DEPARTMENT OF INTERNATIONAL AND EUROPEAN STUDIES

MASTER IN INTERNATIONAL AND EUROPEAN STUDIES

"THE EVOLUTION OF CYBER TERRORISM AND A POSSIBLE ELECTRONIC PEARL HARBOR; THE CASE OF STUXNET"

KOUFOPOULOU, A. IOANNA

ΜΘ14019

SUPERVISING PROFESSOR: DR. BOSSIS, MARY

MAY 2017, PIRAEUS

Η *Ιωάννα Κουφοπούλου* **βεβαιώνω ότι το έργο που εκπονήθηκε και παρουσιάζεται στην υποβαλλόμενη διπλωματική εργασία είναι αποκλειστικά ατομικό δικό μου. Όποιες πληροφορίες και υλικό που περιέχονται έχουν αντληθεί από άλλες πηγές, έχουν καταλλήλως αναφερθεί στην παρούσα διπλωματική εργασία. Επιπλέον τελώ εν γνώσει ότι σε περίπτωση διαπίστωσης ότι δεν συντρέχουν όσα βεβαιώνονται από μέρους μου, μου αφαιρείται ανά πάσα στιγμή αμέσως ο τίτλος.**

(υπογραφή)

"All war is deception"

"Win victory without fighting"

Sun Tzu

Dedicated to my beloved grandmother Felicity

TABLE OF CONTENTS

Abstract

If you consider for a second the radical technological evolution, you will realize that our everyday life has changed dramatically the recent years. Not only at the electronic level of evolution but also at the personal communication. A new era has already started and requires crucial reforms to our everyday life, and to the political, social, military, economical aspects. This sudden change of scene has affected significantly the way we work, we communicate and socialize, the way we inform ourselves about the news, and even when we do the housework. From this revolution, the existing structures cannot respond to these technological evolutions, our thoughts and actions should be adapted to the radical changes and create, for example, new political and economic norms. If someone cannot follow the way technology evolves, he or she will stay in the dark and lose the arsenal at the cyber war.

Of course, the military security of a state could not stay aside from the technological route. From the 90's, electrical grids, data, malware, hardware and software are some vivid examples of the alterations that had been made in the military area. A state cannot concentrate only on the military's physical appearance, but should consider the intelligence and espionage part of a war. The attacker could be a terrorist, a hacker or maybe an activist that tries to spread his/ her ideas and create panic. It is crucial for a state's security to defend first its citizens and its critical infrastructures. The "sophisticated use of communications" (NATO Website) has altered the way an armed conflict flares. Cyber-attacks, cyber espionage, stealing governments' information are few examples of the new form of terrorism which, most importantly, hides a political motive. The weaponized malware introduces a new type of war, Cyber Warfare and Cyber Terrorism. The attackers with their digital weapons, such as worms, viruses and Trojans

can affect not only the defense of a state but also the civilians' life, their opinion on a matter. The leak of vital information to the public may cause panic and armed riots. If people think that the government has manipulated them, they will revolt against it. The attacker may not be limited to cyber-attacks or stealing information, but use public cameras or private ones from laptops for surveillance reasons. He could use the information recorded to threaten the victims with the videos going public. This big new game in cyberspace has many aspects, many that we have not discovered yet, and everyone, especially the states and academic community should plan and promote solutions and defense mechanisms. For the attacker, is not necessary to have a physical appearance in the arena of Cyber War but he needs only a computer for his offense, for his whole plan. Without risking his life and spending a large amount of money, he will offend his target and win the battle. His real identity will remain anonymous by using temporary nicknames and guest names, the Darknet and a variety of cryptography mechanisms, making difficult for the intelligence and security agencies to track down his location and his real personal information. Thus, it is important to address the arising problems of the new era as soon as possible, with the technological evolutions and threats.

However, the weaponized malware is not the only aspect of Cyber Warfare that should notice. Social media have entered vividly to personal communications. In a matter of seconds, people can be informed from their mobile phone, their tablets or laptops while they work, walk or entertain. The rapid spread of information has revolutionized the cyber era and made people media consumers and victims of worthless information. Their personal identity and their desires are shaping according to the global trends that social media present. Mobile applications introduce people to national and international news, help them communicate and share their thoughts for a variety of subjects. Unfortunately, their identity is exposed to the internet, shaped from the desires that the international

community presents and losing their real personal identity, without knowing the threats. It is well obvious that the variety and number of targets are enormous and the future victims are not aware of the cyber dangers and how vulnerable they are against the new cyber threats. As Brian Solis stated, “Social media is about sociology and psychology more than technology” (Brian Solis, “Social Media is About Social Science Not Technology”, March 14, 2012).

Because of the multiple audiences, the feelings of terror and the brand awareness, an information vacuum has been created to this new era. Social sciences are now in need to face the current and future challenges in cyberspace. The traditional social sciences will help promote innovative solutions and ideas, evolve the current political framework and improve the current governmental structure. They will be used as a theoretical basis for the analysts to promote their ideas and propose multiple solutions to the threat of cyber – attacks. With respect to human rights, the academic community must set an analytical framework, deepen her research and suggest ideas for the regulation problem in cyberspace. All levels of governance, political, economic, military, and social must be evolved according to the latest technological developments and in parallel with the technological modernization.

With the alterations at the international and national framework, many states have emerged as the first cyber powers. States are trying to evolve technologically without losing their national identity and stay behind to the electronic weapon arsenal. In an international system where "war of all against all" dominates (Thomas Hobbes, “Leviathan”, 1651), the need for political and social recommendations is demanding. The emerging cyber powers and states trying to follow the technological evolution, in cooperation with the private sector, should share information upon the attackers, their

methods and their targets. Secrecy concerning security issues will not help a unified cyber strategy against attackers and develop the necessary structure for the new cyber era of connectivity. Victims of cyber-attacks should go in public and share their experience upon the new threat, how it has affected its function and how the defenders could collaborate with other actors to retaliate against the terrorists.

Often people say that those cyber threats are exaggerated and there is no risk for the state's and civilian's security. But who will take the risk and ignore the uprising threats? Who will ignore that these cyber-attacks gain access to many critical infrastructures, steal confidential information, take control and cripple of electronic systems? This ability to attack critical infrastructures such as military electronic documents, water supply infrastructures, banks and many more, in a terrorist's hand or a group of terrorists may have significant consequences to regional and national security - sovereignty. It is unavoidable that new vulnerabilities at electronic systems will be discovered constantly, but that does not mean that governments should stop promote their national defense strategy and build step by step cyber defense measures to prevent further consequences of the cyber-attacks. It is common that an actor (terrorist or hacker) will want to intrude military infrastructure, hack a bank or steal personal information of a well-known person for several reasons (political, religious, ideological reasons). A government cannot defend itself against cyber- attacks. But the damage caused could have irreversible results to the state and its bone structure. Thus, states must harden to the newly threats and prevent denial of services from taking national systems getting done to their knees, prevent the manipulation of national critical infrastructures and the spread of panic. No one can dare to ignore that if cyber weapons are in hands of a terrorist will have immeasurable results to the electronic function of a nation and letting the attacker succeed his target. No one knows how destructive an attack of cyber warfare could be.

Preface

This paper will explore the evolution of technology during the last years and how societies have been influenced from this revolution in electronic systems. Globalization, as well, has contributed with a significant way to the rapid spread of those technological innovations. Cyber warfare, Cyber Terrorism, Big Data, Distributed Denial of Services and Cloud computing age are some theoretic definitions we use for the cyberspace and its function. Specifically, with this research, it will be explored the field of Terrorism and Security, how states should be organized, protect their national infrastructures, cooperate internationally and with private companies, and how the non-state actors have contributed to the alteration of the international framework.

