WORKING DRAFT:
PLEASE DO NOT CITE WITHOUT AUTHORS' PERMISSION

Three Controversies on Cyberwar: a Critical Perspective

Marco Cepik – marco.cepik [at] ufrgs.br
Diego Rafael Canabarro – diego.canabarro [at] ufrgs.br / diego [at] pubpol.umass.edu
Thiago Borne – thiago.borne [at] ufrgs.br

Paper to be presented at the

71st MPSA Annual Conference
April 11-14, 2013 – Chicago (IL), USA
Session: 17 - International Security (23 - Ethics and International Security)
04/12/2013

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License

CC BY NC SA

THREE CONTROVERSIES ON CYBERWAR: A CRITICAL PERSPECTIVE

Diego Rafael Canabarro[1]
Thiago Borne[2]
Marco Cepik[3]

Abstract: The spread of contemporary information and communication technologies among state and non-state actors adds new dimensions to the study of diffusion in global politics. The Digital Era brings about different challenges for national and international security policymaking, heating up academic and political debate surrounding the scope and the implications of the term cyberwar. This paper surveys the evolution of academic and technical production on cyberwar with the intention of providing background for the critical evaluation of the Brazilian case. Finally, it details the prospective research agenda that follows from the evaluation of the Brazilian case.[4]

1. Introduction

This paper aims at assessing three widespread assertions related to the highly controversial issue of cyberwar. It does so by using the following approach: Section 2 presents three 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 them is scrutinized according to supportive or contradictory logical, theoretical and empirical evidence (Section 3), with the intention of providing the intellectual background for the critical evaluation of the Brazilian case (Section 4). Finally, it consolidates findings and points out paths for furthering inquiry and policy development in the field, both for the case of Brazil and other countries in general.

Firstly, it seeks to highlight the fact that "the fog of cyberwar" (Tennant, 2009; Morozov, 2009; Greenemeier, 2011; Valeriano & Maness, 2012) encompasses not only the real uncertainties surrounding the interrelations between cyberspace and military planning and operation, but also a

[1] PhD candidate in Political Science at UFRGS and research assistant at CEGOV/UFRGS. Currently, Diego works as a Visiting Doctoral Fellow at the National Center for Digital Government (NCDG) – University of Massachusetts, Amherst.

[2] PhD candidate in Strategic Studies at UFRGS and research assistant at CEGOV/UFRGS.

[3] Professor of Political Science and Strategic Studies at the Federal University of Rio Grande do Sul (UFRGS), Porto Alegre, Brazil. Director of the Center for International Studies on Government (CEGOV/UFRGS).

[4] A first draft of this paper authored by Diego Canabarro and Thiago Borne was presented at the Junior Scholar Symposium of the 54th ISA Annual Conference, in San Francisco, CA, on 04/04/2013. The authors are greatly indebted to Lucas Rezende, Lídia Lage, Michael Mongeau, Fernanda Barasuol, and Raquel Rocha, who kindly reviewed and offered insightful comments to the first draft of this paper. They would also like to thank their fellow researchers at CEGOV for the stimulus and support for writing this paper. Finally, they would like to thank the research community of NCDG – in the person of Dr. Jane Fountain – for the public review meeting on 02/27/2013, which evaluated two working papers ("Reflections on the Fog of Cyberwar" and "Brazil and the Fog of Cyberwar"), and provided important input for the final version submitted for the conference, as well as for the furtherance of our research.

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.

2. Three Controversies Revised

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)[5] 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)

"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.[6] Accordingly,

[5] 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)

[6] 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 changing 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

cc BY NC SA

"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 Martí [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)

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.[7] In recent years, however, "cyber-" became increasingly identified with the pervasiveness of cyberspace[8] – "an operational

---

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."

[7] 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).

[8] 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

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)[9] 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 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 21st 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

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).

[9] 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)

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 Cybesecurity 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.

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.[10] 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.

P1 - 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,

[10] 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. Last accessed: 01/29/2013.

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)

P2 - 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 cybertechnology 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 accidently 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)

P3 - 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 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." (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)

3. 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 innumerous 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:

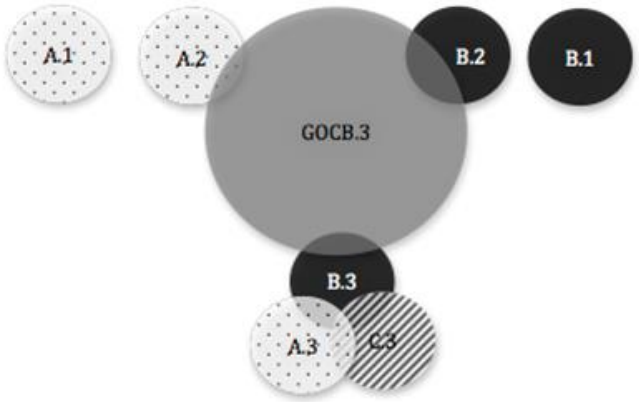

Figure 1: a simplified graphical representation of Cyberspace adapted from Zimet & Barry (2009:288) and Libicki (2012:326).

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).[11]

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 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

[11] The illustration does not intend to represent the different sizes and individual characteristics of each system.

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,[12] 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."[13] 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.[14] Furthermore, according to Betz (2012:696), "the 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)

---

[12] 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)

[13] In depth discussions about the "remarkable trinity" might be found in Paret (1992), Villacres and Bassford (1995), and Echevarria II (2007).

[14] 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.

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.[15]

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 21st-century warfare: invisible, anonymous, and devastating."

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

[15] 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."

