Conference on Cyber Conflict
Proceedings 2010
C. Czosseck and K. Podins (Eds.)
CCD COE Publications, 2010, Tallinn, Estonia.

GETTING THE ESSENCE OF CYBERSPACE; A THEORETICAL FRAMEWORK TO FACE CYBER ISSUES

Vincent JOUBERT[a1]

[a]*Raoul Dandurand Chair, Montréal, Québec, Canada*

Abstract: If a nation wants to be a great cyber power, it must elaborate a comprehensive national cyber strategy that will encompass the changes brought out by cyber capabilities and interconnected networks. This strategy must be conceived within a theoretical framework that defines the essential concepts of the cyber domain. To understand why this theoretical framework is vital to a nation's efficient cyber power, we will analyze the national strategy developed by the United States and the People's Republic of China and set the limits of each strategy.

An analysis of the military approach to the cyber domain of the two nations will show how these powers developed strong capacities and elaborated a holistic doctrine that allows the armies to wage Network Centric Warfare; after this statement, our analysis will lead us to consider the influence of the political and economic regimes on the securitization of the cyber domain.

The limits of the actual strategies will help us demonstrate that the cyber domain and its concept need to be clearly defined by the political, military, economic and academic spheres to provide a theoretical framework; such a framework, in the end, will help the governments adopting an efficient and comprehensive national cyber strategy that will serve the nation's interests and economy.

Keywords: Strategy, theoretical framework, cyberspace, United States, People's Republic of China, political regime.

1 Raoul Dandurand Chair of Strategic and Diplomatic Studies, 455 boul. René-Lévesque Est, UQAM, Pavillon Hubert Aquin, 4e étage, Bureau A-4410, Montréal (Québec) H2L 4Y2, CANADA. Email: vincent.joubert1@hotmail.fr.

INTRODUCTION

Cyber attacks are emerging as one of the types of new threats nations will have to face in future wars. Cyber conflicts are becoming part of more traditional conflicts, and digitalized nations have to elaborate a response plan to secure their networks and the nations' interests against the growing cyber threat. This response plan has to encompass every area affected by cyber conflicts, which pretty much represents all the most important sectors of modern societies as they all deeply rely on digital infrastructures and, therefore, face greater cyber attacks with strong consequences.

Because of its sole nature cyberspace cannot be controlled, even by an international organization such as NATO – the complexity of this man-made domain makes its dominance arguably impossible (Kramer, 2009). However, there are some steps government officials, military chiefs and policymakers must take to fully understand the issues and the consequences cyberspace and cyber conflicts have on international relations and modern societies, and try to regulate its use as well as secure their national networks.

One important step governments must take is the elaboration of a comprehensive national cyber strategy in which national interests would be protected and political objectives pursued. This strategy should provide a global evaluation of the environmental modifications cyberspace and cyber capabilities have created, and shall be derived from a theoretical framework that identifies the existing cyber concepts and from which the political objectives can be identified.

Such a theoretical framework is vital to understanding the cyber domain and developing relevant policies that will allow "digitalized" nations to secure their networks. Like all other new technologies, the cyber domain has created military strategy modifications that impact the global interactions between nations as it affects the very character of war (Cebrowski & Garstka, 1998). In this context, understanding the modifications of the threat perception and what security means in cyberspace will provide an answer on how to secure cyberspace. Because the goal for the governments is to secure their networks and build offensive and defensive cyber capacities, there has to be a theory that defines all the different concepts that exist and cohabit in the cyber domain: cyber attack, cyber threat, cyberwar, cyber crime, cyber espionage, and cyber conflict.

The theoretical framework has to conciliate diverging opinions and define the common vision nations have on the cyber domain and its concepts to provide a comprehensive analytical framework to the decision-makers.

This is a hard task because nations have different national interests and rules that drive their societies. The government must therefore conciliate numerous securities

interests in cyber security, a terrain in which multiple discourses and securities compete (Hansen & Nissenbaum, 2009, 8), and all the referent objects are intertwined.

