

3-1-2013

# Reflections on the Fog of (Cyber) War

Diego Rafael Canabarro  
*University of Massachusetts - Amherst*

Thiago Borne

Follow this and additional works at: <http://scholarworks.umass.edu/ncdg>

 Part of the [Computer Sciences Commons](#), [Political Science Commons](#), and the [Science and Technology Studies Commons](#)

---

Rafael Canabarro, Diego and Borne, Thiago, "Reflections on the Fog of (Cyber) War" (2013). *National Center for Digital Government Working Papers*. 41.

<http://scholarworks.umass.edu/ncdg/41>

This Article is brought to you for free and open access by the Centers and Institutes at ScholarWorks@UMass Amherst. It has been accepted for inclusion in National Center for Digital Government by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact [scholarworks@library.umass.edu](mailto:scholarworks@library.umass.edu).



National Center for Digital Government

## **Reflections on The Fog of (Cyber)War**

**Diego Rafael Canabarro**

PhD candidate in Political Science at the Federal University of Rio Grande do Sul (UFRGS)  
Research assistant at the Center for International Studies on Government (CEGOV/UFRGS)  
NCDG Fellow 2012-2013

and

**Thiago Borne**

PhD candidate in Strategic Studies at UFRGS  
Research assistant at CEGOVI/UFRGS

NCDG Policy Working Paper No. 13-001  
Submitted March 1, 2013



This work is licensed under a [Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-nc-sa/3.0/)

## INTRODUCTION

This paper aims at assessing some widespread assertions related to the highly controversial issue of cyberwar. It does so by using the following approach: First, it reviews the original concept of cyberwar according to its original employ. Second, it presents three general controversial assertions synthesized from the qualitative content analysis of selected academic publications, landmark documents, and news accounts. These assertions are: (a) Cyberspace is a new operational domain for waging 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. Each of the assertions is scrutinized according to supportive or contradictory logical, theoretical and empirical evidence in the following section. Finally, the paper consolidates findings and points out paths for furthering inquiry and policy development in the field.

Deliberately, this text hires the same provocative title employed in the past by some journalistic accounts of the phenomenon. (Tennant, 2009; Morozov, 2009; Greenemeier, 2011; Valeriano & Maness, 2012<sup>1</sup>) This repetition has two reasons. Firstly, it seeks to highlight the fact that “the fog” encompasses not only the real uncertainties surrounding the interrelations between cyberspace and military planning and operation, but also a great deal of confusion and misunderstanding generated by the works of commentators, scholars, and technicians who approach the topic. Secondly, it aims at reconnecting the idea of “fog of war” to its Clausewitzian roots, highlighting the importance of theoretical debates on the securitization of cyberspace.

## CYBERWAR

The book chapter entitled “*Cyberwar is Coming!*” (1997), by John Arquilla and David Ronfeldt, 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 is a subfield of the larger field of “information operations.” The latter “comprises actions taken to affect adversary information and information systems while defending one’s own information and information systems.” Information warfare is a more restrict concept: it refers “to those information operations conducted during times of crisis or conflict intended to affect specific results against a particular opponent.” (Schmitt, 1999:7)<sup>2</sup> Information operations include “electronic warfare (EW), psychological operations (PSYOPS), computer network operations (CNO), military deception and operations security.” (Zimet & Barry, 2009:291) Because of the role of information in war (see, e.g., Clausewitz, 2007, Book I, Chapter VI), “information operations has been recognized as a distinct form of warfare meeting its own separate doctrine, policy, and tactics,” (Schmitt, 1999:32) a trend that has been intensified after the scientific revolution of the 1970s. (Freeman & Louçã, 2001; Rennstich, 2008)

---

<sup>1</sup> The text of Brandon Valeriano and Ryan Maness was published on the *Foreign Affairs* website on 11/21/2012. This article was submitted for the 2013 Annual Conference of the International Studies Association on 06/01/2012.

<sup>2</sup> 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, 1999:7)

“Cyber-” 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. Arquilla and Ronfeldt allegedly tried to catch-up with “some visionaries and technologists who [were] seeking new concepts related to the information revolution.” (Arquilla & Ronfeldt, 1997:59) Cyberwar within that perspective refers to the control of information-related factors in the realm of the preparation and the waging of war through the development and the deployment of different technologies (increasingly electronic in nature), but through the implementation of changes in military organization and doctrine under the scope of what is now known as the “Revolution in Military Affairs,” or RMA.<sup>3</sup> Accordingly, “cyberwar is about organization as much as technology,” in order to “in Clausewitz’s sense, (...) turn knowledge into capability.” (Arquilla & Ronfeldt, 1997:30)

Highlighting the societal implications of the information revolution, 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. [For instance] (...) In some respects, the U.S. and Cuban governments [have been] engaged in a netwar. This is manifested in the activities of Radio and TV Marti [the broadcast scheme established by Reagan to spread the word against Communism in transmissions to Cuba] on the U.S. side, and on Castro’s side by the activities of pro-Cuban support networks around the World.” (Arquilla & Ronfeldt, 1997:28)

Another good example of a netwar is the one that has been waged against the Mexican government since 1994 by the EZNL, which relies on “vast, highly networked, transnational [civil society] coalitions” in support of its overarching agenda for social, economic, and political reforms in Mexico. (Ronfeldt & Martínez, 1997:370) According to Arquilla and Ronfeldt’s framework, despite being non-military in essence, netwar campaigns may deal, as their core motif, with military issues such as nuclear weapons, terrorism, etc. Also, netwars can escalate to the level of cyberwars when they affect military targets. Moreover, they can be employed in parallel to war in general (conventional and cyber). That happened in the 1991 Gulf War: “The construction of an international consensus against the Iraqi aggression, backed by the deployment of large, mechanized forces, was intended to persuade Saddam to retreat.” (Arquilla & Ronfeldt, 1997:39-40)

---

<sup>3</sup> The core of the RMA is the reflection about the role of digital technologies for the Military and the related institutional and organizational reforms that should ensue to better suit with that trend. (Rummsfeld, 2002) The overwhelming victory of the United States over Saddam Hussein’s Iraq in the 1991 Gulf War is the paradigmatic event that institutionalized the RMA as a permanent policy of the U.S. armed forces and as a permanent topic of the intellectual production over the 1990s. Part of the RMA agenda deals with the role of technology in allowing cleaner, cheaper, and faster military campaigns. From this resulted the myth of surgical precision for guided weapons (Biddle, 1996; O’Hanlon, 1998; Cohen, 1999; Mowthorpe, 2005; Martins, 2008; Duarte, 2012) and the myth of information/knowledge supremacy as a tool for softening the effects of attrition between opposing forces. In this regard, Arquilla and Ronfeldt (1997:43) “anticipate that cyberwar, like war in Clausewitz’s view, may be a ‘chameleon.’ It will be adaptable to varying contexts; it will not represent or impose a single, structured approach. Cyberwar may be fought offensively and defensively, at the strategic or tactical levels. It will span the gamut of intensity – from conflicts waged by heavy mechanized forces across wide theaters, to counterinsurgencies where ‘the mobility of the boot’ may be the prime means of maneuver. Cyberwar may also imply – although we are not sure at this point – that victory can be attained without the need to destroy an opposing force.”