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.[16] 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 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

[16] In this sense, one could probably sustain that hacktivist groups such as Anonymous and LulzSec – while performing undercovered actions – could not be accused of perpetrating cyberwar.

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.[17] 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, Waever, et. al., 1998) Treating activism, criminal 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

[17] An in depth analysis of public morality in the work of Clausewitz might be seen in Nielsen (2002).

> "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. Next section looks at the Brazilian approach to cybersecurity, in an attempt to map the country's recent developments on the matter.

4. The Brazilian Approach to Cybersecurity

Data retrieved from the Brazilian Center of Studies on Information and Communication Technologies (CETIC.br, 2011) reveal that figures vary a lot when it comes to the number of households[18] that possess ICTs (related or not to the Internet) in Brazil: TV sets (98%), cell phones (87%), radios (80%), fixed telephone lines (37%), PCs (36%), laptops (18%), satellite TV (52%), and videogames (22%). Only thirty-two percent (32%) of the households in Brazil have access to the Internet. Sixty-five percent (65%) of those connect to the Internet with speeds greater than 256 Kbps. Around fifty-three percent (53%) of the population has already accessed the Internet. [19] During the last surveyed year (2011-2012), thirty-one percent (31%) of the ones who had already accessed the Internet had used some sort of e-government service in order to acquire information (23%) and to perform *on line* transactions such as paying taxes, filling-in forms, and downloading software (11%). Twenty-nine percent (29%) of the Internet users in the country have already purchased goods and services through the Internet.[20]

Mobile technology has also spread on a fast track in the country, following a worldwide trend. (ITU, 2011) The Brazilian Agency for Telecommunications (ANATEL) reports that, by the end of 2012, around 260 million cell phones were operating in the country (more than 1,3 line *per capita*).

Up to the 1990s, the telecom market in Brazil was largely monopolized by the public sector. Liberal policies adopted in the mid-1990s[21] led the government to transfer its assets to the private sector through a process of privatization, and the Federal Government became a mere regulator of the telecom market. (Miranda, Kune & Piani, 2011)

With telecom liberalization, coupled with the commercialization Internet access in the turn of the century, a myriad of service providers of all sorts entered the stage. Today, private foreign and

[18] The last census carried out in Brazil (2010) estimates that the country has a population of over 190 million people living in 67,5 million households. For more information, see the website of the Brazilian Census Bureau (IBGE) on: http://www.ibge.gov.br/english/. Last accessed: 12/13/2012.

[19] From 2005 to 2011, the pool of Internet in Brazil users grew from 32% to the current 53%.At home, at work, at school, at a friend's house, at an Internet café or Telecenter, and through a cell phone. The most common applications are: e-mails exchange (78%), social networking (69%), blogging, twitting, and creating webpages in general (37%).

[20] Among the top-three reasons for not interacting with governmental agencies and online stores are: the need of having interpersonal contact, security/privacy issues, and difficulties for using the services (especially e-government).

[21] The country abided by the tenets of the goods and services trade liberalization advanced within the World Trade Organization. (Schiller, 1999; Drake, 2008)

domestic companies (such as Telefónica/Vivo, Claro Américas/Claro, Embratel/Oi, etc.) own the largest part of the infrastructural backbone of telecom networks. Most notably, the cables for the connection of Brazil's domestic networks to the ones located abroad are property of the formerly government-owned Embratel, currently an open-capital company controlled by *Forbes Magazine* number one billionaire of 2012, Carlos Slim Helú from Mexico.

Governments in the federal, state, and municipal levels maintain exclusive networks for different purposes (finances, health care, education, transportation, law enforcement and security, defense, etc.), and with different levels of interconnectivity among themselves and with other privately-owned networks.[22]

That is just a summarized snapshot of part[23] of the Brazilian cyberspace. It does not include, for example, the (foreign) satellite networks used in the country, dedicated lines of communication used by the private sector, the mix of different networked solutions (in-house and outsourced) that the military rely on for running activities, as well as for maintaining communication lines among its three branches. But it serves to highlight the daunting scope of providing security and defense for Brazil in the Digital Era.

Despite the Brazilian growing reliance on ICT, studying its security policy towards cyberspace might be a particularly daunting task. The lack of information on the subject – even in Portuguese – is an obstacle that any researcher will face. Furthermore, the key official documents dealing with the topic, the *National Strategy of Defense* (NSD) and the *White Paper to Guide Future Defense Priorities*, are sometimes dully repetitive and little enlightening. Both documents are, nonetheless, landmarks in defense policymaking in Brazil. They are part of a movement towards transparency and civilian control over the military, which started with the promulgation of the 1988 Constitution and culminated in the creation of a civilian-led Ministry of Defense (MD) in 1999, responsible for all three branches of the armed forces. Those documents also reflect efforts taken in order to staff the MD with its own professional defense bureaucracy[24] while devising the notion that national development is tightly bound to national defense. (Brazil, 2005; 2008b; 2012) Understanding the

[22] For instance, the Ipê Network – the first Brazilian point of access to the global Internet – operates under the responsibility of the Ministry of Science and Technology and is dedicated to the interconnection of education and research institutions. For further information, please see: http://www.rnp.br/. The Ministry of Planning, Management, and Budgeting is setting up a network called Infovia to supply Brasília (DF), Brazil's capital, with a reliable, exclusive and secure backbone for telephone and Internet communication among agencies of the Federal Government. This model of network is already in place in different states and cities of Brazil. Please see: http://www.governoeletronico.gov.br/acoes-e-projetos/infovia for further information. Recently, Brazil reactivated Telebras. The company, which was the former state-owned monopolistic telephone company running under the responsibility of the Ministry of Communications is the solution adopted by the government to overcome some market distortions in the supply of broadband Internet to some areas of the country. The company was put in charge of building the infrastructure toe advance the National Broadband Plan. It also is supposed to function as an Internet Service Provider. More information about Telebras on: http://www.telebras.com.br/a_telebras.php. For details on the scope of the Brazilian National Broadband plan, see: http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl. See also the case of the cities of Porto Alegre (RS) and Belo Horizonte (MG), respectively, on http://www.procempa.com.br/default.php?p_secao=19 and http://pwweb2.procempa.com.br/pmpa/prefpoa/abemtic/usu_doc/prodabel.pdf. All websites were last accessed on: 01/21/2013.

