomada de decisão em questões estratégicas e gerenciais na área de inteligência governamental, dificultando as abordagens teóricas do ator racional, pois a decisão sob pressão geralmente não leva cálculos racionais estruturados. Isto não significa que a decisão será ruim, pois muitas vezes o tomador de decisão é obrigado a focar toda a sua atenção a determinado problema. O que significa é que, neste contexto, a probabilidade de usarmos atalhos mentais automáticos e suposições preconcebidas são maiores, no intuito de economizarmos tempo.

A restrição de informações também é um fator do ambiente que prejudica os modelos de racionalização perfeita do ator, pois dificultam a comparação de alternativas, de análises de custo e benefício e de determinação de utilidade. Nesse campo, produtores (analistas de inteligência) e consumidores (os tomadores de decisão) de inteligência se relacionam, e é neste processo que se encontram uma série de problemáticas. Uma delas são os vieses psicológicos que já podem vir do processo analítico do oficial de inteligência para o tomador de decisão. A outra problemática são os vieses políticos e burocráticos, no sentido de que o oficial de inteligência quer que o seu relatório seja levado em conta e noticiado, e muitas vezes acaba distorcendo a informação para que seja o que o tomador de decisão quer ler.

A Guerra do Vietnã foi caracterizada por conhecidos problemas informacionais. O Presidente Johnson foi repetidamente noticiado que a guerra estava indo de acordo com o plano e que o aumento de tropas levaria à vitória. O presidente estava sendo alimentado com informações enviesadas que não eram completamente acuradas. Isto tornou difícil para ele comparar alternativas e utilidades realisticamente (MINTZ & DeROUEN, 2010:26). Entretanto, isso não significa que o presidente fez escolhas "irracionais", só mostra que o contexto

não permitia que se chegasse a uma típica escolha maximizadora, assim como a maioria das situações.

A ambiguidade ocorre quando a informação com que se está lidando tem múltiplos e, por vezes, até divergentes significados, ou quando a situação pode ter vários resultados possíveis. As informações ambíguas são geralmente ignoradas ou descontadas de valor, pois elas aumentam a complexidade da tomada de decisão, fazendo com que os decisores ou analistas geralmente usem atalhos cognitivos para simplificar tanto o processamento de informação quanto a tomada de decisão. As informações oferecidas pelas agências de inteligência dos EUA sobre a postura ofensiva das forças iraquianas antes da invasão ao Kuwait foram ignoradas pelo governo em grande parte por causa das estimativas contrárias oferecidas pelos aliados dos americanos na região, como o Egito e a Arábia Saudita (MINTZ & DeROUEN, 2010:27).

A familiaridade com problemas decisórios ou analíticos acontece quando o decisor ou analista encontra uma situação similar a outra que ele viu ou presenciou anteriormente. Nessas situações é comum o indivíduo processar as informações heuristicamente, acreditando que o que funcionou anteriormente funcionará novamente e tendendo a confiar nos seus atos ou decisões prévias. Isto geralmente leva a uma avaliação mais intuitiva, pois ao invés de examinar todos os componentes da informação, o indivíduo costuma ir diretamente para as conclusões baseadas nas experiências prévias sem nem mesmo considerar alternativas de custo e benefício. Este processo de simplificação é útil ao decisor e ao analista, pois permite agilidade na tomada de decisão e nas análises. Entretanto, geralmente, a familiaridade leva a grandes generalizações baseadas em similaridades superficiais que frequentemente escondem informações inconsistentes, as quais levarão a erros e distorções.

Riscos são uma componente importante do ambiente tanto da tomada de decisão quanto da análise de informações nas agências de inteligência, pois geralmente há muito em jogo na arena onde essas atividades ocorrem. O quanto de risco os tomadores de decisão estão dispostos a tomar influencia em muito as suas decisões. Riscos podem ser pensados como a probabilidade de um ator aceitar alcançar resultados negativos. Uma alternativa de alto risco é aquela em que a probabilidade de falha é grande o suficiente para que a utilidade esperada da ação seja negativa. É importante considerar o modo como o tomador de decisão age sob condições de risco, pois isto aponta para o nível de incerteza com que o indivíduo toma atitudes confortavelmente. Ainda que essas atitudes sejam ligadas à idiossincrasia do indivíduo, elas também são afetadas pelo nível de satisfação com o *status quo*: aqueles mais insatisfeitos são mais propensos a tomar mais riscos (MINTZ & DeROUEN, 2010:28).

O estresse pode ser conceituado como resultado emocional de um excesso de demandas sobre a capacidade de resposta. Segundo Mintz e De Rouen (2010: 29), Ole Holsti (1972) sumarizou alguns dos impactos que um ambiente estressante pode ter sob a tomada de decisão durante crises. O estresse causado por constrangimentos de tempo e incerteza podem liberar sentimentos de vergonha e ansiedade, além de influenciar no processamento de informações através da supersimplificação, ignorando certas informações e alternativas e confiando mais em analogias históricas (que abordaremos mais especificamente ao longo da próxima seção). O estresse também pode fazer com que o indivíduo superestime as capacidades do oponente, e, sendo levado ao extremo, pode causar pânico, paralisando o indivíduo na sua tomada de decisão. Estudos revelaram que o estresse leva a um decréscimo do foco de atenção, à regressão a estilos decisórios primitivos ou muito elementares, a um aumento nos erros e a uma tendência a comportamentos aleatórios (MINTZ & DeROUEN, 2010:29).

Como pudemos perceber, os ambientes da tomada de decisão e da análise de informações são propensos a produzir vieses cognitivos causados por atalhos mentais que acabamos tomando, a maior parte das vezes inconscientemente, como reação aos estímulos do ambiente. Apesar de, teoricamente, uma decisão implicar em um processo complexo que envolve várias fases sequenciais racionalmente, a todo o momento da vida corrente aplicamos juízos e decisões tomados de forma intuitiva e para os quais recursos às heurísticas são práticos e inevitáveis (CABECINHAS, 1994:5).[3]

Nem todos reagem ao ambiente da mesma forma. Se todos os indivíduos tendessem a se comportar da mesma forma em uma dada situação, seria inútil estudar as estruturas mentais particulares dos indivíduos. Se os situacionistas, aqueles que acreditam que a situação basta para explicar o comportamento do indivíduo, estão corretos, então há pouco a ser ganho quando olhamos para "dentro da cabeça das pessoas". De acordo com eles, nós podemos ter toda a informação necessária sobre o comportamento do indivíduo especificando a natureza da situação em que o indivíduo se encontra, sem considerar as suas disposições. Já os disposicionistas assumem que indivíduos variam nas suas respostas às situações, e eles se perguntam quais são os fatores específicos que produzem esta variação.

[3] Conforme Cabecinhas (1994:5): "As heurísticas são regras expeditas que simplificam o processo de tomada de decisão, levando os indivíduos a subotimizar os seus juízos. Os investigadores que mais se têm destacado neste domínio são Tversky e Kahneman, tendo efetuado o primeiro levantamento das heurísticas e enviesamentos mais frequentes nos juízos humanos. Segundo Tversky e Kahneman: 'people rely on a limited number of heuristic principles which reduce the complex tasks of assessing probabilities and predicting values to simpler judgment operations. In general, these heuristics are quite useful, but sometimes they lead to severe and systematic errors'" (1974:3).

Desde a década de 1980, psicólogos trabalhando em campos tão diversos quanto o processo de tomada de decisão em política externa e o comportamento eleitoral têm progressivamente se empenhado para explicar essas diferenças individuais, por meio do exame das estruturas do conhecimento ou as "arquiteturas" cognitivas em nossas cabeças (HOUGHTON, 2009:114). Assim, a próxima seção busca compreender um pouco mais sobre essa arquitetura cognitiva, abordando tanto a forma como o nosso cérebro geralmente funciona, o que implica em impactar todos os indivíduos, quanto o que a nossa mente cria para cada um de nós baseado em crenças, experiências, valores e traços de personalidade individuais.

10.2. Percepção, Julgamentos e Distorções Cognitivas

Regras implícitas moldam como o cérebro interpreta uma cena, reconstrói a memória e resolve um problema. Na maioria das vezes, essas regras funcionam para o seu benefício, permitindo inferências automáticas que, caso não existissem, iriam dificultar e sobrecarregar o pensamento consciente cerebral, até o limite de inviabilizar a tomada de uma decisão crucial, imobilizando-nos. Entretanto, outras vezes as suposições automáticas do cérebro podem mascarar a realidade ou encorajar exatamente a reação errada. Enquanto a psicologia moderna manteve a ideia freudiana de que muitos dos nossos processos mentais são inconscientes – por exemplo, nós geralmente usamos vários atalhos cognitivos quase sempre sem sabermos que o estamos fazendo –, a psicologia cognitiva toma emprestada uma série das ideias psicanalíticas, sendo que até mesmo os psicólogos especializados em política as utilizam (HOUGHTON, 2009:114-115).

A discussão sobre o indivíduo como tomador de decisão permite retroceder até os princípios racionalistas do século XIX, como em Bentham e o Utilitarismo. Entretanto, tal tópico só veio a tomar as feições de uma teoria propriamente dita durante a Segunda Guerra Mundial, com o desenvolvimento da Teoria da Decisão, e, posteriormente, da Teoria dos Jogos, devido ao grande interesse de pesquisadores matemáticos e estatísticos quanto à otimização das estratégias militares. A racionalidade na tomada de decisões assumia que os indivíduos percebiam o mundo apuradamente e chegavam a decisões através de um amplo processo intelectual, no qual "objetivos são ordenados, uma busca é feita por informações relevantes, um amplo leque de alternativas é considerado e a opção que maximiza os benefícios enquanto minimiza os custos é selecionada" (ROSATI, 1995:50).

Assim, é interessante notar que os estudos cognitivos e psicológicos nas pesquisas de tomada de decisão surgem como uma ferramenta para explicar as anomalias e erros na racionalidade perfeita do ator. Teóricos da Escolha Racional e Psicólogos especializados em política concordam que a psicologia cognitiva

geralmente tenta explicar apenas desvios à racionalidade (MERCER, 2005:77). A partir da década de 1950, a percepção da dificuldade de estabelecer o ator como totalmente racional suscitou críticas aos teóricos realistas das relações internacionais, dominantes até então (HERZ, 1994:75).

10.3. Racionalidade Limitada, Percepção Ativa e Vieses Cognitivos

Herbert Simon foi um dos primeiros a avançar no conceito da racionalidade limitada. Por causa dos limites naturais da capacidade mental humana, ele argumenta, a mente não consegue lidar diretamente com a complexidade do mundo. Assim, nós construímos modelos mentais simplificados da realidade e trabalhamos dentro desses modelos. Nós nos comportamos racionalmente dentro dos limites do nosso modelo mental, que, contudo, nem sempre está bem adaptado aos requerimentos do mundo real (HEUER, 1999:3). O conceito de racionalidade limitada tornou-se amplamente reconhecido, ainda que não universalmente, tanto pelo retrato acurado do julgamento e escolha humana quanto por uma sensibilidade em reconhecer as limitações inerentes de como a mente humana funciona. Muitos acadêmicos aplicaram esses *insights* psicológicos no estudo do comportamento político internacional, e perspectivas psicológicas similares estão também presentes nos Estudos de Inteligência, principalmente quando se trata de falhas de inteligência e surpresa estratégica (HEUER, 1999:3).

As pessoas tendem a compreender a percepção como um processo passivo, em que nós vemos, ouvimos, cheiramos, sentimos e degustamos os estímulos sobre os nossos sentidos, gravando assim a realidade exatamente como ela é. Entretanto, a percepção é demonstradamente um processo ativo; ele constrói a realidade ao invés de gravá-la (HEUER, 1999:7). Segundo MacDonald (2010: 71), o cérebro é uma máquina de construir realidades. Percepção implica compreender, assim como estar atento. É um processo de inferência em que as pessoas constroem sua própria versão da realidade baseadas nas informações providas através dos seus cinco sentidos. Entretanto, esse *input* sensorial é mediado por um complexo processo mental que determina qual informação será considerada, como será organizada, e que significado será atribuído a ela.

Esse processo pode ser imaginado como a percepção do mundo através de lentes ou telas que canalizam e se focam, podendo assim distorcer as imagens que estão sendo vistas. Dessa forma, para atingir a imagem mais clara possível da China, por exemplo, o analista ou o tomador de decisões precisa mais do que informações sobre a China. Ele também precisa compreender as suas próprias lentes pelas quais essa informação está passando. Chamaremos essas lentes de modelos mentais.

Os modelos mentais seguem tendências cerebrais naturais do nosso cérebro. Eles estão presentes em todos os indivíduos por serem resultado do rumo evolutivo da espécie humana, mas moldam-se especificamente para cada indivíduo por serem constituídos, em parte, pelas nossas crenças, valores éticos, sociais e culturais, imagens e suposições, ou seja, informações externas que internalizamos como sendo a nossa verdade. Os traços pessoais, ou seja, características da personalidade de cada um, também influenciam na construção de modelos mentais. O fato é que esses modelos mentais agem no subconsciente automaticamente, fazendo com que compreendamos a realidade a nossa volta e com que acreditemos que entendemos o mundo a nossa volta da forma que ele realmente é.

A questão é que esses modelos mentais podem nos levar a vieses cognitivos. Vieses Cognitivos (*Cognitive Biases)* são erros mentais causados pelas nossas estratégias de simplificar o processamento de informações. É importante notar que vieses cognitivos são diferentes de outras formas de vieses, como culturais, organizacionais, ou vieses que resultam do próprio interesse consciente de alguém (HEUER, 1999:111). Eles são resultado de procedimentos mentais subconscientes para o processamento de informações. Um viés cognitivo é um erro mental consistente e previsível (HEUER, 1999:111). Entretanto, saber da existência de um viés cognitivo não nos leva automaticamente a evitá-lo. Nesse sentido, podemos ver a armadilha e cair nela, mas ao menos saberemos que estamos em uma armadilha.

Existe uma tendência a pensar modelos mentais como algo ruim, algo a ser evitado. Na verdade, modelos mentais não são nem bons nem ruins, eles são inevitáveis (HEUER, 1999:10). As pessoas não têm maneira concebível de lidar com o volume de estímulos que atingem os seus sentidos, ou com o volume e complexidade de dados que precisam ser analisados, sem algum tipo de preconcepção simplificadora sobre o que é esperado, o que é importante, e o que está relacionado ao que. Analistas ou tomadores de decisão não atingem uma análise objetiva evitando preconcepções. Objetividade é atingida por meio de suposições básicas e raciocinando o mais explicitamente possível, para que a análise possa ser desafiada por outras e os próprios analistas possam, eles mesmos, examinar a sua validade (HEUER, 1999:10). Quanto mais honesto intelectualmente for o analista ou o tomador de decisão, e quanto mais consciente dos seus modelos mentais e possíveis armadilhas que ele possa vir a cair, mais provável será que erros de percepção e julgamento sejam detectados na análise, talvez nem mesmo pelo próprio analista ou tomador de decisão, mas por outro indivíduo.

Muitos estudiosos já conduziram experimentos extensamente testados que mostram que a informação obtida por um observador depende das suposições

e preconcepções do próprio observador. Por exemplo, o que você vê na figura abaixo?

Figura 1

Fonte: HEUER,1998:8

O resultado está na nota de rodapé.[4] Assim sendo, nosso cérebro tende a perceber o que nós esperamos perceber. O que acontece é que precisamos de mais informações, e mais informações não ambíguas, para reconhecer um fenômeno inesperado.

Um experimento clássico para demonstrar a influência da expectativa na percepção usa cartas de baralho misturadas com alguns naipes de espada vermelhos e alguns corações pretos. Quando imagens das cartas eram mostradas brevemente em uma tela, os sujeitos do experimento tendiam, naturalmente, a identificar as cartas normais mais rápida e acuradamente do que as anômalas. Depois que os sujeitos percebiam a existência das cartas anômalas, sua *performance* melhorava um pouco, mais ainda assim, a velocidade e a certeza de reconhecimento da carta normal era muito maior (HEUER, 1999:8). Esse experimento demonstra que os padrões de expectativa tornam-se tão enraizados que eles continuam a influenciar na percepção mesmo quando as pessoas estão alertas e tentam levar em conta a existência daquela informação que não se encaixa nas suas preconcepções.

A posição dos sujeitos do teste é análoga aos analistas de inteligência ou líderes de governo tentando compreender o enorme fluxo de papéis que cruzam a sua mesa (HEUER, 1999:9). O que é realmente percebido naqueles papéis, assim como a maneira com que é interpretado, depende, em partes, dos padrões de expectativa do analista ou do tomador de decisões. Eles têm uma série de suposições e expectativas sobre as motivações das pessoas ou processos do governo de outros países. Assim, eventos consistentes com estas expectativas são percebidos e processados facilmente, enquanto eventos que contradizem estas expectativas prevalentes tendem a ser ignorados ou distorcidos de maneira a satisfazer a expectativa inicial. Dessa forma, as expectativas do indivíduo podem enviesar as observações de variáveis relevantes para determinada

[4] Os artigos estão escritos duas vezes em cada frase. Isto é raramente percebido, pois nossa percepção é influenciada pelas nossas expectativas sobre como estas frases familiares são comumente escritas.

estratégia (CABECINHAS, 1994:6). Claro que essas distorções e enviesamentos são subconscientes ou preconscientes (HEUER, 1999:9).

Um dos primeiros a perceber este fenômeno da mente humana e aplicá-lo para as problemáticas da política externa foi Robert Jervis. A primeira hipótese do autor sobre percepções dos líderes de Estado é: os tomadores de decisões tendem a encaixar informações nas suas teorias já existentes e imagens preconcebidas (1968: 189). Os psicólogos especializados em política começaram a chamar esse fenômeno de Consistência Cognitiva, afirmando que o tomador de decisão irá descartar as informações inconsistentes com as suas imagens e crenças prévias ou prestará excessiva atenção àquelas que se encaixem com as suas expectativas.

10.4. Crenças e Imagens

É importante definirmos aqui o que estamos chamando de crenças e imagens. Alguns analistas conceituam as crenças como atitudes, opiniões, ou ideologias. Existem distinções entre crenças normativas (sobre como deveria ser) e crenças positivas (sobre como é), crenças centrais e periféricas (crenças que são fixas e fundacionais ou crenças que são menos centrais), e crenças abertas e fechadas (ou seja, crenças que são ou não são abertas à mudança em geral) (HOUGHTON, 2009:106). De acordo com Vertzberger, o set de crenças individuais representa todas as hipóteses e teorias que o indivíduo é convencido que são válidas em determinado momento (HOUGHTON, 2009:106). Neste trabalho iremos adotar a definição de Vertzberger.

Na política, assim como em outras esferas da vida, as crenças ajudam a determinar o que nós percebemos; ajudam-nos a definir a natureza da situação que estamos enfrentando (diagnóstico), assim como o tipo de opções ou soluções que achamos apropriadas (prognóstico). Da perspectiva da psicologia cognitiva, crenças podem ser consideradas um tipo de "atalho" mental; indivíduos desenvolvem crenças para ajudá-los a compreender o mundo.[5] Crenças[6] são

[5] Nesse ponto, geralmente surge a discussão baseada na seguinte pergunta: São as crenças que moldam o comportamento, ou é o comportamento que constrói as crenças? O psicólogo Daryl Bem (apud HOUGHTON, 2009:107), que desenvolveu a teoria da autopercepção, argumenta que frequentemente agimos sem saber o porquê o estamos fazendo, mesmo na ausência de crenças específicas. Quando isso acontece, nós geralmente construímos crenças após o fato para justificar o que acabamos de fazer. Se bem está correto, então talvez as nossas crenças não moldam nosso comportamento tanto quanto pensamos (HOUGHTON, 2009:108). O ponto é que não necessariamente um anula o outro. Primeiro porque se primeiro agimos e depois criamos a crença, provavelmente agiremos segundo a nossa crença quando encararmos uma situação similar, em um movimento de retroalimentação do comportamento e da crença. Além disso, a crença pode vir antes do comportamento, pois aprendemos não só através da própria experiência vivencial. Aprendemos a partir dos outros (situações que vemos os outros vivendo) e de fontes externas desenvolvidas por outros (cultura, sociedade, política etc.).

[6] É importante chamar a atenção entre a diferença de crenças e imagens. Argumento que as crenças geralmente servem para encontrarmos explicações de causa e efeito das situações, ou seja, elas nos levam aos nossos porquês. As crenças nos ajudam a observar a dinâmica do que percebemos.

um meio de filtrar sinais e informações que de outra forma esmagariam os nossos sentidos e nos sobrecarregariam (HOUGHTON, 2009:106). Entretanto, é importante tentar estar cientes das nossas próprias crenças e de como elas afetam a nossa percepção.

10.5. Expectativa e Contexto nos Modelos Mentais

As expectativas têm uma grande variedade de fontes, incluindo experiências passadas, treinamento profissional, normas organizacionais e culturas, valores éticos e traços individuais. Tudo isso influencia na predisposição do analista ou do tomador de decisão de dispor particularmente de mais atenção para certos tipos de informação e organizar e interpretar esta informação de determinadas formas.

A percepção também é influenciada pelo contexto em que está ocorrendo. Diferentes circunstâncias evocam diferentes esquemas de expectativas (HEUER, 1999: 9). Por exemplo, é mais provável que a mente seja conduzida a explicações sobrenaturais a cerca de um barulho suspeito quando se está em um cemitério à meia-noite do que se escutamos o mesmo som em um passeio no parque durante o dia. Da mesma forma, é provável que em situações de crise internacional, qualquer ato de algum dos atores envolvidos seja interpretado como um ato agressivo, não importando que seja contra ou a favor do indivíduo que analisa a situação. A situação conflituosa está latente em sua mente, influenciando na sua percepção de qualquer ato externo.

A literatura conceitualiza essa predisposição como Esquema Evocado (*Evoked Set)*, referindo-se à preocupação imediata que está a frente na mente do tomador de decisão (MINTZ & DeROUEN, 2010:99).[7] Em outras palavras, o foco

---

As imagens são um tipo de estereótipo que a mente usa para categorizar eventos e pessoas (MINTZ & DeROUEN, 2010:101). Elas identificam o padrão estático do que observamos; os traços constantes do que percebemos. Um bom exemplo é imaginar um observador que se encontra com um objeto esférico na rua. Ele rapidamente analisa o objeto e o compatibiliza com a imagem de uma bola de futebol. Ele tem a crença de que se ele chutar a bola ela irá se mover. Com a intenção de movê-la, ele a chuta. Entretanto, ele pode ter errado ao compatibilizar aquele objeto como uma bola de futebol, e pode ser um bloco de pedra esférico preso ao chão, que definitivamente não se moveu quando o indivíduo a chutou.

[7] É interessante notar como alguns resultados de pesquisas do campo da neurociência parecem reforçar a hipótese dessa tendência cognitiva. Em pesquisa feita por Rolls (2005), foi demonstrado como que para a memória de curto prazo, associada ao córtex pré-frontal dorsilateral, ser mantida durante períodos em que um novo estímulo está sendo recebido, é preciso ter redes neurais separadas para as funções perceptuais e de memória de curto prazo, e de fato, dois pares de redes neurais (uma no córtex inferior visual temporal para as funções de percepção, e outra no córtex pré-frontal para a manutenção da memória a curto prazo durante o estímulo) ofereceram um modelo preciso da interação dos sistemas perceptuais e de memória a curto prazo. Em particular, esse modelo mostra como um atrativo (autoassociativo) na rede do córtex pré-frontal pode ser disparado por um simples estímulo visual representado no córtex inferior visual temporal, e poderia manter esse atrativo ativo na memória durante o intervalo em que o estímulo está sendo percebido, e além disso, compatibiliza

da atenção do ator pode influenciar na maneira em que a nova informação é percebida. A implicação disso é que, saber o que está latente na mente do tomador de decisão ou do analista, pode ajudar-nos a predizer e compreender a análise ou a decisão. Jervis nota que é difícil para os tomadores de decisão reorientar a sua atenção sob o foco da nova informação.

Uma das características mais importantes dos modelos mentais é que eles tendem a ser criados muito rapidamente, mas são muito resistentes a mudanças (HEUER, 1999:10). Isso é percebido pela sabedoria popular como "a primeira impressão é a que fica". Uma vez que um observador formou uma imagem, isto é, uma vez que ele construiu uma parte do seu modelo mental ou expectativas sobre o fenômeno observado, isto condicionará futuras percepções do fenômeno. Tal observação nos leva a outro princípio geral da percepção: as novas informações são assimiladas às imagens e crenças existentes.

Segundo Heuer (1999:11), isso explica por que mudanças graduais geralmente passam despercebidas. Para o autor, isso também explica o fenômeno de analistas de inteligência designados a trabalhar em determinado tópico ou país pela primeira vez, que geram *insights* acurados, até então despercebidos por analistas experientes que trabalham no mesmo problema há bastante tempo. Essa tendência a assimilar novos dados em modelos preexistentes é maior quanto mais ambígua for a informação, quanto mais confiante estiver o ator na validade do seu modelo e quanto maior for o comprometimento pessoal com esta perspectiva preestabelecida (JERVIS, 1968).[8]

10.6. Teoria dos Esquemas e Analogias Interpretativas

Essa tendência da mente humana a receber toda a nova informação em determinada estrutura nos leva aos esquemas. A Teoria do "Esquema" trata os seres humanos como categorizadores e rotuladores. Para lidar com o excesso de informações, nós nos engajamos em processos de economia mental. Mais do que tratar cada pedaço de nova informação *sui generis* ou no seu próprio mérito, nós assimilamos o conhecimento em categorias preexistentes (normalmente conhecidos como "esquemas" ou *scripts)*. Isso é eficiente cognitivamente, e relativamente fácil de ser feito (HOUGHTON, 2009:121).

---

o estímulo a determinada tarefa ou ação a ser tomada. Assim, quando o mesmo estímulo visual reaparece, o córtex inferior temporal modular mostra uma grande resposta ao estímulo porque ele está sendo ativado tanto pela percepção do estímulo quanto pela consistência da retroprojeção da memória do mesmo estímulo (ROLLS, 2008:511).

[8] Segundo Jervis, alguns acadêmicos e políticos são adaptados ao erro por serem muito apegados às suas visões estabelecidas e muito fechados para novas informações, sendo uma proteção aos custos de se alterar suas teorias (1968: 189).

O termo "esquema" é geralmente usado mais displicentemente do que se deveria, e tem recebido uma grande variedade de definições. Definimos aqui um "esquema" essencialmente como um tipo de estereótipo guardado em nossa memória que fornece informações nos traços típicos de um objeto, evento ou pessoa. Eles seriam a conjugação das crenças e das imagens, entretanto, são mais definidos e estruturados em nossas mentes que os modelos mentais.[9] Dessa forma, os esquemas são mais fáceis de serem reconhecidos que os modelos mentais.

Esquemas são coleções genéricas de conhecimento: conceitos gerais, regras, lições etc. Eles vão além de qualquer caso percebido para fornecer informações do que normalmente ocorre, portanto, nós usamos os esquemas tanto para categorizar uma nova informação quanto para fazer inferências que vão além da informação dada. Podemos pensar o esquema como uma caixa mental contendo valores padrões típicos associados com algo que nos é familiar (HOUGHTON, 2009:121), facilitando o processamento de informações ambíguas.

Esquemas são um importante conceito em análise de inteligência porque é sabido que o impacto das informações prévias é profundo e afeta as decisões em todos os níveis de análise (MINTZ & DeROUEN, 2010:102). O fato é que esquemas são mecanismos de economia mental que podem nos enganar em algumas ocasiões, e na política isso pode trazer sérias consequências (HOUGHTON, 2009:122). Para a política externa, é relevante reconhecer isto, pois os tomadores de decisões quase sempre lidam informação incompleta sobre determinada situação. Atores políticos podem e fazem inferências incorretas situando indivíduos e eventos dentro das categorias erradas ou esquemas baseados em similaridades puramente superficiais (HOUGHTON, 2009:122).