Twenty years have passed since Arquilla and Ronfeldt published “*Cyberwar is Coming!*” and tried to define the boundaries between what they called cyberwars and netwars.<sup>4</sup> In recent years, however, “cyber-” became increasingly identified with the pervasiveness of cyberspace<sup>5</sup> – “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)

In the military, information operations, intelligence operations, routine administrative functions, etc., have all been increasingly developed and transformed with the support of interconnected electro-electronic tools. (Zimet & Barry, 2009; Libicki, 2012; Rid, 2012a) The same applies to the civilian sector. (Blumenthal & Clark, 2009; Kurbalija & Gelbstein, 2005; Zukang, 2007) As a result of the steady growth and the spread of the Internet and interrelated technologies in the last two decades, cyberspace has been greatly enlarged. Data from June 2012 show that more than two billion people in the World are daily connected to the Internet through different applications and technologies. Between 2000 and 2012, the number of Internet users in the World has grown around 528 per cent. (World Internet Users and Population Stats, 2012)<sup>6</sup> Today, the Internet serves as the main entry door for cyberspace. And increasingly, the convergence of “all modes of communication – voice, data, video, etc. – on the Internet platform” (Mueller, 2008:129) has blurred the lines between the cyberspace and the Net.

Bearing in mind Arquilla and Ronfeldt’s labeling framework, the first decade of the 2000s can be characterized by the growing importance of the technological and organizational aspects of cyberwars

---

<sup>4</sup> Their effort was clearly influenced by “*The Rise of the Network Society*,” authored by Manuel Castells (1996). According to his theorization, following Braudelian insights, “technology does not determine society: it embodies it. But neither does society determine technological innovation: it uses it.” (1996:05) It means 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). Indistinctively, 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. Their concern with the interplays of technology and society is fully justified (Mumford, 1960; Winner, 1986; Bijker, 2006; Smit, 2006; Jasanoff, 2006). It seems to us, nonetheless, that the inconvenience of their classification lays on the choice of the word “war” in their core their concepts, especially for the second one. For “war” is *per se* a very slippery term within the realm of Security and Strategic Studies. Moreover, the labeling of inherently non-military phenomena as “war” can lead to unjustified events of securitization, which are a potential feature of cybersecurity policies in general (Hansen & Nissenbaum, 2009).

<sup>5</sup> It is interesting to note that the cyberspace is not the defining character of cyberwars according to the seminal publication of Arquilla and Ronfeldt. In their text, 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). They explain that “cyberwar depends less on the geographic terrain than on the nature of the electronic ‘cyberspace,’ which should be open to domination through advanced technology applications. Cyberwar benefits from an open radio-electronic spectrum and good atmospheric and other conditions for utilizing that spectrum. (...) How, when and where to position battlefield computers and related sensors, communications networks, databases, and REC devices may become as important in future wars as the same questions were for tanks or bomber fleets and their supporting equipment in the Second World War.” (Arquilla & Ronfeldt, 1997:44).

<sup>6</sup> One has to point out the fact that two thirds of the world population still don’t have Internet access. The Internet growth and digital exclusion are two intermingled features of the Digital Era. Digital exclusion is a very complex phenomenon that cannot be restricted to the divide between the digitally “haves” and “have-nots.” (van Dijk, 2005; Eubanks, 2012) It means that the increasing growth in the number of Internet users does not necessarily imply the reduction of digital exclusion worldwide. (Headrick, 2009:143)

and netwars in the academic and political agenda of national and international security. (Weimann, 2004b; Eriksson & Giacomello, 2007; Giles, 2011; Hsiao, 2010; Kramer & Starr, 2009) In parallel, it was also marked by the increasing securitization of cyberspace. (O’Harrow, 2005; Nissenbaum, 2005) The major driving forces to the latter can be summarized as follows: the reliance of criminal and terrorist organizations on Internet-based applications (e.g. the Web, electronic mail, chat servers, social networks) for different type of transactions, including Al-Qaeda’s planning and orchestration of the 9/11 terrorist attacks (Weimann, 2004a; 2004b; 2005; 2006); 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 the *Stuxnet* (Symantec, 2011), the *Flame* (CrySyS Lab, 2012) and the *Gauss* (Kaspersky, 2012); and, finally, the audacious actions of civil society organizations such as the whistleblowers *Wikileaks* and *Openleaks*, as well as “*hacktivists*” clans such as Lulzsec and Anonymous, that employ Internet applications as their main tools for political activism.

In virtue of those facts, this paper suggests that the broad idea of “cyber-” as something related to the complex interactions of technology and networked governance in the 21<sup>st</sup> century, for both the military and the civilian realms, has become subordinated to the narrow conception of “cyber-” as something merely related to cyberspace (and increasingly, to the Internet). Paradoxically, this narrow conception implies an enlargement of the challenges for the study and the practices of security in the Digital Era. Much of the intellectual production in the field lacks consensus surrounding basic concepts, advances unsatisfactory analogies and creates analytical frameworks without theoretical, logical, and empirical consistency. (Libicki, 2012) Great part of that production is not academic in nature. A detailed survey of the database compiled by Harvard’s Berkman Center for Internet and Society (The Berkman Cybeseurity Wiki) shows that the bulk of intellectual background for policy development has been mainly produced by governmental agencies themselves (especially from the U.S.) and by IT corporations. Ergo, despite the relevance of the discussion of potential “cyber Pearl Harbors” and “cyber 9/11s”, much of the securitization of cyberspace remains unchecked and some of the taken-for-granted normative propositions for cyber security and defense might in reality augment the levels of insecurity and vulnerability for specific states and their populations.