[23] For a broader (but still partial) view of the Brazilian cyberspace, please see the technical information provided by ANATEL regarding telecom networks in the country, on: http://www.anatel.gov.br/Portal/exibirPortalInternet.do#. Last accessed: 01/23/2012.

[24] According to Fishman and Manwaring (2011), the MD was initially staffed by "an agglomeration of foreigners," meaning that the Ministry was staffed by technicians and professionals from Petrobras, the Bank of Brazil, and various other government agencies.

broader context that helped shaping these provisions is thus necessary in order to assess the Brazilian approach towards cybersecurity.

The years that followed the 21-year period of military control over Brazil were marked by severe political and economic difficulties. In the political realm, former President Fernando Collor's impeachment and corruption-related scandals distressed the emergent Brazilian democracy, while economic difficulties were mainly related to the necessity to curb inflation, to establish the basis for long-term stability and growth, and to reduce Brazil's extreme socioeconomic inequalities. At the same time, the Brazilian foreign policy adopted a more globalist-oriented view of world politics, which drifted away the realist military influence over the country's international affairs. According to Cervo and Bueno (2002:469), "by separating the two strategic fields [the doctrine of security that guided foreign policy during the military regime and the defense policy], (…) [Brazil] distanced itself from realism and embarked in utopia." In other words, the country's foreign policy underplayed force as a means of action in international relations in favor of persuasion and soft power. It is therefore not astonishing to notice that substantial military reforms have been postponed for almost a decade after liberalization. (Vizentini, 2005)

The first *National Policy of Defense* (NPD) was published in 1996 during former President Fernando Henrique Cardoso's term. The NPD made public the country's security priorities for the first time in history, and thus represented a major milestone for the formulation of a national defense agenda. It was built around two central pillars: active diplomacy (peaceful resolution of conflicts) and conventional deterrence. The document was designed in order to guarantee the country's sovereignty and the safety of national wealth; to guarantee respect for the rule of law and democratic institutions; to maintain the national unity; to protect citizen rights and the Brazilian interests abroad; to provide the country with a more significant role in international affairs; and to contribute to the maintenance of international peace and security. (Brazil, 1996; Oliveira, 2005; Costa, 2006)

The NPD also determined the establishment of a Ministry of Defense (MD) run by civilian administration to subordinate all three branches of the armed forces (the Air Force, the Navy, and the Army), which happened three years after the document was released, in 1999. The creation of the MD meant an important step towards the consolidation of democracy in the country, as it allowed increased civilian control over the military, a tendency that has been widespread all over Latin America since the late 1980s.[25] Once implemented, the Ministry allowed the development of a more cohesive discourse for the drafting of the second NPD, and represented a breakthrough in terms of institutionalization in the field of defense in Brazil. (Fuccille, 2006; Pagliari, 2009)

The second NPD, released during the first term of President Luiz Inácio Lula da Silva in 2005, expanded the concept of security used so far to incorporate an even broader approach whereby political, economic, environmental and social factors might also be seen as threats to the state. Moreover, the document emphasized the threats posed by non-state actors to both national and international security. Following the former policies stipulations, the new NPD also characterized South America as a peaceful continent, despite recognizing the existence of some zones of instability and the occurrence of transnational organized crime in the region. The need to sustain national sovereignty and the defense of the state were reaffirmed as important means of curbing such issues. The commitment to regional integration was also reiterated, as well as the protection of borders and sensitive areas as the "Green Amazon" (land and river areas within the Amazon Basin) and the "Blue Amazon" (coastal areas where major hydro-carbon and other resources are located). (Brazil, 2005)

[25] In fact, Brazil was the last country in the region to unify the military under a single ministry.

All these efforts, however important, did not address cybersecurity issues in depth. Actually, the very first national document to mention anything "cyber-" was the second NPD: "To minimize the harm a cyber attack may cause, it is essential to continuously improve safety devices and to adopt procedures to reduce the vulnerability of [computer] systems and allow their prompt recovery." (Brazil, 2005) The subject was left aside from the political debate until 2008, when the *National Strategy of Defense* was released.

The National Strategy of Defense and the White Paper to Guide Future Defense Priorities

In the beginning of his second term as President of Brazil, Lula da Silva directed the development of the *National Strategy of Defense* (NSD). In the months leading up to the release of the document, a Ministerial Committee was established to design it. The Committee was chaired by the former Minister of Defense Nelson Jobim and coordinated by the former Minister-in-Chief of the Secretariat for Strategic Affairs of the Presidency Roberto Mangabeira Unger, and worked in close consultations with civilian and military experts. The document that ensued from the effort focuses on middle and long term strategic objectives for the country, and aims at modernizing the national defense structure acting upon three structuring axes: (i) the reorganization of the armed forces, (ii) the restructuring of Brazilian defense industry, and (iii) the composition of the troops and the future of the Mandatory Military Service. Along with these guidelines, the role of three "decisive sectors for national defense" is discussed: "space", "nuclear", and "cybernetics [sic]."