O uso de esquemas históricos é muito comum na política internacional. O *Esquema de Munich*, por exemplo, conta-nos a história do que acontece quando um líder expansionista é apaziguado, sugerindo que se a ameaça não for enfrentada logo, certamente terá que ser encarada mais tarde. A Primeira Guerra Mundial teve um efeito devastador na Europa, e o Primeiro Ministro Neville

[9] É importante apontar que o conceito que estamos utilizando aqui de "modelo mental" não advém da Teoria da Consistência Cognitiva. O conceito de "modelo mental" é uma inferência particular da literatura analisada. É relevante sublinhar esta consideração, pois tanto a Teoria da Consistência Cognitiva quanto do Esquema concordam que crenças centrais são relativamente estruturadas, embora eles sejam diferentes no nível de coerência e interconectividade com outras crenças. A literatura da Consistência Cognitiva enfatiza que os indivíduos adquirem conceitos e imagens que são interconectados e formam coerentes sistemas de crenças. A literatura na Teoria da Cognição Social e na Teoria do Esquema descreve as estruturas cognitivas dentro da mente dos indivíduos como sendo de grande complexidade e embaralhadas. Dessa perspectiva, as crenças das pessoas tendem a ser menos coerentes, menos conectadas e mais contraditórias do que originalmente concebidas pela Teoria da Consistência Cognitiva (ROSATI, 1995: 61). Entretanto, aqui supomos que o conceito de modelo mental considera uma "mente humana" ainda mais abrangente e complexa do que aquela da Teoria do Esquema.

Chamberlain não surpreendentemente queria evitar outra guerra. Em 1938, na conferência de paz ocorrida em Munique, Hitler concordou em restringir as suas ambições em troca do que, na época, era a Tchecoslováquia. Chamberlain, em seu famoso ato, saiu da conferência brandindo o acordo e afirmando que havia sido alcançada e garantida a "paz nos nossos tempos". Essa política certamente foi um erro terrível, e a palavra "apaziguamento" tornou-se amaldiçoada nas relações internacionais, ruindo carreiras políticas daqueles que a advogaram (HOUGHTON, 2009:125). Esse esquema foi evocado em diversas ocasiões durante a Guerra Fria, e mais recentemente por George Bush depois de Saddam Hussein invadir o Kuwait em 1990. Bush argumentou que se as agressões de Saddam não fossem confrontadas logo – de fato, se Saddam fosse "apaziguado" – o resto do Oriente Médio brevemente cairia sob seus desejos expansionistas (HOUGHTON, 2009:125).

Dentro dos esquemas mentais, encontra-se o processo de raciocínio análogo. Geralmente, nossa mente busca criar analogias como um "atalho" cognitivo. Uma analogia não é simplesmente o diagnóstico de que alguma coisa é como outra; é, sim, uma comparação na qual o sujeito assume que as similaridades percebidas são estruturais (ou de causalidade significativa), e não apenas semelhanças meramente superficiais. Na prática, os indivíduos geralmente criam analogias entre objetos e eventos que exibem somente uma similaridade superficial (HOUGHTON, 2009:127).

O primeiro cientista político que refletiu extensivamente sobre o uso de analogias no processo de decisão em política externa foi Robert Jervis em *Perception and Misperception in International Politics*. A análise do autor foca-se na origem do raciocínio análogo do tomador de decisão em suas experiências passadas, demonstrando como analogias podem levar o indivíduo a falhar na percepção de características da situação e chegar a escolhas políticas que não são adequadas à situação em questão (MINTZ & DeROUEN, 2010:127).

Um importante estudo de caso sobre analogias históricas no processo de decisão foi feito por Khong. O autor demonstra como decisões feitas sobre a condução da Guerra do Vietnã em 1965 foram influenciadas pelas analogias do conflito coreano: a situação e a natureza do que estava em jogo foi definida como sendo similar, a resposta dos adversários sobre as possíveis ações dos EUA foi antecipada como sendo similares, e as políticas que foram bem-sucedidas na Coreia foram avaliadas como favoráveis no contexto do Vietnã, enquanto aquelas que falharam na Coreia foram ignoradas. O que é particularmente interessante é a habilidade de Khong em mostrar como estratégias diplomáticas e de combate específicas do Vietnã foram avaliadas no contexto da analogia coreana (SHIMKO, 1995: 71).[10]

[10] Para saber mais sobre os estudos das analogias e metáforas em política externa, ver o artigo "Foreing Policy Metaphors: Falling Dominoes and Drug Wars", de Keith L. Shimko (1995).

Considerando a tendência de se reconhecer o mundo através de esquemas mentais e a resistência em modificá-los, um dos exercícios mentais mais difíceis é tomar uma estrutura de informações e reorganizá-la visual ou mentalmente para percebê-la de diferentes perspectivas. Por exemplo, considere a figura abaixo e busque identificar as duas representações presentes no desenho. Após consegui-lo, tente mudar rapidamente a visualização de uma figura para a outra. Nós percebemos que existe grande dificuldade mental inicial para fazê-lo:

Figura 3

It is difficult to look at the same information from different perspectives.

Fonte: HEUER, 1999:12[11]

Entretanto, os analistas de inteligência e tomadores de decisão são constantemente requisitados a fazer isso. Para compreender as interações internacionais, os analistas precisam entender a situação como ela aparece para cada uma das forças opositoras, e mudar constantemente entre uma perspectiva e outra para sondar como cada lado interpretará uma série de eventos interligados (HEUER, 1999:13). Todavia, a dificuldade é que uma vez que o evento foi percebido de uma forma, é natural a resistência para que ele seja percebido sobre outra perspectiva.

[11] O nariz da senhora, a boca e os olhos são, respectivamente, o pescoço, o colar e a orelha da mulher mais nova. A velha senhora é vista de perfil olhando para a esquerda. A mulher mais nova também está olhando para a esquerda, mas nós a vemos principalmente de costas, por isso, muitos de seus traços faciais não são visíveis.

10.7. Espelhamento de Imagem na Análise de Inteligência

Essa tendência pode ser vista como uma das explicações para o fenômeno de espelhamento de imagem. Espelhamento de Imagem (*Mirror Imaging)* é a projeção do modelo mental, esquema ou sistemas de crenças de uma pessoa na outra.[12] Baseia-se em completar lacunas nas informações ou conhecimentos do indivíduo assumindo que o outro irá se comportar como ele mesmo se comportaria em determinada circunstância. O processo do pensamento do analista ou do tomador de decisão é basicamente "se eu fosse um oficial de inteligência colombiano..." ou "se eu estivesse comandando o governo argentino, eu...". É frequentemente o produto de conhecimentos insuficientes sobre as preferências culturais, étnicas, religiosas e políticas do adversário (JERVIS, 1976). A falha em compreender que o outro percebe os seus interesses nacionais diferentemente da maneira como entendemos aqueles mesmos interesses é uma constante fonte de problemas de análise na área de inteligência (HEUER, 1999: 81). Em muitos casos, falhas de inteligência foram causadas pela tendência de cair no espelhamento de imagem, e, através dessa maneira de raciocinar, supor ao adversário uma tendência de aversão ou propensão a riscos (BAR-JOSEPH, 2008:129).

Aversão a risco é a relutância que alguma pessoa tem em aceitar a barganha com um *payoff* incerto no lugar de outra barganha com um *payoff* mais garantido, mas provavelmente mais baixo. Na categoria de falhas de inteligência, essa combinação pode levar tanto a uma superestimação quanto a uma subestimação da tendência do adversário a tomar riscos. Se superestimada a tomada de riscos, isso pode levar a perda de oportunidades, assim como gasto de dinheiro em defesas desnecessárias. Quando subestimada, pela crença do analista de que o oponente irá evitar um ataque ou outro movimento agressivo, pois os custos seriam considerados altos demais, é a maior causa das falhas de inteligência em alertar contra uma possível ameaça (BAR-JOSEPH, 2008:129).

O espelhamento de imagem pode ser necessário quando os analistas ou tomadores de decisão realmente não sabem o que o adversário está pensando. O problema é que geralmente esse modelo mental é utilizado inconscientemente.

---

[12] É importante chamar a atenção para a diferença entre dois conceitos diferentes, mas que podem causar confusão por causa da sua proximidade lexical: o espelhamento de imagem (*Mirror Imaging*) e Imagem Espelhada (*Mirror Images*). O conceito de imagem espelhada refere-se a quando cada líder de estado mantém uma imagem diametralmente "oposta" do outro: cada parte tem uma auto-imagem positiva e benevolente, enquanto mantém uma imagem negativa e malevolente do inimigo. Ralph White (1968 apud Rosati, 1995:55-56) popularizou esse conceito no livro *Nobody Wanted War*: Misperception in Vietnam and Other Wars. Analisando as duas grandes guerras e focando-se na Guerra do Vietnã, White discute como cada parte no conflito mantinha uma imagem diabólica do inimigo e uma autoimagem viril e moral que se tornou fonte de atenção seletiva, ausência de empatia (pelo outro) e sobreconfiança militar. Ainda que resultado de diversas fontes sociais e psicológicas, tal pensamento "preto e branco" leva a escaladas na guerra (ROSATI, 1995:56).

O espelhamento de imagem pode levar a suposições perigosas, porque outras pessoas, principalmente de outras culturas, não pensam da mesma maneira que nós. Essas frequentes suposições são o que David Jeremiah, após rever a falha da inteligência norte-americana em prever os testes nucleares indianos, chamou de "modelo mental todos pensam como nós" (*everybody-think-like-us mind-set)* (HEUER, 1999:80).

O Comitê do Senado das Forças Armadas dos EUA (Senate Armed Services Committee*)* culpou a falha de não antecipar a instalação de mísseis nucleares soviéticos em Cuba em 1962 aos preconceitos da inteligência norte-americana sobre o comportamento soviético (BUTTERFIELD, 1993:5). Existiam duas suposições básicas para compreender as decisões de Khrushchev em 1962: se por um lado a União Soviética raramente havia agido de maneira ousada ou tomado grandes riscos de confrontação direta, por outro, parecia óbvio aos analistas americanos que provocar os EUA iria levar os dois países ao limite do confronto, pois os EUA pensavam que se fizessem o mesmo, este seria o resultado. A Estimativa Nacional Especial de Inteligência, lançada um mês antes dos mísseis serem descobertos, baseava-se em indicadores derivados da política externa soviética precedente (BETTS, 2008:58). Dessa forma, eles atribuíram a causa dos grandes movimentos de navios soviéticos que atracavam nos portos cubanos ao apoio soviético à agricultura de Cuba, ou até mesmo consideravam a possibilidade de serem mísseis táticos de curto e médio alcance. Portanto, os analistas norte-americanos, baseados na suposição de que os soviéticos agiriam da mesma forma que eles quanto às considerações de emprego de armas nucleares, subestimaram a propensão de tomada de riscos da URSS, não conseguindo prever a instalação de mísseis nucleares em Cuba.[13]

[13] Sobre a crise dos mísseis de 1962, existe um estudo central para o desenvolvimento da análise cognitiva e tomada de decisões na política externa feito por Alisson. Alisson proveu três mapas ou, nas suas palavras, três tipos de lentes conceituais para analisar a mesma crise de política externa. O primeiro modelo se fixa na premissa do ator racional e nos princípios do realismo básico. O segundo aborda o processo organizacional e o quanto os caminhos do processo decisório (as instâncias que a informação percorre, os empecilhos burocráticos e o tempo demandado) influenciam nos *outputs* em política externa. Finalmente, o último modelo é relativo ao impacto das políticas internas ao governo, o que ele chamou de "política da burocracia" (*bureaucratic politics*). Ou seja, nesse modelo não existe um "interesse nacional" dado, e sim a interação de atores dentro do processo decisório que conhecem relativamente bem os interesses, as crenças e as percepções dos seus colegas, sendo a política externa um resultado da interação do interesse desses atores (Ripley, 1995:85-90). É importante notar aqui que, em termos analíticos, o último modelo tende a ser, como já o está sendo, cada vez mais descartado como uma ferramenta eficaz, dada a subjetividade da abordagem e da escassez de informações confiáveis quanto ao real jogo interno das burocracias governamentais, resultado da dinâmica veloz e dos interesses ocultos nesse processo.

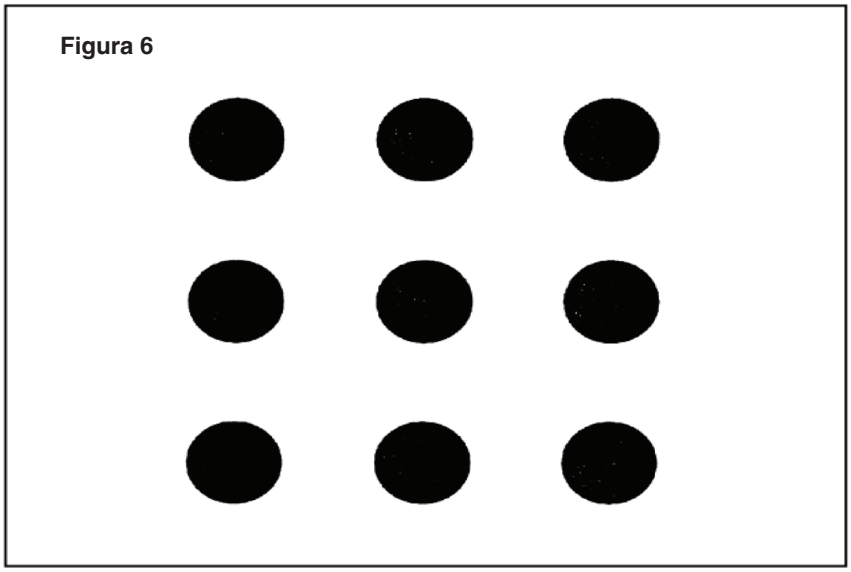
10.8. Fechamento Cognitivo Prematuro

Na sua obra *Hypotheses on Misperception (*JERVIS, 1968*)*, o autor estabelece 14 hipóteses sobre percepções e falsas percepções, que vão desde a tendência dos atores a perceber os outros estados mais hostis do que eles realmente são até a capacidade facilitada de um ator aceitar uma nova informação que vá contra as suas crenças iniciais quando esta é passada para ele aos poucos, e não de uma vez só. A preocupação de Jervis recai sobre os perigos de um "fechamento cognitivo prematuro", quando o decisor não percebe a influência do mecanismo de filtragem (HERZ, 1994:78).

O fechamento cognitivo prematuro é um dos maiores desafios para os analistas de inteligência e tomadores de decisão, pois ele impacta diretamente na capacidade do indivíduo de manter a "mente aberta" a hipóteses não imaginadas.[14] O fechamento cognitivo também deduz uma série de regras de pensamento, hipóteses e comportamentos a determinada situação que não necessariamente é real, só existe na mente do indivíduo. Por exemplo, tente ligar os nove pontos da figura adiante com quatro traços sem retirar o lápis ou a caneta do papel:

[14] A necessidade de fechamento cognitivo envolve o desejo de atingir um julgamento confiante sobre um assunto rápida e decisivamente, no lugar de lenta e cuidadosamente. O grau da necessidade de fechamento cognitivo apontará se este foi prematuro ou não. Quanto maior a necessidade de fechamento cognitivo, maior a probabilidade de ele ocorrer prematuramente. Essa motivação pode vir de duas formas: primeiro, o "aprisionamento" refere-se à necessidade de atingir o fechamento o mais rápido possível; o segundo, o "congelamento", indica o desejo de manter este fechamento o mais perene no tempo possível, normalmente bem depois de resultados objetivos terem demonstrado a invalidez daquela posição. A necessidade para fechamento pode melhorar a previsibilidade e o planejamento; assim, em situações com pressões de tempo tendem a aumentar este desejo. Também pode causar a indivíduos em perseverar em um caminho incorreto muito além do ponto em que correções óbvias deveriam ser requeridas (BAR-JOSEPH, 2008:139). Indivíduos com alta necessidade de fechamento cognitivo se mantêm relutantes em considerar novas informações, especialmente que parecem contrariar as suas crenças preexistentes. A pessoa pode negar tal informação, ou reinterpretá-la de maneira a coincidir com seus pensamentos iniciais. Tais indivíduos frequentemente são ligados a valores como ordem, e mostram uma enfática falta de empatia com os sentimentos, crenças e posições contraditórias dos outros. Eles parecem confiantes ao ponto da arrogância e tornam-se intolerantes, até mesmo hostis, àqueles cuja opinião difere das deles. Eles geralmente demonstram um estilo autoritário de liderança e de tomada de decisão (BAR-JOSEPH, 2008:139). Claramente, um indivíduo com alto grau de fechamento cognitivo iria representar um pobre prospecto para uma posição sênior de inteligência porque eles iriam falhar em considerar informações suficientes antes de atingir uma decisão, que iria manter-se relativamente impenetrável a desafios e evidências empíricas a partir de então (BAR-JOSEPH, 2008:140).

Figura 6

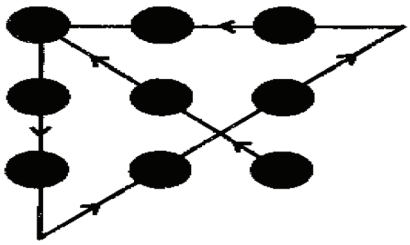


Fonte: HEUER, 1999: 131.

Geralmente, a dificuldade de executar esta tarefa relativamente simples encontra-se na nossa suposição de regras não existentes e não dadas por quem estabelece a tarefa. A partir disso, a tendência é estabelecermos a maioria das nossas hipóteses de resolução do problema dentro das regras que nós mesmos supomos estarem vigentes. Claro que este mecanismo cognitivo é útil em diversas situações, como quando existem restrições de tempo ou situações-limites; entretanto, é importante compreender o seu funcionamento, principalmente no caso dos analistas de inteligência, que têm como função "imaginar o inimaginável". A importância na vida real de entender essa engenharia mental é que, muitas vezes, em contextos sociais e políticos, as regras realmente estão subentendidas e todos os outros atores partem do pressuposto que todos irão entender essas regras sem precisar mencioná-las. Nesse caso, o importante é conseguir distinguir quando essas regras estão realmente subentendidas para todos ou quando só para nós mesmos, dentro dos nossos modelos mentais.

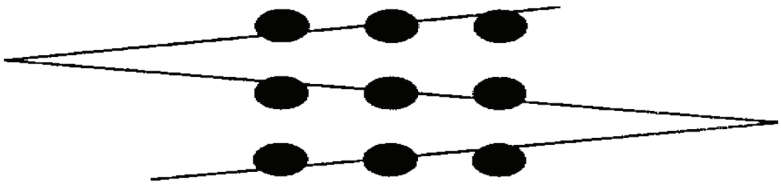
Os resultados desse teste são vários. A primeira resolução trata da possibilidade de imaginar pontos não existentes além do limite hipotético situado nos pontos dos cantos extremos que nós mesmos criamos. Um surpreendente número de pessoas limita-se a resolver o problema dentro do quadrado imaginário ao redor dos 9 pontos (HEUER, 1999:140):

Figura 7



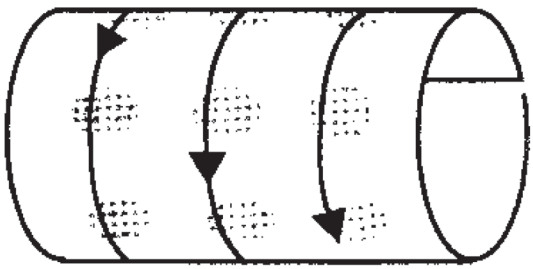
A segunda resolução aponta também para a tendência de supormos que necessitamos cruzar os pontos no seu centro, enquanto que essa regra não foi mencionada:

Figura 8



Por último, um constrangimento inconsciente, subentendido na maior parte dos modelos mentais das pessoas, dos mais difíceis de serem ultrapassados é a suposição de que precisamos resolver este problema bidimensionalmente. Se imaginarmos um contexto tridimensional, é possível passar pelos nove pontos com uma única reta diagonal em espiral:

Figura 9



É interessante notar que muitos psicólogos cognitivos afirmam que, depois do modelo mental ser criado, além de ser difícil mudá-lo, ele resiste até mesmo a informações que veementemente descredibilizam-o como verdadeiro.

A tendência a interpretar as novas informações no contexto de impressões preexistentes é relevante, mas não é o suficiente para explicar por que essas impressões não conseguem ser erradicadas mesmo quando a nova informação descredibiliza a evidência na qual é baseada. Uma interessante explicação, embora especulativa, é baseada na forte tendência em procurar explicações causais para os eventos (HEUER, 1999:125).

10.9. Sobre Explicações Causais, Ilusão de Controle e Atribuição de Culpa

A mente humana é resistente em aceitar que resultados podem ser determinados por forças aleatórias que interagem randomicamente e de modos imprevisíveis. Existe uma grande necessidade de encontrar padrões regulares, relações e ordens estabelecidas nos eventos e objetos que nos rodeiam. As pessoas geralmente não aceitam a noção de chance ou aleatoriedade. Como último recurso, as pessoas atribuem acontecimentos que não conseguem entender à vontade de Deus ou ao destino, que de certa forma são acontecimentos pré-ordenados (HEUER, 1999:129).

Por causa da necessidade de impor ordem no seu ambiente e executar algum controle sobre ele, as pessoas procuram e geralmente acreditam que acharam causas para o que era, na verdade, um fenômeno aleatório. Durante a Segunda Guerra Mundial, os londrinos criaram uma grande variedade de explicações causais para os padrões dos bombardeios alemães. Essas explicações frequentemente guiavam a sua decisão sobre onde ir morar e onde se refugiar. Exames no pós-Guerra, entretanto, determinaram que a aglomeração das bombas arremessadas estava muito próxima de uma distribuição randômica (HEUER, 1999:130). Os alemães presumidamente tinham um padrão a ser atingido, mas a mudança de propósitos e objetivos durante o tempo de guerra e o próprio sucesso ou não de se atingir o objetivo levaram a uma rede de resultados que mostrava um bombardeio quase aleatório.

A busca por explicações causais está ligada à esperança de que podemos executar algum controle sob o nosso ambiente. Para o caso dos analistas de inteligência, procurar explicações causais relaciona-se com a necessidade de encontrar coerência e ordem nos acontecimentos para criar uma narrativa concisa e compreensível. É importante perceber que o uso da coerência ao invés da observação científica como um critério de julgamento da "verdade" leva a vieses que presumidamente influenciam a todos os analistas em algum grau (HEUER, 1999:129). Entretanto, dado os constrangimentos da disponibilidade de informações e evidências, o princípio da lógica precisa ser aplicado, com a ressalva de que seja bem notificado.

No caso dos tomadores de decisão, a busca de explicações causais liga-se diretamente ao grau com que a sua necessidade de controle sobre a situação pesa sobre a decisão. Isso leva à chamada heurística da Ilusão de Controle, em que indivíduos tendem a sobre-estimar o seu grau de controle pessoal sobre os resultados. Dessa forma, Langer (1983 apud CABECINHAS, 1994: 6) apresenta estudos que mostram que sujeitos tomando uma variedade de decisões expressaram uma expectativa de sucesso pessoal maior do que a probabilidade objetiva poderia fundamentar. Portanto, tendemos a enviesar nossa percepção com informações, de acordo com o quanto elas confirmam ou descredibilizam as nossas hipóteses de controle do ambiente, aceitando a nova informação ou ingenuamente ignorando as evidências opostas. Provavelmente, essa tendência varia com o grau em que o indivíduo acredita ser capaz de controlar o ambiente. De certa forma, essa tendência é especialmente presente nos tomadores de decisão, dado que o ambiente da tomada de decisão é envolto em situações de estresse, estando o seu desenvolvimento relacionado à baixa percepção de controle do ambiente. Assim, os tomadores de decisão tendem a acreditar serem capazes de controlar significativamente o seu ambiente como uma forma de diminuir o seu próprio nível de stress.

Por causa do maior ou menor grau na confiança de que controlam o ambiente, segundo Jervis (1968:193), atores geralmente não percebem que ações pretendidas a projetar uma determinada imagem podem não ter o efeito desejado porque as ações por si sós não saem como o planejado. Os atores não atribuem a falha de determinada ação ou mensagem a sua incapacidade de controlar os eventos ou comunicar-se efetivamente, mas sim à capacidade do adversário em neutralizar a ação ou não compreender a mensagem.[15]

Indivíduos e governos raramente consideram a possibilidade de que suas próprias ações tenham tido consequências não intencionais. Eles assumem que as suas intenções foram corretamente percebidas e que as suas ações irão ter o efeito desejado se não forem frustradas por causas externas. Muitas pesquisas e experimentos já mostraram que as pessoas geralmente percebem as suas próprias ações como a causa de seu sucesso, mas não como de suas falhas. Candidatos vitoriosos ao Congresso dos EUA geralmente acreditam que seu próprio comportamento contribuiu fortemente para a sua vitória, enquanto os derrotados culpam a derrota a fatores além do seu controle (HEUER, 1999:139). Quando as ações de um país são consistentes com o desejo de outro, a explicação mais óbvia, na falta de fortes evidências do contrário, é que a política do país

[15] Jervis (1968:190) afirma que quando as pessoas gastam muito tempo criando um plano ou tomando uma decisão, elas tendem a pensar que a mensagem sobre aquilo que elas desejam transmitir está clara por si só para o recebedor, e não percebem que o modo como elas estão transmitindo a mensagem pode ter sido construído de maneira errada ou incompleta. Ou seja, o erro está no outro, e não em nós mesmos.

efetivamente influenciou a decisão. Entretanto, quando o outro país comporta-se de maneira indesejada, isto normalmente é atribuído a fatores externos à sua própria política. Isso nos leva a mais uma afirmação de Jervis (1968:192) sobre falsas percepções: quando nossos interlocutores agem da maneira que gostaríamos, tendemos a superestimar o grau em que isso é resposta a uma ação nossa. Mas quando o comportamento dos outros é indesejável, isto é usualmente visto como resultados de forças internas ao governo estrangeiro ou fatos externos a ele, e não uma falha de nossa abordagem.

Pessoas e governos também tendem a superestimar a sua própria importância como alvo da ação dos outros. Eles são sensíveis ao impacto que a ação dos outros tem sobre eles, e geralmente assumem que pessoas e governos tiveram a intenção de fazer o que fizeram e intentaram atingir o efeito que obtiveram. Eles são muito menos atentos, e consequentemente tendem a diminuir a importância de outras causas ou resultados da ação (HEUER, 1999:140). Por isso, há uma tendência geral dos decisores de ver os Estados mais hostis do que eles realmente são (JERVIS, 1968:194), ou até mesmo, mais benevolentes.

Jervis (1968:191) argumenta que a busca por explicações causais leva os atores a hesitar em admitir, ou até mesmo perceber, que incidentes particulares não podem ser compreendidos por suas teorias. Muitas pessoas não percebem acidentes, consequências não intencionais, coincidências, e pequenas causas levando a grandes efeitos. Ao invés disso, são vistas ações coordenadas, planos e, até mesmo, conspirações. Por causa disso, existe uma grande tendência entre os tomadores de decisão de ver as ações dos outros governos (ou grupos de qualquer tipo) como um resultado intencional de direção e planejamento centralizados.

Esse tipo de suposição leva a importantes consequências. Assumir que as ações de outro governo são resultados de um plano lógico e centralizado leva o analista e o tomador de decisão a: (i) ter expectativas quanto às ações do governo que podem não ser preenchidas, se o comportamento é o produto de mudanças ou inconsistências nos valores dos indivíduos, barganhas burocráticas, ou desvios de conduta resultantes de confusões ou erros; (ii) inferir conclusões de grande alcance, mas possivelmente não justificáveis, de discursos e pronunciamentos isolados ou ações de oficiais do governo que podem estar agindo sob sua própria vontade e não sob o comando de uma direção central; (iii) sobre-estimar a própria habilidade de influenciar as ações de outro governo; e, (iv) perceber inconsistências políticas como um resultado de duplicidade ou manobras maquiavélicas, ao invés de produto de fraca liderança, vacilações, ou barganha entre diversas burocracias e interesses políticos (HEUER, 1999:132).