## THE FOG OF CYBERWAR

We now turn to the core of this study. During the whole year of 2012, we collected some controversial assertions related to the topic of cyberwar from a group of academic publications, landmark documents, and news accounts.<sup>7</sup> They were categorized under three different clusters, which represent general controversies that are not, so far, satisfactorily settled both in academic and in policy terms. Under each cluster, we provide remarkable examples of the assertions we stumbled over while reviewing the content of those publications. This initial categorization effort is an attempt to raise some logical, theoretical, and empirical reasoning that support or contradict each claim. In section 5, we contrast them to the content of the policies recently adopted in Brazil. And, in the end, we try to show how such an approach can be useful to the evaluation of other cases.

---

<sup>7</sup> The sources of the publications studied for this analysis were basically: (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; (3) our own personal physical and digital libraries; and (4) 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 on: [http://cyber.law.harvard.edu/cybersecurity/Main\\_Page](http://cyber.law.harvard.edu/cybersecurity/Main_Page). Last accessed: 01/29/2013.

### ***Cyberspace is a New Operational Domain for Waging War***

Referring to cyber conflict as warfare in the fifth domain has become a standard expression in the debate. “Cyberspace is a new theater of operations,” says the 2005 U.S. National Defense Strategy. (USA, 2005) “As a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain of warfare. Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air, and space” wrote William Lynn, America’s Deputy Secretary of Defense, in a 2010 *Foreign Affairs* article. (Lynn, 2010) “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 South American politicians, intellectuals, the military, and the media.

The popular Argentinean *DEF Magazine* says, for instance, cyberspace is a “new battlefield.” (Lucas, 2012) During the III International Seminar on Cyber Defense, held in Brasilia on October 24, 2012, the Brazilian Minister of Defense – Ambassador Celso Amorim – urged Brazil and the countries in the region to be prepared to face what he called a “new threat” (a cyber-related one), which might bring harmful consequences for society at large. Lt. Col. Roberto Uzal, from the Argentinean armed forces, explains in an article published in 2012 that “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) With a lot more conceptual caution, Brazilian scholar Domício Proença Jr. understands that “cyberspace presents itself as a potential topology (as the land, the sea, the air, and the electromagnetic space [sic]) for the clash of coercive means. However, similarly to the topology of the satellite orbital close to Earth, the certainty that it is possible to do something to influence someone’s will or to protect our own will against the influence of others has not yet been confirmed.” (Proença Jr., 2009:04) A pioneer web portal in Colombia questions: “Are we already in the middle of a global cyber strife without even realizing it? If so, who are the attackers? What are their objectives?” (Colombia.com, 2012)

### ***Cyber Warfare can be as Severe as Conventional Warfare***

Given the difficulties inherent to fully grasping the scope of cyberspace, a lot of speculations have been created about the consequences of cyber operations. “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,” – explains the *Brazilian Green Book on Information Security* (2010). During an event that brought together governmental officials, representatives of the private sector, civil society, and the academia, held in Rio de Janeiro in 2011 (the Cyber Security International Forum), Maj. Brig. Álvaro Knupp from the Brazilian MD highlighted the role of cyber security and defense in the following terms: “At the end of the day, in a war many more civilians die than soldiers.” Accordingly, the *Washington Post* recently stated:

“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. For instance, defense and intelligence agencies discussed using cyber technology to freeze money in Iraqi dictator Saddam Hussein’s bank accounts just before the U.S.-led invasion in March 2003 to blunt his efforts to mount a defense. The plan was aborted because of concern that the cyberattack could disrupt financial systems in Europe and beyond. Within a war zone, the use of a cyberweapon may be limited by other considerations. There is the danger of collateral damage to civilian systems, such as disrupting a power supply to a hospital. A destructive computer code, once released, could be reverse-engineered and sent back at vulnerable U.S. targets or adapted for use by

foreign spy agencies. Cybertechnology also is not always the most efficient way to attack a target – sometimes bombs or electronic warfare are easier or more reliable.” (Washington Post, 2012)

One year before, the same newspaper reported that

“a cyberattack against Libya, said several current and former U.S. officials, could have disrupted Libya’s air defenses 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 defense systems might have, for example, required interrupting power sources, raising the prospect of the cyberweapon accidentally infecting other systems reliant on electricity, such as those in hospitals.” (Nakashima, 2011)

Once again, in the pages of the Argentinian magazine *DEF*, a commentator suggests “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*

It is a widespread idea that the capacity of non-state actors to operate on cyberspace is tantamount to the capacity of state actors. The 2003 U.S. 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 Department of Defense’s *Priorities for 21<sup>st</sup> 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.” (USA, 2012) Harvard Law School Professor, Jack Goldsmith, explains those perceptions:

“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)

In the same tune, Dorothy Denning, Professor at the Naval Postgraduate School, is a bit more skeptical. She contends:

“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)

## **OVERALL ASSESSMENT**

The evaluation of those general claims departs 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 proceed to the segmented study of each concept in order to contribute to the integrated understanding of that “portmanteau.”

By the end of 2012 Martin Libicki (2012) solemnly asserted, “*cyberspace is not a warfighting domain.*” He did so after scrutinizing the structural characteristics of cyberspace and summarizing his conceptual framework for offensive and defensive cyber capabilities. (Libicki, 2007; Libicki, 2009)

One should recall Kuehl’s (2009) definition presented above: 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 of one’s natural impetus to interpret “interconnected ICTs” as a synonym to the Internet, cyberspace is a much more complex environment. It consists of innumerable different systems. “At the very least yours, theirs, and everyone else’s,” says Libicki (2012:326). Considering hypothetical actors A and B, this can be represented in graphical terms as follows:

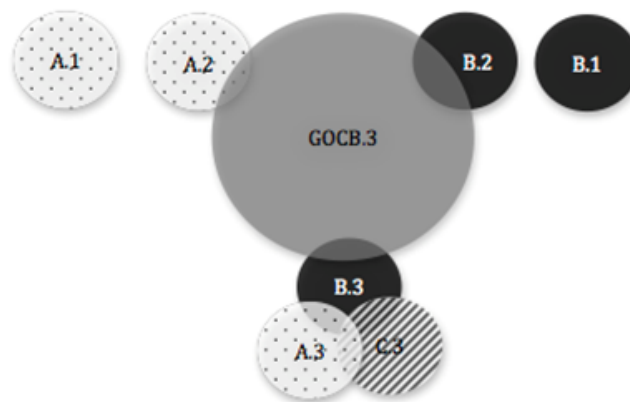


Figure 1: a simplified graphical representation of Cyberspace adapted from Zimet & Barry (2009:288) and Libicki (2012:326).