The NSD thus identifies the need for the development of autonomous technological capabilities in the aforementioned sectors by acknowledging that "whoever does not master critical technologies is neither independent for defense nor for development." (Brazil, 2008b:09) Despite recognizing that "these sectors transcend the border line between development and defense, between the civilian and the military" (Brazil, 2008b:12), the NSD assigns each branch of the armed forces specific mandates to develop each of the decisive sectors.

Special attention is given to the interaction between the "space" and the "cybernetics" [sic] sectors, as the document understands that they, combined, will "enable that the capacity to see one's own country do not depend on foreign technology, and that the armed forces, together, can network supported by a space-based monitoring system." [sic] (Brazil, 2008b:12)

Also according to the NSD,

> "[c]apacity building on cybernetics will be focused on the widest spectrum of industrial, educational and military uses. As a priority, it will include the technologies of communication between all contingents of the armed forces, in order to ensure their capacity to network. They will consider the power of communication between the contingents of the armed forces and space vehicles." (Brazil, 2008b:33)

As to "cybernetics" alone, the NSD simply foresees the establishment of "an organization in charge of developing cybernetic capacities on the industrial and military themes." (Brazil, 2008b:33) Only two years after the release of the NSD, the first steps for the creation of the said organization were taken.

In 2010, the Command of the Army adopted Ordinances ("Portarias") n. 666 and n. 667, which established the Brazilian Cyber Defense Center Nucleus (NU CDCiber) under the responsibility of the Army's Department of Science and Technology. During 2011 and 2012, the Army advanced with the institutionalization of the Center. NU CDCiber's first task was the protection of the

network upon which relied the United Nations Conference on Sustainable Development (Rio +20), held in Rio de Janeiro in 2012.[26]

In 2012, Brazil adopted the *White Paper to Guide Future Defense Priorities*. Among other provisions, the document foresees the creation of a full-fledged Brazilian Center for Cyberdefense (CDCiber) by 2015. The main distinction between the NU CDCiber and the CDCiber deals with institutionalization: the latter is expected to be formally established through a Presidential Decree aimed at changing the regimental structure of the Army.[27]

The White Paper provides details as to how the armed forces will implement the NSD, which laid ground for more open, transparent communication of the country's defense and security objectives. It resulted from a series of seminars held throughout the country in 2012, broken down by the strategic themes outlined in the Paper. Among the themes comprised by the document stand the strategic scenario for the 21st century; national defense policy and strategy; modernization of the armed forces; rationalization and adaptation of defense structures; economic support of national defense; separate analyses on the Army, Navy and Air Force, and finally peacekeeping operations and humanitarian aid. The three decisive sectors pointed by the NSD are also subject of brief scrutiny.

Regarding "cybernetics," the White Paper stresses that "the protection of cyberspace covers a wide range of areas such as training, intelligence, scientific research, doctrine, preparation and operational employment and personnel management. It also comprises protecting their own assets and the ability to networked operations." (Brazil, 2012:49) In this sense, the text does not go far beyond what was previously stated in the 2008 Plan. On the other hand, it reinforces the call on the military to design forces to meet such requirements, on the defense industry to equip the armed forces accordingly, and on the people to serve a role in the execution of the policy.

But the White Paper's greatest importance actually lies in some short-term actions envisioned for cyber defense, such as building CDCiber's permanent headquarters and the acquisition of support infrastructure, the purchase of equipment and the training of human resources, the procurement of hardware and software solutions for cyber defense, and the implementation of structuring cyber-related projects, which would ultimately increase the country's ability to respond to both national and international threats. (Brazil, 2012:198) All these actions are covered by the so-called Cyber

[26] During the II Brazilian Internet Forum, held in Recife in July 2012, Lt. Col. Cláudio Borges Coelho from the Brazilian Army detailed the operation: around R$ 20 million (approximately US$ 10 million) were spent to "ensure the cyber security" of the Conference. The overall mission of the armed forces comprised the protection of lands, waters and the air surrounding the Conference center, as well as counter-terrorism and cybersecurity. The military devised efforts to interoperate with the Federal Police, the Brazilian Agency for Telecommunications (ANATEL), and the Brazilian National Computer Emergency Response Team (CERT.br) of the Brazilian Internet Steering Committee (CGI.br). The expected challenges were said to be, among others, website defacements and the need to reconfigure the network in virtue of overload and tentative attacks. In the occasion, Anonymous managed to post a video on the Conference homepage, protesting against the lack of participation of civil society in the high-level debates on climate change that took place. Also, in a coordinated effort, several activists took down a great number of websites, among them, the Brazilian Senate's website, the website of the Office of the UN in Brazil, and the website of the National Institute for Agrarian Reform and Colonization. A detailed account of the Anonymous action can be seen on the following website: http://www.tecmundo.com.br/ataque-hacker/25395-anonymous-brasil-ophackinrio-tira-do-ar-dezenas-de-sites-governamentais.htm. Last accessed: 11/24/2012.

[27] According to an interview given by Gen. José Carlos dos Santos – the responsible for NU CDCiber – to the largest newspaper in Brazil (*Folha de São Paulo*) in May 2012, the Decree was being analyzed by the Ministry of Planning, Management and Budget before being sent to President Dilma Rousseff's office for her final decision on the matter. Interview available on: http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml. Last accessed: 11/23/2012.

Defense Project, which aims at investing almost R$ 840 million (US$ 420 million) up to 2031. The Project is headed by the Army, but minor efforts are also expected to be launched by the other branches of the armed forces, with an estimated budget of R$ 58 million (US$ 29 million) more.