To understand why a theoretical framework that defines the cyber concepts and their meaning for national cyber security strategies is vital, we will undertake an analysis of the United States' [US] and the People's Republic of China's [PRC] approaches regarding cyberspace.

We will first analyze the United States' cyber strategy by looking at its military doctrine and strategy on cyberspace, the internal organization, the government's role and implication. In a second part, we will proceed with that of the PRC; we will look at how Chinese military strategists have developed a modern doctrine which includes the cyber capabilities in their traditional military doctrine, and then see how the closed nature of the Chinese political regime has allowed the central government to maintain rigid control over China's national networks. The conclusion of this paper will emphasize the limits of both types of cyber security approaches; our former analysis will lead us to question the impact of the governmental regime's nature on national cyber strategies, and to demonstrate the need for a theoretical framework for cyberspace and cyber concepts in order to better understand and manage future cyber conflicts.

1. THE UNITED STATES' LOSS OF CONTROL

The cyber domain as we know it today is the technical development of an American invention which was designed to exchange knowledge through the US in a very short time. The scientists who created the ARPANET network back in 1969 did certainly not imagine the possibilities they initiated then.

As the technologies improved, the United States and the world discovered the power of computers and networking; today, modern societies – the US on top – relies deeply on digital infrastructures and networks, and faces the possibility of being under cyber attack. The United States may even be more at risk for they are the primary world power and therefore are the target of many opponents. For the last twenty years though, the United States has failed to devise a strategy that would enable the nation to counter the new cyber threat and protect the American interests.

1.1 AN IDEALISTIC VISION OF WAR

"Our assessments of conflict scenarios involving state adversaries pointed to the need for improved capabilities to counter threats in cyberspace—a global domain within the information environment that encompasses the interdependent networks of information technology infrastructures, including the Internet and telecommunications networks. Although it is a man-made domain, cyberspace is now as relevant a domain for [Department of Defense] DoD activities as the naturally occurring domains of land, sea, air, and space. There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. In the 21st century, modern armed forces simply cannot conduct high-tempo, effective operations without resilient, reliable information and communications networks and assured access to cyberspace" (*Quadrennial Defense Review Report*, 2010, [QDR report]).

This is how the Department of Defense qualifies the growing relation between the US army, modern conflicts and cyberspace. The presence of a section specifically dedicated to cyberspace in the QDR Report is quite significant and reveals the importance the highest ranked military officials give to this domain (William J. Lynn III, 2010). Both the inclusion of a section in the QDR report and the increasing budget attribution make it clear that the US government has decided to enhance its capacities that will provide the nation with appropriate network defense.

The growing attention given to cyberspace can easily be understood by a simple analysis of the current US military doctrine. As the QDR report determines and expresses the defense strategy of the United States and establishes a defense program for the next 20 years (US State Code, 2004), it provides the government with a comprehensive definition of US strategic objectives and identifies the threats the United States could face in the future. Since the 1990s, the importance given to the technology as a vital tool to improve the army's operations' efficiency has led to the concept of the Revolution in Military Affairs [RMA], which was defined in 1993 by M.J. Mazarr as fundamental progress in technology or in doctrine or in an organization that renders the actual way of waging war obsolete. The RMA concept was based on four major concepts that would lead the US army to rethink its organization and to give technology tremendous importance. Those concepts are: information dominance, disengaged combats, synergy, and civilianization of conflict. Like we said, technology development had a huge impact on the elaboration of the RMA doctrine; taken as a whole, the RMA encompasses three components: the technological component manifested by the development and the use of new Information Technologies, the organizational component manifested by the army's command jointness, and the conceptual component in which technology has given rise to a

major military concept, the Effect-Based Approach to Operations [EBAO]. The EBAO concept is seen as "a process for obtaining a desired strategic outcome or 'effect' on the enemy through the synergistic and cumulative application of the full range of military and non-military capabilities at all levels of conflict" where an effect is "the physical, functional, or psychological outcome, event or consequence that results from specific military or non-military actions" (USJFCOM, 2010). It basically analyzed battlefields as a system in which the US army defined the most sensitive points that would blind and deafen the adversary and therefore render him unable to wage war (Coquet, 2007).