Quando a análise sistemática de covariantes (variáveis que modificam uma a outra em mesma escala) não é factível, mas é possível encontrar uma série de

explicações causais alternativas, um padrão comum no julgamento das pessoas é considerar que causa e efeito possuem atributos similares. As propriedades da causa são inferidas a partir de correspondências com as propriedades do efeito. Quando se trata de objetos físicos, geralmente essas inferências gerais estão corretas: grandes animais deixam grandes pegadas, por exemplo. Entretanto, as pessoas tendem a assumir que esse modo de produzir inferências é válido em circunstâncias em que não o é. Analistas tendem a assumir que eventos econômicos têm causas primordialmente econômicas, que grandes eventos têm consequências importantes, e que pequenos eventos não podem afetar o curso da história (HEUER, 1999:133).

Conjugadas a tendência de se inferir planejamentos centralizados e racionais em todos os acontecimentos e a propensão a acreditar que o grau de impacto do efeito é igualmente relacionado à grandeza da causa, fica fácil explicar a persuasividade das teorias da conspiração. Tais teorias são evocadas, muitas vezes, para explicar grandes efeitos que, aparentemente, não têm grandes causas correspondentes. Por exemplo, parece ultrajante que uma única e fraca figura como Lee Harvey Oswald poderia alterar a história mundial. Como o suposto motivo do assassinato de John Kennedy era tão discrepante do efeito de sua morte, encontrar critérios coerentes para uma explicação narrativa se tornou complicado para a mente de muitos (HEUER, 1999:133).

10.10. Teoria da Atribuição

A busca por explicações causais dá origem nos estudos cognitivos à Teoria da Atribuição, que relaciona as causas do comportamento do indivíduo com a dicotomia entre determinantes internos e determinantes externos às ações humanas. Causas internas de comportamento, de natureza disposicional, incluem atitudes, crenças e a personalidade da pessoa. As causas externas estão nos incentivos e constrangimentos, requerimentos de função, pressões sociais, ou outras forças nas quais os indivíduos tenham pouco controle, ou seja, que sejam de natureza situacional. A teoria da atribuição vê os indivíduos como "cientistas ingênuos" ou solucionadores de problemas. Em vez de ser motivados constantemente a restabelecer a balança entre as suas crenças ou entre suas crenças e seus comportamentos, como afirma a teoria da consistência cognitiva, a teoria da atribuição sugere que os seres humanos estão preocupados em identificar as causas do seu próprio comportamento e dos outros (HOUGHTON, 2009:117).[16]

[16] A Teoria da Consistência Cognitiva tornou-se especialmente popular nos anos 1950 e 1960. Segundo esta teoria, quando as pessoas agem de forma contrária às suas próprias crenças, elas experienciam um estado de desconforto psicológico, tão longo quanto o desencontro entre comportamento e crenças durar. A suposição aqui é que as pessoas não gostam de agir de forma a violar suas próprias crenças, não gostam de manter crenças que são incompatíveis com outras, e

Um tipo de erro particularmente notável, com potenciais consequências políticas, é chamado de "erro fundamental da atribuição". Quando nós explicamos as nossas próprias ações, geralmente usamos atribuições situacionais, ou seja, julgamos que nossas ações são frutos de uma reação legítima ao meio, e geralmente superestimamos a importância da situação para o resultado de nossas ações. Por outro lado, quando explicamos porque outra pessoa está agindo de determinada forma, nós geralmente fazemos o oposto: nós subestimamos a relevância da situação (e assim superestimamos a importância das crenças e atribuições pessoais de disposição daquela pessoa na explicação do seu comportamento). Tomadores de decisão em política externa tendem a inferir que as ações de seus próprios Estados são compelidas pelas circunstâncias, enquanto eles atribuem o comportamento de outros Estados às características fundamentais das nações ou dos seus líderes. Aplicada à problemática de explicar as mudanças na orientação de política externa dos EUA para a União Soviética, a teoria da atribuição iria sugerir que os oficiais de Washington eram muito propensos a perceber motivações ideológicas e expansionistas nas ações soviéticas – que poderiam plausivelmente refletir cálculos de segurança similares àqueles que incentivaram políticas análogas executadas pelos EUA (HOUGHTON, 2009:118).

É interessante notar como a Teoria da Atribuição é consistente ao explicar a forma como os atores conectam relações causais aos comportamentos dos outros atores, quando eles não são os comportamentos desejados. Essa teoria sugere que, a invasão da URSS ao Afeganistão, no fim dos anos 1970, era entendida pelos líderes soviéticos como uma reação aos imperativos da situação no sul da Ásia daqueles tempos – como a ameaça de espraiamento do nacionalismo islâmico do Irã e do Afeganistão para dentro de URSS. Ainda, os líderes comunistas entendiam que a falha norte-americana em compreender os seus "legítimos" interesses nacionais era causada pela hostilidade fundamental dos EUA. Por outro lado, observadores norte-americanos da invasão provavelmente atribuíam tais ações à natureza agressiva e expansionista do regime soviético. Quanto maior a lacuna de informações sobre a situação, maior a propensão do indivíduo a tomar como disposicional o resultado do comportamento alheio.

---

evitam informações ou situações que façam com que tais incompatibilidades fiquem expostas. Leon Festinger chamou este desencontro de um estado de dissonância cognitiva. A teoria da consistência cognitiva gradualmente foi enfraquecida. Susan Fiske e Shelley Taylor oferecem algumas razões: a teoria da consistência parou de dominar o campo. Ironicamente, quanto mais ela se proliferava, em parte porque as variantes no tema tornaram-se indistinguíveis. Ainda, era difícil predizer o que uma pessoa iria perceber como inconsistente, em que grau, e qual rota para resolver a inconsistência a pessoa viria a tomar. Finalmente, indivíduos geralmente toleram um alto grau de inconsistências, por isso a motivação de evitá-las – um princípio maior da teoria – começou a ser posta em xeque (HOUGHTON, 2009:117).

Entretanto, quando o comportamento do adversário vai ao encontro do que o ator desejava inicialmente, ocorre a inversão da tendência da atribuição. O comportamento desejável faz com que o ator associe-o aos constrangimentos da situação, subestimando a disposição interna do outro ator a fazê-lo. Um exemplo é dado por Raymond Tanter (1980 apud HEUER, 1999:137-138, tradução livre), ao analisar as negociações de paz entre Egito e Israel em 1978-1979:

> Os Egípcios atribuíram sua vontade em assinar o acordo com Israel por causa da sua inerente disposição à paz; Israelenses a explicavam como resultado da deterioração econômica egípcia e do aumento da percepção da superioridade militar de Israel. Por outro lado, Israel atribuiu a sua própria orientação à paz como sendo sua preferência duradoura. O Egito, entretanto, explicava os comprometimentos israelenses relacionados com o Sinai, por exemplo, como resultado de pressões externas tal como persuasões positivas e ameaças de sanções negativas pelos EUA. Adicionalmente, alguns egípcios atribuíam o comportamento indesejado de Israel, tal qual o estabelecimento de assentamentos judeus no West Bank do Rio Jordão, como uma demonstração do expansionismo sionista. Se Israel não tivesse colocado os assentamentos naquele território, o Egito provavelmente iria avaliar aquele comportamento como resultado de pressões externas, já que o Ocidente não era a favor dos assentamentos. Israel, por outro lado, explica os comportamentos indesejáveis, tal como as ameaças egípcias de empurrá-los ao mar, a partir da oposição inerente do Egito à instalação de um estado judeu no Oriente Médio. Quando os egípcios pararam de fazer tais ameaças, Israel atribuiu este comportamento desejado à situação externa ao Egito, como a superioridade militar Israelense.

A persistência na tendência de atribuir causas e efeitos dessa maneira não é simplesmente a consequência de interesses próprios ou propaganda dos lados opostos. Mais que isso, pode ser compreendida e prevista pela maneira como as pessoas normalmente atribuem causalidades sob diferentes circunstâncias. Como regra geral, os enviesamentos de atribuição de causalidade auxiliam a plantar o desentendimento e a desconfiança entre povos e governos (HEUER,1999:138).

Até aqui, vimos como nossa mente trabalha sob a forma de modelos mentais que agem, na maior parte das vezes, no subconsciente dos indivíduos. Analisamos os esquemas mentais (imagens e crenças) como padrões que estão fixos e presentes no subconsciente de nossas mentes, agindo constantemente. Entretanto, supomos, a partir de abordagens neurocientíficas, que esses esquemas mentais não são acessados a todo momento. São as emoções do indivíduo, guiadas por liberações hormonais e correntes elétricas cerebrais, que o levam a acessá-los. Esse processo também ocorre no sentido inverso de maneira um pouco diferente, em que o reconhecimento de padrões de esquemas mentais pela percepção do indivíduo faz com que as emoções sejam despertadas, fortalecendo a presença daquele esquema mental na mente do indivíduo, ainda que subconscientemente. É como se os nossos esquemas mentais estivessem sempre *online,* mas o material completo do esquema só é acessado quando

recebe o estímulo de uma emoção. Por isso, é importante estudarmos as emoções para compreender mais sobre o processamento de informações na nossa mente.

Muitos fenômenos em análises políticas, econômicas e de segurança envolvem emoções e sentimentos, para além de um tipo "frio" de processamento de informação. Virtualmente todos os conceitos políticos são carregados de emoções, tanto positivas quanto negativas, algo que muitos psicólogos definem como "cognição quente". Estímulos políticos geralmente provocam emoções fortes; sentimentos como apreço, desprezo, felicidade, tristeza, raiva, culpa, gratidão, desagrado, vingança, prazer, insegurança, medo, ansiedade, e assim por diante. Nós não olhamos para política de forma neutra, como faria algum tipo de inteligência artificial computadorizada superavançada (HOUGHTON, 2009:132). Assim, a próxima seção abordará o papel das emoções na tomada de decisão e no processo de análise de inteligência.

10.10.1 Emoções e neurociência na tomada de decisão e análise de informações

As emoções são imprescindíveis na tomada de decisão – das mais simples, como decidir qual prato escolher no restaurante, às mais complexas, como aceitar ou não um convite para ir trabalhar em outra cidade. Elas são fundamentais também para a sociabilidade, além de organizar a forma como os dados e os acontecimentos são armazenados na memória. Além disso, cada vez mais pesquisas indicam que as emoções estão ligadas a mecanismos evolutivos essenciais à preservação da espécie.

Existe ampla evidência de que as emoções jogam um importante papel nas tomadas de decisão e na análise de informações na área de Inteligência Governamental. Líderes são influenciados pelas emoções da opinião pública, que, ao seu turno, são influenciadas por eventos domésticos e internacionais. As nações geralmente retaliam contra-ataques e provocações aos seus cidadãos e território – atos que evocam emoções e sentimentos como ódio, medo, raiva, desejo por vingança, insegurança, e assim por diante (MINTZ & DeROUEN, 2010:99).

Segundo Jon Elster (1989:89-90), um dos primeiros cientistas sociais a lidar com o tema das emoções, em 1940:

> As emoções importam porque nos comovem e perturbam, e porque através de suas ligações com as normas sociais estabilizam a vida social. Também interferem com nossos processos de pensamento, tornando-os menos racionais do que seriam de outra forma. E, particularmente, induzem expectativas irrealísticas a respeito do que podemos fazer ou realizar, e expectativas irrealísticas em relação à opinião das outras pessoas sobre nós próprios.

Emoções são conhecidas por influenciar como os indivíduos processam a informação e a importância que eles estimam a várias dimensões em situações carregadas emocionalmente *versus* situações neutras. Por exemplo, em março de 2002, mais de 130 civis israelenses foram mortos em ataques cometidos por grupos palestinos como o Hamas, a Jihad Islâmica, e a Al-Aqsa (o braço militar do Fatah). Esses ataques alcançaram o seu pico em 27 de março de 2002, com o que ficou conhecido como o Massacre da Páscoa, no qual um homem-bomba palestino matou trinta pessoas no Park Hotel em Netanya, Israel. A natureza simbólica do ataque – durante um feriado judeu, com pessoas rezando e celebrando – evocou profundas emoções de ódio e vingança contra os palestinos e deu legitimidade a Israel para iniciar a Operação Escudo Defensivo (*Operation Defensive Shield*) (MINTZ & DeROUEN, 2010:100).

Nehemia Geva, Steven Redd e Katrina Mosher (2004 apud MINTZ & DeROUEN, 2010:100) mostraram, através de métodos experimentais, que emoções afetam o modo como as pessoas processam informações e tomam decisões. Ódio, amor, medo, insegurança e confiança, todos produziram não somente diferentes escolhas a partir de emoções opostas, mas também variações na maneira como as pessoas chegaram àquela escolha (espontaneamente *vs* calculadamente; maximizadora vs satisfatória; intuitivamente *vs* racionalmente). De acordo com esses autores, emoções influenciam tanto o processo quanto os resultados da tomada de decisão em política externa.

Emoções podem afetar o processamento de informações de duas maneiras distintas. Em primeiro lugar, emoções afetam a capacidade cognitiva dos indivíduos, inicialmente estreitando o seu leque de escolhas, isto é, o número e tipo de opções que o tomador de decisão pode considerar. Adicionalmente, emoções podem diminuir os constrangimentos em selecionar um curso particular de ação pela redução prévia da quantidade de informações a ser processada em cada alternativa. Em segundo lugar, emoções podem ter um efeito temático no processo de tomada de decisão. Elas podem alterar ou modificar a relevância de uma nova informação durante uma decisão, modificando a informação e introduzindo uma forma de atenção seletiva (MINTZ & DeROUEN, 2010:100).

Por um longo tempo, as emoções foram tratadas como algo visceral, algo que se origina mais nas entranhas do que na mente. Este modo de pensar tem raízes antigas. Na tradição ocidental de pensamento político, ainda é muito comum contrastar "razão" e "emoção"; de um lado, está a razão, ordenada e lógica (algo a ser aspirado e admirado), e, do outro lado, estão as emoções irracionais e impulsivas (algo a ser evitado). Isto é implícito na distinção de Freud entre o Id e o Superego, por exemplo. Nós somos acostumados a pensar nas emoções como algo que prejudica a tomada de decisão informada e factualmente baseada (HOUGHTON, 2009:135).

Entretanto, emoções não são necessariamente algo que deveria ser rotulado como prejudicial, argumenta Stephen Pinker (1997). Combinando a abordagem cognitiva moderna com evolucionismo darwinista, Pinker defende que nós temos emoções porque elas se provaram úteis na propagação da espécie. Nós sentimos amor e solidariedade àqueles próximos a nós, por exemplo, porque somos motivados a garantir a sobrevivência dos nossos genes. O autor dá outro exemplo sobre o medo, que é disparado por um sinal para impedir danos – como um predador, o alto de um penhasco, ou uma ameaça verbal. Isto lança objetivos de curto prazo como fugir, render-se ou reagir ao perigo, dando-lhe alta prioridade, a qual experienciamos como um sentimento de urgência. Até mesmo a tristeza poderia ser vista como auxiliar a uma boa tomada de decisão, pois ela avisa o indivíduo que o momento atual não é oportuno para adquirir bons resultados, levando-o a uma retração que o faz economizar energia, analisar a situação e reestruturar estratégias.

Algumas culturas são geralmente associadas como mais emocionais do que outras – o estereótipo comum do "sangue quente Latino" e do "alemão frio" são exemplos disso – mas Pinker argumenta que as culturas variam somente na forma como seus membros demonstram as emoções, não na extensão na qual eles as sentem. Nós somos pré-programados pela evolução para sentir essencialmente as mesmas emoções. Claro que não sentimos as mesmas emoções como respostas ao mesmo evento, mas desenvolvemos a mesma capacidade de sentir um leque muito similar de diferentes emoções (HOUGHTON, 2009:136).

10.11. Teoria da Inteligência Afetiva e Teoria do Raciocínio Motivado

Duas interessantes teorias foram desenvolvidas para abordar a forma como as emoções influenciam o processamento de informações: a Teoria da Inteligência Afetiva e a Teoria do Raciocínio Motivado. Na primeira, construída através de *insights* da neurociência, George Marcus e seus colegas explicitamente rejeitaram a visão popular de que precisamos primeiro "pensar" para que depois possamos "sentir". Eles distinguem dois sistemas, o de disposição e o de vigilância. O primeiro lida com informações rotineiras, avaliando as informações de acordo com as emoções que um estímulo particular evoca: por exemplo, determinado estímulo pode provocar entusiasmo ou aversão. Enquanto o primeiro mecanismo lida com modos comuns e habituais de pensar, o segundo lida com estímulos novos e inesperados. A emoção dominante nesse segundo sistema é a ansiedade. Uma vez acionado por algo inesperado (leia-se perigoso), o sistema de vigilância aumenta a atenção e prepara-nos para responder aumentando os níveis de "ansiedade". Esse processo não é dirigido por um processo cognitivo do ambiente, mas por uma resposta emocional de um estímulo inesperado. Nesse estado, o

aprendizado é acelerado, pois o indivíduo precisa compreender a natureza de qualquer ameaça em que ele se encontra e, assim, fica motivado a descobrir mais sobre o estímulo. Nós estamos alertas para atender ao estímulo mais centradamente e menos propensos a pensamentos habituais. Dessa maneira, o sistema de vigilância promove um pensamento mais "racional" (HOUGHTON, 2009:137-138).

A partir da Teoria do Raciocínio Motivado, Milton Lodge e Charles Taber foram pioneiros em desenvolver uma abordagem diferente para compreender como as emoções afetam a política. Apesar de concordar com Marcus e seus colegas que a emoção devia ser considerada antes da cognição "fria", eles abordam esse tópico de maneira um pouco diferenciada. Eles assumem três suposições: (1) todos os estímulos políticos são carregados emocionalmente (a hipótese da cognição "quente"); (2) as pessoas mantêm em suas mentes um "registro" ligado e frequentemente atualizado que inclui seus sentimentos sobre esses estímulos; e, (3) a maneira como a pessoa "sente" geralmente afeta a recepção do próprio estímulo. A expectativa é que a maioria das pessoas, se não todas, são racionalistas enviesados, pelos quais é quase impossível avaliar uma nova informação de maneira imparcial (HOUGHTON, 2009:138).

Essas duas perspectivas podem não ser inteiramente complementares. Em particular, elas implicitamente discordam a respeito da seguinte questão: em face de uma nova ou inesperada situação é provável que iremos tomar uma decisão "melhor" ou "pior"? Sob o modelo de Marcus, mecanismos evolucionários nos levaram a possuir a habilidade de agir instantaneamente, antes que o processamento cognitivo "frio" iniciasse. É esperado que isso melhore, e não que prejudique, a tomada de decisão. Na abordagem de Lodge e Taber, por outro lado, emoções enviesam a interpretação de novas informações. Lodge e seus colegas acreditam que as pessoas são propensas a lutar para apoiar as suas crenças anteriores, permitindo assim que as emoções interfiram na atualização do seu "registro". Portanto, a primeira abordagem enfatiza a forma como as emoções nos ajudam a aprender, enquanto a segunda sublinha o modo como os sentimentos enviesam e distorcem o processo cognitivo (HOUGHTON, 2009:139).

10.12. Emoções e Neurociência no Processamento de Informações

Uma razão para não tratar as emoções como necessariamente prejudiciais ao processo racional é que elas podem ativamente auxiliar na formação de uma "boa" tomada de decisão, e podem até mesmo serem julgadas essenciais para tal. Para tomar decisões bem consideradas, primeiro precisamos nos importar sobre os resultados daquela decisão. Esta conclusão tem grande suporte no trabalho do neurocientista Antonio Damasio e seus colegas. Damasio

descobriu que pacientes que tinham danificado o seu córtex pré-frontal – a área do cérebro que controla as respostas emocionais – geralmente tomavam decisões descuidadas, mesmo quando eles tinham demonstrado extensas capacidades intelectuais. Isso aconteceria, segundo ele, pois as emoções (como o medo) existem para prevenir os indivíduos normais de agirem de formas que prejudicariam suas vidas sociais e profissionais. Eles fariam más decisões porque não teriam mais a capacidade de se importar com uma decisão ou outra (HOUGHTON, 2009:136).

Esse argumento está largamente baseado no que acontece quando o indivíduo danifica a área do córtex pré-frontal ventromedial e o seu redor, a região do cérebro que integra a emoção com a razão. Damasio (apud HOUGHTON, 2009:148) começa o seu livro *Descartes' Error* (título que alude ao suposto erro do filósofo francês René Descartes ao tratar razão e emoção como fatores separados e antagônicos em nosso cérebro) contando a famosa história de Phineas Gage, personagem do mais notório e bem documentado caso de que as emoções têm base física no cérebro e são imprescindíveis para o exercício da razão. Gage era um construtor ferroviário que se envolveu em um acidente potencialmente fatal em 1848, quando uma explosão em seu local de trabalho derrubou uma barra de ferro na sua cabeça. Tão forte foi a explosão que fez a barra atravessar o topo de sua cabeça. Para a surpresa dos seus colegas e de seu médico, Gage não só sobreviveu, como pareceu sofrer danos mínimos nas suas funções mentais, até mesmo relatando o incidente calma e racionalmente logo após o ocorrido.

Phineas Gage parecia conduzir uma ótima recuperação, ao menos no sentido físico. Aqueles que o conheciam noticiaram mudanças em sua personalidade, contudo. Gage não era mais o mesmo Gage. Esse "novo" Gage havia passado de religioso a profanador, era impaciente com os outros e poderia debater ideias incansavelmente e desistir delas rapidamente, diferentemente do que fazia anteriormente. Não conseguia mais manter-se em um trabalho e parecia ter perdido todo o interesse em convenções sociais e regras éticas. Ele começou a fazer más escolhas em sua vida, outra mudança marcante em relação a seu comportamento anterior. Por que isso aconteceu? Utilizando-se de avançadas técnicas de imagens do crânio de Gage, para reconstruir a imagem do seu cérebro, Damasio argumenta que Gage sofreu severos danos no córtex pré-frontal ventromedial, uma área crítica para a tomada de decisão regular. Assim, Gage teria perdido a capacidade de antecipar o futuro e de elaborar planos de acordo com essa antecipação em um ambiente social complexo. Demonstrando uma série de casos similares, Damasio mostra que as partes "emocionais" do cérebro são essenciais para tomar decisões racionais, desmistificando a velha suposição de que emoção e razão são atributos separados ou rotas que podem ser tomadas isoladas uma da outra (HOUGHTON, 2009:148).

Como relata o cientista político Jonathan Mercer (2005), as pessoas sem emoções podem saber que elas deveriam ser éticas, podem saber que elas deveriam seguir as normas, podem saber que elas não deveriam tomar decisões financeiramente desastrosas, mas esse conhecimento é abstrato e inerte e não pesa em suas decisões. Elas não se preocupam com os outros ou si mesmos, não tentam evitar seus erros e nem são capazes de "aprender" com eles. Como Pinker e Damasio, Mercer vê as emoções como essenciais, e não competidoras, para a racionalidade. Assim, percebemos que os estudos sobre os mecanismos neurais demonstram, ao menos parcialmente, as possíveis tendências quanto às disposições do indivíduo, às suas emoções e ao seu modo de processar informações.

10.13. Conclusão

A incerteza e a complexidade característica da coleta, análise, disseminação e ação na atividade de inteligência deixa os seus praticantes mais suscetíveis a desvios e erros na interpretação das informações. "As consequências de erros nessas operações podem variar desde a mera ineficiência no uso do dinheiro do contribuinte, até a perda de vidas pela falha em identificar e prevenir ataques terroristas" (KEBBEL & MULLER & MARTIN, 2010:95, tradução livre). Neste capítulo, procuramos demonstrar a parte do universo desses erros e desvios que se restringe aos vieses cognitivos e aos vieses relacionados à emoção.

A diminuição da probabilidade de ocorrência de vieses cognitivos é um esforço que tem reunido muitos especialistas em análise de inteligência, principalmente na comunidade de inteligência norte-americana. Tenta-se desenvolver métodos de análise que os neutralize, ou ao menos os restrinja a situações mínimas. A título de exemplo, algumas das técnicas incluem a análise de hipóteses competitivas, a checagem de suposições-chaves, a tomada de decisão estruturada, a análise de "*red teams*", a institucionalização do "advogado do diabo", Time A/Time B, *brain storm,* desenvolvimento de cenários a partir de Análise Estruturada, entre outros.

Todas essas técnicas encontram limites claros quanto ao sucesso de seu objetivo principal, isto é, de sempre produzir análises precisas, na medida em que os vieses cognitivos muitas vezes passam despercebidos até mesmo pelo controle revisor mais atento. Isso acontece porque os vieses cognitivos fazem parte do modo natural como os seres humanos processam informações. Além disso, as crescentes demandas dos sistemas de inteligência por análises cada vez mais apuradas em um curto espaço de tempo encontra limites de recursos e de tempo, o que pode aumentar as possibilidades de vieses cognitivos.

Mesmo assim, apesar dos desafios e limitações que desesperançam a capacidade de se evitar falhas nas análises de inteligência causadas por vieses

cognitivos, precisamos incorporar ao treinamento dos analistas e à cultura organizacional dos sistemas de inteligência a importância de estar atento às ciladas que nossa mente pode criar quando processamos informações. Para isso, o primeiro passo é a identificação e descrição dessas ciladas, etapa que procurou ser iniciada com este capítulo.

REFERÊNCIAS

AMBROS, Christiano. *Inteligência Governamental e Tomada de Decisão em Política Externa*: Aspectos Cognitivos e Modelos de Personalidade. Trabalho de Conclusão de Curso apresentado na Faculdade de Ciências Econômicas, Curso de Relações Internacionais, da Universidade Federal do Rio Grande do Sul. Disponível em: <http://www.fafich.ufmg.br/ceig/?screen=search&s=&all=1&pg=11&o=&d=d>.

BAR-JOSEPH, Uri e McDERMOTT, Rose. Change the Analyst and Not the System: A Different Approach to Intelligence Reform. *Foreign Policy Analysis* nº 4. 2008.

BETTS, Richard K. (2008) *Enemies of Intelligence*: Knowleadge and Power in America National Security. New York: Columbia University Press.

_____. (2009) Analysis, war, and decision: why intelligence failures are inevitable. In: GILL, Peter & MARRIN, Stephen & PHYTHIAN, Mark (Eds). *Intelligence Theory*: Key questions and debates. New York: Routledge.

_____. (2009). Surprise despite warning: Why sudden attacks succeed. IN: ANDREW, Christopher & ALDRICH, Richard & WARK, Wesley. *Secret Intelligence*: A Reader. New York: Routledge.

BRANDÃO, Priscila Carlos. (2002). *SNI & ABIN*: uma leitura da atuação dos serviços ao longo do século XX. Rio de Janeiro, Editora FGV.

BRUNEAU, Thomas & BORAZ, Steven [Eds.]. (2007). *Reforming Intelligence*: Obstacles to Democratic Control and Effectiveness. Austin-TX, University of Texas Press.

BUTTERFIELD, Alexander P. Jr. (1993). *The Accuracy of Intelligence Assessment*: Bias, Perception, Judgment in Analysis and Decision. Newport: Naval War College.

CABECINHAS, R. (1994). A perspectiva cognitiva sobre a decisão estratégica. *Cadernos do Noroeste*, vol. 7 (2), 19-37.

CEPIK, Marco & BRANDÃO, Priscila Carlos. (2003). The New Brazilian Intelligence System: An Institutional Assessment. *International Journal of Intelligence and Counter Intelligenc*e, Nova York - NY, v. 16, nº 2, p. 167-194.

_____. (2005). The Professionalization of Intelligence in Brazil: knowledge, career path, and values. In: SWENSON, Russell & LEMOZY, Susana [Eds.]. *Intelligence as a Profession in the Americas*: new approaches. Washington -D.C., JMIC Edition. Pages 109-154. 2nd edition.

CEPIK, Marco & BRUNEAU, Thomas. (2008). Brazilian National Approach Towards Intelligence: Concept, Institutions and Contemporary Challenges. In: GILL, Peter & FARSON, Stuart & PHYTHIAN, Mark & SHPIRO Shlomo [Eds.]. *Handbook of Global Security and Intelligence*: National Approaches. Vol 1 - The Americas and Asia. Washington, Praeger.

CEPIK, Marco. (2002). Inteligência e Políticas Públicas. *Security and Defense Studies Review*, 04.

_____. (2003). *Espionagem e Democracia*. Rio de Janeiro: FGV.

CLARK, Robert. *The Technical Collection of Intelligence*. Washington: CQ Press. 2011.