The Green Book on Brazil's Cybersecurity and the (Upcoming) National Cybersecurity Policy

Efforts on the matter are not only under the responsibility of the Ministry of Defense. The Institutional Security Cabinet of the President's Office has set up a Department of Information and Communications Security (DSIC), responsible for "planning and coordinating the cyber and information and communications security of the Federal government in Brazil." (Brazil, 2010c) Despite having a narrow (the Federal sphere) and developmental (capacity building and risk mitigation) scope, the Department, in partnership with the University of Brasilia, functions as a clearinghouse for cyber-related information. DSIC has been working in close collaboration with other branches of the Brazilian government (including the military) in order to foster the adoption of cybersecurity principles, best practices, and standards for safety and security engineering of information systems. In 2010, the department issued a *Reference Guide for the Security of Critical Information Infrastructures*. (Canongia, Gonçalves Jr., & Mandarino, 2010) The publication describes common threats and vulnerabilities (related to hardware, software, networks, peopleware, etc.), and recommends several policies focused on resilience and redundancy of information systems, as well as on capacity-building schemes aimed at creating "a culture of cyber and information security" within the bureaucracy and the population at large. In the same year, DSIC published the *Green Book on Brazil's Cybersecurity*. (Canongia & Mandarino, 2010) The Green Book highlights the challenges Brazil has to tackle in terms of cybersecurity. They range from economic, social and political-institutional aspects (such as the creation of stimuli for the national IT industry and the adaptation of the legal framework surrounding ICT-enactment in the public sector), to strategic aspects (such as the importance of developing in-house capability and the adoption of open source software). The idea behind the publication is to make the Brazilian population sensitive of the importance of the topic, so that it can fully participate in the open debates that will be entertained for the adoption of the White Paper, or the "National Cybersecurity Policy," in a near time in the future.

These efforts show Brazil seems to be following what is possibly the hippest trend in Security Studies: the urgent tackling of what has been commonly called "cyber-"related threats. In fact, this trend has pushed governments throughout South America towards developing similar programs. Efforts have also been made in the multilateral level. Regional organizations like the Southern Common Market (Mercosur) and the Union of South American Nations (Unasur) have established particular *fora* for debating transnational cybercrimes and cyberterrorism.[28] While these moves

[28] Within Mercosur, the topic is discussed together with other actions aimed at curbing organized crime, cross-border trafficking, etc. On the other hand, Unasur has implemented a special Working Group to establish regional policies and mechanisms to address cyber threats and information technology in terms of defense. On the hemispheric level, it is relevant to recall that the Organization for American States (OAS) adopted, in 2004, a "A Comprehensive Inter-American Cybersecurity Strategy" with the objective of developing "a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyberattacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems." The strategy has a civilian character and aims at fostering the development of legal tools for the combat of all sorts of cyber crime. It set up an "Inter-American Alert, Watch, and Warning Network" in order to "rapidly disseminate cybersecurity information and respond to crises, incidents, and threats to computer security." Despite having a larger scope than the scope of this study, this initiative is worth quoting, for it contends without further qualification and precision that "criminals such as 'hackers,' organized crime groups, and terrorists are increasingly

demonstrate South American governments are completely aware of one of the most important current security threats, they must be interpreted with caution: these countries might be replicating controversies that still are not fully comprehended by part of the international community.

As seen hitherto, Brazil has been pursuing information and communications security, as well as cybersecurity and defense through the integrated efforts of the leading DSIC (attached to the office of the President) and through Army's NU CDCiber (in the future, just CDCiber). The fog of (cyber)war blurs the boundaries between those roles. Bellow, we turn to the evaluation of the approach adopted by Brazil between 2008 and 2012 to deal with the complex array of "cyber issues" in light of the content presented in sections 3 and 4. Highlighting the positive and negative aspects of such an enterprise is a small first step that can contribute to qualify research and public policymaking.

5. Concluding Thoughts on Brazil and Further Inquiry

Among the positive aspects of the Brazilian endeavor, the first one to be highlighted is the country's willingness to cope with the challenges inherent to the digitalization of society at large. The incorporation of topics such as information and communications security, and cyberdefense in the policy agenda of the country seems to be a proper initial response for the increasing reliance on cyberspace of a myriad of productive activities in different areas of society. It also underlines that Brazil is tuned to what is happening all over the world, both in terms of disruptive events and policy trends. Before the attacks to web sites that happened during Rio +20 Brazil had not registered any major cyber incident.[29] Even before 2012 the MD and the Institutional Security Cabinet of the President's Office had already been taking measures aimed at mitigating ICT-related risks and at forestalling threats to information systems in general.

That two-front action reveals another positive aspect identified by our evaluation: the Brazilian initiative counts on both civilian and military facets. The first is responsible for the formulation of principles and norms, as well as best practices and frameworks, all intended to foster safety and security engineering in the development and adoption of IT solutions in the federal government. The latter has a more restrict and pragmatic – despite more complex - mandate: the development of defensive and offensive capabilities related to cyberspace as power leverage for Brazil's conducting its international affairs. This specialized approach, if integrated and coordinated, can increase the resilience of the country in face of cyber threats, for it has the potential of creating a common approach for the organization and governance of Brazil's cyberspace, which can facilitate the

exploiting the Internet for illicit purposes and engineering new methods of using the Internet to commit and facilitate crime. These illegal activities, commonly referred to as 'cyber-crimes,' hinder the growth and development of the Internet by fostering the fear that the Internet is neither a secure nor a trustworthy medium for conducting personal, government, or business transactions." This wording is addressed under section 4 of this paper.