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). And these systems can be more or less connected to global open communications backbones (in the case of the illustration, directly through B.3).<sup>8</sup>

All of those systems can be interconnected in some way or another. That 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 and the use of a flash drive to exchange information between different computers). Even when there are no digital bridges that allow the access to a specific system, that 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 seen above, both the military and the civilian sectors of society rely on the correct performance of information systems for a myriad of more or less vital purposes. As man-made creations, information

<sup>8</sup> The illustration does not intend to represent the different sizes and individual characteristics of each system.

systems (and cyberspace as a result of the increasing interconnectivity of different systems) have inherent flaws and vulnerabilities. (Stamp, 2011; Kim & Solomon, 2010) Thus, the more one actor relies on them, the more it is potentially threatened by the eventual exploitation of his systems' vulnerabilities.

“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)

By this token, 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 and exploration of other people's systems. Defensive actions, on the other hand, involve a complex set of preventive and reactive actions. (Clark & Levin, 2009) They comprise engineering and organizational decisions related to the situational environment and the degree of connectivity (to other systems) and openness (to a range of users) of a specific system. Also, they involve the permanent monitoring of the information that circulates through the system and of the use of the system in general.

Goldsmith affirms that cyberspace is “an arena where the offense already has a natural advantage” (Goldsmith, 2010). By doing so, Goldsmith disregards one of Clausewitz's (2007:161) classical claims: the idea that “defense is the stronger form of waging war.” According to the Prussian, the advantages raised by defense strategies arise from what he calls its “passive purpose of preservation.” In defensive engagements one “leave[s] the initiative to [his] opponent and await[s] [their] appearance before [his] lines.” (2007:160) Even if we accept the contention that cyberspace is a warfighting domain, bearing in mind what is shown by the simplified illustration of the cyberspace above, the number of different information systems and the potential lack of uniformity in their compositions mean that the strategic preponderance of defense over offense still holds. The infinite engineering options available for those who develop and rearrange information systems imply that the development of cyber offense capabilities might be way too expensive and ineffective to be translated into a strategic advantage. In that sense, Goldsmith's assertion is only partially true: to be effective the exploration/infiltration phase has to be fulfilled by the development of other code-based tools for commanding the infiltrated system. And the window of opportunity for infiltration and disruption is generally very narrow, because it is expected that once an attack is detected the target system itself or with the support of human operators can be adapted to tackle the threat. In Libicki's words (2012:331),

“a key characteristic of offensive cyberspace operations is that most of them are hard to repeat; 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.” Also, the development of ready-made, mass-produced “cyberarms” might be only useful for those publicly open interoperable systems. As Libicki points out, “a set of tools without the requisite vulnerabilities is not particularly useful.” (Libicki, 2012:323)

Of course one has to consider that in general terms the reliance on the Internet (and its associated networking standards and applications) by governments and the population increases the level of homogeneity of IT solutions adopted in the public and private sectors, which augments the risks inherent to interconnectivity. As a thought experiment, one might say that that interconnectivity could lead to systemic hazardous events; but only if one completely disregards the fact that vital information systems tend to be redundant and resilient. (Sommer & Brown, 2011)

In theory and in practice, it is wrong to fully equate the Internet to cyberspace. Actually, there is no such thing as a static cyberspace: neither in physical (infrastructure), nor in virtual (logic code) terms. Cyberspace itself is (to borrow a Clausewitzian term) a chameleon: its mutations depend on the

decisions of the owners of individual information systems. Reifying it as an operational domain for waging war disregards the inherent malleability of its components, with the consequence of making safety and security engineering/governance secondary in relation to the permanent and vigilant watchdogs with the intention of monitoring the “perimeter” when it comes to defense. On the other hand, when it comes to offense, the development of general capabilities – besides being an overtly aggressive attitude by part of some states – might be of little usefulness in face of the high political and economic costs of exploiting (physically and digitally) the bulk of other actors’ systems (the air-gapped and the interconnected ones). This is not to say that cyberspace is not relevant for security and defense policymaking in the Digital Era. It is just to highlight the fact that valuable resources might be applied to suboptimal alternatives, a trend which might be contradictory during times of economic distress,<sup>9</sup> and might have negative outcomes for countries in the Global South if followed without a great deal of reflection and public debate.

If cyberspace does not seem to be an appropriate warfighting domain, what are the effects of cyberattacks? Can the exploitation of information systems by state and non-state actors yield the same strategic effects of conventional warfare? This leads us to evaluate the concept of war.

Clausewitzian theory of war provides us with the idea that one cannot understand warfare without first understanding its very nature. Some of Clausewitz’s most remarkable lessons teach us that (i) “war is never an isolated act,” (ii) “war does not consist of a single short blow,” and (iii) “in war the result is never final.” (Clausewitz, 2007:17-19) Plus, 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 violence, in Clausewitz’s thinking, is the fundamental aspect of all war. Actually, violence is so important in his understanding of warfare that it plays a central role in his “remarkable trinity.”<sup>10</sup> In this sense, enemies would seek to escalate violence to the extreme in order to dominate, and eventually break, the other’s will.

Taking this very characteristic alone before analyzing Clausewitz’s prerogatives further, it seems hard to compare code-triggered violence to kinetic violence at first sight. “Violence in cyberspace is always indirect,” says Rid. (2012b) Even though it might express itself in other domains (is this not a basic joint operations prerogative after all?), no testified cyber attack has ever caused a single casualty, injured a person, or damaged physical infrastructure.<sup>11</sup> Furthermore, according to Betz (2012:696), “the

---

<sup>9</sup> On January 27, 2013, the *Washington Post* published an article that announced “The Pentagon has approved a major expansion of its cybersecurity force over the next several years, increasing its size more than fivefold to bolster the nation’s ability to defend critical computer systems and conduct offensive computer operations against foreign adversaries.” (Nakashima, 2013) This measure consists of “a huge expansion of U.S. Cyber Command into three ‘teams’ to protect privately owned and operated critical infrastructure such as the electricity grid and banking system; help commanders execute cyberattacks during military operations; and protect Pentagon networks. (...) Not surprisingly, key details of the plan have yet to be worked out.” (Peters, 2013) This comes amidst “the Army Announces a Hiring Freeze” on January 22, 2013, following Secretary of Defense Leon Panetta’s announcing “‘prudent measures’ to prepare for possible budget cuts due to sequestration and an anticipated fight over funding for the rest of the fiscal year. At the time, Panetta said those precautions would include a civilian hiring freeze, delaying some contract awards and trimming non-essential facilities maintenance. The Pentagon also is eliminating 46,000 civilian temp jobs, according to the Associated Press.” (Lunney, 2013)

<sup>10</sup> In depth discussions about the “remarkable trinity” might be found in Paret (1992), Villacres and Bassford (1995), and Echevarria II (2007).

