# Cyberwar: Clausewitzian Encounters

**Marco Cepik, Diego Rafael Canabarro, and Thiago Borne Ferreira**

*As Clausewitz's masterpiece suggests, language matters for how states conceptualize and plan for war. 'Cyberwar', now on the lips of nearly every national security policymaker, may turn out to be a misnomer.*

The Digital Era and the spread of contemporary information and communication technologies (ICT) bring about different challenges for national and international security policymaking, heating up academic and political debate over the scope and the implications of an upcoming cyberwar.[1] This article evaluates three well-known assertions related to this highly controversial issue. The first section defines the concept of cyberwar according to its original employment. The second section presents each controversial assertion synthesized from qualitative content analysis of selected academic publications, landmark documents, and news accounts. The three of them are, respectively: (a) cyberspace is a new operational domain for war; (b) cyber warfare can be as severe as conventional warfare; and (c) cyber warfare can be waged both by state and non-state actors. In the third section we evaluate them collectively through theoretical and empirical lenses. The final section consolidates findings, indicating paths for further inquiry and policy caveats.

This text deliberately evokes an idea employed in the past by other accounts of the phenomenon (Tennant, 2009; Morozov, 2009; Greenemeier, 2011; Valeriano; Maness, 2012). The reference has two justifications. First, it seeks to reconnect the concept of cyber warfare to its Clausewitzian roots, highlighting the ambiguous role of information in war and the need to treat cyberspace as an integral part of the political and strategic realms, not as a completely separated domain. Second, it aims at the importance of careful evaluate propositions about the securitization of cyberspace.

[1] Marco Cepik is Associate Professor, Federal University of Rio Grande do Sul (UFRGS); Diego Rafael Canabarro, Ph.D., is Special Advisor to the Brazilian Internet Steering Committee (CGI.br); Thiago Borne Ferreira, is a Ph.D. candidate in International Strategic Studies, Federal University of Rio Grande do Sul (UFRGS).

## WHAT IS CYBERWAR?

The book chapter entitled *Cyberwar is coming!* by John Arquilla and David Ronfeldt (1997) is directly responsible for the formal incorporation of cyber to the lexicon of Security and Strategic Studies. According to the authors, "a case [existed] for using the prefix [from the Greek root *kybernan*, meaning to steer or govern, and a related word *kybernetes*, meaning pilot, governor, or helmsman] in that it bridges the fields of information and governance better than does any other available prefix or term," such as, for instance, information warfare (Arquilla; Ronfeldt, 1997:57).

Information warfare should be treated as a subfield of larger information operations, which "comprise actions taken to affect adversary information and information systems while defending one's own information and information systems." Information warfare is a more restrictive concept: it refers "to those information operations conducted during times of crisis or conflict intended to affect specific results against a particular opponent" (Schmitt, 1999:07).

The broad concept of information operations includes electronic warfare (EW), psychological operations (PSYOPS), computer network operations (CNO), military deception, and operations security (Zimet; Barry, 2009:291). Because of the ambiguous role of information in war (Clausewitz, 2007, Book I, Chapter VI), "information operations have been recognized as a

distinct form of warfare meeting its own separate doctrine, policy, and tactics," (Schmitt, 1999:32)[2].

Therefore the use of the prefix "cyber" in this context was intended to comprise both the role of digital computers and computerized networks from a technological perspective as well as the organizational and institutional consequences of their application on information gathering, processing and sharing. The authors allegedly tried to catch-up with "some visionaries and technologists who [were] seeking new concepts related to the information revolution" (Arquilla; Ronfeldt, 1997:59).

Basically, we agree with a conceptual definition of cyberwar that refers to the control of information-related factors in the preparation and waging of war. Cyberwar is conducted through the development and deployment of different technologies (increasingly robotic and digital in nature), as well as through the implementation of changes in military organization and doctrine. In this sense, "cyberwar is about organization as much as [it is about] technology" in order to "turn knowledge into capability" (Arquilla; Ronfeldt, 1997:30). The same is valid today, with proper qualifications and caveats.

Highlighting the societal implications of the information revolution[3], Arquilla and Ronfeldt also introduced the broad concept of netwar: a sort of non-military information-related multidimensional conflict, that could be waged by state and non-state actors with a wide range of available tools (public diplomacy, propaganda, interference with local media, the control of computer networks and databases, etc.), with the purpose of "trying to disrupt, damage, or modify what a target population knows or thinks it knows about itself and the world around it" (Arquilla; Ronfeldt, 1997:28). According to Arquilla and Ronfeldt's framework, despite being non-military in essence, netwar campaigns may deal with military issues such as nuclear weapons, terrorism, etc. Netwars may also escalate to the level of cyberwars when they affect military targets. Moreover, they can be employed in parallel to both conventional and cyber war.

More than twenty years later, cyber has become increasingly identified with the pervasiveness of cyberspace: "an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures" (Kuehl, 2009:28)[4].

In the military, information and intelligence operations, routine administrative functions, and a wide array of everyday jobs have been increasingly developed and transformed with the support of interconnected electro-electronic devices (Zimet; Barry, 2009; Libicki, 2012; Rid, 2012a). The same applies to the civilian sector (Blumenthal; Clark, 2009; Kurbalija; Gelbstein,

[2] Schmitt affirms that the terms information and information systems "shall be understood very expansively [...] The United States military defines information as 'facts, data, or instructions in any medium or form' and an information system as the 'entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information" (Schmitt, 1999:07).