Cyber-attacks could come from everywhere, meaning that they do not have any physical appearance; agencies or states cannot discover their real identity or their position to stop the attacker. It is the problem of attribution that paralyzes the states from preventing a hostile attack. Once a digitalized weapon intrudes a system, it takes minutes or even seconds to control the electronic domain and manipulate the system. The gap between attribution and retaliation offers the hostile attacker more time to prepare for another attack, probably with more dramatic consequences such as the health systems, banks, or even the military. They could also possibly escalate the attack and threaten the national security of a government, wreak havoc and force violent actions. Many analysts have shown that national leaders fear the danger of losing their control over their state. Terrorists, terrorist groups, hackers, activists are familiar with this idea, and their main purpose is to force leaders to bend to their will. For now, the recent cyber-attacks have shown that they have only temporary damage consequences, but what if those consequences become permanent? What if paranoia over national structure spreads, or

even to international scale? “Cyberdeterrence strategists should keep in mind that cyberwar is basically the manipulation of ambiguity” (Martin C.Libicki, “Cyberdeterrence and Cyberwar”, THE RAND, 2009).

Cyberspace is not a common place where everyone acts as in his/ her everyday life; internet is an inextricable part of our routine. On the other hand, there are many loops, dangers, and cyber actors that manipulate sites and visitors. In the Darknet is very difficult to realize what is happening, ramifications of the systems need a deep analysis and understanding of the way it works. Internet functions as a human mind, with many ramifications, loops, vulnerabilities, offense and defense mechanisms. With the electronic wires and systems, things become more complicate. Psychologists, IT experts, politicians, academics are on demand for creating a whole new international frame for the new era of cyberspace.

War needs physical appearance, real weapons and soldiers. But that does not mean in cyberspace, that a Cyber War will not escalate from cyber-attacks, paralyzed electronic systems to violent riots. Offense realism shows that states do not trust each other and seek for more power and supremacy. In Cyber world, as well, they try to overcome the technological barriers, build their cyber defense and offense and preserve or gain their supremacy in cyberspace. But their reaction over those problems should follow an analytical basis, a structure and appropriate measures for each field. Vulnerabilities could be found in every hardware and software, in every electronic system. Escalation and counter escalation should be studied in relation with the motives of the enemy. Because of the attribution problem of the attack, the victim does not know which the actor behind this hostile action is. Apart from the terrorist, states may have recruited cyber terrorists for a cyber-attack or created a cyber weapon to fight another state. Trying to succeed cyber

supremacy in cyberspace, they forget that it is not a unitary domain. As Certon and Davis mention, “major concern is no longer weapons of mass destruction but weapons of mass disruption” (Graig B. Greathouse, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” ,2014, p. 47).

For a policy analyst, cyber terrorism evolution is an interesting and challenging field of study. Artificial Intelligence, Internet of Things, Big Data are some of the new evolutions made for the analysts, subjects that need to be discover in combination with the traditional strategies. It is a newly established field that requires attention and consistent research. Evaluation of those novelties, mentioned above, is essential for the robustness of the international and national framework, for the securitization of the state. More attention is required for the safety of the people; internet gives the capability to hostile actors for the exploitation not only of critical infrastructures but also civilians’ privacy. Decision makers should also consider the difference between military cyber defense and civilian cyber defense. The recent cyber-attacks (Estonia, Stuxnet, and Flame) have shown that there is a political motive behind every attack, a specific target that depicts the desire and will of the offender. It is internationally vital to create a doctrine of Cyberdeterrence that will enable the victims to retaliate and protect themselves. Attention should be given also to the supply chain of the hardware and software. Who is the supplier for states, is the equipment appropriate for the needed purpose, does the company provide to the customer all the information for the function and vulnerability of a system are some questions that should be reviewed thoroughly. Private sector plays a key role to the supply of the national domains. Non-state actors generally play an important role to the establishment of a cyber deterrence doctrine.

Cyber-attacks interrupt the balance of electronic systems, manipulate them and force their operators for temporary retreat. A new type of war has entered vividly to the cyber arena and continues to take shape the recent years. Hybrid Warfare is a conventional and irregular type of war, with unorthodox methods and techniques. There are still unofficial definitions for this new type of war that affects Cyber Warfare. However, this is not the only definition that has not yet completed. Cybercrime, cyber terrorism and cyber warfare are some examples. Policy analysts and decision makers have another sense meaning problem, a methodology weakness. The definition problem in cyberspace is a weakness that needs to overcome for the sake of cyber security. "Cyber security dilemma is more than efforts by one actor to enhance its security decrease the security of others. It signifies a multifaceted set of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. It is a heterogeneous set of discourses and practices with multiple, often contradictory effects (Myriam Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", September 2014).

The last cyber-attacks arisen were distributed denial of service (DDOS). The transnational nature of cyber threats forces states to enhance their cyber structure and collaborate with state and non-state actors. Estonia (2007), Georgia (2008), Stuxnet (2010) and many more issues will be discussed as follows, for the results they had, the innovations they caused in many fields and the future measures needed. In the future, cyber shocks, in countless targets and with countless methods, will be increased. A new era in cyber foreign policy will be established, as cyber risks could not only affect a single company or sector, but the entire cyberspace, escalating to non-cyber domains. Not only cyber capabilities but also cyber cooperation will help decision makers to build an offensive doctrine.

"Cyber-risk management needs to look beyond the internal information technology (IT) enterprise to other aggregations of risk, such as outsourcing and contractual agreements, supply chain, upstream infrastructure, and external shocks" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014). The case of Stuxnet, for example, marked a new era in cyber terrorism. The method used was more sophisticated than ever before, the result of the attack was discovered after one year and it started with a physical intrusion, a simple usb, at the nuclear premises of Iran in Natanz. There was a specific target and the malware intruded the system, was modifying continuously according to the existing software of the computer programs.

Cyberspace is an attractive battlefield with many unique features and advantages. Thus, an electronic Pearl Harbor cannot be excluded from the potential future threats. What if cyber terrorists intrude all the electronic systems of national and international field? Cause chaos and fear? The worst-case scenario would be the escalation of an electronic Pearl Harbor into Cybergeddon. Internet is getting more complex every day and electronic systems acquire more vulnerabilities. All policy analysts and decision makers should keep in mind the three laws of Rod Beckstrom: "1. everything that is connected to the internet can be hacked, 2. everything is being connected to the internet, 3. everything else follows from the first two laws" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014).

PART A

State Sovereignty and how it is defined in cyberspace

In the new cyber era, the traditional definition of state sovereignty has been altered, facing a dramatic decline. Below are presented some of the various characteristics of state sovereignty and equality, “Under the principle of territorial sovereignty a State exercises full and exclusive authority over its territory” (Wolff Heintschel von Heinegg, Territorial Sovereignty and Neutrality in Cyberspace, 2013, p.3,), “Perhaps the outstanding characteristic of a state is its independence, or sovereignty. This was defined in the Draft Declaration on the Rights and Duties of States prepared in 1949 by the International Law Commission as the capacity of a state to provide for its own well-being and development free from the domination of other states, providing it does not impair or violate their legitimate rights” (Malcolm N. Shaw, International Law, sixth edition, Cambridge University Press, 2008, p.211).” The principles surrounding sovereignty, such as non-intervention, are essential in the maintenance of a reasonably stable system of competing states” (Malcolm N. Shaw, International Law, sixth edition, Cambridge University Press, 2008, 381), “principle of sovereign equality of all States: The principle that nations have the right to enjoy territorial integrity and political independence, free from intervention by other nations.” ("The Organization is based on the principle of the sovereign equality of all its Members.", Article 2, paragraph 1 of the Charter of the United Nations states)

However, international community should realize that cyberspace is a newly presented domain with global commons, and recognize its importance for their strategic interests. (Lieutenant Colonel Patrick W. Franzese, “Sovereignty in Cyberspace: Can it Exist?”). *Cyberspace* is “the interdependent network of information technology infrastructures, which includes the Internet, telecommunications networks, computer

systems, and embedded processors and controllers." (U.S. National Institute of Standards and Technology). State and non-state actors must realize that the traditional form of state has been altered in two several types, the physical segment of cyberspace and the modern technology world, putting an end to geography. The computing power is a new form of evolution that state should consider and evaluate its capabilities, together with the commercialization of internet. According to Joseph Nye, there is a diffusion of power in cyberspace (Joseph Nye and Cyber Power, Belfer Center, May 2010). It is important for the national government to consider the technical issues regarding "cyber sovereignty", such as information borders and embargoes, and evaluate carefully cooperation with the private sector. It is not power equalization any more, but a continuous cyber arsenal of electronic weapons that allow many dangers to rise.