Following the RMA logic, Donald D. Rumsfeld, then Secretary of Defense, began the US Army's *Transformation* in 2001; this transformation would modify the American army and forge the ideas that would allow the United States to face future threats, by deeply reorganizing the army's structure and focusing on technologies' use to win future conflicts. This technology-centered approach is very typical of American culture; US Army leaders have always considered technology as the key answer to new threats and have developed an almost religious-like trust in it (Henrotin, 2008).

The development of Information Technologies and the fast spread of the Internet network contributed to the rise of a new kind of warfare such as Information Operation [IO] and Network Centric Warfare [NCW]; as the essential component of the EBAO concept and a central component of the RMA, information itself became essential to control in order to win modern wars. Those wars are tightly linked with the capacity for the US Army to achieve full-spectrum dominance in its operations, and the relation between IO and cyberspace was made clear in Joint Publication 3-13 when defining IO as: "the integrated employment of the core capabilities of Electronic Warfare, Computer Network Operations, Psychological Operations, Military Deception, and Operational Security in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision-making while protecting our own". Some authors think it is erroneous to equate cyberspace with IO though; they rather view cyberspace as a critical aspect of the global information environment through which information operations are conducted, but not as the entire environment (Khuel, 2010; England, 2008).

Cyberspace and cyberwar offer unprecedented possibilities to military society, because modern societies rely deeply on networks and digital infrastructures, and moving warfare in cyberspace would give rise to new kinds of threats and new kinds of attacks. Cyberwar perfectly matches the idealistic RMA's vision of war in its possibility to wage a fast, long-distance and conclusive war with no casualties and little collateral damage (Henrotin, 2008).

Unfortunately, even if the networks are nowadays omnipresent the idealistic vision

of war as wanted in the RMA does not mirror the reality of conflicts. The technological answer NCW was supposed to provide to any kind of conflict faced the harsh reality of the vital importance of the human aspect of war (Wilson, 2007). The disillusions created by the tactical and strategic difficulties the US Army faced in the Afghanistani and Iraqi conflicts did not stop the army's organizational and doctrinal adaptations; both the Navy and the Air Force took action to improve their capabilities to operate in cyberspace, and the Army and the Marine Corps are also developing concepts and capabilities for cyber operations (Khuel, 2010). Cyberspace represents a new domain and strategists face the challenge to integrate its capabilities with other elements and instruments of power. Such can be achieved by drafting a national cyber strategy that would define the political objectives, be integrated in the broader national defense strategy, and which would be a strategy of partnership with all the actors present in cyberspace. This is precisely what the United States has failed to do.

1.2 A POLITICAL AND ECONOMIC EXPLANATION OF THE FAILURES

Nearly every day the United States is discovering new threats and attacks against the country's networks. Inadequate cyber security and loss of valuable data have inflicted considerable damage to US national security (CSIS, 2008).

Over the last two decades, the presidential administrations have recognized the strategic importance of cyberspace; governmental measures like the *Presidential Decision Directive/NSC-63* (Clinton administration, 1998) and *The National Strategy to Secure Cyberspace* (The White House, 2003) have been taken to maintain the US's competitiveness in this domain, yet the latest officials' reports reveal a real problem of coordination between federal agencies that are in charge of the US networks' security (GAO-10-338, 2010; McAfee report, 2009). Several simulation exercises were made to evaluate the US cyber defense capabilities such as Cyberstorm I & II, and as for now, the results point out a worrying absence of coordination, task appointment and clear hierarchy between federal agencies (GAO-08-825, 2008). When writing this paper at the very beginning of 2010, there were eight agencies in charge of protecting and defending US networks and vital digital infrastructures; global US networks cannot be efficiently managed if those agencies have overlapping and uncoordinated responsibilities for cyber security. The bureaucratic disputes that can occur between some agencies will also increase delay and inefficiency in the response to a cyber attack and will be damageable to the whole US network (Halperin, Clapp, 2006). Following the 60 Days Cyber Policy Review's recommendations, Barack Obama appointed Howard A. Schmidt New Cyber Coordinator last December; this is a first step in improving the coordination and the collaboration between

those agencies, hence reducing the vulnerabilities on the networks and improving cyber security. Disorganized federal management of cyber attacks is truly harmful to the US networks' security and can be modified with a clear and holistic mission order established by the White House.