[3] The whole field of Digital Era studies was influenced by *The Rise of the Network Society* (1996), where Manuel Castells first recognized that the "ability to use advanced information and communication technologies […] requires an entire reorganization of society" to cope with the decentralized character of networks that give shape to societies in an information age (Castells, 1999:03). Both cyberwars and netwars are founded upon the premise that ICTs entail networked forms of organization: the first category referring specifically to the military sector; the latter to the civilian sector at large. Nonetheless, the labeling of inherently non-military phenomena as "war" can also lead to unjustified events of securitization (Hansen; Nissenbaum, 2009).

[4] It is interesting to note that cyberspace was not a defining character of cyberwars to Arquilla and Ronfeldt. According to them cyberspace is "another new term that some visionaries and practitioners have begun using" to refer "to the new realm of electronic knowledge, information, and communications – parts of which exist in the hardware and software at specific sites, other parts in the transmissions flowing through cables or through air and space" (Arquilla; Ronfeldt, 1997:59).

2005). In the last two decades cyberspace has been greatly enlarged mainly as a result of the steady growth and spread of the Internet and interrelated technologies (Joint Chiefs of Staff, 2013:v). Currently, the Internet is the main entry door for cyberspace, mainly because the convergence of "all modes of communication – voice, data, video, etc. – on the Internet platform" (Mueller, 2010:129) has gradually blurred the lines between cyberspace and the Internet.

In this sense, the first decades of the 21st Century are defined by the growing importance of the technological and organizational aspects of cyberspace politics. Consequently, cyber-related issues increasingly permeate the agenda of national and international security (Weimann, 2004; O'Harrow, 2005; Nissenbaum, 2005; Eriksson; Giacomello, 2007; Kramer; Starr, 2009). As examples, one could just mention the public debate around increasing reliance of criminal and terrorist organizations on Internet-based applications (e.g. the Web, electronic mail, chat servers, social networks); the major assaults on Estonia (2007) and Georgia (2008) carried through Internet-based technologies and applications; the spread of malicious computer codes with unprecedented characteristics and outcomes, such as Stuxnet, Flame, and Gauss (2012); some alleged State-sponsored violations of sensitive political and economic databases, as well as public social networks profiles, such as the attacks reported by CitizenLab to computers associated with Dalai Lama (2008), the stealing of Sony movies and classified documents (2014), and the US Cyber Command Twitter account breach (2015); the Snowden affairs (2014), which publicized documented details of mass-surveillance programs developed mainly by the US National Security Agency; and the actions of civil society organizations such as Wikileaks and Openleaks, as well as hacktivists groups that employ Internet applications as means for political activism, such as Anonymous and Lulzsec.

Because of the need for promptly tackling these different perceived threats from a practical perspective, the theoretical notion of "cyber" as something related to the complex interactions between technology and networked governance has become subordinated to a narrow conception of "cyber" as something identified with the technical and tactical exploitation of cyberspace. As a detailed survey of the database compiled by Harvard's Berkman Center for Internet and Society (The Berkman Cybesecurity Wiki) reveals, the bulk of intellectual background for policy and legal development has been mainly produced by security related governmental agencies and IT corporations. Of course, we have no feud against government or the private sector getting involved in public debates about cyber warfare. Our point here is to stress the need to take a broader, theoretically oriented, political and societal perspective when trying to assess the meaning of cyberspace for national and international security policymaking.

More specifically, critical debate on basic concepts is crucial to avoid analogies without real theoretical or empirical grounds (Libicki, 2012). Therefore, it is a good sign that scholars recently began advancing more rigorous and consistent analyses of publicly known cyber events (Rid, 2013; Deibert, 2013; Gray, 2013; Demchak, 2012). Their works question taken-for-granted normative propositions on cyberwar. At the same time, they delve into the severity and the sophistication of contemporary cyber operations of all sorts.

## THREE CONTROVERSIAL CLAIMS ABOUT CYBERWAR

In order to contribute to a more balanced account of cyberwar, the following paragraphs summarize three common assertions related to the phenomenon. These three were selected from academic publications, landmark documents and news accounts covering the years 2012 and 2013.[5]

[5] The main sources were: (1) the digital database of the Center for International Studies on Government (CEGOV), compiled mainly through the CAPES Foundation Portal, as well as the physical libraries at UFRGS; (2) the physical and digital inventories of the University of Massachusetts, Amherst; and (3) the Cybersecurity Wiki maintained by the Berkman Center for Internet and Society of Harvard Law School, which consists of "a set of evolving resources on cybersecurity, broadly defined, and includes an annotated list of relevant articles and literature". It is available at: http://cyber.law.harvard.edu/cybersecurity/Main_Page (accessed August 18, 2014).

Our goal in debating them is not to dismiss them or prove them entirely false, but to call for a better-established scope of validity. After presenting each of them separately in this section, we shall discuss them collectively in the next section.

***"Cyberspace is a new operational domain for war"***

Referring to cyber-related incidents as warfare in the fifth domain has become a standard expression over the last ten years. "Cyberspace is a new theater of operations," says the 2005 US National Defense Strategy. "As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare […] just as critical to military operations as land, sea, air, and space," wrote the former US Deputy Secretary of Defense William Lynn (2010) in *Foreign Affairs*. "Warfare has entered the fifth domain: cyberspace," alerted The Economist in the same year (*The Economist*, 2010). Indeed, comparable claims have been widely spread in the past years, and the idea has reached politicians, intellectuals, the military, and the media all around the globe.