An international cyber regime is vital for the states to preserve their national sovereignty and their territorial integrity. An international cooperation among the nations would help predict possible cyberattacks and avoid any escalations in all levels of a state. The vacuum between theory and practice, however, is another problem. The measures needed, acquire a common basis for each government and deter possible cyberspies or cyberterrorists from hacking or taking the control of their critical infrastructures, preventing from a collateral damage to the telecommunications network. But not only that, measures will help state actors to develop responsible behavior into the cyberspace and protect both the national critical infrastructures and their civilians. "The starting point must be that states exercise sovereignty over their respective cyberspace, mutatis mutandis" (Pal Wrange, Professor of International Law, Stockholm University, Director, the Stockholm Center for International Law and Justice, 2014, "Intervention in national and private cyberspace and international law", p. 5).

"*Cyberspace* comprises all the world's computer networks, both open and closed, to include the computers themselves, the transactional networks that send data regarding financial transactions, and those networks comprising control systems that enable machines to interact with one another" (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012). The rise of social media has altered our daily life in many ways and has affected dramatically the scene of international relations. Some of the characteristics presented by Joseph Nye are the number of players, the ease of entry and the opportunity for concealment. This war of machines has revolutionized the international relations. New actors, new threats and new conflicts are evolving constantly, causing many asymmetries to the international arena. However, it should be mentioned the distinction between social media and cyber operations. Social media operations are consisted of three types, information gathering, defense and offense. Cyber operations, on the other hand, involve a strategic plan, attackers and defenders who interact continuously.

Yet it is unclear which the functions of the internet are and how they can affect the current structure of a state. The international society should clarify her targets for this sovereign transformation and decide common and fruitful solutions. The 'denationalization' (Nazli Choucri, "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences", 2013) of the states has caused severe problems in the countries not only in the international relations but also in the level of government structure. Most importantly it has affected civilians' minds by shaping opinions upon political debates.

"Under the principle of territorial sovereignty, a State exercises full and exclusive authority over its territory" (Wolff Heintschel von Heinegg, "Territorial Sovereignty and

Neutrality in Cyberspace", 2013, p.3). "Although no State may claim sovereignty over cyberspace per se, States may exercise sovereign prerogatives over any cyber infrastructure located on their territory, as well as activities associated with that cyber infrastructure" (Tallinn Manual, p.22). Cyber infrastructure consists of servers, electronic grids, computers and many more. A State has control over the physical infrastructure not only inside its territory but also when this infrastructure is in another territory. Those prerogatives include a wide range of the function of the physical infrastructures and are not limited only in an area.

There are four major cyber threats to national security: economic espionage, crime, cyber war and cyber terrorism. Those threats cannot be confronted with a state actor only but with a group of state actors who have the knowledge and the capability to help the international community overcome those fears, build 'cyber walls' and defend their national territory. For a long-term stability between governments in the cyberspace, the international community should also include the fragile states that do not have the same governance or regime, for instance authoritarian governments. Not everyone can understand this crucial transformation. Public riots against cyber revolution, government actions, private participation at the public domain are more than likely to spread all over the globe. Wide knowledge of the cyberspace is a factor that every national government should take care first.

"The International Strategy for Cyberspace indicates the following activities may qualify as violations of territorial sovereignty: attacks on networks; exploitation of networks; and other hostile acts in cybercrime that threaten peace, stability, civil liberties and privacy" (Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace", Volume 89, 2013, p.8). The cyber weapons arms race has given the

capability to many hackers, terrorists or a group of hostile actors to attack national infrastructures, steal confidential information or even personal information from simple civilians. The security and defense industry of private sector has made significant steps for preventing cyber-attacks. But as it is shown, these actions are not enough. National governments should cooperate closely with private companies and build a national defense framework against cyberterrorists. Smart grids ("a digitally-enabled electrical grid that gathers, distributes, and acts on information about the behavior of its participants in order to improve the efficiency, importance, reliability, economics, and sustainability of electricity services. The United States is currently looking into the possibility of developing a smart grid" (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012), surveillance, information sharing are some ideas for overcoming this problem, or at least appoint a basis for the upcoming threats. Private companies have the capability to overcome those cyber-attacks more quickly than the national defense mechanisms. And as time is a matter of security in cyberspace, national government should enforce dialogues with the private sector. Even if cyber-attacks in private companies are not published in social media (they want to avoid spreading chaos and panic), it is important for the protection of national confidential and private information to avoid security vulnerabilities. "*A security vulnerability* is a weakness an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource. In this context, a weakness refers to implementation flaws or security implications due to design choices. For instance, being able to overrun a buffer's boundaries while writing data to it introduces a buffer overflow vulnerability. Examples of notable vulnerabilities are Heartbleed, Shellshock/Bash and POODLE." (https://www.enisa.europa.eu/topics/national-csirt-network /glossary/vulnerabilities-and-exploits). "Persistent public pressure, backed up by credible

evidence-based research and campaigns (such as the Electronic Frontier Foundation's privacy scorecard), are the best means to ensure the private sector complies with human rights standards worldwide" (Ronald J. Deibert, "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace", Internet Governance Papers, Paper No. 6, October 2013, p. 14).

Clearly, the need of lawmakers, policy makers and many more experts from the academic community is vivid. The duty of prevention presupposes knowledge not only for the origination of the cyber-attack, but also in what extent this hostile action will affect the electronic systems, how the defense will be organized and in how much time the offensive mechanisms will react. It is duty of state to protect its electronic infrastructure and its civilians. But that could be accomplished with the appropriate knowledge, the appropriate information for each sector and the will for international cooperation.

Why it is a new era in terrorism and in cyber security

"In this second decade of the 21st century, we live in a hyper-connected world with well over six billion mobile cellular subscriptions, and close to two and a half billion people using the internet" ("Where cyber-security is heading", Security Defense Agenda, January 2013, p.14). Malware and cyber weapons are acting as a lure to cyber-terrorism and cyber-crime. "Malware is a malicious software that causes computers or networks to do things that their owners or users would not want done. Examples of malware include logic bombs, worms, and viruses" (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012). The cyber arsenal of weapons reflects the changes been made during the last years. A new concept of war is shaping and needs to be addressed for its confrontation. The software holes have been a motive for the cyber-terrorists to intrude a system and take the control of it, or steal vital information. Those cyber abilities to the hands of hostile actors could threaten national and possibly international security.

Because of the software vacuums, cyber-terrorists can monitor the system's functions and disrupt or control its commands. "As early as 1990, the National Academy of Sciences began a report on computer security with the words: "We are at risk. Increasingly, America depends on computers…Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb" (Gabriel Weinmann, "Cyberterrorism, How Real is the Threat?", UNITED STATES INSTITUTE OF PEACE, Special Report 119, December 2004, p.2). Combating cyber-terrorism holds a political dimension. Political motives are behind of the most hostile actions in cyberspace. Actors holding a political agenda are being triggered from the advantages that the cyber-attacks offer. Thus, internet governance is another factor that should be developed according to the

latest evolutions. Private companies are facing the risk to lose their reputation, because of the cyber-attacks, and for the national governments their security to be underestimated.

Internet forms a great danger for the future of cyberspace. New vulnerabilities are created every day and that is a 'massive electronic Achilles' heel' (Gabriel Weinmann, "Cyberterrorism: The Sum of All Fears?", Studies in Conflict & Terrorism, Routledge, Taylor & Francis Group, 2005). The active participants in internet (chat rooms, forums, hacking manuals) are increasing rapidly and many 'electronic jihads' could evolve. However, the problem cannot be only attributed to electronic factors. "Psychological, political and economic forces have combined to promote fear of cyberterrorism" (Gabriel Weinmann, "Cyberterrorism, How Real is the Threat?", UNITED STATES INSTITUTE OF PEACE, Special Report 119, December 2004). The social and political objectives motivate state and non-state actors to plan a cyber-attack and fight for cyber dominance. Moreover, social media have labeled some cyber-attacks wrong and referred to cyberterrorism with misunderstanding causing anxiety and havoc to the definition of the new dangers. Internet is no longer a trusted tool for communication.