DAVIS, Jack. Combating Mind-Set. *Studies in Intelligence* 36, nº 5. 1992.

_____. A Policymaker's Perspective on Intelligence Analysis. *Studies in Intelligence* 38, nº 5. 1995.

_____. Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship. *Intelligence and National Security* 21, nº 6 . Dec. 2006.

ELSTER, Jon. (1940) *Peças e engrenagens das ciências sociais*. Edição brasileira de 1994. Rio de Janeiro: Relume-Dumará.

FARIA, Carlos Aurélio de Pimenta. & FILGUEIRAS, Cristina Almeida Cunha. As Políticas dos Sistemas de Avaliação da Educação Básica do Chile e do Brasil. In: HOSCHMAN, Gilberto & ARRETCHE, Marta & MARQUES, Eduardo [Org.]. (2007). *Políticas Públicas no Brasil*. Rio de Janeiro: Editora FIOCRUZ.

FARIA, Carlos Aurélio de Pimenta. A Política da Avaliação de Políticas Públicas. *RBCS*, vol. 20, nº 59, out. 2005.

GALLAGHER, Maryann. High Rolling Leaders: The "Big Five" Model of Personality and Risk-Taking during War. Working Paper apresentado na International Studies Association-South Conference. 2005.

GILL, Peter & FARSON, Stuart & PHYTHIAN, Mark & SHPIRO Shlomo [Eds.]. (2008). *Handbook of Global Security and Intelligence*: National Approaches. Washington, Praeger. ISBN: 0-275-99206-3. [Two volumes].

GILL, Peter & MARRIN, Stephen & PHYTHIAN, Mark (Eds). *Intelligence Theory: Key* questions and debates. New York: Routledge. 2009.

GILL, Peter & PHYTHIAN, Mark. Intelligence in an Insecure World. Cambridge: Polity Press. 2006.

GILL, Peter. Thinkig About Intelligence within, without and beyond the state. Paper apresentado no IPSA/ECPR 2011. Disponível em: <http://www.saopaulo2011.ipsa.org/sites/default/files/papers/paper-1248.pdf>.

GILOVICH, Thomas & GRIFFIN, Dale & KAHNEMAN, Daniel (Eds.). *Heuristics and Biases*: The Psychology of Intuitive Judgment. New York: Cambridge University Press. 2002.

HALL, Peter & TAYLOR, Rosemary. *Political Science and the three New Institucionalism*. Political Studies, Dec. 1996.

HALLINAN, Joseph T. *Por que Cometemos Erros*? São Paulo: Globo. 2010.

HERMAN, Michael. (1996). *Intelligence Power in Peace and War*. Cambridge-UK, Cambridge University Press.

HERZ, Monica. Análise Cognitiva e Política Externa. *CONTEXTO INTERNACIONAL*, Rio de Janeiro, vol. 16, nº 1, 1994, p. 75-89.

HEUER, Richard J. & PHERSON, Randolph H. *Structured Analytic Techniques for Intelligence Analysis*. Washington: CQ Press. 2011.

HEUER, Richard J. (1999) The Psychology of Intelligence Analysis. *Center for the Study of Intelligence*. Central Intelligence Agency.

HOUGHTON, David P. (2009) *Political Psychology*: Situations, Individuals and Cases. New York: Routledge.

JERVIS, Robert. Hypothesis on Misperception. *World Politics* 20 nº 3, 1968:189-203

_____. (2006) The Politics and Psychology of Intelligence and Intelligence Reform. *The Forum*, vol. 4: Iss. 1, Artigo 1.

_____. *Perceptions and Misperceptions in Intemational Politics*, New Jersey, Princeton University Press, 1976.

_____. *Why Intelligence Fails*: Lessons from the Iranian Revolution and Iraq War.New York: Cornell University Press. 2010.

JOHNSON, Loch & WIRTZ, James [Eds.]. (2004). *Strategic Intelligence*: windows into the secret world. Oxford, Oxford University Press.

JOHNSON, Loch [Ed.]. (2006). *Handbook of Intelligence Studies*. London, Routledge.

JOHNSON, Loch [Ed.]. (2006). Strategic Intelligence. Washington, Praeger. [Five Volumes, 1824 pages].

JOHNSON, Loch K. (2009). *Sketches for a theory of strategic intelligence*. In: GILL, Peter & MARRIN, Stephen & PHYTHIAN, Mark. *Intelligence Theory*: Key questions and debates. New York: Routledge.

JORDAN, Javier. (2011). Introduccion al analisis de inteligencia. Disponível em: <http://wdb.ugr.es/~gesyp/analisis-inteligencia>.

KAHN, David. (1995). Toward a Theory of Intelligence. *Military History Quarterly*. Vol. 07 n. 02. (Winter), p. 92-97.

KAHNEMAN, Daniel & TVERSKY, Amos (Eds.). *Choices, Values and Frames*. New York: Cambridge University Press. 2000

KEBBELL, Mark R. & MULLER Damon & MARTIN, Kirsty. Understanding and Managing Bias. In: BAMMER, Gabriele (Ed). *Dealing with uncertainties in policing serious crimes*. Canberra: ANU Press. 2010

KEMAN, Hans. Comparative Research Methods. In: CARAMANI, Daniele. *Comparative Politics*. Oxford: Oxford University Press, 2008.

LOWENTHAL, Mark. (2008), Towards a Reasonable Standard for Analysis: How Right, How Often on Wich Issues?, *Intelligence and National Security*, vol. 23, nº 3, (2008), p. 303-315.

MACDONALD, Matthew. (2010). *Mentes Poderosas*. São Paulo: Universo dos Livros.

MERCER, Jonathan. Rationality and Psychology in International Politics. *International Organization*, vol. 58, nº 1, 2005.

MINTZ, Alex & DeROUEN, Karl. (2010). *Understanding Foreign Policy Decision-Making*. New York: Cambridge University Press.

PHYTIAN, Mark. Intelligence Analysis Today and Tomorrow. *Security Challenges*, vol. 5, nº 1, 2009.

RIPLEY, Brian. Cognition, Culture and Bureaucratic Politics. In: NEACK, Laura (Ed.). *Foreign Policy Analysis*: Continuity and Change in its Second Generation. New Jersey: Prentice Hall. 1995.

ROLLS, Edmund T. (2008). Memory, Attention and Decision Making. Oxford: Osford University Press.

ROSATI, Jerel. A cognitive Approach to the Study of Foreign Policy. In: NEACK, Laura (Ed.). *Foreign Policy Analysis*: Continuity and Change in its Second Generation. New Jersey: Prentice Hall. 1995.

SHIMKO, Keith L. Foreign Policy Metaphors: Falling Dominoes and Drug Wars. In: NEACK, Laura (Ed.). *Foreign Policy Analysis*: Continuity and Change in its Second Generation. New Jersey: Prentice Hall. 1995.

SIMON, Herbert A. Rationality in Psychology and Economics. The Journal of Business, vol. 59, nº 4, 1986.

STERNBERG, Robert. *Psicologia Cognitiva*. São Paulo: Cengage Learning Press. 2010.

SWENSON, Russell & LEMOZY, Susana. [Eds.]. *Intelligence as a Profession in the Americas*: New Approaches. Washington, JMIC Edition, 2004. 2nd edition.

TREVERTON, Gregory. Intelligence Analysis: Between Politicization and Irrelevance. In: GEORGE, Roger Z. & BRUCE, James B. *Analyzing Intelligence*: Origins, Obstacles and Innovations. Washington: George University Press. 2008.

WALKER, Stephen. Quantum Politics and Operational Code Analysis: Theories and Methods. In: WALKER, Stephen & MALICI, Akan & SCHAFER, Mark. *Rethinking Foreign Policy Analysis*. New York: Routledge. 2011.

Capítulo 11

INTELIGÊNCIA E CIBERESPAÇO: DESAFIOS DO SÉCULO XXI

Jussara de Oliveira Machado

Em setembro de 2000, um grupo de adolescentes *hackers* israelenses atacou vários sites pertencentes ao Hezbollah, ao Hamas e à Autoridade Nacional Palestina, logo após a eclosão da segunda intifada,[1] dando início ao conflito cibernético entre israelenses e palestinos. Em resposta a esse ataque, "os palestinos e outras organizações islâmicas clamaram por uma guerra santa cibernética, também conhecida por ciber-Jihad ou e-Jihad,"[2] atacando os sites do Parlamento israelense (o Knesset), do Ministério do Exterior e da Força de Defesa de Israel. "Mais tarde, os *hackers* atacaram o Gabinete do Primeiro Ministro israelense, o Banco de Israel e a Bolsa de Valores de Tel Aviv" (ALLEN e DEMCHAK, 2004:51).

Em 27 de abril de 2007, a Estônia removeu um memorial de guerra russo do centro de Tallinn (capital do país) para um cemitério militar. Para os russos, a retirada da estátua significou um desrespeito aos soldados russos. [3] No mesmo dia, os principais web sites do governo da Estônia começaram a receber milhares de ataques distribuídos de negação de serviços (DDoS – Distributed Denial of

---

1 De acordo com o site The Intifada in Palestine, politicamente, a palavra intifada simboliza "o levante palestino contra a ocupação israelense" e "a fraqueza do povo palestino e o seu sofrimento perante a ocupação israelense". Disponível em: <http://www.intifada.com/palestine.html>. Acesso em: 15 mar. 2010. A segunda intifada significou a insurgência de várias ações de palestinos contra israelenses. "Em fevereiro de 2001 um grupo formado por dois palestinos e dois ativistas internacionais de direitos humanos pró-palestinos lançaram um site chamado Electronic Intifada, que é hoje um dos recursos eletrônicos mais seguidos no mundo sobre o conflito israelo-palestiniano" (JOKISIPILÄ, p. 3) Disponível em: <http://vanha.soc.utu.fi/polhist/vaihtuvat/jokisipila_Interfada.pdf>. Acesso em: 15 mar. 2010. O site da Intifada está disponível em: <http://www.intifada.com/>. Acesso em: 15 mar. 2010.

2 Para saber mais sobre a e-Jihad consulte também BUNT, 2003. Disponível em: <http://www.99chan.org/lit/src/Bunt_Islam_in_the_Digital_Age-E-Jihad_Online_Fatwa.pdf>. Acesso em: 15 mar. 2010.

3 *New York Times*. Disponível em: <http://www.nytimes.com/2007/04/28/world/europe/28estonia.html?_r=1>. Acesso em: 06 mar. 2010.

Service),[4] fazendo com que os sistemas operacionais entrassem em colapso. Logo em seguida, estações de televisão, jornais, escolas e bancos foram atacados. Em resposta, o governo estoniano teve de fechar uma grande parte da sua rede para pessoas que estivessem fora do país e acusou a Rússia de ter efetuado tais ataques. A autoria deles foi negada.[5]

Em 2006, quando começou a operar na China, a Google, uma das maiores empresas americanas que oferecem serviços *online* no mundo, se viu obrigada pelo governo chinês a censurar alguns resultados em suas ferramentas de busca. Em 12 de janeiro de 2010, entretanto, anunciou que iria parar de censurar as buscas em seu site chinês e considerou sua retirada do país, caso o governo chinês não concordasse com isso. Essa decisão foi tomada depois de perceber que atuações de *hackers* chineses tinham resultado não apenas em roubo de propriedade intelectual da empresa e ataques a outras empresas, mas também em tentativas de acesso a contas de *e-mail* de ativistas, dado que várias contas americanas, europeias e chinesas de defensores dos direitos humanos teriam sido rotineiramente acessadas por terceiros.[6]

Recentemente, o Centro de Estudos Estratégicos e Internacionais (CSIS – Center for Strategic & International Studies), em parceria com a fabricante de antivírus para computador McAfee, produziu um relatório, denominado *In the Crossfire: Critical Infrastructure in the Age of Cyber War*[7] (No Fogo Cruzado: As infraestruturas críticas na era da guerra cibernética), no qual foram entrevistados 600 diretores de segurança da informação de 14 países que atuam em "empresas de setores financeiro, energético, de recursos naturais, telecomunicações, transportes, químico, alimentício e de serviços públicos".[8] Nesse documento, ficou constatado que mais da metade dos entrevistados acredita que as infraestruturas essenciais de seus países estão sob "constantes ataques cibernéticos, geralmente conduzidos por adversários de alto nível, tais como Estados-nação,

[4] DDoS são ataques que, através do envio indiscriminado de requisições partindo de várias origens, disparados simultânea e coordenadamente sobre um ou mais alvos, visam a causar a indisponibilidade dos serviços oferecidos por estes. Solha, Teixeira e Piccolini. Tudo que você precisa saber sobre os ataques DDos. NewsGeneration: boletim bimestral sobre tecnologia de redes, produzido e publicado pela RNP - Rede Nacional de Ensino e Pesquisa. 17 mar. 2000, v. 4, n. 2. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: 06 mar. 2010.

[5] *New York Times*. Disponível em: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1>. Acesso em: 06 mar. 2010.

[6] The Official Google Blog. A new approach to China. Janeiro de 2010. Disponível em: <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>. Acesso em: 11 mar. 2010.

[7] Disponível em: <http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war>. Acesso em: 05 mar. 2010.

[8] BBC Brasil. Brasil é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa. 01 fev. 2010. Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2010/02/100201_ataque_cibernetico_vdm.shtml>. Acesso em: 05 mar. 2010.

gangues do crime organizado e grupos terroristas[9]". Tal relatório foi apresentado no Fórum Econômico Mundial que ocorreu em Davos, Suíça, entre os dias 27 e 31 de janeiro de 2010, e gerou discussões a respeito da eclosão de uma guerra "catastrófica" no ciberespaço.

Em julho de 2010, a organização WikiLeaks[10] divulgou em seu *website* cerca de 90 mil documentos secretos sobre a Guerra do Afeganistão. Em outubro do mesmo ano, publicou uma coleção com cerca de quase 400 mil relatórios do Exército dos Estados Unidos sobre a Guerra do Iraque. Mais tarde, em novembro de 2010, divulgou relatórios sobre líderes e problemas de diversos países sob o ponto de vista da diplomacia norte-americana.[11] Tais vazamentos desencadearam uma série de debates no mundo inteiro. Embora o serviço de registro de domínios EveryDNS.net tenha fechado o *site* "após repetidos ataques DDoS, que arriscaram os 500 mil outros *sites* que o EveryDNS.net tem registrados",[12] o *website* WikiLeaks.org ainda pode ser acessado de várias outras formas. Tal fato se deve ao empenho de seus especialistas em tecnologia em "tornar o WikiLeaks virtualmente indestrutível e, portanto, a salvo de ataques legais ou cibernéticos de qualquer jurisdição ou fonte" (LEIGH e HARDING, 2011:17).

No Brasil, em 22 de junho de 2011, um grupo de *hackers* que se autodenomina "LulzSecBrazil" anunciou um ataque aos *sites* da Presidência da República e do governo brasileiro. "Os portais atacados foram o www.presidencia.gov.br e www.brasil.gov.br. Os dois sites chegaram a sair do ar por volta das 2h, uma hora após anúncio feito através do microblog Twitter."[13] Também no mesmo mês, de acordo com o jornal *Folha de S. Paulo*, um *hacker* teria violado o correio eletrônico pessoal da presidente Dilma Rousseff e copiado *e-mails* que ela recebeu durante sua campanha à Presidência da República, no ano de 2010.[14]

Diante de tal cenário de insegurança e fortes ameaças surge a seguinte questão, objeto de nosso estudo: quais são os desafios da inteligência no ciberespaço?

O objetivo precípuo deste trabalho é discorrer sobre algumas das principais questões relacionadas à inteligência neste "novo" meio denominado ciberespaço.

---

9 In the Crossfire: Critical Infrastructure in the Age of Cyber War. CSIS. 28 Jan. 2010. Disponível em: <http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war>. Acesso em: 05 mar. 2010. Tradução livre.

10 WikiLeaks. Disponível em: <http://46.59.1.2/>. Acesso em: 12 abr. 2011.

11 Disponível em: <http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20101213151225.pdf?PHPSESSID=9f6fceb2d4519e8c818505eff31619f9>. Acesso em: 12 abr. 2011.

12 Disponível em: <http://www.gizmodo.com.br/conteudo/wikileaksorg-foi-fechado-mas-site-ainda-pode-ser-acessado-de-varias-outras-formas/>. Acesso em: 12 abr. 2011.

13 Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/hackers-derrubam-sites-da-presidencia-e-do-governo-brasileiro.html>. Acesso em: 28 jul. 2011.

14 Disponível em: <http://www1.folha.uol.com.br/poder/936819-hacker-violou-mensagens-de-dilma-na-campanha-de-2010.shtml>. Acesso em: 28 jul. 2011.

Para tal, primeiramente apresentaremos breves conceitos relacionados ao tema, relevantes para a área de inteligência, como os conceitos de ciberespaço e seus atores, apresentando quais são as funções da inteligência e as funções da segurança cibernética. Em seguida, definiremos as três principais ameaças para a inteligência no ciberespaço, quais sejam, a guerra cibernética, o terrorismo cibernético e os crimes cibernéticos.

Apresentados tais conceitos, iniciaremos um pequeno debate acerca dos principais desafios que a inteligência encontra no ciberespaço, na tentativa de construir alguns cenários prospectivos.

Primeiramente, iremos nos referir a questões relacionadas com a ciberguerra, o ciberterrorismo e o cibercrime. Logo em seguida, traremos questionamentos a respeito da privacidade, censura e o controle de tráfego na internet, para então finalizar a pesquisa apresentando discussões relativas ao acesso a fontes ostensivas, coleta e análise em inteligência, cooperação nacional e internacional de inteligência e compartilhamento de informações entre as agências de inteligência.

Relativamente à guerra cibernética e ao ciberterrorismo, além de interessarem à inteligência de Estado e, consequentemente à inteligência estratégica, também interessam à inteligência militar e à inteligência financeira. A ciberguerra, apesar de não ser uma guerra nos moldes convencionais, também requer forte atuação da inteligência militar. Em relação aos crimes cibernéticos, interessam à inteligência de Estado e, precipuamente, à inteligência policial ou criminal.

11.1. Ciberespaço e seus Atores: Breves Conceitos

O termo ciberespaço foi originalmente criado em 1984 por um escritor de ficção científica chamado William Gibson. O autor utilizou o termo em seu livro *Neuromancer* (Neuromante).[15]

De acordo com Lévy (1999:92), o termo "ciberespaço", no livro de Gibson,

> […] designa o universo das redes digitais, descrito como campo de batalha entre as multinacionais, palco de conflitos mundiais, nova fronteira econômica e cultural. Em Neuromante, a exploração do ciberespaço coloca em cena as fortalezas de informações secretas protegidas pelos programas ICE, ilhas banhadas pelos oceanos de dados que se metamorfoseiam e são trocados em grande velocidade ao redor do planeta. Alguns heróis são capazes de entrar "fisicamente" nesse espaço de dados para lá viver todos os tipos de aventuras. O ciberespaço de Gibson torna sensível a geografia móvel da informação, normalmente invisível. O termo foi imediatamente retomado pelos usuários e criadores de redes digitais.

[15] Cyberspace. *International Encyclopedia of the Social Sciences*. 2008. Disponível em: Encyclopedia.com: <http://www.encyclopedia.com/doc/1G2-3045300513.html>. Acesso em: 22 fev. 2010.

Apesar de Gibson ter sido o criador do termo "ciberespaço", Wilson (2010) afirma que Castells foi nomeado "o primeiro grande filósofo do ciberespaço", ao acreditar que o ciberespaço fosse uma representação da experiência humana. Para Castells (1998:336 apud Wilson, 2010), o ciberespaço

> Originou-se na coincidência histórica, em torno do final dos anos 1960 e meados de 1970, de três processos independentes: a revolução da tecnologia da informação, a crise econômica tanto do capitalismo como do estatismo e sua subsequente reestruturação; e o florescimento de movimentos sociais culturais, tais como o libertarismo, os direitos humanos, o feminismo e o ambientalismo. A interação entre esses processos e as reações que eles provocaram trouxeram uma nova estrutura social dominante, a sociedade em rede; uma nova economia, a economia informacional/global; e uma nova cultura, a cultura da virtualidade real. [Tradução livre]

De acordo com Wilson (2010):

> Castells imagina o ciberespaço como uma mistura híbrida do digital e do físico. [A sociedade em rede] [...] é onde os indivíduos, os grupos, os governos estão ligados, tanto digitalmente como fisicamente, e a interconectividade humana através da informação digital e das tecnologias de comunicação é o ciberespaço. Para ele, o ciberespaço é a sociedade em rede – uma rede baseada na humanidade e tecnologicamente conduzida. Não há uma divisão ciberfísica. [Tradução livre]

Para Lévy (1999:92), ciberespaço é "o espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores". O autor explica que esse "novo meio tem a vocação de colocar em sinergia e interfacear todos os dispositivos de criação de informação, de gravação, de comunicação e de simulação", e afirma que, a partir do início deste século, "a perspectiva da digitalização geral das informações provavelmente tornará o ciberespaço o principal canal de comunicação e suporte de memória da humanidade" (LÉVY, 1999:93).

Já a Webopedia (2002, tradução livre) apresenta a seguinte definição:[16]

> O termo ciberespaço é frequentemente utilizado como uma metáfora para descrever um terreno não-físico criado por sistemas de computadores. Sistemas online, por exemplo, criam um ciberespaço no qual as pessoas podem se comunicar umas com as outras (via *e-mail*), fazer pesquisas ou simplesmente navegar em lojas virtuais. Como o espaço físico, o ciberespaço contém objetos (arquivos, mensagens, gráficos etc.) e diferentes modos de transporte e entrega. Ao contrário do que ocorre no espaço real, no entanto, explorar o ciberespaço não requer qualquer movimento físico maior que pressionar as teclas de um teclado ou movimentar um *mouse*. Alguns programas, particularmente os jogos de computador, são concebidos para criar um ciberespaço especial, um espaço que se assemelhe à realidade física em alguns aspectos, mas a desafie em outros. Na sua forma mais extrema, chamada de realidade virtual, os usuários recebem

[16] "Cyberspace". Webopedia: The #1 Online encyclopedia dedicated to computer technology. 2002. Disponível em: <http://webopedia.com/TERM/c/cyberspace.html>. Acesso em: 28 fev. 2010.

> um retorno visual, auditivo, e até mesmo tátil, que faz com que o ciberespaço pareça totalmente real.

Apesar de a internet ser o principal ambiente do ciberespaço, assim como explica Mathers (2007:2, tradução livre), "seu domínio inclui todos os aparelhos eletrônicos, como telefones celulares, dispositivos de mensagens de texto, rádios, vídeo games, [...] os dados associados e informações que estão sendo armazenadas ou movidas por tais dispositivos".

De acordo com Fragoso (2000:4):

> Apropriada para denominar o conjunto das informações que transitam nos servidores e terminais conectados à Internet, a expressão ciberespaço popularizou-se com a rápida expansão do número de usuários da rede na década de 1990. Para grande parte dos usuários não-especialistas, a Internet corresponde à somatória de correio eletrônico e World Wide Web (WWW ou simplesmente Web).

Nesse sentido, explica Guimarães Jr. (1999):

> [...] o termo "Ciberespaço" pode ser definido como *o locus* virtual criado pela conjunção das diferentes tecnologias de telecomunicação e telemática, em especial, mas não exclusivamente, as mediadas por computador. É importante sublinhar que essa definição não circunscreve o Ciberespaço às redes de computadores, mas sim percebe como suas instâncias diferentes aparatos de telecomunicação, desde teleconferências analógicas, passando por redes de computadores, "pagers", comunicação entre radioamadores e por serviços do tipo "teleamigos". A internet, portanto, apesar de ser a mais presente, não é a única instância de CMC, e por extensão, de suporte ao Ciberespaço. Atualmente, contudo, percebe-se uma tendência de unificação da esfera global de telecomunicações a partir de plataformas digitais, seja a partir da rede Internet "pública" ou através de redes privadas.[17]

Para a National Strategy to Secure Cyberspace (Estratégia Nacional para Assegurar o Ciberespaço) dos Estados Unidos da América, de fevereiro de 2003:

> O ciberespaço é composto de centenas de milhares de computadores ligados em rede, servidores, roteadores, tomadas, e cabos de fibra óptica que permitem que nossas infraestruturas críticas trabalhem. Assim, o funcionamento saudável do ciberespaço é essencial para a nossa economia e nossa segurança nacional.[18] [Tradução livre]

As políticas norte-americanas National Security Presidential Directive 54 (Diretiva Presidencial de Segurança Nacional) e Homeland Security Presidential Directive 23 (Diretiva Presidencial de Segurança Interna) – (NSPD-54/HSPD-23),

---

[17] De acordo com Guimarães Jr., o termo CMC significa "Comunicações mediadas por computador". Disponível em: <http://www.cfh.ufsc.br/~guima/papers/ciber_cenario.html>. Acesso em: 11 mar. 2010.

[18] The National Strategy to Secure Cyberspace. Executive Summary vii. United States: February, 2003. Disponível em: <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>. Acesso em: 20 fev. 2010.

apud Cyberspace Policy Review (Revisão da Política do Ciberespaço) (maio, 2009), assim definem o ciberespaço:

> O ciberespaço é uma rede interdependente de infraestruturas de tecnologia da informação, e inclui a Internet, redes de telecomunicações, sistemas de computador e processadores e controladores pertencentes a indústrias críticas. No uso comum, o termo também se refere ao ambiente virtual de informações e interações entre as pessoas.[19] [Tradução livre]

Para o Cybersecurity Act of 2009 (Ato de Cibersegurança 2009) apresentado ao Senado norte-americano perante o Comitê de Comércio, Ciência e Transporte em 1º de abril de 2009, o termo "cyber" significa:

> (A) qualquer processo, programa ou protocolo relativo à utilização da internet ou intranet, processamento automático de dados ou sua transmissão, ou de telecomunicações através da internet ou intranet; e, (B) qualquer questão relacionada ou que envolva a utilização de computadores ou redes de computadores.[20] [Tradução livre]

De acordo com Libicki (2009:12-13), uma forma de entender o ciberespaço e os ataques que nele ocorrem é através da compreensão dos seus mecanismos, que giram em torno de três níveis: o físico, o sintático e o semântico. Todos os sistemas de informações se situam numa camada física que os sustenta, a qual consiste em caixas e fios. A camada sintática contém instruções que os criadores de programas e os usuários dão à máquina, bem como os protocolos através dos quais as máquinas interagem (elaboração de dados, reconhecimento de dispositivos, formatação de documentos etc.). É nesse nível que os *hackers* tendem a atuar. O nível semântico consiste em informações que as máquinas contêm. Esse nível pode sofrer ataques *hacker*, como anexos que contenham vírus e *sites* com códigos embutidos, mas, na maioria das vezes, apenas as máquinas que foram afetadas em seu nível sintático é que são capazes de aceitar informações falsas (LIBICKI, 2009:12-13).

Todos que têm acesso ao ciberespaço atuam nele, desde adolescentes e estudantes universitários até criminosos e espiões. Aqueles que, de alguma forma, possam influenciar as relações ora existentes, sejam elas pessoais, econômicas, políticas, sociais, culturais, tecnológicas, públicas ou privadas, nacionais ou transnacionais, ambientais, entre outras, interessam particularmente à inteligência. Entre tais atores, podemos destacar *hackers*, espiões, cibercriminosos, ciberterroristas, governos, instituições privadas, organizações criminosas e religiosas.

---

[19] Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 28 fev. 2010.

[20] Disponível em: <http://www.opencongress.org/bill/111-s773/text>. Acesso em: 28 fev. 2010.