Securing the US's critical digital infrastructures cannot be done only by federal agencies though, for the majority of the network is designed, owned and used by private companies. Private sector interests and national security challenges are therefore intertwined in the cyber domain and the government has to find the right balance to involve these companies in building strong cyber defenses without creating obstacles to their business. The public and the private sectors have different objectives and different budget management, and where the public sector will spend more money on securing the networks to avoid intrusions or attacks, the private sector will be more likely to think in terms of profits and business expansion at the expense of security improvement (Cyber Policy Review, 2009).

There is little doubt that cyberwarfare will have a significant impact on the private sector, but the roles and responsibilities remain unclear in case of a conflict and neither the government nor the private sector will benefit from this situation. Companies that design and produce software will have to play a role in cyber security, but the limits of their responsibility and the exact nature of their role in detection and response are not specified and nobody can provide an answer on that specific point (McAfee, 2009).

The recent cyber incidents show that deregulation has proven its inability to create a safe and secured cyber environment because self-regulation obviously did not work.

The absence of regulation in today's cyberspace represents a great danger to cyber security. The intellectual heritage of deregulation of the last administration leaves a continuing feeling that regulation is an obstacle to free-market economics and innovation and is not a solution to improving cyber security. Some comparisons with other regulated areas aim to prove that regulation is a danger for innovation and not the key to a secure cyberspace. The key argument of deregulation partisans is that regulation will impose certain standards and forbid experimentations, which is a vital aspect of competitiveness and free-market economics (Harper, 2009; Lewis, 2009). The pro-regulation answer is that regulation is not always bad for development of the market and innovation in a society where security and safe products are highly demanded. Therefore it would be adequate to ask private companies for more security standards in the cyber products and services they provide, and the companies could manage to find in security competitiveness new market opportunities. Regulation must not be overly prescriptive, but looking at the actual cyber environment, regulation will be better than no regulation at all (Lewis, 2009).

Here the US government faces a problem that is directly linked to the economic regime of the country; the economic principles that drive the American market emphasize individual freedom and market freedom and free enterprise that have not precluded a major role for the government (United States Information Agency, 1992). However, the threats created by cyberspace might affect the whole of US security and the economy if the *status quo* is maintained. The government will have to work in close collaboration with the private sector to find a solution that won't affect those pillars of American state power.

Another problem that inhibits efficient collaboration between the public and the private sectors is about privacy points; this concern tends to restrain the private sector from automatically sharing information with the federal agencies to strengthen security on their networks. Industry has also expressed reservations about disclosing to the Federal government sensitive or proprietary business information, such as vulnerabilities and data or network breaches (Cyber Policy Review, 2009). The private sector believes that sharing a vulnerability with the government authorities might expose their company to potential economic disadvantage, for their customers would not trust the company and therefore deal with the competitor. A vulnerability disclosure would financially affect their business so the company will try to manage the problem alone, hiding the attack and not alerting the authorities.

The government must take a strong decision to conceal those concerns and tighten private-public sector collaboration. An efficiently secured global network cannot be possible without it. China, on the other hand, does not face such a problem.

2. THE PEOPLE'S REPUBLIC OF CHINA'S INFORMATION WARFARE STRATEGY

The People's Republic of China (PRC) developed an Information Warfare (IW) strategy a decade ago to leapfrog the technological-military delay they had *vis-à-vis* the United States. When looking at the PRC's actual cyber capabilities, you can easily come to the conclusion that the strategy they elaborated and established was a success.

2.1 CHINESE MILITARY STRATEGY THINKING

The Chinese strategic mind-set differs markedly from that of the US. The People's Liberation Army's (PLA) officers and military strategists have developed specific concepts that guide the strategic choices of the PRC and that led the PLA to conduct its own Revolution in Military Affairs.