For terrorists and hackers, internet is ideal for their purposes in many ways. It is much cheaper from traditional weapons and their origin remains anonymous to the victims. Cyber-attacks could affect innumerous targets and expand their control over different and various domains by simply pushing a button. It is easier for terrorist organizations to recruit new members, and hide their identity into the cyberspace. If a state actor wants to attack another state for political purposes, it could hire professional terrorists of hackers to 'do the job' without the risk of exposing its identity. This virtual warfare has created limitless loopholes for cyber terrorists to threaten international stability. Many studies have shown that electronic systems of critical infrastructures are so

complex, automatically creating system loopholes, making it impossible for states and organisations to limit those weaknesses and build a cyber defense wall.

"The failure to develop 'offensive' capabilities condemns a nation to obsolete technology, outdated forces and inadequate defences. Not it is desirable to leave cyber capabilities spread piecemal across many units with disparate skills, missions and doctrines" (James A. Lewis, "Cyberspace and armed forces, The rationale for offensive cyber capabilities", Australian Strategic Policy Institute, May 2016, p.2). It is the coercion over governments and citizens that international community should worry about. The need for an international regime will help the global commons of states to be preserved and secure their integral sovereignty.

A new concept of war has made its presence clearly to the international arena. The distribution of power in the international system has emphasized the fact if a state can acquire its technological superiority, and then automatically is classified as an important state power. The cyber weapons arsenal in cyberspace has created a battlefield where cyber-attacks are increasing in sophistication and complexity. Thus, a national technological evolution offers various defense mechanisms for the security of sovereignty and infrastructures. Adopting a new strategic behavior in cyber security is crucial, as cyber-attacks on military infrastructures, weapons, command and control are more effective and dangerous than attacking civilians' emails.

The obstacles that cyber security is facing

"The virtual nature of cyberspace implies dematerialization (everything is paperless), detemporalization (instant communication) and deterritorialization (breaking the geographical boundaries and distances) of online activities. "The problem in cyberspace activities is that they occur outside of the real time and take place from everywhere" (Jackson Adams, Mohamad Albakajai, "Cyberspace: A New Threat to the Sovereignty of the State", University of Essex, Colchester, UK, Volume 4, No. 6, 256 - 265, Management Studies, Nov. – Dec. 2016, p.1 and p.3).

In cyber era where interconnected networks dominate, to ensure cyber security, we need to develop a cyber resilience plan. National responsibility is not limited only by technical obstacles, but also from jurisdictional vacuums that should be promoted and eliminated. For example, the organized crime had been a major catalyst to the expansion of illicit crime. The authorities must have a complete knowledge of what they are facing and how catastrophic are the threats of cyberspace. Norms and definitions will provide a full strategy plan and automatically solutions for each case.

National responsibility should be expanded also in cyberspace issues as well as in society and the protection of civilians from cyber threats. The internet has become a vital tool for financial transactions, communication, fun, systems for electronic pumps, generators and military security globally. Due to these new evolutional trends (Big Data, Internet of Things, e-banking etc.), national governments are responsible for the smooth transition of society and nation's structure into virtual ones with the help of the private sector. Although, private companies could provide technical knowledge and ideas upon the issue, they do not have the capability to defeat military services or countries with technological background such as China or Russia, or even organizations that invest

millions of moneys. They do not have the capability by themselves to trace the origin of cyber-attacks and eliminate illegal action. The government's responsibility is to interact with the private sector and intervene to all actions concerning national cyber security. National security and sovereignty is a whole different matter that only a government is responsible for.

In an information age where every device, sector or network is interconnected, a domino effect is more than possible to occur. *Domino effect* means a disruption of a system or a network could expand and possibly affect another. As cyber weapons, can execute the cyber-attacks just after the order has been given, how quickly could a system be paralyzed and this cyber-attack be transmitted to other systems? It is unclear how effective a cyber-attack could be after the command has been given. Even if there where automatic response systems to those threats, how sure could we be for their function and their effectiveness?

The most common obstacle is the DDoS *(Distributed Denial of Service)*. "It is a type of cyber-attack that employs a number of computers simultaneously to flood the victim (usually an Internet site, server, or router) with large amounts of traffic, thereby overwhelming the site's ability to respond and effectively shutting it down" (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012). The dependence on the Internet is growing more and more, and it is worrying what the vulnerabilities that will occur are.

The media have a great responsibility for the presentation of the cyber-attacks to the civilians. The way they will present the subject to the public plays a significant role. The desire of cyber dominance in combination with risky leaders, has the potential of creating cyber wars not only with the form of cyber-attacks but with the presentation of

news to the media. A risky leader or a hacker may cause chaos and panic, with the spread of inaccurate information, national secrets, and military information are possible examples. Governments should expand its control to the social media also, without infringing on civilians' liberties. Authoritarian leaders, for example, may suppress the mass media and sharing information, use surveillance and propaganda techniques if an individual has a different opinion from them. The internet is ideal for expressing your own view, but authoritarian regimes may exploit the media for protesting 'electronically' against an individual or a state actor. Media must remain solid and provide people the correct information for the evolution of cyberspace and its threats.

The rationale for offensive cyber capabilities, cyber arsenal, cyberwarfare in small or large scale, interconnected networks are some examples of how our everyday life will be formed. The cyber revolution has entered vividly into societies, and state actors, internationally, have a great responsibility to preserve the stability of the world with cyber policy strategies. Someone could suggest closed systems (computers isolated from internet) but it will not be a permanent solution. The evolution cannot be stopped because of fear and innumerous dangers or terrorists. Technology has many ramifications, but an appropriate management plan can help overcome panic, cyber-threats, system vacuums and domino effects. It is not all about technology, it is the human element that has not been emphasized yet. It is the human factor that should be stated as a priority to protect and secure, not only technology and military weapons. Awareness and proper information of the cyber dangers could help overcome the fear and protect national security and stability.

Global Cyber Deterrence – the USA, Russia, China and India

Andrew Nagorski, at his paper "Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway" (EastWest Institute, 2010), wrote thoroughly the ideas and the solutions proposed of the aforementioned countries concerning cyberspace. The massively interconnected networks are growing up creating many cyber vacuums. Consequently, countries must reinforce close international cooperation for cyber deterrence and introduce solutions for the various vacuums.

It is unique how a cyber-attack can be launched in a few seconds from anywhere in world and by any person without risking discovering himself and his place. And the problem is that cyber threats are increasing every day at all levels of state (economy, policy, people). In cyberspace era, we talk about weapons of mass disruption, and not of mass destruction. Fragile systems, without organization and basic knowledge of cyberspace, are impossible to build resilience against those attacks. Countries should build trust, first, between them and then plan their defense. Dark Web offers to terrorists many possibilities, for example hide their identity, take control over electronic systems, steal information, recruit new members and deepen their knowledge over cyberspace by chatting into forums. State actors have the responsibility to discover what Dark Web really is, and how they can plan their cyber strategy resilience from now on. Governments against innumerous and coordinated cyber-attacks will need a global response.

As the next war, will take place in cyberspace with electronic force systems, some countries such as China, the USA, Russia and India have useful constructed ideas for developing cyber capabilities. China promotes internet research and information technology. Through recent years, China has made noteworthy progress and now her purpose is to solve cybercrime, as it has become a crucial social problem. The USA, on

the other hand, insists on a public – private cooperation as dependence between countries is increasing. With the Cyber Triad, resilience, attribution and offensive capabilities, the victim will be able to strengthen its power and defend its critical infrastructures. Russia insists on defining correctly and comprehensively the new cyber phenomena. If you know exactly what the threat you are facing is, then you will be able to promote defense and offense mechanisms and trace the terrorist. However, for Russia is crucial to isolate political and economic interests from cyberspace. As a newly established domain, it would be wiser to remain solid from personal of state interests. Finally, the case of India is admiring since it has constituted an effective cyber law and planned a complete cyber defense strategy. Although in 2000, India enacted the Information Technology Act, becoming the twelfth nation in the world to enact cyber law ("Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway", p.17, Andrew Nagorski, EastWest Institute, 2010), India has not a national cyber plan.