O *site* IWS – The Information Warfare Site (*site* sobre guerra informacional) traz algumas definições que nos são relevantes:

> *Hacker* – é alguém que gosta do desafio intelectual de superar ou contornar limitações criativamente, principalmente em suas áreas de interesse, ou seja, programação ou engenharia elétrica.[21] [...] Usuário não autorizado que tenta ou obtém acesso a um sistema de informação (NSTISSI 4009).[22]
>
> *Cracker* – é aquele que quebra a segurança de um sistema. O termo foi cunhado por *hackers* em 1985 na tentativa de autodefesa contra o mau uso jornalístico do termo *hacker* [...].[23] [Tradução livre]

De acordo com o Jargão Hacker (*The Hacker's Jargon File*), o *cracker* seria o *hacker* maligno.[24]

Santos (2008:11) também faz a distinção entre *hackers* e *crackers*, ressaltando que ambos, em determinado momento, podem ser considerados criminosos:

> Por *Hacker* podemos compreender aquele que possui alta habilidade técnica para lidar com sistemas de computação ou comunicações em rede; sua denominação tem origem no inglês, significando "fuçador". Seu propósito é de invadir sistemas alheios para satisfação pessoal, vale dizer, não tem intuito de prejudicar terceiros. O *Cracker*, por sua vez, também é um invasor, cujo objetivo é danificar a máquina ou sistema; trata-se do pirata digital. Entendo que ambos, em determinado momento, podem ser considerados criminosos e suas condutas não devem ser aprovadas, nem pela ética, nem pelo direito.

De acordo com o filme *Hackers: Outlaws and Angels* (Hackers: Criminosos e Anjos), o:

> temor aos *hackers* fez nascer uma nova profissão: os *hackers* éticos – são pagos para invadirem computadores de grandes empresas, suas redes. São os "times dos tigres". Eles testam sistemas de segurança poderosos para identificar os problemas de segurança e minimizar o risco de inimigos fazerem o mesmo.[25]

---

[21] Disponível em: <http://www.iwar.org.uk>. Acesso em: 06 mar. 2010.

[22] National Information Systems Security (Infosec) Glossary – NSTISSI No. 4009, Setembro 2000. Disponível em: <http://security.isu.edu/pdf/4009.pdf>. Acesso em: 06 mar. 2010.

[23] Disponível em: <http://www.iwar.org.uk>. Acesso em: 06 mar. 2010.

[24] *The Hacker's Jargon File*. Disponível em: <http://www.catb.org/jargon/html/index.html>. Acesso em: 06 mar. 2010.

[25] Cf. *Hackers: Outlaws and Angels*. Produzido por September Films para TLC Life Unscripted. Versão [puxando.com] Hackers: Criminosos e Anjos – Dvdrip Legendado. Acesso em: 2009. Outro exemplo da contratação de "hackers éticos" é o US Cyber Challenge. "Sua finalidade é identificar 10.000 jovens norte-americanos com interesses e conhecimentos técnicos de informática para preencher as posições de profissionais da segurança cibernética, pesquisadores e guerreiros" (Tradução livre). Disponível em: <http://csis.org/uscc>. Acesso em: 10 mar. 2010.

Já os "phishers" praticam o *phishing*. De acordo com o *site* da Microsoft, o *phishing* tornou-se o crime cibernético de roubo de finanças e identidade que mais cresce":

> Estes golpes consistem em mensagens de *e-mail* fraudulentas que parecem vir de um endereço legítimo da internet com uma solicitação justificável – geralmente direcionando o usuário para um *site* da internet para verificação ou atualização de dados pessoais ou detalhes de contas (senhas, números de cartão de crédito, inscrições na previdência social e contas bancárias). As mensagens sugerem consequências negativas caso o *link* embutido não seja aberto, tais como "sua conta será desativada ou suspensa". Esses tipos de *e-mails* fraudulentos são comumente chamados de "phishing" porque eles usam iscas para atrair vítimas desavisadas. O objetivo do "phisher" (remetente) é fazer o usuário morder a isca fornecendo informações pessoais ou detalhes de contas de modo que o "cyber-escroque" possa sacar dinheiro diretamente das contas bancárias das vítimas ou ir freneticamente às compras com as informações dos cartões de crédito.[26, 27]

11.2. Funções da Cibersegurança e Funções da Inteligência no Ciberespaço

A inteligência e a área de segurança informacional exercem "funções simétricas e mutuamente dependentes" (CEPIK, 2003:57). Entretanto, no que tange à diferença entre inteligência e segurança informacional, discorre Cepik (2003:57):

> [...] enquanto a inteligência procura conhecer o que os comandantes e governantes que a dirigem necessitam saber sobre as ameaças e problemas relativos à segurança do Estado e dos cidadãos, a área de segurança de informações (infosec,[28] ou *informations security*) procura proteger as informações que, uma vez obtidas por um adversário ou inimigo – por exemplo, através das operações de inteligência de um governo estrangeiro –, poderiam tornar vulneráveis e inseguros o Estado e os cidadãos. [...] Do ponto de vista operacional, enquanto a principal missão na área de inteligência é tentar conhecer o "outro", a principal missão da área de infosec é garantir que os "outros" só conhecerão o que quisermos que eles conheçam sobre nós mesmos. As duas missões são cumpridas no Estado contemporâneo por organizações distintas, sendo que segurança pode ser considerada uma função gerencial nas organizações civis e uma responsabilidade nas organizações militares.

No campo cibernético, a dicotomia gira em torno de vulnerabilidades e ameaças. A segurança cibernética tem como principal objetivo conhecer as vulnerabilidades existentes em seu país ou organização. Já a inteligência tem

[26] Disponível em: <http://technet.microsoft.com/pt-br/library/cc512621.aspx>. Acesso em: 17 mar. 2010.
[27] Fraudador, que pratica ações com o objetivo de enganar alguém ou burlar as regras vigentes.
[28] "Infosec significa "segurança de informações" ou "informations security" (CEPIK, 2003:57).

como principal objetivo conhecer as potenciais ameaças que possam resultar em um dano para aquele Estado ou organização.

No que concerne à cibersegurança, de acordo com a estratégia nacional norte-americana para assegurar o ciberespaço (*National Strategy to Secure Cyberspace*), de fevereiro de 2003, são completamente vulneráveis suas infraestruturas críticas compostas por:

> instituições públicas e privadas nos setores de agricultura, alimentação, água, saúde pública, serviços de emergência, governo, base industrial de defesa, informação e telecomunicações, energia, transportes, banco e finanças, produtos químicos e materiais perigosos, e dos serviços postais e de entrega. [29] [THE NATIONAL STRATEGY TO SECURE CYBERSPACE. United States: February, 2003. Tradução livre]

O'Brien (2002:4, tradução livre), por sua vez, define infraestruturas críticas nacionais (The Critical National Infrastructure – CNI) como:

> [...] instalações físicas e de tecnologia da informação, redes e ativos cuja perturbação ou destruição teria um impacto grave sobre a saúde, a segurança, o bem-estar econômico dos cidadãos ou sobre o funcionamento efetivo dos governos e dos negócios.

De acordo com a Portaria nº 34, de 5 de agosto de 2009 (Apud CANONGIA e MANDARINO JÚNIOR, 2009:27):

> Tem-se que dois conceitos adotados no Brasil na esfera pública dão sustentação à abordagem da segurança cibernética, quais sejam, "infraestrutura crítica da informação", bem como "ativos de informação". No âmbito do governo federal brasileiro, considera-se "infraestrutura crítica da informação" o subconjunto de ativos de informação que afetam diretamente a consecução e a continuidade da missão do Estado e a segurança da sociedade. E, complementarmente, consideram-se "ativos de informação", os meios de armazenamento, transmissão e processamento da informação, os sistemas de informação, bem como os locais onde se encontram esses meios, e as pessoas que a eles têm acesso.

São exemplos de vulnerabilidades retirados do caderno de oficinas sobre segurança cibernética entregue na Oficina de Gestão de Riscos de Segurança da Informação e Comunicações do GSIPR/DSIC:[30]

- falta de cuidado durante o descarte da informação;
- realização de cópias não controlada;
- não execução do "logout" ao se deixar uma estação de trabalho desassistida;
- tabelas de senhas desprotegidas;
- treinamento insuficiente em segurança;

[29] The National Strategy to Secure Cyberspace. United States: February, 2003.

[30] XXI Seminário de Segurança da Informação e Comunicações (SEMSIC-MG) promovido pelo GSIPR/DSIC, realizado nos dias 23 e 24 de novembro de 2009, na cidade de Belo Horizonte/MG.

• inexistência de cópias de segurança ("backup");

• inexistência de política de uso de correspondência eletrônica *(e-mail)*;

• uso incorreto de *software* e *hardware*.

No Brasil, o Gabinete de Segurança Institucional da Presidência da República – GSIPR, mais precisamente o Departamento de Segurança da Informação e Comunicações – DSIC é o responsável pela segurança cibernética no âmbito da Administração Pública Federal, direta e indireta.

De acordo com o art. 8º do Decreto nº 6.931, de 11 de agosto de 2009, são missões do DSIC:

1. Adotar as medidas necessárias e coordenar a implantação e o funcionamento do Sistema de Segurança e Credenciamento – SISC, de pessoas e empresas, no trato de assuntos, documentos e tecnologia sigilosos;
2. Planejar e coordenar a execução das atividades de segurança da informação e comunicações na administração pública federal;
3. Definir requisitos metodológicos para implementação da segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;
4. Operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
5. Estudar legislações correlatas e implementar as propostas sobre matérias relacionadas à segurança da informação e comunicações; e
6. Avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações.[31]

Ao se referir à situação da segurança cibernética de vários países, ressalta Bezerra (2009):

> O Governo Brasileiro felizmente também está se organizando, com o Departamento de Segurança da Informação e Comunicações (DSIC), que faz parte do Gabinete de Segurança Institucional da Presidência da República, o que é bom sinal, já que está subordinado diretamente ao Presidente. Uma estrutura centralizada de coordenação e planejamento é mesmo essencial. De acordo com o *site* Convergência Digital, do portal Terra, a administração pública federal possui 320 redes informatizadas e, em apenas uma delas, os ataques de *hackers* chegaram a três milhões em 2008.[32]

De acordo com estatísticas do CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), só em 2009, um total de 358.343 incidentes foram reportados.[33]

---

[31] Disponível em: <http://dsic.planalto.gov.br/missao>. Acesso em: 01 mar 2010.

[32] Disponível em: <http://dsic.planalto.gov.br/noticias/71-artigo-sobre-guerra-cibernetica-qcyberwarq>. Acesso em: 10 mar. 2010.

[33] Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 17 mar. 2010.

A respeito da normatização brasileira relacionada à segurança da informação, Vieira (2008), procuradora federal da Advocacia-Geral da União, compilou e analisou a legislação vigente a fim de subsidiar trabalhos de operadores, técnicos e juristas da área de segurança da informação, atualizada até o dia 5 de novembro de 2008.[34] Acrescentam-se a essa legislação as normas complementares 01 a 06 do DSIC-GSIPR, que podem ser encontradas no *site* desse departamento.[35]

Os Estados Unidos, desde 2003, possui uma estratégia nacional para assegurar o ciberespaço.[36] Tal estratégia já sofreu uma revisão em 2009 e, em maio de 2011, os Estados Unidos lançaram sua estratégia internacional para o ciberespaço.[37, 38] O Brasil ainda não possui uma estratégia nacional para assegurar o ciberespaço, mas o Gabinete de Segurança Institucional da Presidência – GSI, através do Departamento de Segurança da Informação e Comunicações – DSIC vem elaborando vários documentos com o propósito de instituir diretrizes capazes de regular o exercício da cibersegurança no Brasil. Alguns documentos que se destacam são: "Gestão da Segurança da Informação e Comunicações", "Guia de Referência para a Segurança das Infraestruturas Críticas da Informação" e o "Livro Verde sobre a Segurança Cibernética no Brasil".[39]

De acordo com a estratégia nacional norte-americana para assegurar o ciberespaço (National Strategy to Secure Cyberspace), são objetivos da segurança cibernética "prevenir ataques contra as infraestruturas críticas, reduzir as vulnerabilidades e minimizar os danos e o tempo de recuperação pós-ataques."[40]

Embora as funções que se atribui à inteligência tenham sido suficientemente discutidas pela literatura disponível (CEPIK, 2003:64-65), pouco se diz ou se sabe sobre quais funções a inteligência assumiria no contexto do ciberespaço. Assim, se transpusermos algumas dessas funções para o campo cibernético, justamente no sentido de tentar adaptar as funções da inteligência às exigências impostas pelo ciberespaço, poderíamos então vislumbrar as seguintes funções: (i) apoiar o desenvolvimento e/ou aquisição de armas cibernéticas (*softwares*) que, tecnologicamente falando, sejam capazes de neutralizar o inimigo e até mesmo contra-atacar (caso uma guerra cibernética venha a ocorrer); (ii) desenvolver

[34] Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 1 mar. 2010.

[35] Site do DSIC/GSIPR. Disponível em: <http://dsic.planalto.gov.br/>. Acesso em: 1 mar. 2010.

[36] Disponível em: <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>. Acesso em: 28 fev. 2010.

[37] Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 28 fev. 2010.

[38] Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 30 jul. 2011.

[39] Disponível em: <http://dsic.planalto.gov.br/>. Acesso em: 30 jul. 2011.

[40] The National Strategy to Secure Cyberspace. Fev. 2003. Tradução livre.

tecnologias que sejam capazes de detectar a presença de um inimigo ou de um ataque cibernético e de identificá-los nas redes informacionais do seu país; (iii) subsidiar a área militar no planejamento e execução de suas operações no ciberespaço, bem como auxiliá-la na elaboração de normas transnacionais que regulem a guerra no ciberespaço, contribuindo para a definição de formas "autorizadas" internacionalmente de retaliação e procedimentos a serem adotados diante de ações isoladas (grupos não-estatais) de caráter ofensivo; (iv) alertar os responsáveis civis e militares para que possam evitar a surpresa de uma guerra cibernética ou de um ataque ciberterrorista; (v) obter e organizar informações concretas, a respeito de ataques ou crimes na rede, que propiciem apoio a negociações entre os países acerca de novos tratados e convenções relacionados à guerra cibernética, ao ciberterrorismo e aos crimes cometidos no ciberespaço; (vi) apoiar as agências nacionais de inteligência no estabelecimento de relações seguras entre si ou com agências de outros países, ao viabilizar sua interação através da criação de recursos que tornem viável a transferência de informações, sem que haja sua perda, extravio, adulteração, vazamento, roubo ou destruição; (vii) desenvolver mecanismos de filtragem de informação, principalmente a de caráter ostensivo, de forma a tornar mais ágeis os processos de coleta e análise de inteligência; (viii) capacitar profissionais de inteligência no ensino de idiomas, no sentido de ampliar seu leque de atuação na rede, principalmente na busca/coleta de informações que estão cada vez mais disponíveis na internet; (ix) proporcionar treinamento constante aos profissionais de inteligência, diante das novas ameaças no ciberespaço; (x) auxiliar os responsáveis pela segurança pública no combate à criminalidade no ciberespaço; (xi) auxiliar na elaboração de regras de monitoramento do ciberespaço, tanto nacionais quanto internacionais; (xii) monitorar o ciberespaço e seus atores, dentro de práticas e parâmetros democráticos legais estabelecidos; (xiii) preservar o segredo sobre as atividades de inteligência realizadas no ciberespaço diante de algum adversário que queira saber sobre isso.

Gabbard (2008), cofundador e diretor de tecnologia da empresa Lookingglass,[41] que oferece serviços na área de inteligência, e ex-membro da equipe técnica da CERT@ – Computer Security Incident Response Team (Grupo de Resposta a Incidentes de Segurança),[42] enumera como funções da ciberinteligência (*cyber intelligence*):

- compreender as arquiteturas globais e ameaças associadas;
- determinar como essas ameaças e vulnerabilidades podem impactar um negócio, um governo ou uma organização militar;

[41] Lookingglass. Disponível em: <http://www.lgscout.com/>. Acesso em: 11 mar. 2010.
[42] CERT@ Disponível em: <http://www.cert.org/>. Acesso em 11 mar. 2010.

- avaliar os riscos, os cursos de ação, e outros fatores que dependem da rede global;
- correlacionar eventos globais com os riscos dos negócios.[43] [Tradução livre]

Após termos definido as funções da cibersegurança e as funções da "ciberinteligência", percebe-se crucial a integração da área de segurança com a área de inteligência. Assim como Cepik (2003:61) já sugeriu,

> Ainda que as ameaças de inteligência sejam mais difíceis de se identificar no atual contexto internacional, o que necessariamente obriga a uma redefinição das missões de contrainteligência, os temas associados à segurança informacional (infosec) são cada vez mais centrais e deveriam ser pensados a partir de suas interações com a área de inteligência como um todo.

11.3. Principais Ameaças para a Inteligência no Ciberespaço

As principais ameaças para a inteligência no ciberespaço, de acordo com a literatura consultada, são a guerra cibernética, o ciberterrorismo e o cibercrime.

Ciberguerra

De acordo com Libicki (1995), a ciberguerra ou guerra cibernética faz parte de um conjunto de conflitos que envolvem a proteção, a manipulação, a degradação e a negação de informações, denominado guerra informacional (*information warfare*, em inglês):

1. Guerra de comando e controle [C2W];
2. Guerra baseada na inteligência [IBW];
3. Guerra eletrônica [EW];
4. Operações psicológicas [PSYOPS];
5. Guerra *hacker* baseada em ataques a sistemas de informações;
6. Guerra de informação econômica [IEW], guerra através do controle das informações relacionadas ao comércio; e
7. Ciberguerra [combate no mundo virtual]. [Tradução livre]

Sobre o conceito de guerra informacional, leciona Cepik (2003:69):

> O conceito de *information warfare* (IW) resulta da tentativa de integração e expansão das operações de guerra eletrônica, guerra de comando e controle (*C2 warfare*) e disciplinas defensivas em inteligência. Por analogia com a guerra terrestre ou marítima, a guerra informacional compreende o conjunto de ações ofensivas e defensivas conduzidas no ambiente informacional para controlar o *cyberspace*. Ciberespaço é aqui entendido como o "lugar" onde interagem

[43] Disponível em: <http://www.dataconnectors.com/events/2008/09washingtondc/pres/SSES.pdf>. Acesso em: 11 mar. 2010.

> computadores, programas, sistemas de comunicação e equipamentos que operam via irradiação de energia no espectro eletromagnético. Porém, menos por um "lugar" ou um conjunto classificável de ações, a guerra informacional define-se melhor por seus objetivos: obter e manter superioridade informacional na batalha ou na guerra. Ações tão diferentes entre si como um ataque aéreo a uma central de telecomunicações, operações de sigint, [44] missões aéreas para reconhecimento do campo de batalha ou a implantação clandestina de códigos de computador com "bombas lógicas" poderiam ser parte de uma campanha de guerra informacional. Destaque-se que essas operações de IW não devem ser tomadas como configurando uma "guerra" à parte. A guerra permanece una e indivisível enquanto realidade; o que está em jogo é a perspectiva – ainda não consolidada ou atestada como mais útil do que a preocupação com esse tema por organizações combatentes já consolidadas – de criação de uma "arma" ou especialidade combatente de informações.

Szafranski define "warfare" como: "um conjunto de atividades letais e não-letais capazes de subjugar a vontade hostil de um adversário ou inimigo" e salienta que a guerra informacional não é sinônimo de guerra em seu sentido convencional, ou seja, não requer uma declaração de guerra e não requer a "existência de uma condição largamente reconhecida como um 'estado de guerra'".[45] Seus atores podem ser controlados ou patrocinados por um Estado, mas, ao mesmo tempo, também podem ser atores não-estatais. O objetivo da "warfare" é afetar os sistemas de informação do inimigo (SZAFRANSKI, 1995:1-2).[46] (Tradução livre)

Para Arquilla e Ronfeldt (1993 apud SZAFRANSKI, 1995:2-3), "a guerra informacional é uma forma de conflito que ataca diretamente os sistemas de informações do adversário, a fim de atacar os seus conhecimentos e crenças". (Tradução livre)

Diante do exposto, podemos concluir que a ciberguerra pode ser considerada como um aspecto da guerra informacional travada no ciberespaço.

A ideia de ciberguerra ou guerra cibernética tem como origem uma palavra grega, *kybernetiké*, e significa "a arte de controle". Tal conceito foi introduzido por Norbert Wiener no final da década de 1940 ao lançar o livro *Cibernética ou controle e comunicação no animal e na máquina* (WIENER, 1948 apud SAMPAIO, 2001:2).

Wiener afirmava:

> Decidimos denominar todo o reino da teoria do comando e da transmissão de informações, quer seja em máquinas ou em seres vivos, de cibernética. […] A cibernética não se ocupa primordialmente nem de organismos nem de produtos técnicos, **mas sim daquilo que é comum a ambos**, ou seja,

[44] "Sigint – informações obtidas a partir da interceptação e decodificação de comunicações e sinais eletromagnéticos" (CEPIK, 2003:36).

[45] Disponível em: <http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm>. Acesso em: 5 mar. 2010.

[46] Para Szafranski, "sistemas de informação são um conjunto de conhecimentos, crenças e processos e sistemas de tomadas de decisão do adversário" (Tradução livre).

> a cibernética se centraliza não na eletrotécnica, mas no conceito mais fundamental de informação, quer ela seja transmitida por meios elétricos, mecânicos ou nervosos. [WIENER, Simpósio sobre Cibernética do Sistema Nervoso, Amsterdã, 1962 apud SAMPAIO, 2001:2, grifos do autor.]

Para Sampaio (2001:2-3, grifos do autor), "sendo a cibernética a arte de comandar ou controlar, sua forma primordial de agir é pelo comando ou controle de **todo o ciclo de informações**". Nesse sentido, o autor (2001:3-4) afirma:

> [...] a Ciberguerra visa à paralisação de um adversário, no caso um país ou até um Bloco Econômico, ou uma aliança militar, pela penetração nas redes de computadores que dirigem a maioria das atividades vitais da economia, criando o caos e difundindo um estado de medo generalizado. Tal quadro permite o enfraquecimento das defesas convencionais, podendo-se, então, por técnicas de infiltração, atacar o país, bloco ou aliança, por meio de ações terroristas, boatos (difundidos por agentes infiltrados), notícias falsas veiculadas pelos meios de informação de massa e mesmo técnicas mais sofisticadas, umas em desenvolvimento, outras já utilizáveis, que destruiriam a coesão, a capacidade de resistência e levariam a um colapso total, que seria a paralisação estratégica, elevada, porém, a um potencial muito maior do que o previsto até hoje.

Hackers "podem roubar informações, emitir comandos falsos aos sistemas de informação a fim de afetar seu funcionamento e injetar informações falsas para conduzir homens e máquinas a chegar a conclusões falsas e a tomarem más, ou nenhuma decisão" (LIBICKI, 2009, p. xiii). (Tradução livre)

Sampaio (2001:4-5) salienta que os "alvos preferenciais para serem penetrados e desvirtuados são os programas de computadores que controlam ou gerenciam os seguintes aspectos":

1 – comando das redes de distribuição de energia elétrica;

2 – comando das redes de distribuição de água potável;

3 – comando das redes de direção das estradas de ferro;

4 – comando das redes de direção do tráfego aéreo;

5 – comando das redes de informação de emergência:

a. pronto-socorro;

b. polícia;

c. bombeiros;

6 – comando das redes bancárias, possibilitando a inabilitação das contas, ou seja, apagando o dinheiro registrado em nome dos cidadãos (o potencial para o caos e a desmoralização de um país embutido neste tipo de ataque é por demais evidente);

7 – comando das redes de comunicações em geral, em particular:

a. redes de estações de rádio;

b. redes de estações de televisão;

8 – comando dos "links" com sistemas de satélites artificiais:

a. fornecedores de sistemas telefônicos;

b. fornecedores de sistemas de sinais para TV;

c. fornecedores de previsões de tempo;

d. fornecedores de sistemas GPS;

9 – comandos das redes dos Ministérios da Defesa e, também:

a. Banco Central;

b. Outros Ministérios Importantes (Justiça, Interior);

10 – comandos dos sistemas de ordenamento e recuperação de dados nos sistemas judiciais, incluindo os de justiça eleitoral.

Podem existir outros alvos, que serão apontados/selecionados pelos serviços de coleta de informações (inteligência), pelo estudo, por adidos militares, adidos de informações (outros) ou, ainda, agentes implantados no país sob outras coberturas (comércio, serviços, professorado etc.).

De acordo com Sampaio (2001:5, grifos do autor), ainda em relação aos alvos:

> As possibilidades são imensas, pois, cada vez mais, a própria complexidade e tamanho das atividades comerciais, dos governos e das populações, leva a uma dependência dos computadores, que armazenam informações **que não estão mais disponíveis de outra forma**. Muitos sistemas de comando e controle, civis, governamentais e mesmo alguns militares já estão, inclusive, automatizados e em alguns casos confia-se na velocidade de resposta do computador, muito acima da humana, para reagir a ataques que virão com antecipação de minutos ou até mesmo segundos, quando o homem não teria condições de dirigir o sistema de defesa. Os meios sofisticados de alta velocidade e, mais recentemente, as técnicas ditas invisíveis (para o radar), tornam a dependência de sistemas automatizados de previsão de ataque/defesa cada vez mais uma necessidade, o que é confiado a computadores. A penetração nestes sistemas pode inutilizar, portanto, toda uma estratégia de defesa e levar a rendição, **pela total paralisia estratégica de um país, bloco ou aliança**.

Libicki (2009:117) ainda subdivide a ciberguerra em ciberguerra estratégica e ciberguerra operacional. A ciberguerra estratégica seria "uma campanha de ataques cibernéticos lançada por uma entidade contra um Estado e sua sociedade, principalmente, mas não exclusivamente, com o propósito de afetar o comportamento do Estado-alvo."[47] A ciberguerra operacional gira em torno da "utilização de um ataque à rede como um apoio às operações militares executadas no plano físico." (Tradução livre)

[47] Para saber mais sobre os tipos de ataques de guerra cibernéticos vide Jokisipilä (2004, p. 3). Disponível em: <http://vanha.soc.utu.fi/polhist/vaihtuvat/jokisipila_Interfada.pdf>. Acesso em: 18. mar. 2010.

Ciberterrorismo

Além da guerra cibernética, o terrorismo cibernético é também considerado uma ameaça para a inteligência no século XXI. O ciberterrorismo é uma modalidade de terrorismo.

Denning (2000), uma professora de ciência da computação da Georgetown University, em um depoimento apresentado para o House Armed Services Committee (Comitê de Serviços Armados), em 23 de maio de 2000, propôs uma definição precisa acerca do termo:

> Ciberterrorismo é a convergência de terrorismo e ciberespaço.[48] É geralmente entendido como ataques ilegais e ameaças de ataque contra computadores, redes e as informações neles armazenadas, com o intuito de intimidar ou coagir um governo ou o seu povo em prol de objetivos políticos ou sociais. Além disso, para se qualificar como ciberterrorismo, um ataque deve resultar em violência contra pessoas ou bens, ou pelo menos causar dano suficiente para gerar medo. Ataques que levam à morte ou à lesão corporal, explosões, acidentes de avião, à contaminação da água ou perdas econômicas graves seriam alguns exemplos de ciberterrorismo. Ataques graves contra infraestruturas críticas podem ser atos de ciberterrorismo, dependendo do seu impacto. Os ataques que interrompem serviços não essenciais ou que são meramente um incômodo dispendioso não são considerados atos de ciberterrorismo. [Tradução livre]

Para Weimann (2004), é importante fazer a distinção entre ciberterrorismo e "hacktivismo", termo utilizado por estudiosos para descrever a junção de "hacking" com o ativismo político. De acordo com Weimann, enquanto o principal objetivo dos hacktivistas é protestar e perturbar politicamente um governo através do uso de bloqueios virtuais [49], bombardeios de *e-mail*, invasões de computadores e do uso de vírus e *worms* [50] para infectar redes computacionais, o principal objetivo dos ciberterroristas é matar ou aterrorizar, deixando claro que essa diferença pode, em algum momento, tornar-se um pouco confusa:

> especialmente se os grupos terroristas forem capazes de recrutar ou contratar hacktivistas expertos em computadores ou se hacktivistas decidirem elevar suas ações, atacando sistemas que operam elementos críticos da infraestrutura nacional, tais como redes de energia elétrica e serviços de emergência (WEIMANN, 2004:5). [Tradução livre]

---

[48] O termo terrorismo significa "violência premeditada, politicamente motivada, perpetrada contra alvos não combatentes por grupos subnacionais ou agentes clandestinos" (Tradução livre) Web site da CIA. Título 22 do Código americano, sessão 2656f(d). Disponível em: <http://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html>. Acesso em: 6 mar. 2010.