Even though the Chinese don't use the word cyber in their lexicon to qualify the new technologies and rather talk about *informatization*, one must not be misled here; they are talking about cyber capabilities and cyberspace to wage information warfare (Thomas, 2009).

An ongoing critic of the Chinese military doctrine regarding information warfare is that it is not really a Chinese doctrine; the literature on this subject describes the strong similarities of the Chinese Information Warfare strategy with that of America (Mulvenon, 1999). Ten years ago, some of the most respectable American researchers stated that the PLA did not have a coherent information warfare doctrine, nothing compared to the US's writings on the subject, and that even though the PLA's capabilities were growing, they did not match their strategies. Since then, opinions have changed as the PLA developed a coherent doctrine and the matching capabilities (Gertz, 2009).

Two of the most important and influential Chinese military strategists, Li Bingyan and Dai Qingmin, characterized the modifications cyber capabilities brought to modern conflicts. They both agree on the fact that the perception of war has changed and that the strategy must therefore be adapted to these changes; Chinese military strategy should absorb new methodologies such as cybernetics and information theories but also integrate them to ancient military stratagems. A new strategy that includes cyber capabilities will also give the PRC the opportunity to use asymmetric means against more powerful nations such as the United States (Li, 2004; Dai, 2002). In other words, cyberspace gives new tools to the PRC that they can use to improve their military assets and capabilities that could eventually challenge greater nations.

One of the most important writings that had a huge impact on the PLA's approach to new types of conflicts created by new technologies, *The Science of Military Strategy*, written and published in 2001 by Peng Guangqian and Yao Youzhi, two major PLA's generals, elaborated strategic analyses and offered a holistic definition of the modern Chinese strategy.

The main point discussed in the book that defines the broader concept of the Chinese strategy is the Science of Strategy (SOS); the US has not yet defined this concept but the authors see it as a military science characterized by politics, antagonism, comprehensiveness, stratagem, practice and prediction (Thomas, 2007).

A detailed analysis of *The Science of Military Strategy* made by Lieutenant Colonel Timothy L. Thomas (2007) reveals the major differences between the Chinese and the Western strategies and makes it clear that Peng and Yao's work provides a deep theoretical analysis of the Chinese strategy. Thomas describes how the SOS is divided into two categories, the basic theory of strategy and the applied theory of

strategy which both contribute to the elaboration of the broader concept of the PLA's military strategy using its cultural legacy and incorporating technology to fight future wars. Those elements reveal the essence of the Chinese strategic elements and therefore give us a good comprehension of their strategic mind-set (Thomas, 2007).

"Chinese military planners studied the high-tech experiences of US forces to examine the effects of information technology on military strategy and future warfare" says Thomas, and they came to the conclusion that war and strategy "have never been changed so dramatically and profoundly" (Thomas, 2007, p. 54). Peng and Yao even say that dramatic developments in the practice of wars urgently require new theoretical explanations about the emerging situation (Peng and Yao, 2001).

In 2007, the *China National Defense News* defined cyberwarfare as a "struggle between opposing sides making use of network technology and methods to struggle for an information advantage in the fields of politics, economics, military affairs, and technology". Cyberwarfare is an important means of achieving control of networks, which is a vital aspect of China's information operations' theory. Control of networks requires broad reconnaissance and espionage activities during peacetime to know the enemy and to provide the Chinese with the possibility of preemptive attacks. The emphasis on an active offense is one of the most important points on which the Chinese strategists insist for they consider a defense-only attitude to be irrelevant in information warfare. This is also a major shift in the Chinese military doctrine for they traditionally adopt a strategy of active defense and it shows that Chinese strategists have found a new scope for the PLA's operations in information warfare (Thomas, 2009).

Chinese strategists have theorized the transformation of modern conflicts by analyzing the new capabilities involved and the impact they had on warfare. Consequently, they adapted the Chinese military strategy to those changes by incorporating new technologies to ancient stratagems. Where US strategists seek a technological solution, the Chinese rather use stratagems and strategic sophistications. The Chinese strategy hence gives us a very interesting approach to cyberspace and indicates that theoretical work is an essential step for an efficient military doctrine that will provide the army with a holistic understanding of cyberspace.