For a global harmonization, an international cyber regime will bring closely countries and help them design a cyber architecture plan. An international cyber regime constituted from ideas and knowledge of various countries, from suggestions and debates that have produced a fruitful resolution. To avoid a World-Wide Cyber War, governments must develop an international cyber regime and at the same time a rational cyber behavior, modernize their military infrastructures and their offensive capabilities. Power is not restricted anymore to geography but it has opened the interactions between the national borders.

The engagement zone of war has been transferred to cyberspace, even with ‘innocent machines’ such as drones, raising the issue of surveillance and intrusion and espionage into a state. The challenge we face has a few common characteristics that should be emphasized. For instance, the digitalization of our lifestyle, that governments will need to cooperate with private companies and that the nature of the attacks and actors can be adapted anywhere and everywhere in no time. Due to the plurality of actors in cyberspace and the capabilities of internet, governments should raise awareness for immediate solutions.

Conclusions of part A

"States have an obligation to resolve peacefully cyber disputes that may endanger international peace and security" (Eric Talbot Jensen, "Cyber Sovereignty: The Way Ahead", Texas International Law Journal, Volume 50, Symposium Issue 2, p.15). Today, it is challenging for governments to develop policies for technology, policies that will secure their sovereignty and stability in cyberspace, a new cyber political technology. Technical issues regarding sovereignty must be solved as soon as possible to prevent future cyber-threats becoming even more catastrophic. "Electronic borders" could be a solution but after having evaluated their ability to stop cyber-attacks and having secured electronic infrastructures. Apart from their cost and necessity, "electronic borders" should be tested for their capability to stop cyber-threat penetrations and refrain from being controlled by cyber terrorists.

The identification of actors in the cyber domain is vital. Knowing your enemy, it will help you can plan your strategy and attack the intruder efficiently. The defense and offense strategies would be more accurate and the time gap between attribution and retaliation should be eliminated. If the hostile actor is preparing for another attack, you will be able to track his position and return the attack in a few seconds. You must convince your enemy that an eminent cyber-attack to your infrastructures will not weaken you, but it will make you stronger and the hostile actor will be locked to your own game. Of course, military modernization is a high priority for all countries. Every day technology systems are revolutionized, pc experts suggest new multitasked electronic programs, drivers and computers are improved, and networks are becoming more immune to cyber-attacks. However, as the 'good side' tends to modernize its infrastructures, so the 'bad side' – the terrorists – tends to steal crucial information for their own purposes and

intrude systems (security dilemma). These cyber arsenals are increasing even more and in the future cyberwarfare will be even more frequent. As Paul MacGregor, Director of Finmeccanica Cyber Solutions states: “There’s a tendency to say that threats are new un-attributable, or that it is impossible to stop attacks – it isn’t – in fact 80% of vulnerabilities can be removed by simple technology, education and good practices” (Security & Defense Agenda, “Where cyber-security is heading”, January 2013, p.10).

The rise of megacities, urbanization, and virtual communities are some of the dangers threatening the stability of national sovereignty. It is the cyber governance within the states that promotes and strengthens their organization, not only in a national level but also in an international one. Strategic behavior in cyber security is essential for protecting civilian and state interests. Information sharing on potential targets and cyber-attacks are the key for common defense. The procedure of evaluating the new cyber domain should follow the steps of learning, monitoring, analyzing, deciding and responding. In the cyber era we live in, we must understand that things change rapidly, so as our actions and reactions to the cyber threats should be rapid. With the appropriate education, sharing of information and mutual trust, the international community will build capabilities for serving in an interconnected world; avoid building sensitive systems and losing sensitive information from cyber terrorists, and most importantly avoid spreading those cyber-attacks and having national and international size effect.

PART B

Definition of Cyber-attack and Cyber Warfare

Ever since the attacks in Estonia in 2007 (DDoS cyber-attacks) and in the nuclear infrastructures of Iran in Natanz in 2010 with Stuxnet, international community has stated clearly the need for an effective cyber strategy plan. A new form of terrorism has made its presence, a new warfare in cyberspace. The power of states has come into focus for the governments and how they can avoid an international cyber shock. Those cyber-attacks, and the latest ones, have forced governments to combine powers and try to build "borders" over cyberspace. Cyber terrorism is the fear of random violence. For a further understanding of this crucial threat, below there are presented definitions of cyber-attack and Cyber Warfare.

Cyber-attack is "an attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity. Extended Definition: The intentional act of attempting to bypass one or more security services or controls of an information system." (Source: Compilation of Existing Cybersecurity and Information Security Related Definitions, Open Technology Institute New America - 2015 July). For NATO, a cyber-attack is an "action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber-attack." (NATO Glossary of Terms and Definitions, Edition 2014).

For EU, there is no definition as cyber-attack. The term that is used is the *'attack vendor'*. "An attack vector is a path or means by which a hacker can gain access to a computer or network server in order to deliver a payload or malicious outcome", or "Attack vectors are routes or methods used to get into computer systems, usually for nefarious purposes. They take advantage of known weak spots to gain entry. Many attack

vectors take advantage of the human element in the system, because that's often the weakest link" (Marco Morana & Scott Nusbaum, "Input Validation Vulnerabilities, Encoded Attack Vectors and Mitigations", The OWASP Foundation, Cincinnati Chapter September 08 Meeting, 2008).

For US, a cyber-attack is "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." (Richard Kissel, Editor Computer Security Division Information Technology Laboratory, "Glossary of Key Information Security Terms", U.S. Department of Commerce, May 2013).

"*Cyber Warfare* is the actions by nation-states and non-state actors to penetrate computers or networks for the purpose of inserting, corrupting, or falsifying data; disrupting or damaging a computer or network device; and inflicting damage or disruption to computer control systems." (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012).

"Virtually no cyber operation – not even espionage through computer network exploitation or manipulations as simple as entering a password – can be carried out without at least temporarily deleting or changing data in the intruded systems" (Nils Milzer, "Cyber Operations and jus in bello", International Law Studies, volume 87. p. 31). The digitalization of the world has made significant changes at the security domain, and at military strategy policies. Many systems have flaws because of their complexity and they are vulnerable to many cyber threats. Furthermore, most of the cyber-attacks have a purpose, a strategic objective, a technical or even political objectives.

However, it is difficult to discover the clear motives of the attacker, creating the fear of escalation from a simple cyber-attack into a global cyber warfare. Cyber threats could create terrible shocks completely out of control in the international community. Thus, it is very risky to ignore the scale of cyber-attacks and what are the consequences they may have not only in a national level, but also in an international one. This is an operational problem that governments should solve as soon as possible for an effective backbone strategy in the field of security with ‘best available techniques’ (BATs).

Non-state actors – Cyberspace – Cyber Terrorism – Cyber Security

Modern terrorism has a wide audience, a global stage that influences and manipulates, individuals with the information that leaks all over the world. Although, the internet is a feature of the modern and future society, it is the cause for creating various problems to governments. Non-state actors are a new crucial factor in cyberspace and in cyberwarfare to consider. A few examples of non-state actors are groups of hackers, terrorists, hacktivists, of groups sponsored by states, private sector and social media. Each one of these actors, with their own way, have a responsibility for the security in cyberspace. Social media, for example, contribute to state stability and spread the threat of Information Warfare. They empower Information Warfare with terrible impacts on state and society. *Information Warfare* is "the use and management of information technology in pursuit of a competitive advantage over an opponent" (Andrew F. Krepinevich, "Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012). The internet helps create mass media news and threaten the cyber security.

Cyber Security is '[T]he collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

availability; integrity, which may include authenticity and non-repudiation; and confidentiality (NATO).