In 2012, the popular Argentinean *DEF Magazine* defined cyberspace as "a new battlefield" (Lucas, 2012). The idea was reaffirmed by an Argentinean official in the same year: "electronic warfare relates to more traditional domains of conflict: land, sea, and air. Cyberwar is undertaken in a new domain of hostility among nation-states" (Uzal, 2012).

***"Cyber warfare can be as severe as conventional warfare"***

According to the 2010 Brazilian Green Book on Information Security, "natural threats (posed by forces of nature) or intentional ones (sabotage, crime, terrorism, and war) acquire a greater dimension when the use of cyberspace is involved". During the III International Seminar on Cyber Defense held in Brasilia in 2012, the Brazilian Minister of Defense reaffirmed the idea, urging Brazil and other countries to get ready to face a new cyber-related threat capable of bringing harmful consequences to society at large.

In 2011 the *Washington Post* reported: "a cyber attack against Libya […] could have disrupted Libya's air defences but not destroyed them. For that job, conventional weapons were faster, and more potent. Had the debate gone forward, there also would have been the question of collateral damage. Damaging air defence systems might have, for example, required interrupting power sources, raising the prospect of the cyber weapon accidentally infecting other systems reliant on electricity, such as those in hospitals" (Nakashima, 2011).

One year later the same newspaper stated that "over the past decade, instances have been reported in which cyber tools were contemplated but not used because of concern they would result in collateral damage […] There is the danger of collateral damage to civilian systems, such as disrupting a power supply to a hospital" (*Washington Post*, 2012).

The already mentioned Argentinean *DEF Magazine* also suggested in 2012 that "a new sort of conflict is dominating the world stage: cyberwar. It doesn't matter the size and the available resources of the opponents. With an adequate IT capacity, the aftermath can be lethal and irreparable" (Noro, 2012).

***"Cyber warfare can be waged both by state and non-state actors"***

The 2003 US National Strategy to Secure Cyberspace alerts: "because of the increasing sophistication of computer attack tools, an increasing number of actors are capable of launching nationally significant assaults against our infrastructures and cyberspace." This notion is further developed by the 2012 DoD Priorities for 21st Century Defense: "both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland".

Harvard Law School Professor, Jack Goldsmith, summarizes these perceptions as follows:

> "Taken together, these factors – our intimate and growing reliance on computer systems, the inherent vulnerability of these systems, the network's global nature and capacity for

> near instant communication (and thus attack), the territorial limits on police power, the very high threshold for military action abroad, the anonymity that the Internet confers on bad actors, and the difficulty anonymity poses for any response to a cyber attack or cyber exploitation – make it much easier than ever for people outside one country to commit very bad acts against computer systems and all that they support inside another country. On the Internet, states and their agents, criminals and criminal organizations, hackers and terrorists are empowered to impose significant harm on computers anywhere in the world with a very low probability of detection" (Goldsmith, 2010).

On the other hand, Dorothy Denning, Professor at the Naval Postgraduate School, is more doubtful. She contends that:

> "There are several factors that contribute to a sense that the barriers to entry for cyber operations are lower than for other domains. These include remote execution, cheap and available weapons, easy-to-use weapons, low infrastructure costs, low risk to personnel, and perceived harmlessness. [...] Cyber weapons are cheap and plentiful. Indeed, many are free, and most can be downloaded from the Web. Some cost money, but even then the price is likely to be well under US$ 100,000. By comparison, many kinetic weapons, for example, fighter jets, aircraft carriers, and submarines, can run into the millions or even billions of dollars. Again, however, there are exceptions. Custom-built software can cost millions of dollars and take years to develop, while kinetic weapons such as matches, knives, and spray paint are cheap and readily available" (Denning, 2009).

As core propositions in the current debate regarding cyberwar, the three claims just presented cannot either be accepted or dismissed without strong empirical and logical tests, both beyond the scope of this article. However, in order to better define their scope of validity and the risks involved in accepting them as unqualified truth, we shall evaluate them collectively from the standpoint of a scientific research program such as Clausewitz's theory of war.

## TOWARDS A CLAUSEWIZIAN CONCEPT OF CYBERWAR

We shall depart from Betz's perception that cyberwar is a "portmanteau of two concepts": "cyberspace and war, which are themselves undefined and equivocal; it takes one complex non-linear system and layers it on another complex non-linear system […] As a result, it does not clarify understanding of the state of war today; it muddies waters that were not very transparent to start with" (2012:692). Hence we need to clearly define each concept before integrating them, starting with cyberspace.

Allow us to recall Kuehl's (2009) definition presented in the first section: cyberspace is "framed by the use of electronics and the electromagnetic spectrum." It is employed "to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures." Despite one's natural impetus to interpret interconnected ICTs as synonymous with Internet, cyberspace is a much more complex environment composed by many different systems. "At the very least yours, theirs, and everyone else's", says Libicki (2012:326).

Considering hypothetical actors A and B, this idea can be represented in graphical terms, as in Figure 1.

Both actors own closed (air-gapped) information systems (represented on circles A.1 and B.1); they also own systems (circles A.2 and B.2) that more or less overlap with global open communications backbones (GOBC) such as telecom lines, the radio spectrum, the Internet, etc. (represented on circle GOBC.3). Naturally, A and B can also have overlapping systems between themselves and/or between each one and other actors (circles A.3, B.3, and C.3). These systems can also be more or

less connected to global open communications backbones (in this case, directly through B.3).