2.2 A GOVERNMENTAL CIVIL STRATEGY

The PRC's officials have long considered the Internet and information technologies as a lever to the PRC's economic modernization and as a tool to maintaining its international competitiveness. They assumed they needed to integrate the information and communications technologies to Chinese society and started an *informatization* process back in the 1990s (Foster & Goodman, 2000).

This process was established by the central government and was part of a broader strategy to develop a knowledge-based economy, which relied on a series of "Golden Projects". The main objective of those projects was to build a national information network that would facilitate the economic modernization of the PRC, develop information and communications technologies, and interconnect the PRC's states to allow better interaction and control of the central government upon the other departments (China Internet Network Information Center, 2006).

This vast project was divided in three stages that would progressively build the national PRC's cyber capacity. The first stage was the establishment of physical infrastructures and digitalization of information in databases to provide the central government with knowledge of international commercial transactions and the ability to communicate with the Party's officials; the second stage centered its improvements on the PRC's economic and financial areas and education, and the last stage focused on the other economic areas that were not digitalized – enterprise, agriculture, health, information, housing, and manufacturing of communications devices (Lovelock & Ure, 2002).

The establishment of an "e-government" reveals the proactive Internet management strategy of the central government where they use the Internet as a lever to modernize and develop the national economy and keep international competitiveness but also as a tool to promote the Party's ideas, to fight existing corruption and to interact with the population (Foster & Goodman, 2000).

A plan such as the Golden Projects is part of the broader national cyber strategy to set up control over the national networks. The different Party leaders took the necessary steps to establish a governmental strategy that would modernize Chinese society and lead the nation to become one of the most influential in cyberspace.

The Golden Projects allowed the PRC to become the nation with the most Internet users today and one of the most active in terms of cyber capabilities' use. The nation continues to develop its networks through plans that will bring information and communication across the whole country (CINIC report, 2009); even though the technical challenge is great, this interconnectivity development follows the strategy established by the central government and will be used as a way of controlling the population.

The PRC has released in 2006 the *2006-2020 State Informatization Development Strategy* in which it set forth China's goals in informatization development for a 15-year period. Among those objectives, the PRC is willing to become independent in innovation of information technology in order to boost the research and development as well as the manufacturing sectors, and the strategy also emphasizes orienting the national economy and society toward information to develop those sectors; it

also calls for a national information security system that would provide security and control of the networks. The PRC has already begun doing so with the Kylin exploitation system, which provides high-level security to the Chinese Internet network.

This cyber strategy established by the PRC aims to promote social and economic development through informatization development of the entire nation. The PRC clearly wishes to use cyber capabilities as a lever to meet the challenges and grasp the opportunities arising in the economic, military, social and scientific areas. The central government maintains its control over the networks by imposing strict rules and regulations to the foreign companies that come and settle in China so that it does not lose control over the population (US-China Economic and Security Review Report, 2009).

To date, China has succeeded in building an advanced digitalized society that would improve its economic profits and its society's access to information and communications technologies while modeling this connected nation within the Party's ideas and guidelines.

The military theoretical works provided by the most influent strategists and the establishment of a national cyber strategy allowed the PRC to fully integrate cyberspace and its capabilities in Chinese society.

As a result of this, China is quite arguably the greatest opponent to the United States in cyberspace; it is not yet an enemy, but the recent events involving US firms and the allegations of Chinese governmental intrusions only tend to tense the relations. Moreover, the PRC is making significant moves to tie its cyber capabilities to its strategic concepts and is taking a more active posture than that of the United States (Thomas, 2009).

3. CONCLUSION

The United States and the People's Republic of China are two nations that are competing in cyberspace, testing their technologies and their strategies against each other's networks.

To better understand their vision of cyberspace and how the governments apprehend the cyber issues arisen from the growing cyber capabilities, an analysis of each national strategy is necessary. We have seen that both countries have adapted their military doctrine to this new strategic domain to ensure that they have the capacities to conduct network-centric warfare; the United States focuses on technology where the PLA will include ancient Chinese stratagems to the existing technologies.