Daily the active participants in internet are increasing. In chats, forums and blogs, the users can share opinions, ideas or even stolen classified information. Terrorists, for instance, may use the internet to communicate and share information about an operation or a future target. The internet helps them stay in anonymity, search for classified data allowing them to attack multiple targets, increasing the danger of cyberterrorism in a global scale. "*Cyberterrorism* is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not." (Sarah Gordon, Senior Research Fellow Symantec Security Response, and Richard Ford, Ph.D. Independent Consultant, "Cyberterrorism?", Symantec Security Response, p.4).

Social media create worthless information, influencing people's psychology and spreading panic. With the same tactic, cyber terrorists use the internet to upload data, arrange efficient propaganda methods or even recruit sympathizers, creating an 'electronic jihad' against politicians or governments. For example, with Facebook they can share ideas and recruit new 'cyber warriors', plan a propaganda and influence people's minds.

Then, panic and chaos will wreak in a national and international level through an ‘innocent’ application. With a click of a button, classified information within seconds will be uploaded in different sites, governmental secrets that citizens will discover and start doubting about the effectiveness and honesty of politicians. Riots will begin, vandalisms, guerrilla warfare and many more will threaten the stability and security from inside out (from a national to international community). The virality of the news, because of the globalization and the digitalization, will be shared within seconds all over the world from internet users. The media coverage of cyber-attacks should be done carefully and correctly. The news that will be presented should be accurate and not create fear over the society. It is the way that you present something that has a widespread effect to the public.

Using internet and social media, we talk about cyber threats and not exactly about cyber-attacks. It is a matter of time for cyber-attacks and cyber threats to be executed, but the difference here is that the cyber threats do not penetrate an electronic system, they do not change electronic data or destroy computer networks. Cyber threats are about the management of information, how the top secrets or even fake secrets go viral, how they are spread to the international community and how cyber terrorists coerce politicians and force them to follow their orders. Terrorists show a great mastery in technological networks and releasing cyber-attacks. The Dark Web in the hands of cyber terrorists could cause severe damage at national infrastructures and the national stability threatening at the same time national security. Because of technology the world has become one, and the governments should rethink and re-establish politics for decisive results in all levels.

More than ever, a well-planned basis for cyberspace and cyber security is challenging for the security of the states. The internationalization of the system flaws has caused many problems at the function of the electronic systems, but for the international

community this is not the only issue. Through soft power, cyber terrorists using internet and social media have gained power in cyberspace setting a new scene for defense measures. The battleground of the future warfare will be in chats, forums, blogs and in any cyber form possible, not with physical appearance such as weapons and bombs. The internet is the new weapon and in the hands of terrorists could release a Cybergeddon with inevitable consequences.

The importance of political leadership in cyberspace

Cyberspace is poorly understood, especially from politicians and governments. With the rising of Cyber Warfare and Cyber Terrorism, policy makers should be more organized and realize the danger that is lurking into the dark. Coherent defense plans and strategies will help promote security and stability in international community, designing an integrated security plan against sophisticated cyber-attacks. As the internet is currently unstable, with many ramifications (ex. The Dark Web), it is time for policy makers to take the lead and start creating a culture of cyber-risk managers. Flexibility and robustness in response of a cyber-attack are essential for this new framework. Because of the lack of response time in many cyber-attack cases, cyber risk managers should simulate in extreme situations under pressure, infiltrate the incoming information and categorize the attack. This new framework of cyber political management requires persons with knowledge, simulation awareness and strategic background. Cyber policy managers should be prepared for any circumstance and learn how to manipulate your opponent even in the case of cyberspace where you cannot know the origin of the attacker.

"Preparation of strategic cyber defenders is critical because instinctive behaviors exhibited in the face of uncertainty are invariably incorrect and counterproductive" (Martin R. Stytz, Sheila B. Banks, "Toward Attaining Cyber Dominance", Strategic Studies Quarterly; winter 2013, Vol. 7 Issue 4, December 2013, p. 19). Cyber policy managers need to attain political leadership skills, adequate for future global shocks. They need to look beyond the current information technology and emphasize the danger of outsourcing, the supply chain as well as external shocks and agreements. The sociopolitical tools will help the analysis of cyberspace, experts and policy makers to frame a new structure and develop new areas of study.

Knowing your enemy, it will help you deepen your research and develop your offense strategy. A new area of foreign policy in the field of cyber diplomacy, will assist the international community to promote cooperation and information sharing. High-skilled policy experts are already needed for this new development and research.

Leadership, however, is the skill that will make a difference. “Leadership will be needed to prevent a more dangerous slide into conflict, and provide a needed breathing space for societies across the world to work out internal problems and begin to stabilize” (Mathew J. Burrows, Foreword by Brent Scowcroft, “Global Risks 2035: The Search for a New Normal”, Atlantic Council Strategy Papers, September 2016, p. 2). Cyber policy managers will prevent cyber-attacks escalating from small scale to full-scale attacks in a state’s territory, they will react quickly and prevent any chaos or destruction. Their approach will be adapted to each case that will occur and develop offensive coordination. They will develop a post-incident analysis, to deepen their work and effort for better defense and offense mechanisms. Today, the challenges are various given the fact that the world is hyperconnected and most of the cyber-attack cases are politically motivated. Imagine an ‘electronic Pearl Harbor’ in a global scale destabilizing the international community.

The lack of a global institutional framework could be very dangerous. From now on our everyday life will depend exclusively on internet (nanotechnology, smart cities, big data, robotics), it is important to grant a security defense agenda. Leadership skills, simulation experience, knowledge concerning cyberspace and its capabilities, will reinforce cyber policy makers to promote a new holistic approach for the cyber era. However, it should be made clear that cyberspace is a domain with sociopolitical characteristics as well as technical one.

Experts from different field will be needed to express their ideas for these asymmetrical attacks and the Cyber Warfare phenomenon. As Sun Tzu stated, “all warfare is based on deception”. “The cyber competition appears to be an offense-dominant competition. If both the attacker and defender are given equal resources, the attacker will prevail” (Andrew F. Krepinevich, “Cyber Warfare: A ‘Nuclear Option’?”, Center for Strategic and Budgetary Assessments, p. 101, 2012).

The role of private sector and the public – private partnership against Cyber Warfare

Internet governance is one of the topics that are discussed thoroughly the recent years for the confrontation of Cyber Warfare, Cyber Terrorism and cyber-attacks. A fight that begins in cyberspace is possible that will spill over to national and private infrastructures. The fear of escalation has forced states and private companies to cooperate closely for the implementation of a new regime, new plans and defense measures. As cyberspace cannot be disarmed, state and non-state actors are trying to enforce cyber defense mechanisms and build an effective collaboration.

"Having policies, plans, and procedures in place to guide agencies in responding to a cyber incident is critically important to minimizing loss and destruction, mitigating the weaknesses that have been exploited, and restoring IT services" ("Agencies Need to Improve Cyber Incident Response Practices", GAO, United States Government Accountability Office, Information Security, April 2014, p. 5). Although, state is the dominant actor, private companies can very effectively contribute to this battle with technical knowledge and management experience. To combat cyber threats, private companies can address the real problems of the cyber era, and suggest solutions for each case. With management risk expertise, the private sector will evaluate the cyber-attacks and the cyber battlefield, identify the weaknesses and build defense walls, capable enough to repel multiple cyber intrusions.

Some issues concerning the internet governance are technically originated, and they need technical recommendations. Even if companies are monitoring the cyber-attacks, hardening security measures and scanning networks for malware, they still seek guidance from the governments. When it comes to implementation of laws, 'chase' cyber

criminals and terrorists, it is the state that must take the lead. Private companies cannot fight against states or attackers who are funded from state actors.

Networks are fragile and the public-private collaboration should be expanded in all levels of a state. “This increasingly tight coupling of the internet with the real economy and society means a full-scale cyber shock is far more likely to occur than some risk managers (and internet professionals) care to admit: internet failures could cascade directly to internet-connected banks, water systems, care medical devices, hydroelectric dams, transformers, and power stations” (“Risk Nexus, beyond data breaches: global interconnections of cyber risk”, Atlantic Council, April 2014, p.5). Critical infrastructures have been or will be connected to the internet as global networks, increasing every day. Although absolute cyber security is impossible, security companies may advice governments for cyber security plans, evolutions and cyber strategic behavior, having a constant feedback of the cyber-attacks between companies and governments, planning at the same a coherent retaliation.