[49] Bloqueios virtuais, de acordo com o autor, são tentativas de gerar tráfego para o site que está sendo visitado de forma a impossibilitar que outros usuários o acessem, e assim, causar a interrupção das operações normais do site (WEIMANN, 2004:4).

[50] "Vírus são *malwares* (*softwares* maliciosos) criados com o objetivo de danificar arquivos armazenados no disco rígido (especialmente arquivos críticos para o funcionamento do sistema), tornando o sistema inoperante. *Worms* são como os vírus, mas têm a capacidade de se propagar para outros computadores. Normalmente, os *worms* geram um aumento considerável no tráfego de dados, prejudicando o acesso aos serviços de rede. Os *worms* costumam se propagar buscando vulnerabilidades em sistemas e em *e-mails*." (*Crimes Cibernéticos*: Manual Prático de Investigação do Ministério Público Federal – Procuradoria da República no Estado de São Paulo, 2006, p. 14).

De acordo com Weimann (2004:6), são inúmeras as vantagens que o terrorista tradicional encontra no ciberespaço:

- Primeiro, é mais barato do que os métodos terroristas tradicionais. Tudo o que um terrorista precisa é de um computador pessoal e uma conexão *online*. Os terroristas não precisam comprar armas, tais como revólveres e explosivos; em vez disso, eles podem criar e enviar vírus de computador através de uma linha telefônica, um cabo ou uma conexão sem fio.
- Em segundo lugar, o ciberterrorismo é mais anônimo do que os métodos terroristas tradicionais. Como muitos internautas, os terroristas usam apelidos *online* – "nomes na tela" – ou logam em um *site* como um usuário "convidado" não identificado, o que torna muito difícil para as agências de segurança e as forças policiais rastrearem a identidade real dos terroristas. E no ciberespaço não existem barreiras físicas, tais como postos de controle de navegação; também não existem fronteiras para cruzar e nem agentes da alfândega para trapacear.
- Em terceiro lugar, a variedade e o número de alvos são enormes. O ciberterrorista pode alvejar computadores e redes de computadores de governos, pessoas, serviços públicos, companhias aéreas privadas e assim por diante. O número e a complexidade dos alvos em potencial garante que os terroristas possam encontrar fraquezas e vulnerabilidades para explorar. Diversos estudos têm demonstrado que infraestruturas críticas, tais como redes de energia elétrica e serviços de emergência, são vulneráveis a um ataque ciberterrorista porque as infraestruturas e os sistemas de computador que as executam são muito complexos, tornando-se efetivamente impossível eliminar todos os pontos fracos nelas existentes.
- Em quarto lugar, o ciberterrorismo pode ser realizado remotamente, uma característica que é especialmente atraente para os terroristas. O ciberterrorismo exige menos treinamento físico, menos investimento psicológico, tem menos risco de mortalidade e menos viagens do que as formas convencionais de terrorismo, tornando-se mais fácil para organizações terroristas recrutar e reter seguidores.
- Em quinto lugar, como o vírus I LOVE YOU[51] demonstrou, o ciberterrorismo tem o potencial de afetar diretamente um número maior de pessoas do que os métodos terroristas tradicionais, gerando

[51] De acordo com o site da Microsoft, o vírus I LOVE YOU substitui e desorganiza nomes e extensões de arquivos e se autorreenvia para os destinatários existentes no catálogo de endereços do Outlook. Disponível em: <http://support.microsoft.com/kb/282832/pt-br>. Acesso em: 11 mar. 2010.

assim maior cobertura da mídia, que é basicamente o que os terroristas querem.[52] [Tradução livre]

Cibercrimes

Outra ameaça existente no ciberespaço são os chamados crimes cibernéticos. Conceituá-los é tarefa difícil, tendo em vista que a literatura diverge quanto à sua nomenclatura.

Uma definição mais geral, da Webopedia (2005),[53] nos diz:

> O cibercrime engloba qualquer ato criminoso relacionado com computadores e redes (chamados de "hacking"). Além disso, o crime cibernético também inclui crimes tradicionais realizados através da internet. Por exemplo, os crimes de ódio, de telemarketing e de fraude na internet, de roubo de identidade e de furtos de contas de cartão de crédito são considerados como crimes cibernéticos quando as atividades ilegais são cometidas com o uso de um computador e da internet. [Tradução livre]

Já Damásio de Jesus (apud Wendt, 2009:3) faz a seguinte distinção de crimes cibernéticos:

1. **Impróprios, comuns ou impuros**: o computador é um meio/instrumento. Realizado através do uso de um computador (furto mediante fraude ou com abuso de confiança, estelionato, falsos, crimes contra a honra etc.).
2. **Próprios, autênticos ou puros**: o computador/informação é o fim ou o objeto material. Contra os dados ou sistemas informáticos (dano, interceptação ilegítima, acesso ilegítimo, inserção de dados falsos em sistema de informações). A informática é o bem jurídico tutelado, ou seja, a segurança dos sistemas, a titularidade das informações, a integridade dos dados, das máquinas e dos periféricos.

Também Roque (2000 apud CRISPIN,[54] p. 12)[55] faz tal distinção, utilizando-se do termo "crimes de informática":

> crime de informática é a conduta definida em lei como crime em que o computador tiver sido utilizado com instrumento para a sua perpetração ou consistir em seu objeto material. Ao primeiro chamaremos de crime de informática impróprio ou comum, ao segundo de próprio ou autêntico.

---

[52] Disponível em: <http://www.usip.org/resources/cyberterrorism-how-real-threat>. Acesso em: 19 fev. 2010.

[53] Disponível em: <http://www.webopedia.com/TERM/C/cyber_crime.html>. Acesso em: 3 mar. 2010.

[54] Para saber mais sobre o dano informático, vide Crispin, p. 13-14. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/13020/12584>. Acesso em: 3 mar. 2010.

[55] Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/13020/12584>. Acesso em: 3 mar. 2010.

A "Convenção sobre o Cibercrime",[56] adotada pelo Conselho da Europa (2001:3-7 apud *Crimes Cibernéticos* – Manual Prático de Investigação do Ministério Público Federal – Procuradoria da República no Estado de São Paulo, 2006:6-7), obriga os Estados signatários a tipificar as seguintes infrações:

1. Infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos:
   a) acesso doloso e ilegal a um sistema de informática;
   b) interceptação ilegal de dados ou comunicações telemáticas;
   c) atentado à integridade dos dados (conduta própria de um subgrupo *hacker*, conhecido como *cracker*);
   d) atentado à integridade de um sistema;
   e) produção, comercialização, obtenção ou posse de aplicativos ou códigos de acesso que permitam a prática dos crimes acima indicados;
2. Infrações informáticas:
   a) falsificação de dados;
   b) estelionatos eletrônicos (*v.g.*, os *phishing scams*);
3. Infrações relativas ao conteúdo:
   a) pornografia infantil (produção, oferta, procura, transmissão e posse de fotografias ou imagens realistas de menores ou de pessoas que aparecem como menores, em comportamento sexual explícito);
   b) racismo e xenofobia (difusão de imagens, ideias ou teorias que preconizem ou incentivem o ódio, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica; injúria e ameaça qualificadas pela motivação racista ou xenófoba; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade);[57]

Santos (2008:9 e 12, grifos do autor) também elenca alguns crimes cibernéticos:

> Dentre as práticas criminosas mais comuns podemos listar: furto de dados, estelionato, clonagem de cartões, injúria, calúnia, difamação,[58] apologia ao

[56] Disponível em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf>. Acesso em: 6 mar. 2010.

[57] A repressão aos crimes de racismo e xenofobia praticados por intermédio de um sistema de informática está prevista no Protocolo Adicional à Convenção sobre o Cibercrime, de 30 de jan. de 2003. Disponível em: <http://conventions.coe.int/Treaty/EN/Treaties/Html/189.htm>. Acesso em: 6 mar. 2010.

[58] Crimes de injúria, calúnia e difamação podem ser cometidos no ciberespaço através da prática de *cyberbullying* (intimidação virtual). Para saber mais sobre *cyberbulling* visite o *website* Cyberbulling.org disponível em: <http://www.cyberbullying.org/>. Acesso em: 19 mar. 2010 e o Portal do Fórum

> racismo, homofobia, pedofilia, [...] vandalismo informático (*cyberpunk*), terrorismo, rufianismo, conspirações criminosas, tráfico de substâncias entorpecentes, crimes contra a propriedade intelectual (como pirataria de informação, falsificação e contrafação), crimes de lavagem de dinheiro, evasão fiscal, inserção de dados falsos em sistemas de informações, modificação ou alteração não autorizada de sistema de informações, interceptação de comunicações em sistema de informática, fraudes (dos mais variados tipos). [...] **O roubo de identidades via internet, em especial, é apontado como um dos crimes emergentes do século XXI**. Tipicamente associado a fraudes com cartões de crédito ou a extravios de correspondências, esse tipo de delito acontece agora predominantemente na *web*. Os métodos mais comuns empregados com esse fim atendem pelos nomes de "phishing" (mensagens que induzem o usuário a clicar em um *link* que desencadeia a ação de um *software* que infecta a máquina e rouba informações contidas nela) e "pharming" (modificações no sistema de endereços DNS, de Domain Name System, levando o internauta a uma página de risco, que não corresponde àquela que havia sido digitada).

Wingfield e Michael (2004:3) fazem as seguintes considerações a respeito dos crimes de computador:

> Crimes de computador se dividem em duas grandes categorias: aqueles que têm um alvo no ciberespaço e aqueles que meramente empregam computadores como um meio para um fim penal mais tradicional. O primeiro tipo inclui ataques à confidencialidade, integridade e disponibilidade de informações ou sistemas. Esses crimes incluem também o roubo de informações armazenadas em computadores ou serviços baseados no ciberespaço. Invasões de computador deste tipo incluem: (i) Danificações/estrago de sistemas de computadores; (ii) Invasões; (iii) Ameaças de causar danos; (iv) Atentados contra a integridade e confidencialidade de uma rede. O roubo de informações geralmente envolve uma destas três categorias: governo (áreas militar, legal e judicial), informações de negócios (segredos comerciais ou informações confidenciais, tais como planos de negócios), e informações financeiras (números de contas bancárias e transferência eletrônica de fundos). Os roubos de serviços podem incluir "phreaking" (penetração em um sistema de telefonia para roubar serviços de chamada de longa distância), roubo de senhas e criação de contas que dão acesso à distribuição de programas (softwares) ilegalmente. O segundo tipo, no qual o computador é um instrumento para o crime, inclui jogos de azar, pornografia infantil, espionagem, fraude no mercado de ações, fraude bancária e a pirataria de direitos autorais. [Tradução livre]

11.4. Principais Desafios da Inteligência no Ciberespaço

> *The course of cyberwar depends on the systems being targeted, which in turn will depend on which ones have what vulnerabilities and to what extent exploiting them can discomfort the state.* (Martin C. Libicki).[59]

Cidadania e Paz nas Escolas, disponível em: <http://www.ssp.se.gov.br/cidadania/modules/tinyd0/index.php?id=18>. Acesso em: 19 mar. 2010.

[59] "O curso da ciberguerra depende dos sistemas que estão sendo almejados que, por sua vez, dependem de quem tem quais vulnerabilidades e até que ponto explorá-las pode trazer um desconforto para o Estado" (Martin C. Libicki).

Alguns aspectos complexos relacionados aos ataques cibernéticos remetem à sua origem e natureza (HILDRETH, 2001:2). O anonimato dos ataques e o desconhecimento da intensidade do dano que pretendem causar dificultam sua repressão.

Embora muitos ataques cibernéticos possam ser detectados em tempo relativamente suficiente para que alguns danos sejam evitados,[60] nem sempre é possível avaliar a dimensão dos danos sofridos (HILDRETH, 2001:2). De acordo com Allen e Demchak (2004:53), o "custo de um ataque cibernético é geralmente maior para os alvos comerciais do que para os sites governamentais". E continua: "Quando um *site* governamental fica fora do ar ou é desconfigurado, a nação talvez seja um pouco humilhada. No entanto, quando o *site* de uma companhia sai do ar, ela perde lucro".

Além da perda instantânea de lucros, as empresas correm o risco de sofrer "uma prolongada desconfiança por parte de seus clientes, referente à segurança das transações feitas pela rede". (GENTILE, 2000 apud ALLEN e DEMCHAK, 2004:53). As proporções que tal insegurança pode alcançar são de difícil mensuração.

Delio (2001 apud ALLEN e DEMCHAK, 2004:53) reconhece: "Apesar de os *sites* comerciais terem interesse em se defender contra ataques cibernéticos", a busca por uma melhor relação custo-benefício "faz com que a maioria das companhias ignore as vulnerabilidades da rede até que seja vítima de um ataque pelos *hackers*".[61]

Dessa forma, Allen e Demchak (2004:53) sugerem: "[...] existe uma necessidade de criar incentivos maiores para que os negócios obtenham maior segurança no espaço cibernético, e deveriam existir penalidades para aqueles que não estiverem seguros em uma determinada data".

"A parceria público-privada é um componente chave da nossa estratégia para assegurar o ciberespaço", afirma o documento Estratégia Nacional para Assegurar o Ciberespaço (*National Strategy to Secure Cyberspace*), de fevereiro de 2003.[62]

Em relação ao anonimato, Sampaio (2001:16) também nos chama a atenção para a possibilidade de "terceirização" da guerra, ou seja, um país inimigo pode fazer uso de "*hackers* que podem estar já trabalhando para o crime internacional organizado, seja no tráfico de drogas, de armas, de prostituição, de elementos

---

[60] Cf. *Hackers: Outlaws and Angels*. Produzido por September Films para TLC Life Unscripted. Versão [puxando.com] Hackers: Criminosos e Anjos – Dvdrip Legendado. Acesso em: 2009.

[61] Parte traduzida pela autora do texto original de Allen e Demchak (2004:54) denominado "The Palestinian-Israeli Cyberwar", disponível em: <http://findarticles.com/p/articles/mi_m0PBZ/is_2_83/ai_106732244/>. Acesso em: 19 mar. 2010.

[62] Parte retirada do prefácio escrito por James M. Smith, diretor, na época, do INSS (Institute for National Security Studies).

proibidos", com o objetivo de evitar qualquer forma de rastreamento da origem do ataque. Nesse sentido:

> A entrada de motins de rua, a exploração de fricções raciais ou étnicas dentro da sociedade, pela exploração por agentes plantados, boatos e desinformação, levaria ao caos urbano (guerrilha urbana), mas os elementos em luta seriam locais e seria difícil dizer que a ordem veio de fora [SAMPAIO, 2001:17].

Hildreth (2001:5) ainda levanta as seguintes questões:

> Sistemas de computador no Pentágono e em outras instalações militares são "atacados" milhares de vezes a cada ano. Mas podemos considerar isto uma guerra se muitos ou a maioria desses ataques vierem de adolescentes aqui nos Estados Unidos, ou mesmo do estrangeiro? Será que os militares sequer sabem com quantos desses ataques eles devem realmente se preocupar? A tentativa por parte de um país estrangeiro de coletar segredos militares através da internet ou modem é um ato de guerra para o qual os Estados Unidos deverão estar preparados para responder coercitivamente? Os Estados Unidos devem responder em espécie, fazendo guerra no ciberespaço? O que constitui a vitória no ciberespaço? A espionagem é tradicionalmente considerada outra coisa, algo menos significante do que uma guerra? Se outra nação sistematicamente ataca as redes empresariais dos EUA para roubar segredos comerciais em prol de seus próprios interesses econômicos ou para passar os segredos adiante para suas próprias empresas para obter vantagem competitiva, isto é considerado guerra? Será que a resposta muda se a nação que está atacando é uma aliada dos EUA, ou amiga? [Tradução livre]

Também em relação à atuação dos *hackers*, Sampaio (2001:7, grifo do autor) questiona: "**como distinguir uma ação intencional, de ciberguerra, de um acidente, de um problema natural (manchas solares, por ex.) ou de uma ação de um particular, até mesmo de um paranóico**"?

Libicki (2009:23), ao tentar definir ciberataque, discute se espionagem na rede é considerada, ou não, um ataque cibernético. De acordo com o autor, como o espião não priva o usuário do completo uso da máquina e rouba segredos, mas não traz nenhuma outra consequência além desta, sua atuação não seria considerada um ataque cibernético. Além disso, o autor afirma que atos de espionagem são praticados por todos os governos, fazendo com que a criação de políticas de proibição ou retaliação de tal prática se torne inviável (LIBICKI, 2009:24). Ele continua:

> Aqueles que tentam estabelecer políticas de dissuasão para evitar que outros façam o que eles mesmos fazem, se revelam idiotas ou hipócritas – a menos que sejam tão poderosos a ponto de não precisarem de tais práticas. É duvidoso que até mesmo os Estados Unidos se qualifiquem como sendo tão poderosos. Uma postura de intimidação contra a CNE [63] [espionagem] seria vista como hipócrita e provavelmente não confiável – na verdade, inconcebível. [Tradução livre]

[63] Para saber um pouco mais sobre CNE veja LIBICKI (2009:15).

Ainda tentando definir a natureza dos ciberataques e a quem eles remetem responsabilidade, Hildreth (2001:6) faz uma diferenciação entre os ataques que se caracterizam como atividades de ciberguerra (patrocinados por nações-estados) e vários outros ataques que ocorrem no ciberespaço todos os dias (HILDRETH, 2001:6). A caracterização correta dos ataques determina quem será o responsável legal para lidar com a situação (Os serviços de inteligência? A polícia propriamente dita? As instituições governamentais de segurança da informação?)

Explica Hildreth (2001:6):

> Estes outros ataques ou intrusões também são tentativas não autorizadas de acesso a computadores, sistemas controlados por computadores ou redes. Tais atividades podem variar de uma simples invasão a um sistema para examiná-lo pelo desafio, a emoção ou interesse; de adentrar um sistema por vingança, para roubar informações, causar embaraços, extorquir dinheiro, a causar danos locais determinados a computadores ou a uma infraestrutura muito maior, tais como os sistemas de abastecimento de água e energia. Esses ataques cibernéticos são considerados ataques de *hackers*, má conduta no ciberespaço, hooliganismo cibernético (comportamento destrutivo e desregrado), roubos pessoais ou corporativos, vingança, espionagem, ou atividades do crime organizado (estrangeiras ou domésticas). O universo para a sua resolução pode estar na aplicação da lei e nos sistemas judiciais, e, ainda, num remédio legislativo, onde seja necessário. [Tradução livre]

A ciberguerra periférica também é outra preocupação: quem podem ser nossos futuros adversários? (SAMPAIO, 2001:17). Estamos sujeitos a receber ataques de nações de quem não somos diretamente "inimigos", mas que são adversárias daquelas com as quais nos aliamos? As alianças e iniciativas diplomáticas que os governos realizam agora certamente repercutirão a favor ou contra suas nações futuramente, fazendo com que a presença dos serviços de inteligência nesse âmbito se torne bastante necessária.

Outro ponto discutido é a possibilidade de o computador ser considerado uma "arma" e o "hacker" um combatente. Para Sampaio, o computador não é uma arma, mas o que ele pode "efetuar" o enquadra nessa categoria, salientando que "muito mais provavelmente e quase certamente, a ação de guerra por meio de computadores pode configurar uma utilização dos mesmos como arma de destruição de massas" (SAMPAIO, 2001:7-8).

Relativamente ao Brasil, Sampaio (2001:9, grifos do autor) sugere, entre outras, a criação de um órgão de inteligência especializado como uma alternativa para minimizar as inseguranças:

> A necessidade de inteligência, monitoração e quadros altamente preparados se faz, portanto, mais do que nunca, necessários. [*sic*.] **Ainda assim**, nada impedirá, no futuro, que o quadro de um acidente não sirva, se monitorado devidamente, como cobertura para o desencadeamento de ações de ciberguerra. [...] Marchamos, portanto, para um ambiente de alta tecnologia e que implica em conhecer muito bem e em tempo real tanto o comportamento

> do Sol, em seus ciclos explosivos, como as modas dos terroristas individuais, que atos estão praticando comumente e o que podem preparar. Assim, a **infiltração de contra-hackers** se torna outra necessidade dos órgãos de governo, infiltração esta que deve ser autorizada por alguma medida judicial e ser centralizada em um só serviço de inteligência, sem o que de nada servirá, pela competição, dispersão e demora em reunir informações, que as diversas agências, historicamente, sempre apresentaram. **A necessidade de contar com psicólogos comportamentais, sociólogos, peritos em computadores e planejadores de segurança/militares se apresenta como um impositivo imediato para os governos e a alta administração estratégico-político-militar.**

Em relação aos cibercrimes, as questões (domésticas e internacionais) giram em torno de conflitos de competência para processá-los, problemas para a fixação do local do crime, responsabilidade dos provedores de internet no armazenamento e disponibilização de informações, atualização legislativa (WENDT, 2009:6) e dificuldades na produção de provas e na identificação de criminosos (SANTOS, 2008:2).

Aldrich (2000:vii, tradução livre), ao analisar "questões conceituais e jurisdicionais, interesses constitucionais e legais, bem como a necessidade e a conveniência da existência de um tratado internacional abordando o ciberterrorismo e o cibercrime", explica que são vários os desafios das nações ao elaborar tratados abordando tais temas: (i) É difícil definir o seu conteúdo, uma vez que os termos "guerra informacional", "terrorismo informacional" e "crimes cibernéticos" são de difícil conceituação e, às vezes, se confundem; (ii) Estabelecer regras de jurisdição para facilitar extradições e evitar duplos julgamentos é tarefa complexa, uma vez que envolve legislações de vários países; (iii) Também é trabalhoso criar regras que agilizem a produção legal de provas e sua utilização por todos os países membros (ALDRICH, 2000:ix, x, xi).

A Convenção sobre o Cibercrime, também denominada Convenção de Budapeste ou Convenção do Conselho Europeu sobre o Cibercrime (DANTAS, 2009:25), "foi o primeiro acordo multilateral sobre crime cibernético firmado entre países europeus em 23 de novembro de 2001, em Budapeste, Hungria, sem a participação do Brasil".[64] De acordo com a minuta explicativa do relatório, item 16:

> A Convenção tem por objeto principal (1) a harmonização dos elementos relativos a infrações no contexto do direito penal substantivo de âmbito nacional e das disposições conexas na área de cibercriminalidade; (2) a definição, ao abrigo do código de processo penal interno, dos poderes necessários para investigar e intentar ações penais relativamente a tais infrações, assim como outras infracções cometidas por meio de um sistema informático ou às provas com elas relacionadas e existentes sob a forma eletrônica; (3) a implantação de um regime rápido e eficaz de cooperação internacional.

[64] Disponível em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf>. Acesso em: 19 mar. 2010.

Assim como explica Dantas (2009:25-26):

> O acordo entrou em vigor em 1º de julho de 2004, depois que cinco países o ratificaram, sendo três integrantes do Conselho Europeu. Quarenta e sete países já ratificaram o tratado. Os EUA são o único país de fora do Conselho Europeu que o ratificou, em 29 de setembro de 2006. O Japão e o Canadá o assinaram.

A uniformização da legislação internacional centrada na convenção ainda é bastante limitada e precisa ter a participação de um maior número de países, no âmbito das Nações Unidas, para poder potencializar suas chances de sucesso. Além disso, precisa sofrer adição de outras modalidades de delitos cibernéticos.

A convenção define crime cibernético e permite que as polícias de cada país cooperem nas investigações desses delitos, podendo até mesmo prender suspeitos de crimes cometidos fora de seu território. Críticos do documento questionam os poderes atribuídos à polícia, que, segundo eles, poderiam comprometer a preservação da liberdade na internet. Muitos países já dispõem de legislações que permitem que organismos de segurança monitorem o espaço cibernético, mas especialistas temem que esses poderes sejam ampliados nos países que adotarem o tratado.

"Com a intenção de, posteriormente, harmonizar o combate ao ciberterrorismo no continente," a Convenção de Budapeste já adicionou "três novos delitos cibernéticos: propaganda, recrutamento e treinamento de terroristas" (DANTAS, 2009:27).

Apesar de não ter assinado a Convenção de Budapeste, o Brasil é um dos países que fez parte da agenda de trabalhos do Projeto em Cibercrimes (Fase 1) do Conselho Europeu, que teve seu início em setembro de 2006 e conclusão em fevereiro de 2009.[65] O projeto teve por objetivo "promover a ampla implementação da Convenção sobre o Cibercrime (ETS 185) e seu Protocolo sobre Xenofobia e Racismo (ETS 189)". Um exemplo das atividades que o projeto apoiou foi o evento ICCyber 2007: Conferência Internacional em Cibercrime, que ocorreu entre os dias 26 e 28 de setembro de 2007 na cidade de São Paulo.[66]

O Projeto Global em Cibercrimes (Fase 2)[67] para continuar a implementação da Convenção e seu protocolo teve início em março de 2009 e pretende obter resultados nas seguintes áreas:

---

[65] Disponível em: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/projectcyber_en.asp>. Acesso em: 16 mar. 2010.

[66] O ICCyber é o maior evento sobre perícia em crimes cibernéticos da América Latina. Em sua sexta edição, o ICCyber 2009 contou com especialistas e empresas de vários países e trouxe as últimas novidades e metodologias de combate aos crimes cibernéticos. Disponível em: <http://www.iccyber.org/2009/>. Acesso em: 16 mar. 2010.

[67] Disponível em: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/projectcyber_en.asp>. Acesso em: 16 mar. 2010.

> legislação e políticas; cooperação internacional; aplicação da lei – a cooperação de provedores de serviço na investigação do cibercrime; investigações financeiras; treinamento de juízes e procuradores; proteção de dados e privacidade; exploração de crianças e tráfico de seres humanos. [Tradução livre]

De acordo com Lupion (2011):

> Durante o 12º Congresso das Nações Unidas sobre a Prevenção ao Crime e à Justiça Criminal, realizado em Salvador em abril do ano passado, o Brasil propôs a construção de uma nova convenção para substituir a de Budapeste, e foi escolhido para liderar o processo. A primeira reunião do grupo de trabalho ocorreu em fevereiro, na sede das Organizações das Nações Unidas em Viena, na Áustria.

Como explica Santos (2008:12), "não podemos afirmar [...] que não existe nenhum tipo de regulamentação no que tange a criminalidade informática no Brasil. Algumas condutas podem ser subsumidas a tipos penais já existentes [...]":

> Merece destaque, assim, no plano de edição de normas, a Lei 9.296, de 24 de junho de 1996, que pune o indivíduo que realiza interceptação de comunicações em sistema de informática, impondo reprimenda de reclusão de dois a quatro anos, assim como os artigos 313-A e 313-B, incluídos no Código Penal, pela Lei 9.983, de 14 de julho de 2000, que versam, respectivamente, sobre a inserção de dados falsos em sistema de informações e modificação ou alteração não autorizada de sistema de informações. Por fim, o art. 241 do Estatuto da Criança e do Adolescente que trata da pornografia infantil na internet: art. 214 – Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.

Entretanto, afirma Santos (2008:12), "nem todas as práticas se enquadram perfeitamente no que já temos e, tendo em vista o princípio da legalidade, que norteia o Direito Penal pátrio, torna-se, muitas vezes, impossível uma punição pelos crimes cometidos em ambiente virtual".

Diante desse contexto, em junho de 2008, o substitutivo aos PLS 76/2000, PLS 137/2000 e PLC 89/2003, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei nº 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei nº 7.716, de 5 de janeiro de 1989, e a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 10.446, de 8 de maio de 2002, foi aprovado pela Comissão de Assuntos Econômicos (CAE) e segue em tramitação (DANTAS, 2009:26), com o objetivo de tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares.[68] Tais projetos receberam grande influência da Convenção Europeia sobre o Cibercrime (SANTOS, 2008:13).

[68] Disponível em: <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em: 16 mar. 2010.

O substitutivo prevê como crimes, entre outros: a) acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado; b) obtenção, transferência ou fornecimento não autorizado de dado ou informação; c) divulgação ou utilização indevida de informações e dados pessoais; d) interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático, dispositivo de comunicação, rede de computadores ou sistema informatizado etc.