[29] In 2009, Brazil suffered severe blackouts as a result of a general failure of transmission lines related to the Itaipu hydroelectric plant, owned by Brazil and Paraguay. Ninety per cent of the territory of the latter was affected and remained in the dark for more than half an hour. Four different states in Brazil were also severely affected, and around ninety million people lost electric power for more than five hours. Some days before the blackouts, CBS's "60 Minutes" program had displayed a piece of news contending that prior blackouts that happened in Brazil (2005 and 2007), as well as in the U.S., were caused by hack attacks. The Brazilian government promptly denied those claims, explaining that dirty insulators on transmission towers caused the blackouts. Some leaked diplomatic cables released by Wikileaks in 2010 reinforced the government's explanation. For further information on the topic, see: http://www.wired.com/threatlevel/2010/12/brazil-blackout/. Last accessed: 01/20/2013.

planning and orchestration of emergency responses and of defense policy-making and operations. Evidence of this trend can be found in the express recognition by MD officials that a collaborative approach to cyber security and defense could yield better results in terms of preparation for dealing with and of the appropriateness and effectiveness of responses to cyber events. Another piece of evidence of this trend can be found in the assembly of a joint task force responsible for assuring the security and defense of the networks that supported communication channels during Rio +20. A closer scrutiny of the action of that task force reveals that several of the IT-systems adopted for the conference were not off-the-shelf. They were customized not only in order to better suit the needs of the users, but also as a way of increasing their inviolability.

When it comes to the issue of offensive capabilities, though, the boundaries of what is legal and what is not within the scope of International Law are completely blurred. This lack of common ground on the international level coupled with the concerns raised before in this text – about the complexity of offense on cyberspace – reveals a potential pitfall for the Brazilian strategy: developing offensive capabilities that deal essentially with the surveillance of other actors in the context of a normative vacuum can lead the country to cross the line of legality and to decrease instead of increasing its national security.

A final positive aspect that must be highlighted is the collaborative and participatory policy-making process that characterizes the adoption of documents such as the END, the White Paper, and the Green Book presented in section 2. During the preparatory phase, as well as in the review and publication phases, the MD and the Department of Information and Communications Security of the President's Cabinet have realized public seminars and openly published documents on the Web to allow the participation of citizens and stakeholders interested in the debates. For instance, in the case of the *White Paper to Guide Future Defense Priorities*, the MD conducted a series of six national seminars in the five major regions of Brazil to present and debate the document through the lenses of specialists, and to gather inputs from the participants. In the case of the *Green Book on Brazil's Cybersecurity*, DSIC started publicizing the document with the intention of fostering the dialogue among different state and non-state actors that shall serve as the basis for the production of a more definite White Book on the matter. These efforts reflect the willingness of the Brazilian state not only to broaden dialogue between civil society, the public administration, and the military, but also to strengthen the country's transparency and democracy levels.

Despite having adopted some very sound paths for enhancing its security and increasing its defense capabilities in the Digital Era, the current Brazilian approach might suffer from the conceptual flaws discussed in this article, entailing negative effects on national security and broader societal relations.

First, Brazil treats "cybernetics" as a fifth domain for waging war. As pointed out above, two lines of reasoning contradict this position. Firstly, the progressive digital convergence of all media to Internet-based technologies, as well as the pervasive character of the Net, tends to "cyber" everything. But this homogeneous set of systems, however big, is still only part of cyberspace. As long as the level of interconnectivity among IT systems matters, it is practically impossible to determine the full scope of cyberspace. Secondly, granting a system more or less interconnectivity is a decision taken mainly by the people who design and develop such systems. And engineering decisions cannot be segregated from broader sociopolitical contexts. Thus, it might be relevant to retrieve "cyber-"s original meaning from its Greek root. Instead of narrowly focusing only on technological systems, a turn to the myriad of institutional and organizational settings that influence the adoption of those systems could be more fruitful for the development of security and defense policies. Addressing, for instance, the *locus* of ICT-related decisions within the military and its ties

with other civilian agencies may be better than just institutionalizing cyber cabinets in charge of developing policies to be applied elsewhere.

From this perspective arise the following questions: what is the precise role of cyber commands and cyber battalions? How should they relate to the overarching organization of government? Should they be a privileged group of experts capable of operating IT systems more or less connected to each other even if agreed that cyberspace has no clearly defined boundaries? Or should they function as focal points for the adaptation of all other sectors of the military to better operate in the Digital Era? Shouldn't cyber capabilities and skills be a fundamental competence for top-ranking officials in charge of developing military strategies in the 21st century?

Moreover, governance transcends the sphere of government, for it also encompasses the whole of state–society relations. As shown in section 3, the securitization of cyberspace has been based on a very diffuse perception of what the contemporary threats to national and international security are. State and non-state actors have been equated as major foes. This is also the case in Brazil. Take, for instance, the list of cyberspace-related threats presented by public officials during the seminars that preceded the White Paper's release: in order of increasing severity, hacktivism, cybercrimes, espionage, sabotage, terrorism and war were commonly mentioned. It is pretty rare, though, to see such list enriched with a thorough evaluation of the inherent complexity of each of those acts.

Treating those categories alike tend to disregard important power asymmetries that are analytically and practically relevant to compare and contrast states among themselves, and states *vis-à-vis* non-state actors. While the Internet offers a cheap and easy way of entering cyberspace, it does not automatically mean that they are synonyms. Since cyberspace is a complex set of more or less interconnected information systems, the capacity to mobilize resources (political, financial, societal, human, technical, etc.) to explore – and eventually exploit – them matters as it does in every other realm of social life. An intelligence report on China's cyber activities recently published by the private information security company Mandiant shows that the country "maintains an extensive infrastructure of computer systems around the world", which "implies a large organization with at least dozens, but potentially hundreds of human operators." (Mandiant, 2013:04-05) In the U.S., for instance, amidst several budgetary constraints to the military, investment on cyber security and defense has steadily risen. In the near future, it is hard to believe that non-state actors might match state capacity, and that states with less overall capacity might overcome asymmetries by merely turning to the "cyber".