“A working definition of *Internet governance* is the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet” (John E. Savage, Brown University, Bruce W. McConnell, EastWest Institute, “Exploring Multi-Stakeholder Internet Governance”, cybersummit 2014, p. 1). “There are three approaches that frame the debate on cyberspace governance: distributed governance, multilateral governance, and multi-stakeholderism” (A. Liaropoulos, “Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multistakeholderism, and Power Politics”, Journal of Information Warfare, Fall 2016, Volume 15, Issue 4, p. 9).

The most discussed model is the multi-stakeholder internet governance. “The Internet has flourished because of the approach taken from its infancy to resolve technical and policy questions. Known as the multi-stakeholder process, it involves the full involvement of all stakeholders, consensus-based decision-making and operating in an open, transparent and accountable manner” (John E. Savage, Brown University, Bruce W. McConnell, EastWest Institute, “Exploring Multi-Stakeholder Internet Governance”, cybersummit 2014, p. 3). This model involves state and non-state actors, freedom of expression, innovation and investments, wealth, open and transparent decision procedures. Furthermore, it is responsible for the implementation of policy rules in a global scale. Classified goals against Cyber Warfare have a large international impact. However, it is not a panacea as the absence of rules and the control of implementation of policies, do not create a consensus for an organized structure against the cyber threats. Cybercrime, Cyber Terrorism and cyber-attacks have created a sense of mistrust for the weak legitimacy and the inefficiency of decision makers. States fear the loss of control. Governments should interact closely with the private sector, design and implement a private agenda dialogue promoting innovation and dialogue, but without minimizing their control over cyberspace. In issues like nanotechnology, Artificial Intelligence, biotechnology, companies are reacting faster than governments, as they have the technical knowledge and equipment to support innovations like these.

To address cyber threats, a consistent public-private collaboration would clear what the real cyber dangers are and promote fruitful solutions. With continuous dialogues, each side will state clear what is trying to achieve and what ‘weapons’ can contribute against Cyber Warfare. Private companies need to legitimize their strategies and governments need technical recommendations for the ongoing cyber war. The agencies created by governments will be informed by IT experts from private firms, promoting

awareness to all state's levels as well as to civilians. Evaluating and analyzing cyber threats, preparing for possible cyber-attacks and enhancing retaliation methods, this relationship, based on mutual trust and understanding, will promote a new international cyber security strategy. Even if they do not know the origin of the attacker, the preparation procedure will assist them defend their infrastructures, activate their defense mechanisms and cultivate a coherent cyber behavior.

The new framework in Cyberspace – Power and States

The USA is planning cyber defense strategy against cyber operations, separating its military and intelligence services, trying to upgrade its electronic networks, China and Russia as the most wired countries can release cyber-attacks, Estonia is an experienced state of cyber knowledge, Israel is building 'cyber defense walls' and France provides full analysis of the cyber-attacks. Cyber-attacks are the new threat for the international community and a new dimension that changes the overall security planning. "Decisive results come sooner from sudden shocks than long-drawn-out pressure. Shocks allow the opponent off balance. [Gradual] pressure allows him time to adjust to it" (Andrew F. Krepinevich, [Liddell Hart], "Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary Assessments, p. 24, 2012). Illicit behavior and hostile intentions are included in the landscape of cyber security and are multiplying every minute.

As cyberspace is not a unitary domain, cybersupremacy for a nation is impossible. The volume of cyber shocks will multiply within the next years, because of our reliance in internet. Cyberspace is a dynamic domain, with various cyber challenges and threats for the governments. In the realm of Cyber Power, states will need experts from military, political, social and economic fields. The traditional meaning of power will get a new shape in cyberspace, and the power of states will be translated into words of cyberspace culture. Cyber Power will be based on attraction and cooperation, attraction for innovative technologies, technical systems and the cooperation between states for the knowledge of the cyberspace domain and the supply of technical equipment. Governments will grow their influence over private companies and enhance their role in cyberspace with IT expertise, new electronic systems and prioritization of research. The ambiguous nature of network developments, with social, political and technological capacities in the modern

world, also creates a new national potential in a different level. National mobilization is shaped in accordance with digital development, with risk assessments to address cyber deterrence and extended analyses to all levels of power as well as the security strengthening of critical infrastructures.

"The combination of large numbers of cyber competitors - perhaps including non-state entities - and highly risk-tolerant leaders also suggest a significant potential for cyber proxy wars" (Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary Assessments, 2012, p. 11). Even though cyber supremacy is impossible in cyberspace, prospective cyber powers are trying to win cyber arsenals and find technical equipment and strategies that will establish their primacy. The most common way is cyber espionage. *Cyber espionage* according to NATO, is "particularly when targeting commercial intellectual property, risks, over time, undermining a national economy. Many countries use espionage to spur rapid economic growth based on advanced technology, targeting science and technology initiatives of other nations". If a government may use hackers to steal information from another state, hack military and governmental electronic systems without risking uncovering its identity, raising concerns for the growth of illicit activity and cybercrime. *Cybercrime* is "the use of cyberspace for criminal purposes as defined by national or international law" (as defined from US/RUSSIA, NATO Cooperative Cyber Defence Center of Excellence).

Another concern is the use of civilians as cyber soldiers by China, named as 'patriotic netizens'. They are "Chinese civilians who take it upon themselves to attack targets than question the Chinese state and its ideals" (Tobias Feakin, "Enter the Cyber Dragon, Understanding Chinese intelligence agencies' cyber capabilities", Issue 50, Australian Strategic Policy Institute, June 2013, p. 4). The complexity of internet and

electronic systems has forced states to adopt a whole new different approach to the upcoming problems. Military approach should differ from the civilian one. Military are different systems from the civilian one. The military guarantees the national sovereignty and stability, its systems are more complex and their cyber defense capabilities should be enhanced, in tandem with resilience. Crucial information for a state are saved in military electronic systems, for example cyber capabilities, research for the enhancing internet systems and creating new cyber weapons, information for the political and economic stability. This does not mean that the civilian electronic systems should be undermined, but each government should adopt a total defense concept, as EU did, ensuring the national sovereignty.

"Given the broader geopolitical and technological trends, in the best case, the world is looking at multipolarity with limited multilaterism" (Mathew J. Burrows, Foreword by Brent Scowcroft, "Global Risks 2035: The Search for a New Normal", Atlantic Council Strategy Papers, September 2016, p. 8). Cyberspace has become a key battleground for both states and terrorists. Offensive Realism dominates in the new international arena, where each state has an offensive behavior because of its national interests. Moreover, through international cooperation tries to multiply its power for the sake of its national stability and security. The system now is polycentric than unipolar, as no country has the networks and connections that could prevail in the cyberspace. Many researchers claim that the USA has the cyber weapons for the primacy in the international system, but China and Russia or even Israel cannot be excluded for the cyber race arsenal. Secrecy and sabotaging key infrastructures in other territories are the keys for turning cyberspace into a battleground.

Cyber Power is “the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power”, and *National Cyber Security* is “the focused application of specific governmental levers and information assurance principles to public, private and relevant international ICT systems, and their associated content, where these systems directly pertain to national security” (Alexander Klimburg, “National Cyber Security Framework Manual”, NATO CCD COE Publication, Tallinn 2012, p. 28 and 29). These two definitions clarify that the new framework is still ongoing in the modern world. The capabilities to pursue political and economic interests while ensuring the security of critical infrastructures and the resilience of the state is the Cyber Power set the new cyber battleground. With new threats and challenges arising in cyberspace, governments should adopt a more active foreign policy, creating internal and external cyber security policies.

Cooperation or Competition

The recognition of threats and challenges is a necessary step for states to protect their national sovereignty in cyberspace. Even if they have recognized some of the existed dangers, the digital world hides many loopholes. Political will is still limited in national and international level. Cyber infrastructure is privately held and the cooperation between governments and companies should have a common ground, where cyber security is set as a priority.