A military strategy alone is not sufficient to acquire a holistic understanding of cyber concepts though; modifying the national military strategies to adapt it to the modifications the cyber domain created is an essential step but not an end. The obvious reason for which a military solution alone is irrelevant in cyberspace is because cyberspace is not confined to the military sphere – it reaches every sector of modern societies.

The civil sphere is using cyberspace at least as much as the military; the entire globalized economy relies on cyberspace and every digitalized nation has "computerized" its vital infrastructure. The direct consequence of this strong dependence is that the government has to provide cyber security to the whole nation to protect its national and economic interests.

The United States and China have very different approaches to securitizing their national networks. The difference resides in the political and economic regimes of those nations, which define the government implication in control and protecting the networks and digital infrastructures of the country.

The Chinese Communist regime gives the central government the capacities to control and conduct repression measures on the party's dissidents. Because of this strict control on the Internet and infrastructures as well as on innovation and development programs, Chinese information technology and networks look safer than other networks in other countries; but the security those networks enjoy is closer to censorship than to an effective securitization of cyberspace. Chinese networks face the same types of attacks as the US, and security in Chinese cyberspace may not be this elevated.

The democratic regime and liberal economy of the United States have allowed the country to develop a strong economy and design high technologies that are the structural elements of cyberspace, but because the vast majority of the networks is owned by private companies the government cannot impose arbitrary regulations; the problem here is to balance the privacy rights owned by the private sector – market freedom, information privacy – with the security vulnerabilities that threaten the national power. A closer collaboration with the private partners associated with a privacy guarantee would benefit both the private and public sectors.

This collaboration has to be completed with an essential step; there is no consensus on those notions that are the fundamental concepts defining cyber threats today; this will inevitably lead the policies to failure. No single national strategy will be efficient until the expectations on these fundamental security concepts are clearly defined. To provide a better understanding of cyberspace and cyber threats, the nations must elaborate a theoretical framework in which the essential concepts are analyzed and explained to the decision-makers.

The multiplicity of actors in cyberspace creates complex interactions and expectations that are not necessarily the same, diverging from one actor/referent object to another. The first step is the appropriation of the military strategic modifications arisen from the new capabilities created by cyberspace, which we find in both the US and Chinese military doctrines. Once these new capabilities have been fully understood, the government must define the meaning of the new security and strategic issues created, which are here the main cyber concepts: cyber threats, cyber security, cyber espionage, cyber attack, and cyberwar. Theorizing the cyber domain requires identifying the actors that are the referent objects, and linking the different security discourses to provide a securitization framework (Hansen & Nissembaum, 2009).

The semantic appropriation is also essential to clearly define thresholds and avoid any undesired escalation of violence. Once the government has adopted definitions of cyber concepts, it should integrate these notions in a comprehensive national cyber strategy, in which it will work with the appropriate actors to meet the political objectives it defined in the earlier step. The elaboration of such a theoretical framework is absolutely vital for better appropriation of the cyber domain.