All of these systems – mounted over a variable set of infrastructure, logical, and application layers – can be some way or another interconnected. The interconnection can be permanent and synchronous (such as in the case of Internet-based connections), as well as intermittent and asynchronous (such as in the case of software updating or in the use of a flash drive to exchange information between computers). Even when there are no digital bridges that allow access to a specific system, the isolation "can be defeated by those willing to penetrate physical security perimeters or by the insertion of rogue components. But efforts to penetrate air-gapped systems are costly and do not scale well" (Libicki, 2012:326).

As stated before, society relies on the correct performance of information systems for a myriad of more or less vital purposes. As man-made creations, information systems, and consequently cyberspace, have inherent flaws and vulnerabilities (Stamp, 2011; Kim; Solomon, 2010). Thus, the more one relies on them, the more it is potentially threatened by the eventual exploitation of the systems' vulnerabilities.

Nonetheless, we agree with Martin Libicki (2012) in highlighting that cyberspace is not a domain that can be isolated from others exactly due its pervasiveness to all human activities. In this sense, cyberspace can be treated as a separated warfighting domain only for logistical and command and control purposes, and even this trend could be argued against. However, it is more important to accurately communicate to the armed forces and the citizens that physical and logical realities of cyberspace are much harder to separate from land, water, air, and outer space than each of these other four domains can be separated from each other. Moreover, the whole concept of jointness depends, to become reality, on acknowledging the pervasiveness of cyberspace.

Since it is not correct to fully equate Internet with cyberspace, or treat cyberspace as something that can be isolated from the whole contemporary social fabric, there are operational implications when war reaches cyberspace. As Martin Libicki said regarding his conceptual framework for offensive and defensive cyber capabilities:

> "The more these tasks require correct working of the systems, the greater the potential for disruption or corruption that can be wreaked by others. Similarly, the more widely connected the information systems, the larger the population of those who can access such systems to wreak such havoc. Conversely, the tighter the control of information going into or leaving information systems, the lower the risk from the threat" (Libicki, 2012:323).

Following this idea, offensive actions in cyberspace aim at exploiting systems' flaws and vulnerabilities to "interfere with the ability of their victims to carry out military or other tasks, such as production" (Libicki, 2012:323). It is in essence a matter of reconnaissance, exploration, and exploitation of an opponent's entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Defense, on the other hand, involves a complex set of preventive and reactive actions in order to secure the systems (Clark; Levin, 2009). They comprise engineering and organizational decisions related to the situational environment, the set of technologies employed, and the degree of connectivity (to other systems) and openness (to a range of users) of a specific system. They also involve the permanent monitoring of the information flowing through the system, and its operation and functioning according to given parameters.

To be effective, the exploration/infiltration phase of a given attack has to be supplemented by the development of other code-based tools for disrupting the infiltrated system. However, the window of opportunity for infiltration and disruption is generally very narrow after vulnerability is discovered. Once an attack is detected, the target system can be adapted to tackle the threat. The number of different information systems and their potential lack of

structural uniformity (shown in Figure 1) mean that the strategic preponderance of defense over offense is not easily overturned. In other words, there are so many engineering options available for information systems' designers that the development of cyber offense capabilities might be way too expensive and ineffective to be translated into a strategic advantage.

In this sense, most offensive cyber actions are hard to repeat in patterned operational fashion: "once the target understands what has happened to its system in the wake of an attack, the target can often understand how its system was penetrated and close the hole that let the attack happen" (Libicki, 2012:323). Furthermore, as sensitive ICT systems generally entail great amounts of customization, the development of ready-made, mass-produced cyber weapons might be useful only for a few publicly open interoperable systems. The development of custom cyber weapons not only demands great amounts of resources (intelligence, funding, working-hours, etc.), but also means that the more customized the cyber weapon, the narrower its scope of application (Rid, 2013).

On the other hand, one might still affirm that the greater the Internet reliance, the greater the homogeneity of IT solutions and the greater the risks inherent to interconnectivity. Despite the suggestion that interconnectivity can lead to systemic hazardous events, vital information systems tend to be – and are increasingly becoming – more and more redundant and resilient (Sommer; Brown, 2011).

Actually, there is no such thing as a static cyberspace, neither in physical (infrastructure) nor in virtual (code) terms. To borrow a Clausewitzian term, cyberspace is a chameleon: its mutations depend on the decisions taken by individual information systems' owners. Therefore, calling cyberspace an operational domain without proper qualification entails the risk of overshadowing the inherent malleability of its components and consequently stresses the need of deploying permanent and vigilant tools for "perimeter" monitoring instead of making safety and security engineering/governance a priority when it comes to defense.

When it comes to offense, the development of general-purpose capabilities also needs to be balanced against the political and economic costs of exploiting (physically and digitally) the bulk of other actors' systems, as highlighted by the Snowden affair and the following diplomatic chorus of disapproval. This is not to say that cyberspace is not relevant for security and defense policymaking. On the contrary, it is a way to mind the fact that a large amount of resources might have been applied to suboptimal alternatives for ensuring national security – due to the hubris involved in treating as a self-contained operational domain something as ubiquitous and pervasive as cyberspace. That trend might be even more severe during times of economic or political distress, and might have negative outcomes if great powers develop a preemptive approach towards each other and third countries.