<sup>11</sup> Thomas C. Reed’s memoir book *At the Abyss* (2004) 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 some casualties, even though there are no media reports or official documents to confirm Reed’s allegation. Also, it is not definitely settled whether the Stuxnet attack caused real damage to the Iranian nuclear centrifuges, or if it only rendered them inoperative.

problem is that when [people] talk of ‘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.”

This leads us to the second fundamental aspect of war: its instrumental character. An act of war is always instrumental. 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)

If it is most likely that no cyber offense has ever caused physical harm, on the other hand it is also hard to sustain that any cyber attack reported so far has forced the target to accept the offender’s will. Denial of service attacks such as those perpetrated by groups like Anonymous to take down or deface websites tend to be easily remedied by the victims. And the bulk of scams and espionage that have been happening in the last years through ICT systems does not aim at exercising power over an enemy, but only to exploit information for political, economic, commercial, and other purposes. One could say that it is only a matter of time until the use of coercion takes place: as long as countries keep training people to wage cyberwars and as long as they keep developing digital weapons, a disruptive and decisive attack might actually happen. This idea, as logical as it may be, disregards cyberspace’s malleability pointed out by Libicki (2012) and explained previously. It also disregards a fundamental trait of warfare history: claims that some new technological development or practice will easily cure a major prevailing weakness in war have been repeated vigorously throughout time. “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 unarmed aerial vehicles (UAVs) follows that thread. Nonetheless, despite all past alleged “silver bullets,” warfare main characteristics are still the same. And they will probably remain the same as long as humans are humans.<sup>12</sup>

The third element Clausewitz identified is war’s political nature. According to him, warfare must transcend the use of force. To become “the continuation of policy by other means,” (Clausewitz, 2007:28) warfare has to be attached to a political entity or to a representative of a political entity, whatever its constitutional form. That entity, in its turn, must have an intention, an articulated will which ought to be transmitted to the adversary at some point during the conflict. Finally, violent acts and its larger political intention must also be attributed to one side at some point. As Thomas Rid tells us, “history does not know acts of war without eventual attribution.” (Rid, 2012a:08)

At the same time, it has been exhaustively repeated that one of the basic features of a standalone cyberwar would be its undercover nature. 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, Micheal Gross wrote for *Vanity Fair* in April 2011: “[this] is the new face of 21<sup>st</sup>-century warfare: invisible, anonymous, and devastating.”

---

<sup>12</sup> Nonetheless, van Creveld (2007) points out one exception: “With the advent of nuclear technology, things changed. Provided enough bombs are available, war in its old sense, consisting of action, counteraction, an counter-counteraction, has probably become impossible; if not for all time to come, at any rate as far into the future as we can look at present. Provided both belligerents are nuclear armed, the purpose it serves has also become extremely problematic. The second of these factors explains why, since 1945, wars waged between powerful countries have become exceedingly rare. Technological superiority could only be used, if it could be used at all, against non-nuclear, weak opponents.”

There is no doubt some cyber incidents – despite not being definitely attributable – have been increasingly political in nature (or have been at least 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 (if it was possible to confirm the Russian cyber action against Georgia that would be the only case that would match Clausewitz’s third element).

Some other attacks present political motivation, and have been carried on by apparently institutionalized groups, such as Anonymous, Lulz, and others. The largest operation coordinated by Anonymous so far, “Operation Payback”, was aimed at disrupting on line 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 politicians, e.g., Gov. Sarah Palin and Sen. Joseph Lieberman. The 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 pursuit unleashed against Julian Assange. Those operations comprised website defacements, distributed denial of services attacks, leaks of classified information, etc. But they have simply not been translated into violent acts of any nature. Also, it is hard to precise the real cohesion and political power of these groups, for they seem to lack common grounds, 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 LulzSec and Anonymous (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 of criminal rewards and benefits. (Roberts, 2012; Biddle, 2012) So, it is reasonable to argue that it is very difficult to sustain the idea that such groups already form full political entities. It is also hard to say that they might acquire high levels of allegiance and cohesion (*esprit de corps*) among their ranks. And finally, it is hard to believe that actors other than states do have - at the present time - capabilities to cause continuous harm and havoc through digital means. As it will be shown below, treating the actions perpetrated by such groups as military business might be dangerously biased.

This brings us back to the problem of escalation: “Technology can alter the way in which force is applied – perhaps (though it remains to be seen in practice) it enables an attacker to compel another bloodlessly but it does not obviate the necessity to declare one’s will (even if after the event) (...).” (Betz, 2012:696) As long as war remains as an act of force to compel the enemy to do our will, it requires commitment, not anonymity.<sup>13</sup> In spite of this, opinions *à la Vanity Affair* are not uncommonly seen. Such arguments, however, not only admit the “silver bullet” hypothesis but also exaggerate the conceptual use of the term *war*.

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 travelling (the application of concepts to new cases) and conceptual stretching (the distortion that

---

<sup>13</sup> In this sense, one could probably sustain that hacktivist groups such as Anonymous and LulzSec – while performing undercover actions – could not be accused of perpetrating cyberwar.

occurs when concepts do not fit the new cases). According to him, understanding the extension of a category (the set of entities in the world to which it refers) as well as its intension (the set of meanings or attributes that define the category and determine membership) is essential in order to avoid such mistakes.

This is particularly the case when one refers to *war*. While the use of war as a metaphor is a longstanding literary and rhetorical trope, its political usage might lead to some serious trouble. Childress (2001:181) 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.” While Clausewitz himself does not define anything related to “moral limits in real war,” he does suggest that under certain circumstances limits derived from political calculations may be observed.<sup>14</sup> In this sense, it would not be absurd to “ask of each use of war as a metaphor: Does it generate insights or does it obscure what is going on and what should be done?” (Childress, 2001:195)

Childress however is not suggesting that one should avoid metaphors at all; it is true that we do sometimes use them as merely decorative or dramatic ways to call attention to some point. On the other hand, it does not mean that one should not be conscious of their usage in order to critically assess them. The loose use of the metaphor of war might not only lead to the aforementioned conceptual stretching and distortion of the word, but also to unnecessary alarm regarding, for instance, what has been called “cyberwar.” Asking the right questions while assessing anything “cyber-”related is thus necessary in order not to trivialize real wars and exaggerate other conflicts and problems our society face. Plus, it helps one ward off the use of incongruous or dissonant taxonomies, which might lead to further problems.