Além de trabalhar na atualização legislativa, o Brasil possui vários "Projetos Governamentais e Empresariais voltados à tecnologia na era da Sociedade da Informação". Um exemplo é o "Sistema de Rastreamento de Exploração Infantil (*CETS – Child Exploitation Tracking System*) – fruto de uma aliança entre a Microsoft do Brasil e a Polícia Federal", no combate à pedofilia no Brasil (SANTOS, 2008:5). O surgimento da Nota Fiscal Eletrônica (NF-E) também é outra tentativa de evitar que ocorra o "sequestro, furto, adulteração, danificação, controle ou geração da perda proposital de informações confidenciais do fisco, acarretando na quebra do sigilo fiscal do contribuinte" (SANTOS, 2006 apud SANTOS, 2008:4).

Também na tentativa de estabelecer "procedimentos básicos de coleta, preservação da integridade e análise das provas e de identificação dos autores" dos crimes cibernéticos, o grupo de combate aos crimes cibernéticos da Procuradoria da República no Estado de SP (Ministério Público Federal) elaborou um "Manual Prático de Investigação" em 2006, depois de entender que

> a aplicação da lei penal em relação a esses crimes depende da aquisição de conhecimentos mínimos de informática pelos operadores do direito, [bem como] de uma postura menos burocrática [...], já que o tempo da internet é muitíssimo mais rápido do que o tempo dos órgãos envolvidos na persecução penal [*Crimes cibernéticos*: Manual Prático de Investigação. Apresentação].

Além de auxiliar na atualização legislativa e na elaboração de projetos e políticas contra o cibercrime, os serviços de inteligência policiais em todo o mundo têm tomado a iniciativa de convergir seus bancos de dados, no intuito de aumentar a cooperação global no combate a crimes que afetam mais de uma nação (BIGNAMI, 2007:663).

No que tange ao ciberterrorismo, os questionamentos são relativos ao grau de ameaça que os ataques terroristas representam no ciberespaço.

De acordo com Dantas (2009:24), para muitos especialistas [69] em áreas de inteligência de estado,

[69] No Brasil, o "acompanhamento de manifestações do terrorismo de bases científica ou tecnológica integra a relação de assuntos acompanhados sob ótica analítica e estratégica pela Abin – especificamente, por meio do Departamento de Contraterrorismo –, com a finalidade de prevenir o terrorismo e seu financiamento, no Brasil ou contra interesses brasileiros no exterior" (DANTAS, 2009:24).

> é pouco provável que a Al-Qaeda ou qualquer outra organização terrorista conhecida tenha capacidade de realizar ações que demandem emprego de recursos de alta tecnologia. Entretanto, há concordância de que fatores críticos para a continuidade da al Qaeda incluem planejamento operacional aprimorado; ênfase no sigilo das informações; uso planejado de técnicas de comunicação e propaganda; exploração de lacunas legais, além de criatividade e inovação na utilização de táticas convencionais de ataque.

Lewis (2002 apud WEIMANN, 2004:9) afirma que as nações são mais fortes do que os primeiros analistas em ciberterrorismo e ciberguerra acreditavam que eram, possuindo sistemas de infraestrutura mais flexíveis e adequados para o rápido restabelecimento dos serviços.

Weimann (2004:9, tradução livre) também afirma que "muitos especialistas em segurança computacional não acreditam que seja possível utilizar a internet para causar mortes em larga escala". Entretanto, o sistema de controle de tráfego aéreo, "os sistemas de metrô, as linhas de gasodutos, os oleodutos, as redes elétricas, os sistemas de comunicação, as represas de água e os serviços públicos" podem ser atacados para causar destruição em massa, gerando preocupações (WEIMANN, 2004:9, tradução livre).

Weimann (2004:10, tradução livre) afirma que

> para avaliar a ameaça potencial de ciberterrorismo, especialistas como Denning sugerem que duas questões sejam feitas: 1. Existem alvos que são vulneráveis a ataques cibernéticos? 2. Existem atores [ciberterroristas] com capacidade e motivação suficiente para realizar tais ataques? A resposta à primeira pergunta é sim: os sistemas de infraestruturas críticas são complexos e, portanto, estão "condenados" a conter deficiências que possam ser exploradas, e até sistemas que parecem "endurecidos" para manipulação por quem está de fora podem ser acessados por membros, que agem isoladamente ou em conjunto com terroristas, podendo causar danos consideráveis.

A resposta à segunda pergunta é um pouco mais complexa. Green (apud WEIMANN, 2004:10) acredita que poucos empregados dentro de uma empresa têm conhecimentos técnicos específicos para controlar sistemas mais complexos de computador. Ainda assim, completa Weimann (2004:10), mesmo existindo a possibilidade de esses empregados ou ex-empregados serem recrutados por grupos terroristas, o grau de danos que poderiam causar seria limitado (GREEN apud WEIMANN, 2004:10, tradução livre),

> uma vez que todos os empregados de empresas que cuidam de redes elétricas, utilitários de petróleo e gás, e comunicações são bem treinados para lidar com os estragos causados por desastres naturais, como enchentes, e estão igualmente preparados para lidar com problemas que decorrem da ação humana.

Além disso, Denning (apud WEIMANN, 2004:10) faz referência a um estudo que demonstrou que os terroristas, em geral, carecem de recursos e capital

humano necessário para promover ataques em proporções consideravelmente catastróficas.[70]

Por outro lado, embora os especialistas acreditem que ataques ciberterroristas que causem danos maiores estejam longe de acontecer, o uso da internet por terroristas é recurso valioso para se fazer uso de uma técnica essencial para o terrorismo: a propaganda. Explica Dantas (2009:22):

> A propaganda é técnica essencial de que se valem organizações extremistas, especialmente com a finalidade de atrair seguidores. Por décadas, material impresso, vídeos com operações e treinamentos, discursos, história e realizações têm estado à disposição de interessados, em redes de distribuição difusas, clandestinas e de acesso limitado. Entretanto, no século XXI, pessoa interessada em conhecer, apoiar ou aderir a esse tipo de organização pode individualmente e de maneira aberta se valer da internet e obter a informação desejada, tanto por meio de páginas estáticas quanto interativas, como salas e fóruns de discussão. Ao unir o efeito de demonstração do fanatismo do século XII com o alcance global da comunicação do século XXI, as palavras "terrorismo" e "cibernética" fundem-se e geram nova expressão, dimensão e conceito – terrorismo cibernético ou ciberterrorismo –, que capitaliza efeitos psicológicos decorrentes do temor do desconhecido e da imprevisibilidade do ato, embasados na dependência das sociedades nas redes de informação.

Numa tentativa de promover atividades de coordenação e cooperação no mundo todo contra o terrorismo, em 8 de setembro de 2006 foi adotada a Estratégia Global das Nações Unidas de Contraterrorismo (DANTAS, 2009:23):

> Atividades de coordenação e cooperação da estratégia incluem tarefas relacionadas a: facilitar sua implementação; fazer frente a ações radicais e extremistas que possam resultar em atos terroristas; impedir o uso da internet com finalidades terroristas; proteger os direitos humanos, mesmo ao se combater o terrorismo; proteger e fortalecer alvos vulneráveis; apoiar e destacar as vítimas do terrorismo; e combater o financiamento do terrorismo. No que se refere à utilização da internet com finalidades terroristas, os Estados-membros acordaram que a estratégia teria por objetivo identificar e proporcionar o debate com atores públicos e privados sobre o assunto e identificar maneiras possíveis de combater essa ação, nos níveis global, regional e sub-regional. Ainda que se tenha incluído tópico sobre a prevenção ao uso criminal, é escasso o conhecimento sobre a ameaça representada pela utilização da internet por terroristas, que a têm utilizado para recrutar adeptos, arrecadar fundos e estabelecer ações de propaganda, em escala global (DANTAS, 2009:23).[71]

---

[70] Denominado "Cyberterror: Prospects and Implications" (Ciberterror: Perspectivas e Implicações), o estudo foi realizado pelo Center for the Study of Terrorism and Irregular Warfare da Escola de Pós-graduação Naval (NPS) em Monterrey, Califórnia. Esse estudo analisou "cinco tipos de grupos terroristas: religioso, New Age (Nova Era), etno-nacionalista separatista, revolucionário, e da extrema-direita. Desses, apenas os grupos religiosos foram julgados como prováveis atores a procurar obter capacidade suficiente para causar danos em massa". O estudo também determinou que grupos *hacker* "são psicologicamente e organizacionalmente fracos para se adequar ao ciberterrorismo, e qualquer perturbação em massa de infraestruturas de informação seria contrária ao seu próprio interesse." (DENNING apud WEIMANN, 2004:10). (Tradução livre)

[71] UN. The United Nations Global Counter-Terrorism Strategy. 8 set. 2006. Disponível em: <http://www.un.org/terrorism/strategy-counter-terrorism.shtml>. Acesso em: 18 mar. 2010.

Em relação ao papel do Brasil na luta contra o terrorismo, um recente estudo realizado por Souza (2009:29, tradução livre) aponta que "os brasileiros, em geral, e a maioria das autoridades brasileiras, consideram o terrorismo como uma ameaça exógena", ou seja, "geograficamente associada com o Oriente Médio, tendo, como alvos, Israel e os Estados Unidos da América (US)".[72]

Entretanto, afirma Souza (2009:29, tradução livre), "embora o terrorismo internacional ainda não tenha ocorrido no Brasil, os cidadãos brasileiros têm sido suas vítimas indiretas", quando inúmeros brasileiros são mortos em ataques terroristas que ocorrem em todo o mundo. Além disso, Vidigal (2004, v. 2:25 apud SOUZA, 2009:31) também ressalta que a Amazônia, pela grande relevância estratégica que tem para o Brasil, pode ser considerada uma grande vulnerabilidade brasileira, principalmente em relação ao conflito existente entre as Forças Armadas Colombianas e as Forças Armadas Revolucionárias da Colômbia (FARC).

Cooperação internacional, ratificação e assinatura de convenções internacionais sobre terrorismo e a adaptação de leis nacionais a estes instrumentos têm sido a política que o Brasil vem adotando no combate ao terrorismo (SOUZA, 2009:32). Tal postura, esclarece Cepik (2004:58 apud SOUZA, 2009:34, tradução livre), se deve ao fato de que, "nos debates sobre assuntos de segurança internacional no Brasil, existe uma persistente tendência a restringir as questões a aspectos normativos e jurídicos".

Souza (2009:33-34) sugere que o Brasil tenha "uma estratégia nacional e um melhor aparato institucional para combater o terrorismo internacional" e aponta que a inércia brasileira em criar tais alternativas o afeta indiretamente, dificultando a obtenção de um assento permanente no Conselho de Segurança da ONU (UNSC – United Nations Security Council) e prejudicando as relações bilaterais e multilaterais que possui, principalmente com os EUA, a UE e alguns membros do Mercosul.

No entanto, a recente escolha do país para sediar a Copa do Mundo em 2014 e as Olimpíadas em 2016 (Rio de Janeiro) tem aumentado o interesse, principalmente da comunidade de inteligência de segurança pública, para tal tema, a fim de evitar que atos de terrorismo ocorram durante os jogos.[73]

---

[72] Em interessante consulta à ferramenta do Google denominada "Insights para pesquisa", podemos perceber que os termos "cyber terrorism" e "cyberterrorism" são mais pesquisados por pessoas na Índia, nos Estados Unidos e no Reino Unido. Em relação ao Brasil, a ferramenta acusa que não há volume de pesquisas suficiente para exibir os gráficos. Disponível em: <http://www.google.com/insights/search/#q=cyber%20terrorism%2Ccyberterrorism&cmpt=q>. Acesso em: 18 mar. 2010.

[73] "I Seminário Regional de Inteligência de Segurança Pública – Região Sudeste", que ocorreu em Belo Horizonte/MG, nos dias 9, 10 e 11 de setembro de 2009.

Trazendo tal estudo para o campo cibernético, junto com as medidas que devem ser adotadas para que se tenha um efetivo combate ao terrorismo no Brasil, também devem ser aperfeiçoados os mecanismos técnicos e legais que previnem e reprimem o uso da internet para fins terroristas.

Censura, direito de privacidade e controle de tráfego na internet

> *How does the right to privacy fare in today's borderless world of national security threats and networked spy agencies*? Bignami[74]

A privacidade e a censura são dois assuntos muito discutidos quando se fala em tentar estabelecer parâmetros legais nacionais e internacionais de controle de tráfego de informações na internet, com o objetivo de evitar "surpresas" desagradáveis, como a atuação de *hackers*.[75,76]

De acordo com Markoff e Kamer (2009) em reportagem ao *New York Times*, negociações têm sido feitas entre a Rússia e os Estados Unidos em torno da elaboração de um tratado sobre o ciberespaço. A Rússia sugere a elaboração de um tratado nos mesmos moldes dos tratados sobre armas químicas, que persuadiram muitas nações a não estocar tais armas. A proposta russa também sugere a aplicação de leis humanitárias, no intuito de banir ataques a não combatentes e diminuir a probabilidade do seu anonimato, promovendo a existência de um controle internacional maior dos governos sob o tráfego de informações na internet. Os argumentos norte-americanos são totalmente opostos. Os Estados Unidos são resistentes à censura da internet, sustentando que tal ato proporcionaria um fortalecimento de respaldo às ações de regimes totalitários. Também acreditam que um tratado nesses moldes seja desnecessário, uma vez que uma melhora na cooperação internacional para uma efetiva aplicação das leis já existentes seria suficiente (MARKOFF e KAMER, 2009).

Quando se trata de estabelecer políticas de segurança, o governo brasileiro tem adotado várias práticas de controle de tráfico do ambiente cibernético que esteja delimitado ao âmbito de atuação dos órgãos públicos. Ao bloquear o acesso a *e-mails* pessoais ou a redes sociais de relacionamento, como o Orkut e o Facebook, e proibir a abertura de certos arquivos de extensão duvidosa, como

---

74 Como fica o direito de privacidade nesse mundo atual sem fronteiras, de ameaças à segurança nacional e agências de espionagem interligadas?" Bignami.

75 "'Dados de tráfego' significa todos os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data, o tamanho, a duração ou o tipo do serviço subjacente" (Convenção sobre o Cibercrime, 2003, art. 1, alínea d).

76 U.S. and Russia Differ on a Treaty for Cyberspace. *New York Times*, 28 Jun. 2009. Disponível em: <http://www.nytimes.com/2009/06/28/world/28cyber.html>. Acesso em: 1 mar. 2010.

".scr", ".exe" e "cmd.bat", em computadores dentro de repartições públicas, o departamento de cibersegurança estaria evitando o processamento de ataques.[77]

De acordo com Bezerra (2009):

> Em alguns países totalitários, como China e Irã, já há uma "guerra cibernética" em curso, entre o governo que tenta bloquear o acesso livre à internet e grupos de dissidentes com suas ferramentas para burlar os sistemas de controle. É uma situação diferente, porém o motivo da censura é político. Uma preocupação dos países ocidentais é impedir que a internet seja usada para coordenar e sincronizar ações terroristas "físicas". Porém aqui já entramos em outra discussão: como prevenir o mau uso sem atingir a privacidade.

Nesse sentido, explica Bignami (2007:663), por mais que as nações sejam "amigas", nem todos os governos operam dentro de um sistema institucional suficientemente estável e democrático, carecendo de uma fiscalização mais efetiva, principalmente em relação aos direitos humanos.

Dessa forma, verifica-se que o estabelecimento de normas de controle de tráfego internacional é bastante complexo: como a monitoração do ciberespaço deve ocorrer de forma a não violar as mínimas expectativas de privacidade de cada indivíduo ou organização? (WINGFIELD e MICHAEL, 2004:4) O que pode ser objeto de monitoramento? Que parâmetros de privacidade seriam adotados? (BIGNAMI, 2007:680-684). O ciberespaço nacional e o estrangeiro podem ser monitorados da mesma forma? A soberania dos Estados estaria sendo respeitada?

Acesso a fontes e cooperação entre as agências de inteligência

Para o setor de inteligência, a explosão informacional caracterizou-se por mudanças significativas nas técnicas de coleta e análise de informações, uma vez que o acesso à informação (principalmente a ostensiva) aumentou drasticamente com a intensa utilização do ciberespaço (DCAF Backgrounder, 03/2008:3).[78]

De acordo com DCAF Backgrounder (03/2008:3-4), a revolução da informação:

(i) alterou as relações entre analistas individuais e grupos de análise no setor de inteligência, enquanto novos padrões de tecnologia ampliaram

[77] XXI Seminário de Segurança da Informação e Comunicações (SEMSIC-MG) promovido pelo GSIPR/DSIC, realizado nos dias 23 e 24 de novembro de 2009, na cidade de Belo Horizonte/MG.

[78] Inteligência de fontes ostensivas ou Osint (Open Sources Intelligence), para Cepik (2003:51), "consiste na obtenção legal de documentos oficiais sem restrições de segurança, da observação direta e não-clandestina dos aspectos políticos, militares e econômicos da vida interna de outros países ou alvos, do monitoramento da mídia (jornais, rádio e televisão), da aquisição legal de livros e revistas especializadas de caráter técnico-científico, enfim, de um leque mais ou menos amplo de fontes disponíveis cujo acesso é permitido sem restrições especiais de segurança. Quanto mais abertos os regimes políticos e menos estritas as medidas de segurança de um alvo para a circulação de informações, maior a quantidade de inteligência potencialmente obtida a partir de programas de osint".

as redes horizontais e facilitaram a descentralização; (ii) possibilitou a privatização do trato das informações e da análise global de riscos; nesse sentido, os produtos e serviços produzidos por empresas privadas são superiores aos disponibilizados por organizações intergovernamentais de inteligência; e, (iii) contribuiu para a criação de redes informais de informação que concorrem com os serviços de inteligência na disputa pela atenção dos responsáveis governamentais pela tomada de decisões.

Essas questões requerem mudanças importantes na gestão do setor de inteligência; por exemplo, determinar em que circunstâncias é possível a utilização de fontes públicas para a coleta de informações, e em quais áreas são necessários novos métodos. Outra questão se relaciona com o desenvolvimento de novos métodos para troca e proteção de informações entre diferentes agências de inteligência.

Exemplos de avanços na área tecnológica por empresas privadas, voltados para o aperfeiçoamento da coleta e análise de inteligência no Brasil[79] são:

- IDSeg – Ambiente de Inteligência Investigativa e Estratégica by IntelleTotum, que "provê um conjunto de ferramentas e recursos para coletar, integrar e armazenar dados de diversas bases em uma só base de conhecimento. Possibilita também a disseminação do conhecimento de forma segura e personalizável". O IDSeg "é ideal para identificar, acompanhar e avaliar ameaças reais ou potenciais".[80]
- Método Grumbach: através dos programas "Puma e Lince", "permite que qualquer instituição, pública ou privada, elabore seu Plano Estratégico, podendo utilizar-se da técnica de Cenários Prospectivos, de forma prática e objetiva".[81]

  Entretanto, de acordo com o DCAF Backgrounder (03/2008:4), apesar de a Revolução informacional ter trazido várias mudanças positivas, ela ainda não soluciona problemas como:

  - os sistemas de alta tecnologia e de custo elevado elaborados para monitorar o ambiente eletrônico podem se revelar ineficazes contra organizações que utilizam sistemas mais simples de comunicação;
  - muitas organizações criminais e terroristas apresentam uma infraestrutura dificilmente identificável pelos métodos tecnológicos de coleta de informações;
  - avanços tecnológicos podem auxiliar os serviços de inteligência a proteger suas próprias informações confidenciais facilitando

[79] Empresas privadas utilizam a "inteligência competitiva" com o objetivo de maximizar seus lucros, neutralizar ou prejudicar a concorrência (GONÇALVES, 2009:35).

[80] Disponível em: <www.digitro.com>. Acesso em: 7 mar. 2010.

[81] Disponível em: <http://www.brainstorming.com.br/Home.do>. Acesso em: 7 mar. 2010.

assim suas atividades; exemplos incluem métodos para criptologia das comunicações disponíveis para o público em geral, ampliação do acesso à internet (o que facilita a troca de fundos e informações) e o aumento dos satélites para transmissão de imagens disponíveis comercialmente; e

- muitas das novas ameaças requerem que uma atenção especial seja dada à inteligência humana, sobretudo indivíduos cuja cultura e cuja língua facilitem a sua infiltração em grupos terroristas e criminais.

Cepik (2003:56), para "ilustrar a centralidade das novas tecnologias", ainda cita como exemplo a Intelink,[82] "a rede que integra as diversas organizações de inteligência do governo norte-americano", ressaltando:

> Em 1994, quando iniciou suas operações, o Intelink já operava com mais de 400 servidores e centenas de milhares de usuários, sendo que apenas a camada de serviços com restrição de acesso para informações classificadas como *secret* já provia acesso para 265 mil usuários interligados através de redes de fibras ópticas ou via satélite.

Com relação à cooperação e coordenação nacional, "os serviços de inteligência devem atuar de modo coordenado e em cooperação com os demais serviços de segurança nacional. Sobretudo nos países em que a inteligência é desempenhada por inúmeras agências, ou por inúmeros atores" (DCAF Backgrounder 03/2008:4). Esse é o caso do Brasil.

Transpondo a necessidade de cooperação para o plano internacional, de acordo com Bignami (2007:663), a troca de informações entre as agências de inteligência de todo o mundo é uma das formas mais promissoras de combate às grandes ameaças hoje existentes, como o terrorismo e o tráfico de drogas. Como muitos crimes envolvem indivíduos e fundos de múltiplos países (BIGNAMI, 2007:665), estabelecer procedimentos transnacionais para a troca de inteligência (criação de base de dados contendo, entre outras coisas, informações sobre criminosos perigosos e registros de passaportes roubados) facilitaria o combate a tais crimes.

Entretanto, o compartilhamento de informações pode ser desastroso. Afirma Bignami (2007:663 e 667, tradução livre):

> Mesmo em nível nacional, o sigilo e os imperativos de segurança nacional têm colocado as agências de inteligência muito além da fiscalização legal

[82] A Intelink faz parte do Global Information Grid (GIG), um projeto de comunicação do Departamento de Defesa norte-americano (DOD), que visa a facilitar a transferência de informações de inteligência. Para saber mais sobre o projeto e a Intelink veja o capítulo V da Joint Publication 2-01. Joint and National Intelligence: Support to Military Operations de 7 de outubro de 2004. Disponível em: <http://www.bits.de/NRANEU/others/jp-doctrine/jp2_01.pdf>. Acesso em: 18 mar. 2010.

e democrática. Mas em nível global, a *accountability*[83] está totalmente ausente. A cooperação global entre as agências nacionais de inteligência é extraordinariamente opaca. A natureza do sistema internacional compõe o problema: os atores não operam dentro de um sólido quadro institucional de democracia liberal e de direitos humanos. Salvaguardar direitos na esfera transnacional quando os governos conspiram para espionar, deter, interrogar e prender, não é fácil.

Para Bignami (2007:667-668):

> Um dos direitos mais fundamentais em questão, em relação às atividades de coleta de informações, é a privacidade das informações. O direito à privacidade limita o uso, pelo governo, de informações pessoais, protegendo, assim, indivíduos contra um vasto leque de abusos de poder governamental. Talvez os mais óbvios desses abusos, especialmente cometidos em operações de inteligência,[84] sejam as privações de vida, liberdade e propriedade baseadas em informações imprecisas. [E ainda ressalta:] Devido à facilidade com que os dados podem ser coletados, armazenados e combinados na era da tecnologia da informação, é difícil garantir a sua precisão. Num exemplo bem simples, dados podem ser gravados indevidamente por um mero erro humano. Quando diferentes conjuntos de dados são combinados, as informações em um dos sistemas de conjuntos de dados podem ser mal interpretadas pelo fato de seus sistemas de codificação e programação diferirem do outro sistema de conjunto de dados. Além disso, a capacidade de armazenamento de sistemas de computador é tão grande que as informações que já se tornaram obsoletas e, portanto, imprecisas, podem ser ali mantidas indefinidamente.

Em tempos em que os serviços de inteligência buscam estabilidade e legitimidade, é desafiante atuar de forma a preservar garantias e direitos fundamentais, como os direitos de liberdade e privacidade, bem como agir com transparência. Sobre a transparência, afirma Cepik (2003:188):

> Na medida em que a institucionalização dos serviços de inteligência envolveria não apenas a obtenção de "estabilidade" organizacional, mas também um longo processo através do qual eles se tornam (ou não) organizações "valiosas" para o público, esse é um processo que está fortemente relacionado à transparência, ou seja, à capacidade de o público ver e julgar por si mesmo os atos dos governantes na área de inteligência. Mesmo que os serviços de inteligência contemporâneos se tornem suficientemente ágeis para se estabilizarem organizacionalmente no novo contexto internacional, sua eventual institucionalização dependerá ainda da difícil resolução do dilema da transparência.

O compartilhamento de inteligência entre agências nacionais já é caótico, e esse compartilhamento além das fronteiras nacionais amplia o perigo de decisões governamentais serem tomadas com base em informações imprecisas. Além disso, estando as várias agências de inteligência interconectadas no ciberespaço, se uma delas viola o direito de privacidade, por exemplo, todas as

[83] *Accountability*: avaliação posterior das ações dos governantes pelos governados (CEPIK, 2003:158).

[84] Operações de inteligência, para relembrar, são ações realizadas com a finalidade de obter dados não-disponíveis ou negados (PACHECO, 2005 apud CASTRO, 2009:31).

outras agências se tornam cúmplices de tal violação, direta ou indiretamente (BIGNAMI, 2007:673).

Por outro lado, redes de inteligência interconectadas (*intelligence* networks) que possuem padrões próprios de proteção de dados exigem níveis altos de precisão informacionais, possuem limitações quanto ao período de tempo em que os dados poderão ser retidos em seus bancos de dados, possuem medidas de segurança especificadas e exigem de seus membros adequação desses parâmetros a seus regimes nacionais, como a Europol Information System (EIS), são exemplos plausíveis de tentativas de diminuir as impropriedades no compartilhamento de inteligência (BIGNAMI, 2007:681-684).[85]

Por fim, o DCAF Backgrounder (03/2008:5,6) cita como prioridades dos serviços de inteligência:

- conformar um sistema nacional integrado de inteligência capaz de otimizar os recursos disponíveis;
- ampliar o conhecimento técnico, os métodos e as práticas dos atores do setor de inteligência, incentivando a criatividade;
- remover as barreiras ao compartilhamento de inteligência, e estabelecer políticas que reflitam a "necessidade de compartilhamento" de todos os dados, ao invés de uma política de inteligência "nacionalista";
- explorar os avanços científico-tecnológicos, sobretudo as mudanças no plano da tecnologia da informação que possibilitam a manutenção e a ampliação do trato das questões relacionadas com as novas ameaças;
- criar uma "comunidade cibernética" de inteligência em que os produtores, consumidores e demais atores do setor de inteligência possam interagir, tanto no plano interno quando internacional;
- ampliar as capacidades tecnológicas para tratar do volume crescente de sinais interceptados;
- privilegiar questões que não apresentam grande interesse para o setor privado de inteligência por não serem rentáveis, demandarem tecnologia excessiva ou exporem seus atores a riscos legais excessivos em termos de responsabilidade.

  E, sobretudo:

- desenvolver novos *standards* para práticas de governança democrática, previstas em lei, para lidar com novas tecnologias e novas ameaças.

[85] Disponível em: <http://www.europol.europa.eu/>. Acesso em: 8 mar. 2010.

11.5. Conclusão

Conclui-se que são inúmeros os desafios da inteligência no ciberespaço, tanto técnicos quanto operacionais e legais. As questões relacionadas à ciberguerra, ao ciberterrorismo, à cibercriminalidade, à atualização legislativa diante do surgimento de novos crimes, à integração e cooperação internacional no ciberespaço, às formas de aperfeiçoamento da coleta e análise de inteligência em face da vasta quantidade de informações e em face da tendência de troca de informações interagências, nacional e internacionalmente, bem como as questões de privacidade e censura na rede merecem uma atenção especial da inteligência, constituindo-se em desafios à inteligência no ciberespaço.