Regarding the second claim, that cyberwar can be as severe as conventional warfare; we first need to define the concept of war. According to Clausewitz, (1) war is never an isolated act, (2) war does not consist of a single blow, and (3) in war the result is never final (Clausewitz, 2007:17-19). Furthermore, as Clausewitz (2007:13) also reminds us, "war is […] an act of force to compel our enemy to do our will". The ultimate consequence of this prerogative is that war is necessarily violent. Potential or actual use of force, in Clausewitz's thinking, is the fundamental aspect of all war. Actually, violence plays a central role in his 'wondrous trinity' (*wunderliche Dreifaltigkeit*), which is made up of reason, natural force, and chance. The unifying concept of war in Clausewitz encompasses singular motives and dynamics that yet form an indivisible whole (Echevarria, 2007:69-70).

From a material point of view, every act of war is always instrumental to its ends. There has to be a means – physical violence or the threat of force – and there has to be an end – to impose one's will on the enemy. To achieve the end of war "the opponent has to be brought into a position, against his will, where any change of that position brought about by the continued use of arms would bring only more disadvantages for him, at least in that opponent's view" (Rid, 2012a:08). In this

sense, actual violence in actual wars does not easily escalate towards the logically possible extreme because of its instrumental and interactive nature.

Denial of service attacks such as those perpetrated by groups like Anonymous to take down or deface websites tend to be easily remedied or counteracted by the victims. And the bulk of scams that have been happening in the last years through ICT systems do not aim at exercising political power over an enemy, but only to exploit information for illegal commercial purposes. Intelligence related operations through cyberspace are obviously related to power struggles, but they are not warfare. In short, no testified cyber attack has ever caused a single casualty, injured a person, or severely damaged physical infrastructure. Taking this very characteristic alone before analyzing Clausewitz's prerogatives further, it seems exaggerated (or at least precipitate) to treat code-triggered consequences as equal to kinetic violence. "Violence in cyberspace is always indirect", says Rid (2012b).

It means that ICT systems first have to be weaponized in order to produce physical and functional damage to people, infrastructure, and organizations. One could arguably say that code weaponizing is exactly what is happening right now in the realm of international security; physical harm would be only a matter of time or disclosure about what is going on. Maybe, but empirical public evidence so far does not corroborate the second claim.[6]

Besides, it is hard to sustain at this point that any cyber attack reported so far has irrefutably forced the target to accept the offender's will. Nonetheless, that might not be the case if one considers the potential massive social-psychological risk inherent to the consequences of having governmental and banking web servers shutdown; personal and financial data stolen from cloud computing providers; SCADA systems unexpectedly operating anomalously without proper technical explanation as they did in the Stuxnet event; things from satellites to webcams and computer speakers turning on and off randomly and without direct user control, etc.

As Thomas Rid recognizes: "Cyber attacks, both non-violent as well as violent ones, have a significant utility in undermining social trust in established institutions, be they governments, companies, or broader social norms. Cyber attacks are more precise than more conventional political violence: they do not necessarily undermine the state's monopoly of force in a wholesale fashion. Instead they can be tailored to specific companies or public sector or organizations and used to undermine their authority selectively" (Rid, 2013:26).

The reiteration and persistence of non-violent cyber attacks (in isolation or in combination with other offensive activities short of war), coupled with the ever going preparation for responding to and retaliating cyber attacks in different political playing fields could escalate tensions up to the point of full-blown violent conflict. This possibility, as logical as it may be, has to be reconciled with some empirical corroboration before any government or armed force start to treat cyber incidents as equivalent of using kinetic or direct-energy weapons.

Finally, there is the risk of treating "the cyber" as another technological tool that would easily give the offensive a brutal advantage in war. "Technology has always driven war, and been driven by it [...] and yet the quest for technological superiority is eternal", explains Van Creveld (2007). For instance, in the 1930s and 1940s, air force superiority was thought to be the decisive feature for winning a war. In the 1990s, air force superiority was coupled with microelectronics in the development of precision-guided ammo, which would avoid the excessive loss of money and lives in war. The development of unmanned aerial vehicles (UAVs) follows that trend. "The problem is that when [people] talk of

[6] To be fair, Thomas C. Reed's memoir book *At the Abyss* (2005) describes how an American covert operation allegedly used malicious software to cause an explosion in Russia's Urengoy–Surgut–Chelyabinsk pipeline back in 1982. The incident might have caused casualties, even though there are no media reports, official documents, or similar accounts to confirm Reed's allegation. Also, it is not settled whether the Stuxnet attack caused destruction to the Iranian nuclear centrifuges, or if it only rendered them inoperative.

'stand-alone' cyberwars they are arguing a theory of a new form of war in which decisive results are achieved without triggering the thorny problem of escalation" – says Betz (2012:696).

Against the idea of a "cyber silver bullet" stands Clausewitz's third fundamental element of war: its political and interactive nature. According to him, warfare is "the continuation of politics by other means" (Clausewitz, 2007:28) because politics is the ever-open interaction of wills among individuals and political entities with potential contradictory ends, whatever constitutional form such polities may have. Individuals, groups, and polities have intentions (or emotional desires) to be transmitted to (and understood by) the adversary at some point during the conflict.

In contrast, Richard Clarke (2010:67-68), for instance, describes a hypothetical overwhelming cyber attack on the United States "without a single terrorist or soldier ever appearing". Addressing Stuxnet, Michael Gross wrote for *Vanity Fair* in April 2011: "[this] is the new face of 21st-century warfare: invisible, anonymous, and devastating". This brings us back to the problem of attribution and to the third controversy, regarding state and non-state actors alike being able to wage cyber warfare.