REFERENCES

- Cebrowski, A. & Garstka J., 1998. *Network-Centric Warfare: Its Origin and Future.* Proceedings, pp. 28-36.
- Center for Strategic and International Studies, 2008. *Securing Cyberspace for the 44th Presidency.* A Report of the CSIS Commission on Cybersecurity for the 44th Presidency, Washington D.C.
- China Internet Network Information Center (CINIC), 2009. *Statistical Report on Internet Development in China.*
- Coquet, P., 2007. « Opérations basées sur les effets : rationalité et réalité », *Focus Stratégique No 1*, Laboratoire de Recherche et de Défense, IFRI, Paris.
- Dai Q., 2002. "Discourse on Armed Forces Informationization Building and Information Warfare Building," in *China Military Science, 2002.*
- Department of Defense, *2010 Quadrennial Defense Review Report,* Department of Defense, Washington D.C
- England G., 2008. Deputy Secretary of Defense Memorandum to the Military Departments et al., "The Definition of Cyberspace", Washington D.C.
- Foster W. & Goodman S., 2000. *The Diffusion of the Internet in China*, Center for International Security and Cooperation (CISAC), Stanford University
- Gertz, Bill, 2009. China blocks U.S. from cyber warfare. *The Washington Post.*
- Guangqian, Peng, & Youzhi, Yao eds., 2001. *The Science of Military Strategy*, English version (China: Military Science Publishing House, Academy of Military Science of the Chinese People's Liberation Army, 2001).
- Hansen, Lene & Nissenbaum, Helen, 2009. "Digital disaster, cyber security, and the Copenhagen school", *International Studies Quarterly*, vol. 53, 2009, pp.1155-1175.
- Harper, Jim, 2009. *"Government-run cyber security? No thanks"*, CATO institute, TechKnowledge.com, 13 march 2009, available: http://www.cato.org/tech/tk/090313-tk.html [February 14th, 2010].
- Henrotin, J., 2008. *"La technologie militaire en question – Le cas américain"*, Paris, éd. Economica, Coll. Stratégies & Doctrines.
- Khuel D., 2009. "From Cyberspace to Cyberpower: Defining the Problem", in F.D. Kramer, S.H. Starr, and L.K. Wentz (Ed), *Cyberpower and National Security,* (pp.24-42). Washington D.C, USA : Potomac Books, Inc. 2009
- Kramer, Franklin, Starr, Stuart, & Wentz, Larry, 2009. *Cyberpower and National Security*, Ed. Washington D.C.: Potomac Books.
- Lewis, James, 2009. « Innovation and Cybersecurity Regulation », Washington D.C: Center for Strategic and International Studies, May 2009, available: http://csis.org/files/media/csis/pubs/090327_lewis_innovation_cybersecurity.pdf [February 14th, 2010].
- Li B., 2004. "Applying Military Strategy in the Age of the New Revolution in Military Affairs," in *The Chinese Revolution in Military Affairs*, ed. Shen Weiguang (Beijing: New China Press), 2-31.
- Lovelock P. and Ure J., 2002. "E-government in China", pre-publication version of the chapter to appear in Zhang Junhua, Martin Woesler, eds. *China's Digital Dream – the Impact of the Internet on the Chinese Society*, the University Press Bochum
- McAfee Virtual Criminology Report 2009: "Virtually Here, The Age of Cyber Warfare", Santa Clara, CA.
- Mulvenon, James, 1999. "The PLA and information warfare", in *The PLA in the Information Age,* James C. Mulvenon & Richard H. Yang, Santa Monica, USA: RAND cop, pp.175-186.
- Office of the Law Revision Councel, 2004. *United States Code, Titre 10, Section 118*, Washington D.C.
- The White House, 2009. *Cyberspace Policy Review, Assuring a trusted and resilient information and communications infrastructure*, Washington D.C.
- The White House, 2003. *The National Strategy to Secure Cyberspace*, Washington D.C.

- Thomas T., 2009. "Nation-state Cyber Strategies: Examples from China and Russia", in F.D. Kramer, S.H. Starr, and L.K. Wentz (Ed), *Cyberpower and National Security*, (pp.465-488). Washington D.C, USA : Potomac Books, Inc.
- Thomas, Timothy L., 2007. "The Chinese Military's Strategic Mind-Set", *Military Review*, November-December 2007, pp.47-55.
- United States Government Accountability Office (GAO), 2008. Report to Congressional Requesters, *"Critical Infrastructure Protection, DHS Needs to Fully Address Lessons Learned from Its First Cyber Storm Exercise"*, Washington D.C
- United States Government Accountability Office (GAO), 2010. *"Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative"*, Washington D.C.
- United States Information Agency, 1992. *An Outline of the American Economy,* Washington D.C.
- US Joint Forces Command, definition available at http://www.jfcom.mil/index.htm [March 25th, 2010].
- US-China Economic and Security Review Commission, *2009 US-China Economic and Security Review Report,* Washington D.C.: 2009.