O grau de dependência das nações, cada vez mais crescente em relação ao que o espaço cibernético lhes oferece, é relativamente alto. Embora tenha trazido benefícios incalculáveis para a humanidade, o uso do ciberespaço também é palco de fortes ameaças. As vulnerabilidades às ameaças cibernéticas são universais. Respostas legais, políticas, éticas, culturais, tecnológicas, sociais, diplomáticas e econômicas ainda não são suficientes para solucionar todas as questões que envolvem o ciberespaço.

Encontrar caminhos para que os serviços de inteligência se ajustem às novas exigências globais e propiciar mecanismos que auxiliem os governos a interromper o ciclo do "terror" cibernético que vigora mundialmente, através da redução de incertezas e inseguranças, são difíceis tarefas que a inteligência encontra no século XXI.

REFERÊNCIAS

ALDRICH, Richard W. *Cyberterrorism and computer crimes*: issues surrounding the establishment of an international legal regime. INSS Occasional Paper 32. Information Operations Series. USAF Institute for National Security Studies. Colorado: USAF Academy, April 2000. 91 p. Disponível em: <http://www.au.af.mil/au/awc/awcgate/usafa/ocp32.pdf>. Acesso em: 18 mar. 2010.

ALLEN, Patrick D.; DEMCHAK, Chris. A *guerra cibernética entre a Palestina e Israel*. Military Review 2001-2005, p. 51-58, 2004. Disponível em: <http://usacac.leavenworth.army.mil/CAC/milreview/download/portuguese/1stQtr04/allen.pdf>. Acesso em: 6 mar. 2010.

ARQUILLA, John; Ronfeldt, David. Cyberwar is Coming! Comparative Strategy 2 (abr.-jun.1993). In: SZAFRANSKI, Richard. *A Theory of Information Warfare*: preparing for 2020. Airpower Journal: 1995. Disponível em: <http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm>. Acesso em: 5 mar. 2010.

BBC BRASIL. Brasil é um dos países mais vulneráveis a ataques cibernéticos, diz pesquisa. 01 fev. 2010. Disponível em: <http://www.bbc.co.uk/portuguese/noticias/2010/02/100201_ataque_cibernetico_vdm.shtml>. Acesso em: 5 mar. 2010.

BEZERRA, Marcelo. *Cyberwar*. Disponível em: <http://dsic.planalto.gov.br/noticias/71-artigo-sobre-guerra-cibernetica-qcyberwarq>. Acesso em: 10 mar. 2010.

BIGNAMI, Francesca. Toward a right to privacy in transnational intelligence networks. *Michigan Journal of International Law*: 2007. Vol 28. p. 663-686. Disponível em: <http://students.law.umich.edu/mjil/article-pdfs/v28n3-bignami.pdf>. Acesso em: 11 mar. 2010.

BRASIL. Decreto nº 6.931 de 11 de agosto de 2009. Disponível em: <http://dsic.planalto.gov.br/missao>. Acesso em: 1 mar. 2010.

_____. Decreto nº 6.931, de 11 de agosto de 2009. (Publicado no DOU Nº 153, de 12 Ago. 2009 - Seção 1. Missões do DSIC. Disponível em: <http://dsic.planalto.gov.br/missao>. Acesso em: 18 mar. 2010.

_____. Gabinete de Segurança Institucional da Presidência da República. Departamento de Segurança da Informação e Comunicações. Gestão da Segurança da Informação e Comunicações, Guia de Referência para a Segurança das Infraestruturas Críticas da Informação e Livro Verde sobre a Segurança Cibernética no Brasil. Disponível em: < http://dsic.planalto.gov.br/>. Acesso em: 30 jul. 2011.

_____. Ministério Público Federal. Procuradoria da República no Estado de São Paulo. Grupo de combate aos crimes cibernéticos. Crimes cibernéticos: Manual prático de investigação. São Paulo: 2006. Disponível em: <http://www.mpdft.gov.br/portal/pdf/unidades/promotorias/pdij/TAC/Manual_de_Crimes_de__Inform%C3%A1tica_-_vers%C3%A3o_final2.pdf>. Acesso em: 16 mar. 2010.

_____. Portaria nº 34, de 5 de agosto de 2009. In: CANONGIA, Cláudia; MANDARINO, Júnior. Segurança cibernética: o desafio da nova Sociedade da Informação. *Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos (CGEE)*. Brasília-DF: nº 29, vol. 14, dez. 2009. Disponível em: <http://www.cgee.org.br/parcerias/p29.php>. Acesso em: 1 mar. 2010.

_____. Substitutivo aos PLS 76/2000, PLS 137/2000 e PLC 89/2003. Disponível em: <http://www.senado.gov.br/comunica/agencia/pags/01.html>. Acesso em: 16 mar. 2010.

BUNT, Gary R. *Islam in the Digital Age*: E-Jihad, Online Fatwas and Cyber Islamic Environments. Londres, Inglaterra: 2003. 237 p. Disponível em: <http://www.99chan.org/lit/src/Bunt_Islam_in_the_Digital_Age-E-Jihad_Online_Fatwa.pdf>. Acesso em: 18 mar. 2010.

CANONGIA, Cláudia; MANDARINO, Júnior. Segurança cibernética: o desafio da nova Sociedade da Informação. *Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos (CGEE)*. Brasília-DF: nº 29, vol. 14, dez. 2009. Disponível em: <http://www.cgee.org.br/parcerias/p29.php>. Acesso em: 1 mar. 2010.

CASTELLS, Manuel. End of Millennium, The Information Age: Economy, Society and Culture. Vol. III. Cambridge, MA: Blackwell Publishing, 1998. 366 p. In: WILSON, Jason. Defining Cyberspace. 05 fev. 2010. Disponível em: <http://www.cybertheorist.com/defining-cyberspace/>. Acesso em: 6 mar. 2010.

CENTER FOR STRATEGIC & INTERNATIONAL STUDIES (CSIS). In the Crossfire: Critical Infrastructure in the Age of Cyber War. 28 de Jan. 2010. Disponível em: <http://csis.org/event/crossfire-critical-infrastructure-age-cyber-war>. Acesso em: 5 mar. 2010.

CEPIK, Marco A. C. *Espionagem e democracia*. Rio de Janeiro: Editora FGV, 2003, 232 p.

_____. Adequação e preparo institucional para o enfrentamento da ameaça terrorista: avaliação crítica e sugestões preliminares. In: ENCONTRO DE ESTUDOS DE TERRORISMO, 2., 2003, Brasília. Anais... Brasília: Gabinete de Segurança Institucional da Presidência da República, 2004. p. 47-77. In: SOUZA, Delanne Novaes de. Brazil's role in the fight against terrorism. *REVISTA BRASILEIRA DE INTELIGÊNCIA*. Brasília: Abin, n. 5, out. 2009. 102 p. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf>. Acesso em: 16 mar. 2010.

CONVENÇÃO sobre o Cibercrime. Conselho da Europa, 2001. Disponível em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf>. Acesso em: 6 mar. 2010.

CONVENÇÃO sobre o Cibercrime. Conselho da Europa, 2001. Disponível em: <http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS_185_Portugese.pdf>. Acesso em: 6 mar. 2010. In: BRASIL. Crimes Cibernéticos – Manual Prático de Investigação do Ministério Público Federal – Procuradoria da República no Estado de São Paulo, 2006.

COUNCIL OF EUROPE. Global Project on Cybercrime (Phase 2). Março de 2009. Disponível em: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project%20global%20phase%202/projectcyber_en.asp>. Acesso em: 18 mar. 2010.

_____. Project on Cybercrime (Phase 1). Set. 2006 a Fev. 2009. Disponível em: <http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20Project/projectcyber_en.asp>. Acesso em: 18 mar. 2010.

CRISPIN, Mirian Cristina Generoso Ribeiro. *Doutrina nacional*: Crimes praticados pela internet e crimes de informática. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/13020/12584>. Acesso em: 3 mar. 2010.

CYBERBULLING. In: Cyberbullying: a perversidade virtual – Saiba o que é e o que fazer. Portal do Fórum Cidadania e Paz nas escolas. Disponível em: <http://www.ssp.se.gov.br/cidadania/modules/tinyd0/index.php?id=18>. Acesso em: 19 mar. 2010.

CYBERCRIME. In: Webopedia: The #1 Online encyclopedia dedicated to computer technology. 2005. Disponível em: <http://www.webopedia.com/TERM/C/cyber_crime.html>. Acesso em: 3 mar. 2010.

CYBERSPACE. In: International Encyclopedia of the Social Sciences. 2008. Disponível em: <http://www.encyclopedia.com/doc/1G2-3045300513.html.>. Acesso em: 22 fev. 2010.

_____. In: Webopedia: The #1 Online encyclopedia dedicated to computer technology. 2002. Disponível em: <http://webopedia.com/TERM/c/cyberspace.html.> Acesso em: 28 fev. 2010.

DANTAS, Romulo Rodrigues. Decorrências da utilização da internet por organizações terroristas: o recurso da comunicação tecnológica como proposta de mudança não-democrática de poder. *REVISTA BRASILEIRA DE INTELIGÊNCIA*. Brasília: Abin, n. 5, out. 2009. 102 p. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf>. Acesso em: 16 mar. 2010.

DCAF Backgrounder 03/2008. Contemporary Challenges for the Intelligence Community ou Desafios do Setor de Inteligência. (Versão em português). Geneva Centre for the Democratic Control of Armed Forces, março de 2008. Disponível em: <http://www.dcaf.ch/publications/kms/series_backgrounders.cfm?lng=en&size269=20&page269=0>. Acesso em: 10 mar. 2010.

DCAF Intelligence Working Group. Intelligence Practice and Democratic Oversight: A Practitioner's View. Occasional Paper nº3. Geneva, July 2003. Disponível em: <http://www.dcaf.ch/publications/kms/details.cfm?lng=en&id=18354&nav1=4>. Acesso em: 19 mar. 2010.

DELIO, Michelle. Got a virus? Blame the Tightwads. 2001. In: ALLEN, Patrick D.; DEMCHAK, Chris. *A guerra cibernética entre a Palestina e Israel*. Military Review 2001-2005, p. 51-58, 2004. Disponível em: <http://usacac.leavenworth.army.mil/CAC/milreview/download/portuguese/1stQtr04/allen.pdf>. Acesso em: 6 mar. 2010.

DENNING, Dorothy E. Cyberterrorism. Testimony before the SPECIAL OVERSIGHT PANEL ON TERRORISM, COMMITTEE ON ARMED SERVICES, U.S. HOUSE OF REPRESENTATIVE, May 23, 2000. Disponível em: <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>. Acesso em: 17 fev. 2010.

DENNING, Dorothy E. In: WEIMANN, Gabriel. *Cyberterrorism*: How Real is the Threat? Special Report 119 written to the United States Institute of Peace. December 2004. Disponível em <http://www.usip.org/resources/cyberterrorism-how-real-threat>. Acesso em: 19 fev. 2010.

FOLHA DE S.PAULO. Hacker violou mensagens de Dilma na campanha de 2010. 30 de jun. 2011. Disponível em: <http://www1.folha.uol.com.br/poder/936819-hacker-violou-mensagens-de-dilma-na-campanha-de-2010.shtml>. Acesso em: 28 jul. 2011.

FRAGOSO, Suely. *Espaço, Ciberespaço, Hiperespaço*: textos de comunicação e cultura, n. 42, UFBa, 2000, p. 105-113. Disponível em: <http://www.midiasdigitais.org/wp-content/uploads/2008/06/hiperespaco.pdf>. Acesso em: 2 mar. 2010.

G1. *Hackers anunciam ataques a sites da Presidência e do governo brasileiro*. 22 de jun. 2011. Disponível em: <http://g1.globo.com/tecnologia/noticia/2011/06/hackers-derrubam-sites-da-presidencia-e-do-governo-brasileiro.html>. Acesso em: 28 jul. 2011.

GABBARD, Derek. Cloud Computing, Security, and Cyber Intelligence. In: DC Tech-Security Conference, 11 set. 2008, Arlington/Washington. Disponível em: <http://www.dataconnectors.com/events/2008/09washingtondc/pres/SSES.pdf> Acesso em: 18 mar. 2010.

GENTILE, Carmen J. Hacker War Rages In Holy Land. 2000. In: ALLEN, Patrick D.; DEMCHAK, Chris. A guerra cibernética entre a Palestina e Israel. Military Review

2001-2005, p. 51-58, 2004. Disponível em: <http://usacac.leavenworth.army.mil/CAC/milreview/download/portuguese/1stQtr04/allen.pdf>. Acesso em: 6 mar. 2010.

GIBSON, William. Neuromante. 1948. In: LÉVY, Pierre. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Ed. 34, 1999. 264 p.

GLASS, Roberto R.; DAVIDSON, Phillip B. Conheça o inimigo! Trad. Paulo Enéas Ferreira da Silva. Rio de Janeiro: Biblioteca do Exército, 1956. In: GONÇALVES, Joanisval Brito. *Atividade de inteligência e legislação correlata*. Niterói: Impetus, 2009, 262 p.

GONÇALVES, Joanisval Brito. *Atividade de inteligência e legislação correlata*. Niterói: Impetus, 2009, 262 p.

GREEN. In: WEIMANN, Gabriel. *Cyberterrorism*: How Real is the Threat? Special Report 119 written to the United States Institute of Peace. December 2004. Disponível em: <http://www.usip.org/resources/cyberterrorism-how-real-threat>. Acesso em: 19 fev. 2010.

GRUMBACH, Raul José dos Santos. Cenários Prospectivos e Planejamentos Estratégicos. Aula ministrada no Curso de Pós-Graduação *Lato Sensu* de Especialização em Inteligência de Estado e Inteligência de Segurança Pública, oferecido pela Fundação Escola Superior do Ministério Público de Minas Gerais em parceria com o Centro Universitário Newton Paiva, 27 fev. 2010.

GUIMARÃES JR, Mário J.L. O Ciberespaço como Cenário para as Ciências Sociais. In: IX CONGRESSO BRASILEIRO DE SOCIOLOGIA, set. 1999, Porto Alegre. Trabalho apresentado no Grupo Temático "A sociedade da informação e a transformação da sociologia". Disponível em: <http://www.cfh.ufsc.br/~guima/papers/ciber_cenario.html>. Acesso em: 18 mar. 2010.

HACKERS: Outlaws and Angels (Hackers: criminosos e anjos). Produzido por September Films para TLC Life Unscripted. Versão [puxando.com] Hackers: Criminosos e Anjos – Dvdrip Legendado. Acesso em: 2009. Filme apresentado em sala de aula no Curso de Pós-Graduação *Lato Sensu* de Especialização em Inteligência de Estado e Inteligência de Segurança Pública, oferecido pela Fundação Escola Superior do Ministério Público de Minas Gerais em parceria com o Centro Universitário Newton Paiva, 2010.

HANNAFORD, Kat. Wikileaks.org foi fechado, mas site ainda pode ser acessado de várias outras formas. Gizmodo Brasil. 3 de dez. de 2010. Disponível em: <http://www.gizmodo.com.br/conteudo/wikileaksorg-foi-fechado-mas-site-ainda-pode-ser-acessado-de-varias-outras-formas/>. Acesso em: 12 abr. 2011.

HILDRETH, Steven A. Cyberwarfare. Congressional Research Service. Junho 2001. Disponível em: <http://fas.org/irp/crs/RL30735.pdf>. Acesso em: 11 mar. 2010.

I SEMINÁRIO REGIONAL DE INTELIGÊNCIA DE SEGURANÇA PÚBLICA – REGIÃO SUDESTE, 9, 10 e 11 set. 2009, Belo Horizonte/MG.

IDseg. Ferramentas analíticas de inteligência. Aula ministrada no Curso de Pós-graduação *Lato Sensu* de Especialização em Inteligência de Estado e Inteligência de Segurança Pública, oferecido pela Fundação Escola Superior do Ministério

Público de Minas Gerais em parceria com o Centro Universitário Newton Paiva, 20 nov. 2009.

JESUS, Damásio Evangelista. *Direito Penal*. 20. ed. São Paulo: Saraiva, 1998. In: WENDT, Emerson. *Criminalização dos crimes praticados pela internet*. Setembro de 2009. Slides. 52 p.

JOKISIPILÄ, Markku. Interfada: The Israeli-Palestinian Cyberconflict. In: WAR AND VIRTUAL WAR CONFERENCE, 19 out. 2004, Salzburg, Áustria. 8 p. Disponível em: <http://vanha.soc.utu.fi/polhist/vaihtuvat/jokisipila_Interfada.pdf>. Acesso em: 18 mar. 2010.

LANDLER, Mark; MARKOFF, John. Digital Fears Emerge After Data Siege in Estonia. *NEW YORK TIMES*. Tallinn, Estônia, 24 de maio de 2007. Publicado em 29 de maio de 2007. Disponível em: <http://www.nytimes.com/2007/05/29/technology/29estonia.html?pagewanted=1>. Acesso em: 6 mar. 2010.

LEIGH, David; HARDING, Luke. *WikiLeaks*: a guerra de Julian Assange contra os Segredos de Estado. Campinas, SP: Verus, 2011. 336 p.

LÉVY, Pierre. *Cibercultura*. Trad. Carlos Irineu da Costa. São Paulo: Ed. 34, 1999. 264 p.

LEWIS, Jim. Assessing the Risks of Cyberterrorism, Cyber War, and Other Cyber Threats. Report for the Center for Strategic and International Studies (CSIS). 2002. In: WEIMANN, Gabriel. Cyberterrorism: *How Real is the Threat*? Special Report 119 written to the United States Institute of Peace. December 2004. Disponível em: <http://www.usip.org/resources/cyberterrorism-how-real-threat>. Acesso em: 19 fev. 2010.

LIBICKI, Martin C. Cyberdeterrence and cyberwar. RAND Corporation, 2009. 214 p. Disponível em: <http://www.rand.org/pubs/monographs/2009/RAND_MG877.pdf>. Acesso em: 9 mar. 2010.

LIBICKI, Martin C. What Is Information Warfare? *Strategic Forum,* n. 28, May 1995. Disponível em: <http://www.dodccrp.org/files/Libicki_What_Is.pdf>. Acesso em: 3 mar. 2010.

LUPION, Bruno. Brasil ainda não tem Política Nacional de Segurança Cibernética. *Estadão*. 8 de Jun. 2011. Disponível em: <http://www.estadao.com.br/noticias/nacional,brasil-ainda-nao-tem-politica-nacional-de-seguranca-cibernetica,729292,0.htm>. Acesso em: 24 set. 2011.

MARKOFF, John; KAMER, Andrew E. U.S. and Russia Differ on a Treaty for Cyberspace. *NEW YORK TIMES*, 28 jun. 2009. Disponível em: <http://www.nytimes.com/2009/06/28/world/28cyber.html?scp=1&sq=U.s%20and%20russia%20differ%20on%20a%20treaty%20for%20cyberspace&st=cse>. Acesso em: 11 mar. 2010.

MATHERS, Russel F. Cyberspace Coercion in phase 0/I: How to deter armed conflict. 06 nov. 2007. Disponível em: <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA476693>. Acesso em: 7 mar. 2010.

MYERS, Steven Lee. After Violent Night, Estonia Removes a Soviet-Era Memorial. *NEW YORK TIMES*. Moscou, 27 de abril de 2007. Publicado em 28 de abril de 2007.

Disponível em: <http://www.nytimes.com/2007/04/28/world/europe/28estonia.html?_r=1>. Acesso em: 18 mar. 2010.

O'BRIEN, Kevin A. Cyber-Intelligence: For Threat-Profiling of Sub-State Actors in the Information Age. RAND Europe, 2002. Disponível em: <http://www.isodarco.it/courses/trento02/paper/trento02-brien_cyber.pdf>. Acesso em: 9 mar. 2010.

RODRIGUES, Rúbia. Wikileaks e os arquivos não mais secretos estadunidenses. Análise América. Cenários PUC Minas. Conjuntura Internacional. 6 de nov. de 2010. Disponível em: <http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20101213151225.pdf?PHPSESSID=9f6fceb2d4519e8c818505eff31619f9>. Acesso em: 12 abr. 2011.

ROQUE, Sérgio Marques. Crimes de Informática e investigação criminal. In: Justiça Criminal Moderna: Proteção à vítima e à testemunha, trabalho infantil, tv e crime. Coordenador: Jaques de Camargo Penteado. São Paulo: RT, 2000. In: CRISPIN, Mirian Cristina Generoso Ribeiro. Doutrina nacional: Crimes praticados pela internet e crimes de informática. Disponível em: <http://www.buscalegis.ufsc.br/revistas/index.php/buscalegis/article/viewFile/13020/12584>. Acesso em: 3 mar. 2010.

SAMPAIO, Fernando G. Ciberguerra, guerra eletrônica e informacional: um novo desafio estratégico. Escola Superior de Geopolítica e Estratégia (ESGE). 2001, 21p. Disponível em: <http://www.defesanet.com.br/esge/ciberguerra.pdf>. Acesso em: 9 mar. 2010.

SANTOS, Aloísio Rodrigues dos Santos. In: SEMINÁRIO ATIVIDADES DE INTELIGÊNCIA NO BRASIL: CONTRIBUIÇÕES PARA A SOBERANIA E A DEMOCRACIA, 6 e 7 nov., 2002, Brasília. In: GONÇALVES, Joanisval Brito. *Atividade de inteligência e legislação correlata*. Niterói: Impetus, 2009, 262 p.

SANTOS, Coriolano Aurélio Almeida Camargo. A nota fiscal eletrônica e o atual cenário do cibercrime. Tema para o trabalho preventivo do Instituto Nacional de Criminalística da Polícia Federal. 2006. Disponível em: <http://www.almeidacamargo.com.br/almeidacamargo/downloads/Iccyber%20IV.pdf>. Acesso em: 18 mar. 2010.

SANTOS, Coriolano Aurélio Almeida Camargo. Atual cenário dos crimes cibernéticos no Brasil. 2008. 16 p. Disponível em: <http://www2.oabsp.org.br/asp/comissoes/sociedade_informacao/artigos/crimes_ciberneticos.pdf>. Acesso em: 6 mar. 2010.

SOLHA, Liliana Esther Velásquez Alegre; TEIXEIRA, Renata Cicilini; PICCOLINI, Jacomo Dimmit Boca. Tudo que você precisa saber sobre os ataques DDos. NewsGeneration: boletim bimestral sobre tecnologia de redes, produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa. 17 mar. 2000, v. 4, número 2. Disponível em: <http://www.rnp.br/newsgen/0003/ddos.html>. Acesso em: 18 mar. 2010.

SOUZA, Delanne Novaes de. Brazil's role in the fight against terrorism. *REVISTA BRASILEIRA DE INTELIGÊNCIA*. Brasília: Abin, n. 5, out. 2009. 102 p. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf>. Acesso em: 16 mar. 2010.

SZAFRANSKI, Richard. A Theory of Information Warfare: preparing for 2020. *Airpower Journal*: 1995. Disponível em: < http://www.iwar.org.uk/iwar/resources/airchronicles/szfran.htm>. Acesso em: 5 mar. 2010.

TERRORISM. In: U.S. GOVERNMENT. Web site da CIA – Central Intelligence Agency. Título 22 do Código americano, sessão 2656f(d). Disponível em: <https://www.cia.gov/news-information/cia-the-war-on-terrorism/terrorism-faqs.html>. Acesso em: 6 mar. 2010.

THE OFFICIAL GOOGLE BLOG. A new approach to China. 12 de jan. 2010. Disponível em: <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>. Acesso em: 11 mar. 2010.

U.S. DEPARTMENT OF DEFENSE. Joint Publication 2-01. Joint and National Intelligence: Support to Military Operations. 7 de out. 2004. Disponível em: <http://www.bits.de/NRANEU/others/jp-doctrine/jp2_01.pdf>. Acesso em: 18 mar. 2010.

U.S GOVERNMENT. National Information Systems Security (Infosec) Glossary – NSTISSI No. 4009, Setembro 2000. Disponível em: <http://security.isu.edu/pdf/4009.pdf>. Acesso em: 6 mar. 2010.

U.S. GOVERNMENT. Cyberspace Policy Review. Maio, 2009. Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 28 fev. 2010.

U.S. GOVERNMENT. International Strategy for Cyberspace. Disponível em: <http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf>. Acesso em: 30 jul. 2011.

U.S. GOVERNMENT. National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23). In: Cyberspace Policy Review. Maio, 2009. Disponível em: <http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>. Acesso em: 28 fev. 2010.

U.S. GOVERNMENT. The National Strategy to Secure Cyberspace. Fev. 2003. Disponível em: <http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf>. Acesso em: 28 fev. 2010.

U.S. SENATE. Cybersecurity Act of 2009. Bill presented to the Committee on Commerce, Science, and Transportation. 01 Abr. 2009. Disponível em: <http://www.opencongress.org/bill/111-s773/text>. Acesso em: 28 fev. 2010.

UN. The United Nations Global Counter-Terrorism Strategy. 8 set. 2006. Disponível em: <http://www.un.org/terrorism/strategy-counter-terrorism.shtml>. Acesso em: 18 mar. 2010. In: DANTAS, Romulo Rodrigues. Decorrências da utilização da internet por organizações terroristas: o recurso da comunicação tecnológica como proposta de mudança não-democrática de poder. *REVISTA BRASILEIRA DE INTELIGÊNCIA*. Brasília: Abin, n. 5, out. 2009. 102 p. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf>. Acesso em: 16 mar. 2010.

VIDIGAL, Armando Amorim Ferreira. O Brasil diante dos desafios internacionais em segurança e defesa. In: ALMEIDA J. R. de; ROCHA, A.J. Ramalho da; SILVA, R. Doring Pinho da. Pensamento brasileiro sobre segurança e defesa. Brasília:

Ministério da Defesa, Secretaria de Estudos e de Cooperação, 2004. v.2, p. 13-36. In: SOUZA, Delanne Novaes de. Brazil's role in the fight against terrorism. *REVISTA BRASILEIRA DE INTELIGÊNCIA*. Brasília: Abin, n. 5, out. 2009. 102 p. Disponível em: <http://www.abin.gov.br/modules/mastop_publish/files/files_4b8d519458ebd.pdf>. Acesso em: 16 mar. 2010.

VIEIRA, Tatiana Malta. *Quadro da legislação relacionada à segurança da informação*. 2008. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm> Acesso em: 1º mar. 2010.

WEIMANN, Gabriel. *Cyberterrorism*: How Real is the Threat? Special Report 119 written to the United States Institute of Peace. December 2004. Disponível em: <http://www.usip.org/resources/cyberterrorism-how-real-threat>. Acesso em: 19 fev. 2010.

WENDT, Emerson. *Criminalização dos crimes praticados pela internet*. Setembro de 2009. Slides. 52 p.

WIENER. Cibernética ou controle e comunicação no animal e na máquina. 1948. In: SIMPÓSIO SOBRE CIBERNÉTICA DO SISTEMA NERVOSO, 1962, Amsterdã. In: SAMPAIO, Fernando G. Ciberguerra, guerra eletrônica e informacional: um novo desafio estratégico. Escola Superior de Geopolítica e Estratégia (ESGE). 2001, 21p. Disponível em: <http://www.defesanet.com.br/esge/ciberguerra.pdf>. Acesso em: 9 mar. 2010.

WIKILEAKS. Disponível em: <http://46.59.1.2/>. Acesso em: 12 abr. 2011.

WILSON, Jason. Defining Cyberspace. 05 fev. 2010. Disponível em: <http://www.cybertheorist.com/defining-cyberspace/>. Acesso em: 6 mar. 2010.

WINGFIELD, Thomas C.; MICHAEL, James B. An Introduction to Legal Aspects of Operations in Cyberspace. Naval Postgraduate School. Monterey, California, 2004. 16p. Disponível em: <http://www.au.af.mil/au/awc/awcgate/nps>.

XXI SEMINÁRIO DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (SEMSIC-MG) – GSIPR/DSIC, 23 e 24 nov. 2009, Belo Horizonte/MG.

EDITORA IMPETUS

Rua Alexandre Moura, 51
24210-200 – Gragoatá – Niterói – RJ
Telefax: (21) 2621-7007

www.impetus.com.br

Esta obra foi impressa em papel offset 75 gr/m²