The equation of cyber foes has two major consequences. In the first place, it makes it more difficult to adopt appropriate policies for dealing with cyber insecurity. As a result, it can compromise the adoption of preemptive measures and actual responses to disruptive cyber events. After all, the requirements for dealing with web page defacements are different than those required for protecting and assuring air-gapped communication lines. But more importantly, the fog that surrounds the precise definition of cyber threats and foes has a lot to do with the proper balance between the fundamental rights of individuals (civil and political) and the rights of the states (that enable them to fulfill their role in the provision of security, justice and welfare). What are the limits for state action in relation to the privacy of its citizens? In virtue of the decentralized and distributed architecture of cyberspace, what sort of extraterritorial side effects should one expect from the monitoring and surveillance activities developed by a state in order either to secure or to defend its own cyberspace or to explore other actors' cyberspace? Are the penalties that have been summoned to cyber events reasonable and suitable for what they entail? How open and participatory are decision-making processes that deal with such trade-off?

The Brazilian case shows that it is reasonable to say that despite the participatory approach to the development of its cyber security and defense policy, the implementation and institutionalization processes detailed by the documents reviewed in section 2 still lack oversight and accountability.

Following the Brazilian case up can enlighten the criticisms raised in this text. The positive and negative aspects pointed out above are not exclusive to Brazil. In fact, they pave the way for further comparative inquiry in the field.

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 is necessary for furthering the research. 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 comparative studies can be employed to pair and correlate academic, technical, and political production to the content of public policies. The development of appropriate variables for each of those research strategies is an imperative first step.

6. References

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

Arquilla, J. and D. Ronfeldt (2001). Networks and Netwars: The Future of Terror, Crime and Militancy. 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.

Brazil (1996). Política de Defesa Nacional. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Last accessed: 02/20/2013.

Brazil (2005). Política de Defesa Nacional. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Last accessed: 02/20/2013.

Brazil (2008a). Estratégia Nacional de Defesa. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm. Last accessed: 02/20/2013.

Brazil (2008b). National Strategy of Defense. Available on: http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_ingles.pdf. Last accessed: 02/20/2013.

Brazil (2010) Census 2010. Available on: http://censo2010.ibge.gov.br/. Last accessed: 02/20/2013.

Brazil (2010a). Ordinance n. 666, issued by the Command of the Army on August 4th, 2010. Available on:

cc BY NC SA

http://tinyurl.com/aebz5yw. Last accessed: 02/19/2013.

Brazil (2010b). Ordinance n. 667, issued by the Command of the Army on August 4th, 2010. Available on: http://tinyurl.com/aebz5yw. Last accessed: 02/19/2013.

Brazil (2010c). Presidential Decree n. 7.411/2010, issued on December 12th, 2010. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7411.htm. Last accessed: 02/20/2013.

Brazil (2012). Livro Branco de Defesa Nacional. Available on: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf. Last accessed: 02/21/2013.

Bruneau, T. (1992). "Brazil's Political Transition." Elites and Democratic Consolidation in Latin America and Southern Europe. J. HIGLEY, R. GUNTHER. Cambridge, UK: Cambridge University Press.

Buzan, B., O. Waever, et al. (1998). Security: A New Framework for Analysis. Boulder, Colorado, USA: Lynne Rienne Publishers.

Canongia, C., A. G. Junior, et al. (2010). Guia de Referência para a Segurança das Infraestruturas Críticas da Informação. Brasília, DF, Brasil: GSIPR/SE/DSIC.

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. 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. Last accessed: 08/12/2012.

Cervo A. L. and C. Bueno (2002). História da Política Exterior do Brasil. Brasília, DF, Brazil: Editora UnB.

CETIC.br (2011). ICT Households and Enterprises (2011) - Survey on the Use of InformatIon and CommunIcation Technologies in Brazil. Available on: http://cetic.br. Last accessed: 01/25/2013.

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 'Cibernética'." 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.

Costa, T. G. (2006). "Em Busca da Relevância: Os Desafios do Brasil na Segurança Internacional do Pós-Guerra Fria." Relações Internacionais do Brasil: Temas e Agendas. H. OLIVEIRA and A. C. LESSA. São Paulo, SP, Brasil: Saraiva.

CrySyS Lab (2012). sKyWIper (a.k.a. Flame a.k.a. Flamer): A Complex Malware for Targeted Attacks. Available on:

cc BY NC SA

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.

Diamond, L., J. Linz and S. Lipset (1989). Democracy in Developing Countries: Latin America. London, UK: Adamantine Press.

Drake, W. (2008). "Introduction. Governing Global Electronic Networks: International Perspective on Policy and Power." W. J. DRAKE and E. J. WILSON. London, UK, MIT Press.

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.

Fishman A. and M. Manwaring (2011). "Brazil's Security Strategy and Defense Doctrine." Colloquium Brief. U.S. Army War College, Strategic Studies Institute.

Fogarty, K. (2011). "LulzSec vs. Anonymous: Doing Hacktivism Wrong." IT World. Available on: http://www.itworld.com/security/174917/lulzsec-vs-anonymous-doing-hactivism-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.

Fuccille, A. Democracia e Questão Militar: A Criação do Ministério da Defesa no Brasil. PhD Dissertation (Political Science). Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Ciência Política, Universidade Estadual de Campinas (UNICAMP), Campinas, SP, Brazil. Available on: http://cutter.unicamp.br/document/?code=vtls000378085. Last accessed: 09/10/2012.