There is no doubt some cyber incidents are hard to publicly attribute to a specific actor, even if many have been increasingly political in nature or indirectly connected to political events. The Web War in Estonia is allegedly related to the government's discretionary removal of a Soviet-era statue from downtown Tallinn. The cyber attacks against Georgian official websites preceded the 2008 Russia-Georgia War. Some other attacks present political motivation, having been carried on by groups such as Anonymous, LulzSec, and others. The "Operation Payback", so far the largest operation coordinated by Anonymous, was aimed at disrupting online services of organizations that work in favor of copyright and anti-piracy policies, such as the Swedish Prosecution Authority, the Motion Pictures Association of America (MPAA), the International Federation of Phonographic Industry (IFPI), the Recording Industry Association of America, a large number of Law Firms, as well as individual American politicians, like Gov. Sarah Palin or Sen. Joseph Lieberman. That operation escalated to "Operation Avenge Assange" and started targeting the different companies and governments involved in the financial siege imposed on Wikileaks and the criminal prosecution unleashed against Julian Assange. The operations comprised website defacements, distributed denial of services attacks, leaks of classified information, and so on.

But they have not been translated into violent acts of any nature. Also, it is hard to establish the real cohesion and political power of these groups, for they seem to lack much common ground, put aside an ideological identity, for their activities. According to Betz (2012:706), "the means for them to exert noteworthy power – to compel, or attempt to compel, their enemies to do their will are available and growing in scale and sophistication. […] [Nonetheless] no networked social movements as of yet have attached existing, albeit new, ways and means to an end compelling enough to mass mobilize." A clear example of that lack of critical mass and political cohesion is reflected in the generally known rivalry and competition between Anonymous and LulzSec (Fogarty, 2011), which became dramatic after a leader of the first (and probably founder of the second) was arrested by the FBI and turned in a lot of "Anons" in exchange for clemency and legal benefits (Roberts, 2012; Biddle, 2012).

It is reasonable to argue that it is difficult to sustain the idea that such groups match state-like capabilities. It is also hard to establish the level of allegiance, competence, and cohesion (*esprit de corps*) among their ranks. Even so, there is scant if any evidence that actors other than states - for now at least - do have capabilities to harm and continuously cause havoc through digital means. As it will be shown below, treating the actions perpetrated by such groups as military operations, or even as terrorist activities in cyberspace might be dangerous for democracy without allowing clear improvement in security levels.

Sure, even non-state actors could employ cyber attacks as part of a larger operation also involving direct political violence. However, such actions might be best captured by terms such as sabotage,

espionage, subversion, or even terrorism in a more extreme possibility (Rid, 2013). The notion that non-state actors can wage cyberwar properly defined resemble the once popular notion that non-state actors were capable of developing and using weapons of mass destruction in a sustained confrontation against states. One can imagine a scenario where a highly organized, rich, secretive and skilled non-state actor could acquire one such weapon and use it, but even that is not the same as waging chemical, biological, or nuclear war. In short, Clausewitzian criteria provide a better framework to assess cyber events and actors and decide if they are instantiations of war or something else. The Clausewitzean scientific research program is capable of incorporating and explaining such heuristic novelty represented by the concept of cyberwar in the 21st Century.

## CONCLUSION

The controversies explored above not only encompass conceptual aspects of warfare, but also delve into some practical implications that are relevant for the overarching policy cycle in different countries. In sum, they highlight the political, economic, and societal trade-offs that are involved thereon. This article argues for a more precise and circumscribed concept of cyberwar that is better for addressing the phenomenon at various levels of concern and planning, related to both national and international security.

As Collier and Mahon (1993:845) remind us, "stable concepts and a shared understanding of categories are routinely viewed as a foundation of any research community. Yet ambiguity, confusion, and disputes about categories are common in the social sciences". The perpetual quest for generalization and the effort to achieve broader knowledge generate what Sartori (1970; 1984) called conceptual traveling (the application of concepts to new cases), but also may cause conceptual stretching (the distortion that occurs when concepts do not fit the new cases). According to him, understanding the proper scope of validity of a concept (the set of entities in the world to which it refers) as well as its intention (the set of meanings or attributes that define the category and determine membership) is essential in order to avoid overstretching. While the use of cyberwar is a recurrent rhetorical trope in public debates, it demands more than heat and loudness to call for the attention it deserves. Democracy and security can only be preserved and nurtured by serious consideration of the consequences and proper scope of political concepts, along with their policy implications.

Childress (2001:181), for example, provides an interesting view on the morality of using the language of warfare in social policy debates: "in debating social policy through the language of war, we often forget the moral reality of war. Among other lapses, we forget important moral limits in real war – both limited objectives and limited means". Childress however is not suggesting that one should avoid metaphors at all. However, the loose use of the metaphor of cyberwar, for instance, might not only lead to the aforementioned conceptual stretching, but also to improper or ineffective responses.

Consider for instance two widely adopted categorizations of cyber threats and cyber conflicts. The first one categorizes cyber terror, hacktivism, black hat hacking, cyber crime, cyber espionage, and information war on the bases of motivation, target, and method (Lachow, 2009:439). The second one deals mainly with the purposes of hacktivism, cyber crime, cyber espionage, cyber sabotage, cyber terror, and cyber war (displayed from the lower to the higher level of potential damage, and from the higher to the lower level of potential probability) (Cavelty, 2012:116).