Consider, for instance, two widely adopted categorizations of cyber threats and 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 of the classifications are very abstract and treat the same events with different labels. For Lachow (2009:440), Estonia was just a case of *hacktivism*. For Cavelty (2012:109), Estonia should be understood as one of the “main incidents dubbed as cyber war.” What do both say about *hacktivism*? Lachow presents his *hacktivism* matrix this way: *motivation* = *political or social change*; *target* = *decision makers or innocent victims*; *method* = *protests via Web page defacements or distributed denial of service attacks*. For Cavelty, it is *the combination of hacking and activism, including operations that use hacking techniques against a target’s Internet site with the intention of disrupting normal operations*. For Lachow, information war [which encompasses cyberwars] has the following characteristics: *motivation* = *political or military gain*; *target* = *infrastructure, information technology systems and data (public and private)*; *method* = *range of techniques for attack or influence operations*. Cavelty (2012:116) defines cyber war as “the use of computers to disrupt the activities of an enemy country, especially deliberate attacks on communication systems. The term is also used loosely for cyber incidents of a political nature.”

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, Waeber, et. al., 1998) Treating activism, criminal

---

<sup>14</sup> An in depth analysis of public morality in the work of Clausewitz might be seen in Nielsen (2002).

activities, terrorism, and acts of war interchangeably is something that ignores the complexity of those phenomena. And, by throwing different categories of actors under the same umbrella, it poses severe threats to the civil liberties and political rights of individuals all around the world, both in democratic and in autocratic regimes. 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 programme, 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 programme.”

In sum, asking the right questions while assessing anything “cyber-”related is thus necessary in order not to trivialize real wars and exaggerate other conflicts and problems our society face.

## CONCLUSIONS

The following general ideas for furthering inquiry in the field of Security and Strategic Studies are the outcome of the insights and the gaps of this initial exploratory study. It is relevant to state that the list presented below is non exhaustive.

On the theoretical level, a first task is the enlargement of the literature pool revised. Permanent monitoring the academic and technical production in the field, as well as news accounts, might be of great use for furthering the research. Such effort would not only enable the literature’s constant examination, but also provide support for developing complementary knowledge. The use of an online crowdsourcing platform may be a proper way to involve other researchers and institutions in the endeavor.

On the methodological level, longitudinal studies of individual cases can be employed to work with the gathered content in order to pair and correlate academic, technical, and political production to the content of public policies. An increase in the number of cases can enable comparative evaluations, both in longitudinal and in transversal studies. Naturally, the development of appropriate variables for each of those research strategies is an imperative first step to be considered.

Another useful path can be the identification of controversies other than the ones presented above. Initially, this study intended to present two other controversies: the idea that “there is a cyber arms race going on in the world;” and the claim that “international regimes on cyber warfare and on cyber weapons can yield cyber peace and stability.” Due to the inceptive character of this paper, we decided to narrow down the scope of the study. Nonetheless, there is plenty of supportive and contradictory evidence for each of them, which will certainly be subject to scrutiny in upcoming papers. Identifying such controversies, contrasting them to the empirical reality of specific cases, and monitoring how those understandings evolve, both on theoretical terms, as well as on the level of policy-making, might contribute to dissipate part of the fog of (cyber)war.

The furtherance of this research foresees as an immediate first task the buildup of a web platform to offer the general public the pieces that can be freely accessed and shared in order to enable the crowdsourcing of an overarching research agenda for cybersecurity in the Global South.

## REFERENCES

- Arquilla, J. and D. Ronfeldt (1997). In *Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, CA, USA: Rand Publishing.
- Betz, D. (2012). "Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed." *Journal of Strategic Studies*, 35:5, 689-711.
- Biddle, S. (1996). "Victory Misunderstood: What the Gulf War Tells Us About the Future of Conflict." *International Security*, 21:2, 139-180.
- Biddle, S. (2012). "LulzSec Leader Betrays All of Anonymous." Gizmodo. Available on: <http://gizmodo.com/5890825/lulzsec-leader-betrays-all-of-anonymous>. Last accessed: 02/20/2013.
- Bijker, W. E. (2006). "Why and How Technology Matters." *The Oxford Handbook of Contextual Analysis*. R. GOODIN and C. TILLY. New York, NY, USA: Oxford University Press.
- Blumenthal, M. and D. D. Clark (2009). "The Future of the Internet and Cyberpower. Cyberpower and National Security." F. KRAMER, S. STARR and L. WENTZ. Washington, DC, USA: National Defense University Press.
- Buzan, B., O. Waeber, et al. (1998). *Security: A New Framework for Analysis*. Boulder, Colorado, USA: Lynne Rienne Publishers.
- Castells, M. (1996). *The Rise of the Network Society*. Oxford, UK: Blackwell.
- Castells, M. (1999). *Information Technology, Globalization and Social Development*. Geneva, Switzerland: United Nations Research Institute for Social Development. Available on: [http://www.unrisd.org/unrisd/website/document.nsf/ab82a6805797760f80256b4f005da1ab/f270e0c066f3de7780256b67005b728c/\\$file/dp114.pdf](http://www.unrisd.org/unrisd/website/document.nsf/ab82a6805797760f80256b4f005da1ab/f270e0c066f3de7780256b67005b728c/$file/dp114.pdf). Last accessed: 02/12/2013.
- Cavelty, M. D. (2012). "The Militarisation of Cyber Security as a Source of Global Tension. Strategic Trends 2012: Key Developments in Global Affairs." D. MÖCKLY. Zurich, Switzerland, Center for Security Studies (CSS), ETH Zurich. Available on: [http://www.css.ethz.ch/publications/Strategic\\_Trends\\_EN](http://www.css.ethz.ch/publications/Strategic_Trends_EN). Last accessed: 08/12/2012.
- Childress, J. F. (2001). "The War Metaphor in Public Policy: Some Moral Reflections. The Leader's Imperative: Ethics, Integrity, and Responsibility." J. C. FICARROTA. West Lafayette, Indiana, USA: 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):2-10.
- Clarke, R. and R. Knake (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. New York, NY, USA: Ecco Press.
- Clausewitz, C. V. (2007). *On War*. Oxford, UK, Oxford University Press.
- Cohen, E. (1999). "American Views of the Revolution in Military Affairs." *Mideast Security and Policy Studies*, 28.
- 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 'Cibernetica'." Colombia.com. Available on: <http://www.colombia.com/tecnologia/actualidad/sdi/31440/expertos-creen-que-estamos-frente-a-una-guerra-cibernetica>. Last accessed: 15/12/2012.
- CrySyS Lab (2012). sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks. Available on: [www.crysys.hu/skywiper/skywiper.pdf](http://www.crysys.hu/skywiper/skywiper.pdf). Last accessed: 08/27/2012.
- Denning, D. E. (2009). "Barriers to Entry: Are They Lower for Cyber Warfare?" *IO Journal* 1(1):4.
- Duarte, E. E. (2012). *Conduta na Guerra na Era Digital e suas Implicações para o Brasil: Uma Análise de Conceitos, Políticas e Práticas de Defesa*. Rio de Janeiro, RJ, Brasil: Instituto de Pesquisa Econômica Aplicada.
- Echevarria II, A. (2007). *Clausewitz and Contemporary War*. Oxford, UK: Oxford University Press.
- Eriksson, J. and G. Giacomello (2007). *International Relations and Security in the Digital Age*. New York, NY, USA: Routledge.