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.

Greenemeier, L. (2011). "The Fog of Cyberwar: What are the Rules of Engagement?" Scientific American (June 13, 2011). Available on: http://www.scientificamerican.com/article.cfm?id=fog-of-cyber-warfare. Last accessed: 02/21/2013.

Gross, M. J. (2011). "A Declaration of Cyber-War." Vanity Fair. Available on: http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104. Last accessed: 02/20/2013.

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. Last accessed: 08/27/2012.

ITU (2011). World Telecommunication/ICT Indicators Database. Available on: http://www.itu.int/ITU-D/ict/statistics/.

cc BY NC SA

Last accessed: 12/05/2012.

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. Last accessed: 08/27/2012.

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

Kinzo, M. (1993). “Consolidation of Democracy: Governability and Political Parties in Brazil.” Growth and Development in Brazil: Cardoso’s Real Challenge. M. KINZO and V. BULMER-THOMAS. London, UK, Institute of Latin American Studies: University of London.

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.

Lamounier, B. (1993). “Institutional Structure and Governability in the 1990s.” M. KINZO and V. BULMER-THOMAS. London, UK, Institute of Latin American Studies: University of London.

Libicki, M. C. (2007). Conquest in Cyberspace. Cambridge, MA, USA: Cambridge University Press.

Libicki, M. C. (2012). “Cyberspace Is Not a Warfighting Domain.” I/S: A Journal of Law and Policy, 8:2.

Libicki, M. C. and P. A. Force (2009). Cyberdeterrence and Cyberwar, Santa Monica, CA, USA: RAND Corporation.

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. Last accessed: 04/11/2012.

Mandarino, R. and C. Canongia (2010). Livro Verde de Segurança Cibernética no Brasil. Brasília, DF, Brasil: GSIPR/SE/DSIC.

Mandiant (2013). APT1: Exposing One of China's Cyber Espionage Units. Available on: http://intelreport.mandiant.com/. Last accessed: 02/21/2013.

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.

Miranda, P., H. Kume, et al. (2011). Liberalização do Comércio de Serviços: O Caso do Setor de Telecomunicações no

Brasil. Rio de Janeiro, RJ, Brasil: IPEA.

Morozov, E. (2009). "The Fog of Cyberwar." Newsweek International 153(17). Available on: http://www.thedailybeast.com/newsweek/2009/04/17/the-fog-of-cyberwar.html. Last accessed: 02/10/2013.

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. 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. 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. Las accessed: 02/21/2013.

Nissenbaum, H. (2005). "Where Computer Security Meets Mational 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'Donnell, G., P. Schmitter and L. Whitehead (1986). Transitions from Authoritarian Rule: Latin America. London, UK: John Hopkins University Press.

O'Hanlon, M. (1998). Beware the "RMA'nia!", Washington, DC, USA: National.

OAS (2004). A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Available on: http://www.oas.org/juridico/english/cyber_security.htm. Last accessed: 12/28/2012.

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

Oliveira, H. A. (2005). Política Externa Brasileira. São Paulo, SP, Brasil: Saraiva.

Pagliari, G. C. (2009). O Brasil e a Segurança na América do Sul. São Paulo, SP, Brasil: Juruá Editora.

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.

Sadek, M. (1995). “Institutional Fragility and Judicial Problems in Brazil.” M. KINZO and V. BULMER-THOMAS. London, UK, Institute of Latin American Studies: University of London.

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

Sartori, G. (1984). “Guidelines for Concepts Analysis.” Social Science Concepts: A Systematic Analysis. G. SARTORI. Beverly Hills, CA, USA: Sage.

Schiller, D. (2000). Digital Capitalism: Networking the Global Market System. Cambridge, MA, USA: MIT Press.

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.

Selcher, W. (1 986). Political Liberalization in Brazil: Dynamics, Dilemmas, and Future Prospects. Boulder, CO, USA: Westview Press.

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.

Souza, C. (1996). “Redemocratization and Decentralization in Brazil: The Strength of the Member States.” Development and Change, 27, 529-555.

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

Stepan, A. (1989). Democratizing Brazil: Problems of Transition and Consolidation. Oxford, UK: Oxford University Press.

Symantec (2011). W32. Stuxnet Dossier. Available on: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf. Last accessed: 08/27/2012.

Tennant, D. (2009). “The Fog of (Cyber) War.” Government IT. Available on: http://www.computerworld.com/s/article/9130830/The_fog_of_cyber_war. Last accessed: 02/22/2013.

The Economist (2010). War in the Fifth Domain. Available on: http://www.economist.com/node/16478792. Last accessed: 02/21/2012.

USA (2003). U.S. National Strategy to Secure Cyberspace. Available on: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf. Last accessed: 01/20/2013.

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. 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.

Valeriano, B. and R. Maness (2012). "The Fog of Cyberwar." Foreign Affairs (November 21st, 2012). Available on: http://www.foreignaffairs.com/articles/138443/brandon-valeriano-and-ryan-maness/the-fog-of-cyberwar?cid=nlc-this_week_on_foreignaffairs_co-120612-the_fog_of_cyberwar_4-120612. Last accessed: 02/20/2013.

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.

Vizentini, P. G. F. (2002). Relações Internacionais do Brasil: de Vargas a Lula. São Paulo, SP, Brasil: Fundação Perseu Abramo.

Vizentini, P. G. F. (2005). "De FHC a Lula: Uma Década de Política Externa (1995-2005)." Civitas – Revista de Ciências Sociais, 5:2, 381-397.

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. 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. Last Access: 07/12/2012.