Both classifications are very abstract and treat the same events with different labels. For Lachow (2009:440) Estonia was just a case of hacktivism, while for Cavelty (2012:109) Estonia should be understood as one of the "main incidents dubbed as cyber war". Why do those differences matter? Mainly because depending on the framing of a problem, the ensuing political responses will vary. The more securitized a social event is, the more exceptional and extreme can be the governmental responses to it (Buzan, Waever, et. al., 1998).

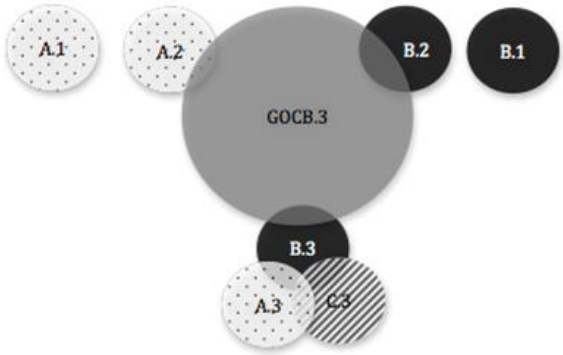
Treating activism, criminal activities, terrorism, and acts of war interchangeably undermines the state capability to adequately respond to a specific threat or conflict. Equally important, by throwing

different categories of actors under the same umbrella, it poses real threats to the civil liberties and political rights of individuals all around the world, despite the type of political regime they live under. For as Betz (2012:694-695) reminds us, cyberspace

> "[…] Extended a number of command, control, communications and intelligence capabilities [to non-state actors] which only the richest states could afford two decades ago; but the best picture is rather different with the state use of cyberspace as a means of war. For one thing, as the Stuxnet virus, which targeted the Iranian nuclear program, demonstrates very well, such capabilities do not come cheap […] For the purposes at hand, however, the significant thing about Stuxnet (which in historical perspective may be seen as the Zeppelin bomber of its day – more important as a harbinger of what is to come than for its material contribution to the conflict at hand) is that it was not the work of hackers alone but of a deep-pocketed team which had both excellent technical skills and high-grade intelligence on the Iranian program."

In sum, asking the right questions while assessing anything "cyber" is thus necessary to avoid either trivializing real wars that might come or undermining civil and political rights when treating all cyber conflicts as war.

**Figure 1. Simplified Graphical Representation of Cyberspace**




The illustration does not intend to represent the different sizes and individual characteristics of each system. Adapted from Zimet; Barry (2009:288) and Libicki (2012:326).

**REFERENCES**


Arquilla, J. and D. Ronfeldt (1997). *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica: Rand Publishing.

Betz, D. (2012). "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies*, 35:5, 689-711.

Biddle, S. (2012). "LulzSec Leader Betrays All of Anonymous." Gizmodo. http://gizmodo.com/5890825/lulzsec-leader-betrays-all-of-anonymous (accessed August 8, 2014).

Blumenthal, M. and D. Clark (2009). "The Future of the Internet and Cyberpower." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Buzan, B. and O. Waever, et al. (1998). *Security: A New Framework for Analysis*. Boulder: Lynne Rienner Publishers.

Castells, M. (1996). *The Rise of the Network Society*. Oxford: Blackwell.

Castells, M. (1999). *Information Technology, Globalization and Social Development*. Geneva, Switzerland: United Nations Research Institute for Social Development. http://www.unrisd.org/unrisd/website/document.nsf/ab82a6805797760f80256b4f005da1ab/f270e0c066f3de7780256b67005b728c/$file/dp114.pdf (accessed August 8, 2014).

Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension." In *Strategic Trends 2012: Key Developments in Global Affairs*. D. Möckly. Zurich: Center for Security Studies (CSS), ETH Zurich. http://www.css.ethz.ch/publications/Strategic_Trends_EN (accessed August 8, 2014).

Childress, J. F. (2001). "The War Metaphor in Public Policy: Some Moral Reflections." In *The Leader's Imperative: Ethics, Integrity, and Responsibility*. J. C. Ficarrota. West Lafayette: Purdue University Press.

Clark, W. K. and P. L. Levin (2009). "Securing the Information Highway: How to Enhance the United States' Electronic Defenses." *Foreign Affairs*, 88:6 (November/December 2009). http://www.foreignaffairs.com/articles/65499/wesley-k-clark-and-peter-l-levin/securing-the-information-highway (accessed March 27, 2015).

Clarke, R. and R. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It.* New York: Ecco Press.

Clausewitz, Carl von. (2007). *On War*. Oxford: Oxford University Press.

Collier D. and J. Mahon (1993). "Conceptual 'Stretching' Revisited: Adapting Categories in Comparative Analysis." *The American Political Science Review*, 87:4, 845-855.

Colombia.com (2012). "Expertos Creen que Estamos Frente a una Guerra 'Cibernética'." Colombia.com. http://www.colombia.com/tecnologia/actualidad/sdi/31440/expertos-creen-que-estamos-frente-a-una-guerra-cibernetica (accessed August 8, 2014).

Demchak, C. (2012). "Cybered Conflict, Cyber Power, and Security Resilience as Strategy." In *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World.* D. S. Reveron. Washington, D.C.: Georgetown University Press.

Denning, D. E. (2009). "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal*, 1:1, 6-10.

Echevarria II, A. J. (2007). *Clausewitz and Contemporary War*. Oxford: Oxford University Press.

Eriksson, J. and G. Giacomello (2007). *International Relations and Security in the Digital Age.* New York: Routledge.