- Eubanks, V. (2012). *Digital Dead End: Fighting for Social Justice in the Information Age*. Cambridge, MA, USA: MIT Press.
- Fogarty, K. (2011). "LulzSec vs. Anonymous: Doing Hacktivism Wrong." *IT World*. Available on: <http://www.itworld.com/security/174917/lulzsec-vs-anonymous-doing-hacktivism-wrong>. Last accessed: 02/20/2013.
- Freeman, C. and F. Louçã (2001). *As Time Goes By: From the Industrial Revolutions to the Information Revolution*. New York, NY, USA: Oxford University Press.
- Giles, K. (2011). "Information Troops" – A Russian Cyber Command? 2011 3rd International Conference on Cyber Conflict, Tallinn, Estonia: CCD COE Publications. Available on: <http://www.ccdcoe.org/publications/2011proceedings/InformationTroopsARussianCyberCommand-Giles.pdf>. Last accessed: 03/23/2012.
- Goldsmith, J. (2010). *The New Vulnerability*, *The New Republic* (June 24, 2010). Available on: <http://www.tnr.com/article/books-and-arts/75262/the-new-vulnerability>. Last accessed: 09/12/2012.
- Hansen, L. and H. Nissenbaum (2009). "Digital Disaster, Cyber Security, and the Copenhagen School." *International Studies Quarterly*, 53, 1155-1175.
- Headrick, D. (2009). *Technology: A World History*. Oxford, UK: Oxford University Press.
- Hsiao, R. (2010). "China's Cyber Command?" *China Brief*, 10:15, 01-02. Available on: [http://www.jamestown.org/uploads/media/cb\\_010\\_74.pdf](http://www.jamestown.org/uploads/media/cb_010_74.pdf). Last accessed: 08/27/2012.
- Jasanoff, S. (2006). "Technology as a Site and Object of Politics." *The Oxford Handbook of Contextual Analysis*. R. GOODIN and C. TILLY. New York, NY, USA: Oxford University Press.
- Kaspersky (2012). *Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts*. Available on: [http://www.kaspersky.com/about/news/virus/2012/Kaspersky\\_Lab\\_and\\_ITU\\_Discover\\_Gauss\\_A\\_New\\_Complex\\_Cyber\\_Threat\\_Designed\\_to\\_Monitor\\_Online\\_Banking\\_Accounts](http://www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts). Last accessed: 08/27/2012.
- Kim, D. and M. G. Solomon (2010). *Fundamentals of Information Systems Security*. Burlington, MA, USA: Jones & Bartlett Learning.
- Kramer, F., S. Starr, et al. (2009). *Cyberpower and National Security*. Washington, DC, USA: National Defense University Press.
- Kuehl, D. (2009). "From Cyberspace to Cyberpower: Defining the Problem. *Cyberpower and National Security*." F. KRAMER, S. STARR and L. WENTZ. Washington, DC, USA: National Defense University Press.
- Kurbalija, J. and E. Gelbstein (2005). *Gobernanza de Internet: Asuntos, Actores y Brechas*. Geneva, Switzerland: Diplo Foundation.
- Lachow, I. (2009). "Cyberterrorism: Menace or Myth. *Cyberpower and National Security*." F. KRAMER, S. STARR and L. WENTZ. Washington, DC, USA: National Defense University Press.
- Libicki, M. C. (2012). "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy*, 8:2.
- Lucas, M. (2012). "Matrix, o el Nuevo Campo de Batalla." *Revista DEF*. Available on: <http://www.defonline.com.ar/?p=8935>. Last accessed: 01/05/2013.
- Lunney, K. (2013). "Army Announces Hiring Freeze." *Government Executive*. Available on: <http://www.govexec.com/defense/2013/01/army-announces-hiring-freeze/60893/>. Last Accessed: 01/28/2013.
- Lynn, W. F. (2010). "Defending a New Domain: The Pentagon's New Cyberstrategy." *Foreign Affairs* 89(September/October 2010). Also Available on: [http://www.defense.gov/home/features/2010/0410\\_cybersec/lynn-article1.aspx](http://www.defense.gov/home/features/2010/0410_cybersec/lynn-article1.aspx). Last accessed: 04/11/2012.
- Martins, J. M. Q. (2008). *Digitalização e Guerra Local: Como Fatores do Equilíbrio Internacional*. PhD Dissertation (Political Science). Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Ciência Política, Universidade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, RS, Brazil. Available on: <http://hdl.handle.net/10183/14405>. Last accessed: 03/07/2011.
- Mowthorpe, M. (2005). "The Revolution in Military Affairs (RMA): the United States, Russian and Chinese Views." *Journal of Social, Political and Economic Studies*, 30:2, 137.