Fogarty, K. (2011). "LulzSec vs. Anonymous: Doing Hacktivism Wrong." *IT World*. http://www.itworld.com/security/174917/lulzsec-vs-anonymous-doing-hactivism-wrong (accessed August 8, 2014).

Gray, C. (2013). *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling*. Carlisle Barracks, PA: Strategic Studies Institute. http://www.strategicstudiesinstitute.army.mil/pdffiles/PUB1147.pdf (accessed March 27. 2015).

Goldsmith, J. (2010). "The New Vulnerability." *The New Republic* (June 24, 2010). http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability (accessed August 8, 2014).

Hansen, L. and H. Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53, 1155-1175.

Joint Chiefs of Staff (2013). "Cyberspace Operations". Joint Publication 3-12(R). http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf. (accessed December 12, 2014).

Kim, D. and M. G. Solomon (2010). *Fundamentals of Information Systems Security*. Burlington: Jones & Bartlett Learning.

Kramer, F. and S. Starr and L. Wentz. (2009). *Cyberpower and National Security*. Washington, D.C.: National Defense University Press.

Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Kurbalija, J. and E. Gelbstein (2005). *Gobernanza de Internet: Asuntos, Actores y Brechas*. Geneva: Diplo Foundation.

Lachow, I. (2009). "Cyberterrorism: Menace or Myth." In *Cyberpower and National Security*. F. Kramer, S. Starr and L. Wentz. Washington, D.C.: National Defense University Press.

Libicki, M. C. (2012). "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy*, 8:2, 325-340.

Lucas, M. (2012). "Matrix, o el Nuevo Campo de Batalla." *Revista DEF*. http://www.defonline.com.ar/?p=8935 (accessed August 8, 2014).

Lynn, W. F. (2010). "Defending a New Domain: The Pentagon's New Cyberstrategy." *Foreign Affairs* 89:5 (September/October 2010). http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx (accessed August 8, 2014).

Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA: The MIT Press.

Nakashima, E. (2011). "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses." *The Washington Post* (October 17, 2001). http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn (accessed August 8, 2014).

Nissenbaum, H. (2005). "Where Computer Security Meets National Security." *Ethics and Information Technology*, 7, 61-73.

Noro, L. (2012). "Cyber War: La Guerra Silente." *Revista DEF*. http://www.defonline.com.ar/?p=9064 (accessed August 8, 2014).

O'Harrow, R. (2006). *No Place to Hide*. New York: Free Press.

Reed, T. (2005). *At the Abyss: An Insider's History of the Cold War*. New York: Random House Publishing Group.

Rid, T. (2012a). "Cyber War Will Not Take Place." *Journal of Strategic Studies*, 35:1, 5-32.

Rid, T. (2012b). "What War in the Fifth Domain?" Kings of War (9 August, 2012). http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/ (accessed August 8, 2014).

Rid, T. (2013) *Cyber War Will Not Take Place*. London: Oxford University Press.

Roberts, P. (2012). "LulzSec informant Sabu Rewarded with Six Months Freedom for Helping Feds." Naked Security (August 23, 2012). http://nakedsecurity.sophos.com/2012/08/23/sabu-lulzsec-freedom/ (accessed August 8, 2014).

Sartori, G. (1970). "Concept Misinformation in Comparative Politics." *American Political Science Review*, 64, 1033-1053.

Schmitt, M. N. (1999). "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework." *The Columbia Journal of Transnational Law*, 37, 885-937.

Sommer, P. and I. Brown (2011). *Reducing Systemic Cybersecurity Risk.* Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. http://eprints.lse.ac.uk/31964/ (accessed August 8, 2014).

Stamp, M. (2011). *Information Security: Principles and Practices*. Hoboken: Wiley.

The Economist (2010). "War in the Fifth Domain." *The Economist* (July 1, 2010) http://www.economist.com/node/16478792 (accessed August 8, 2014).

USA (2005). "U.S. National Defense Strategy." http://www.defense.gov/news/mar2005/d20050318nds1.pdf (accessed August 8, 2014).

USA (2012). "Sustaining US Global Leadership: Priorities for 21st Century Defense."http://www.defense.gov/news/defense_strategic_guidance.pdf (accessed August 8, 2014).

Uzal, R. (2012). "¿Es la Guerra Cibernética el Desafío más Relevante de la Defensa Nacional?" Mochila Virtual - Infantería Argentina (December 5, 2012). http://www.mochiladelinfante.com.ar/defensa/89-yies-la-guerra-cibernytica-el-desafno-mbs-relevante-de-la-defensa-nacional.html (accessed August 8, 2014).

Van Creveld, M. (2007). "War and Technology." Foreign Policy Research Institute Footnotes, 12:25. http://www.fpri.org/articles/2007/10/war-and-technology (accessed March 27, 2015).

Washington Post (2012). "U.S. Accelerating Cyberweapon Research." *The Washington Post* (March 13, 2012). http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story_1.html (accessed August 8, 2014).

Weimann, G. (2004). *Cyberterrorism: How Real Is the Threat?* Washington, D.C.: United States Institute of Peace. http://www.usip.org/files/resources/sr119.pdf (accessed August 8, 2014).

World Internet Users and Populations (2012). "Internet Usage Statistics – The Internet Big Picture." http://www.internetworldstats.com/stats.htm (accessed August 8, 2014).

Zimet, E. and C. L. Barry (2009). "Military Service Overview." In *Cyberpower and National Security.* F. Kramer, S. Starr, and L. Wentz. Washington, D.C.: National Defense University Press.