- Mueller, M. (2010). *Networks and States: The Global Politics of Internet Governance*. Cambridge, MA, USA, The MIT Press.
- Mumford, L. (1964). "Authoritarian and Democratic Technics." *Technology and Culture* 5, 01-08.
- Nakashima, E. (2011). "U.S. Cyberweapons Had Been Considered to Disrupt Gaddafi's Air Defenses." *The Washington Post*. Available on: [http://articles.washingtonpost.com/2011-10-17/world/35276890\\_1\\_cyberattack-air-defenses-operation-odyssey-dawn](http://articles.washingtonpost.com/2011-10-17/world/35276890_1_cyberattack-air-defenses-operation-odyssey-dawn). Last accessed: 11/23/2011.
- Nakashima, E. (2013). "Pentagon to Boost Cybersecurity Force." *The Washington Post*. Available on: [http://articles.washingtonpost.com/2013-01-27/world/36583575\\_1\\_cyber-protection-forces-cyber-command-cybersecurity](http://articles.washingtonpost.com/2013-01-27/world/36583575_1_cyber-protection-forces-cyber-command-cybersecurity). Last accessed: 01/28/2013.
- Nielsen, S. (2002). *The Public Morality of Carl von Clausewitz*. Available on: <http://isanet.ccit.arizona.edu/noarchive/nielsen.html>. Last accessed: 02/21/2013.
- 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*. Available on: <http://www.defonline.com.ar/?p=9064>. Last accessed: 01/05/2013.
- O'Hanlon, M. (1998). *Beware the "RMA'nia!"*, Washington, DC, USA: National.
- O'Harrow, R. (2006). *No Place to Hide*. New York, NY, USA: Free Press.
- Paret, P. (1992). *Understanding War: Essays on Clausewitz and the History of Military Power*. Princeton, NJ, Princeton: University Press.
- Peters, K. M. (2013). "Cyber Command's Growth Plan Raises a Lot of Questions." *Netxgov*. Available on: <http://www.nextgov.com/cybersecurity/cybersecurity-report/2013/01/cyber-commands-growth-plan-raises-lot-questions/60909/>. Last accessed: 02/01/2013.
- Proença Jr., D. (2009). *Nota Técnica: Condicionantes e Requisitos para um Sistema de Inteligência Vantajoso para o Brasil*. Centro Gestão e Estudos Estratégicos. Brasília, DF, Brasil: GSI/PR: 1-23.
- Reed, T. (2007). *At the Abyss: An Insider's History of the Cold War*. New York, NY, USA: Random House Publishing Group.
- Rennstich, J. K. (2008). *The Making of a Digital World: The Evolution of Technological Change and How it Shaped Our World*. New York, NY, USA: Palgrave Macmillan.
- Rid, T. (2012a). "Cyber War Will Not Take Place." *Journal of Strategic Studies*, 35:1, 05-32.
- Rid, T. (2012b). "What War in the Fifth Domain?" *Kings of War*. Available on: <http://kingsofwar.org.uk/2012/08/what-war-in-the-fifth-domain/>. Last accessed: 21/02/2013.
- Roberts, P. (2012). "LulzSec informant Sabu Rewarded with Six Months Freedom for Helping Feds." *Naked Security*. Available on: <http://nakedsecurity.sophos.com/2012/08/23/sabu-lulzsec-freedom/>. Last accessed: 02/20/2013.
- Ronfeldt, D. and A. Martínez (1997). "A Comment on the Zapatista 'Netwar'." In *Athena's Camp: Preparing for Conflict in the Information A. J. ARQUILLA and D. RONFELDT*. Santa Monica, CA, USA: Rand Publishing.
- Rumsfeld, D. H. (2002). "Transforming the Military." *Foreign Affairs* 81(3): 20-32.
- 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.
- Smit, W. A. (2006). *Military Technology and Politics. The Oxford Handbook of Contextual Analysis*. R. GOODIN and C. TILLY. New York, NY, USA: Oxford University Press.
- Sommer, P. and I. Brown (2011). *Reducing Systemic Cybersecurity Risk*. Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS(2011)3. Available on: <http://eprints.lse.ac.uk/31964/>. Last accessed: 02/26/2012.
- Stamp, M. (2011). *Information Security: Principles and Practices*. Hoboken, New Jersey: Wiley.



- The Economist (2010). War in the Fifth Domain. Available on: <http://www.economist.com/node/16478792>. Last accessed: 02/21/2012.
- USA (2005). U.S. National Defense Strategy. Available on: <http://www.defense.gov/news/mar2005/d20050318nds1.pdf>. Last accessed: 01/20/2013.
- USA (2012). Sustaining US Global Leadership: Priorities for 21st Century Defense. Available on: [http://www.defense.gov/news/defense\\_strategic\\_guidance.pdf](http://www.defense.gov/news/defense_strategic_guidance.pdf). Last accessed: 01/17/2013.
- Uzal, R. (2012). “¿Es la Guerra Cibernética el Desafío más Relevante de la Defensa Nacional?” Mochila Virtual - Infantería Argentina. Available on: <http://www.mochiladelinfante.com.ar/defensa/89-yies-la-guerra-cibernytica-el-desafno-mbs-relevante-de-la-defensa-nacional.html>. Last accessed: 01/21/2013.
- Van Creveld, M. (2007). “War and Technology.” The Newsletter of FPRI’s Wachman Center, 12:25.
- Van Dijk, J. A. G. (2005). The Deepening Divide: Inequality in the Information Society. Thousand Oaks, CA, USA: Sage.
- Villacres, E. and C. Bassford (1995). “Reclaiming the Clausewitzian Trinity.” Parameters, 25, 09-19.
- Washington Post (2012). “U.S. Accelerating Cyberweapon Research.” The Washington Post. Available on: [http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS\\_story\\_1.html](http://www.washingtonpost.com/world/national-security/us-accelerating-cyberweapon-research/2012/03/13/gIQAMRGVLS_story_1.html). Last accessed: 04/25/2012.
- Weimann, G. (2004a). www.terror.net: How Modern Terrorism Uses the Internet. Washington, DC, USA: United States Institute of Peace. Available on: <http://www.usip.org/files/resources/sr116.pdf>. Last accessed: 08/27/2012.
- Weimann, G. (2004b). Cyberterrorism: How Real Is the Threat? Washington, DC, USA: United States Institute of Peace. Available at <http://www.usip.org/files/resources/sr119.pdf>. Last accessed: 08/27/2012.
- Weimann, G. (2005). “Cyberterrorism: The Sum of All Fears?” Studies in Conflicts & Terrorism, 28:2, 219-149.
- Weimann, G. (2006). “Virtual Disputes: The Use of the Internet for Terrorist Debates.” Studies in Conflicts & Terrorism, 29:7, 623-639.
- Winner, L. (1986). The Whale and the Reactor: A Search for Limits in an Age of High Technology. Chicago, IL, USA: The University of Chicago Press.
- World Internet Users and Populations (2012). Internet Usage Statistics – The Internet Big Picture. Available on: <http://www.internetworldstats.com/stats.htm>. Las access: 07/12/2012.
- Zimet, E. and C. L. Barry (2009). “Military Service Overview. Cyberpower and National Security.” F. KRAMER, S. STARR and L. WENTZ. Washington, DC, USA: National Defense University Press.
- Zukang, S. (2007). “Message by Sha Zukang, Under-Secretary-General, United Nations Department of Economic and Social Affairs (UNDESA).” Internet Governance Forum: The First Two Years. KLEINWÄCHTER, W. Available on: [http://www.intgovforum.org/cms/hydera/IGFBook\\_the\\_first\\_two\\_years.pdf](http://www.intgovforum.org/cms/hydera/IGFBook_the_first_two_years.pdf). Last Access: 07/12/2012.