Dependency on internet is growing, highlighting the need for a closer collaboration between states. Each government in the international arena tries to satisfy its own interests and gain more power, becoming the only power in the international system. However, this power arsenal cannot be continued in cyberspace, if a state wants to secure its national sovereignty. Because of the many loopholes in cyberspace, states should collaborate closely, share information and develop productive dialogues. There are still many things to learn for the cyber world, and trust among the states is the most key factor against the rising Cyber Warfare. Can someone risk ignoring that a cyber threat in one country can have remarkable results in another country? Cyber security issues affect not only all states, but also every person. A more active foreign policy for achieving internal and external security is on demand (Alexander Klimburg, "National Cyber Security, Framework Manual", NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn 2012).

The multinational sharing of knowledge and information between the countries is necessary for identify key threats and develop strategies that will prevent those dangers from intruding electronic systems. Cyberstrategy should explore actions against cyber espionage, and cyber power should focus on addressing the risks that are developed in

cyberspace daily. The distribution of power in the international system has altered the modern era we live in. A good example is that cyber-attacks are considered from many countries as an act of war. The complexity of cyberspace acquires a collective manner for building a whole new framework in the cyber era, with policies that concern all levels of governing. Furthermore, cyber policy makers should re-evaluate the digital development, the trend of posting videos, creating blogs or uploading classified information as they threaten the internal security of a nation and could be evolved into a geopolitical crisis. Non-state actors add a new complexity in the global system, emphasizing the fragility that exists in the modern era.

The threats that states are facing have a common basis, they have global effect and they are all nearly digital. The international cooperation should have a collective understanding on the nature of threats and the sophistication of cyber-attacks. “We must realize that globally we have entered an age of interdependence where each nation’s security and prosperity is increasingly dependent in the actions of the other nations of the world” (Andrew Nagorski, “Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway”, EastWest Institute, 2010, p. 13).

The definition of Hybrid Warfare and its Evolution

"The term *'hybrid warfare'* appeared at least as early as 2005 and was subsequently used to describe the strategy used by the Hezbollah in the 2006 Lebanon War." ("Hybrid war – does it even exist?", NATO Review Magazine). The evolving character of conflict has affected all the levels of organization of a country, not only the political and social ones, but also the military. It is unclear in the international community how to define Hybrid Warfare. There is no common definition and the use of the word 'war or warfare' is still a problem for all analysts. "The implication that the use of information in various guises to influence public opinion or political processes is or can be an act of war in and of itself is problematic and, in the words of Samuel Charap, a, 'a dangerous misuse of the word "war"'. There are no wars in history that were won by non-military means, or by the use of information, alone." (Bettina Renz and Hanna Smith, "Russia and Hybrid Warfare – Going Beyond the Label", Aleksanteri Papers, 1/2016, p. 15).

National interests are shaped in accordance with the latest technological evolutions, not culture. Globalization has affected in a large scale the way of political thinking as state actors are cooperating for their common interests in a unified arena affecting also military plans. Hybrid Warfare is an asymmetrical war by the weak against the strong. It has given birth to new war possibilities, using new irregular methods to break the leadership's will. It combines irregular and conventional tactics to achieve numerous advantages and possibilities in the conflict. For the United States Government Accountability Office, *Hybrid Warfare* is a "conflict executed by either state and/or non-state threats that employs multiple modes of warfare to include conventional capabilities, irregular tactics, and criminal disorder. (U.S. Joint Forces Command, Joint Center for

Operational Analysis briefing on "Joint Adaptation to Hybrid War")". (United States Government Accountability Office Washington, DC 20548, September 10, 2010, "Subject: Hybrid Warfare", p. 18). *"Hybrid war* is a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (i.e. economic, political, and diplomatic)." ("Understanding Hybrid Threats", European Parliamentary Research Service Blog, June 24, 2015).

The concept of Hybrid Warfare is a blend of warfare types (political, irregular, conventional) and cannot be categorized. A new generation of warfare has started a few years ago with the evolution of technology. Soft power instruments and high-tech capabilities with high speed and profound effect, have given birth to a new 'military operational approach' (2007, Frank Hoffman, Former US Marine Officer). Hybrid Warfare can be conducted from state and non-state actors using irregular and conventional methods, including the warfare in cyberspace. Most importantly, non-state actors, for example terrorist organisations, may use sophisticated technology to achieve their targets in physical and psychological dimension of a conflict, simultaneously. At operational level, if you want to win the battle you must know where the enemy is vulnerable. "Strategic cyber warfare is a contest for access, control, use, and manipulation of the opponents' data coupled with protection and confident use of your own data. In contrast, the offensive tactical level of cyber warfare comprises the technologies used to penetrate opponents' cyber defenses and technologies to exfiltrate, alter, or manipulate their data" (Martin R. Stytz, Sheila B. Banks, "Toward Attaining Cyber Dominance", Strategic Studies Quarterly; winter 2013, Vol. 7 Issue, 4 December 2013, p. 2).

"Cyberspace would be turned into a key battleground, where states and terrorist groups would seek advantage by sabotaging key infrastructure in each other's territories.

There would be always the chance that hybrid warfare would escalate into full-scale conventional or nuclear exchange" (Mathew J. Burrows, Foreword by Brent Scowcroft, "Global Risks 2035: The Search for a New Normal", Atlantic Council Strategy Papers, September 2016, p. 9).

This modern warfare has still many blurring lines that should be discovered as it is not clear for any actor which method to use. Cyber warriors have multiplied the last decade with extreme possibilities of creating criminal disorder not only in cyberspace as well as in the physical layer of a government's organization. Hybrid Warfare demands innovative thinking as the combination of irregular and conventional tactics is challenging. If a problem occurs, this is because of the lack of coordination organization. The retaliation against a hostile actor must be immediate and accurate, the defense and offense teams should be synchronized for preventing the escalation of the conflict. Modern threats and use of information provide the capability to influence political strategies and international cooperation. High-tech capabilities such as drones, artificial intelligence, encrypted command systems, nanotechnology and many more are a few of these examples. Future conflicts will be more complex and will demand more innovative strategies and structures.

Non-state actors, and specifically terrorist groups, have presented a great adaptivity to latest evolutions and espionage tactics for studying and analyzing the vulnerabilities of victims. The maneuvers of those hostile actors must be prevented from causing severe damages. Success will come with the contribution of small scale leaders with decision-making skills and innovative thinking, with cooperation in international level and adaption to the new modern threats.

"Today's strategists need to remember the frustrated Spartans outside Athens' long wall and remember the bloody success of the British, Russians, and Israelis in their long wars against hybrid threats—and prepare accordingly" (Frank G. Hoffman, "Hybrid Warfare and Challenges", issue 52, 1st quarter 2009 / JFQ, p. 6).

The importance of Soft Power

Information warfare has influenced the nature of threats and attacks, not only in international policies but at the internal organization of a country. Cyberspace is a digital and complex world with many dangers and ramifications. Each country tries to adapt to the technological evolution and build cyber strategies. As mentioned above, conflicts and wars have an asymmetrical form using conventional and irregular tactics. Cyber-attacks and Cyber Warfare influences international policies and defense strategies. The 'militarization' of internet and the cyber weapons arsenal has given to battlefield a whole different approach. Cyber-attacks have an impact on foreign policies and countries are shaping their offense and defense mechanisms according to the latest attacks, pointing out the importance soft power skills.

In an information age, relationship building and legitimacy are more effective and applicable rather than conflicts and competition. *Soft power* is "the ability to shape the preferences of others, and getting others to want the outcomes you want" (Joseph Nye, 1990). If a country wants to retaliate against cyber attackers, its technological capabilities are not enough for an effective attack. International cooperation and information sharing will help the interested states minimize their vulnerabilities. As everything becomes more intelligent, adaptability and quick-responding will enhance the state's policies. With this revolutionary technological transformation for a government and a society, their facing numerous risks.

The diffusion of power is still an issue for the international community as it is reinforced with the rising of cyberspace era. The flow of information has caused severe damage to national and international systems. Cyber-attacks target important infrastructures, systems or profiles. Leaking confidential secrets, they create mistrust and

chaos. The rise of ‘cyber jihads’ influences ideas and shapes preferences. They use internet as a platform to recruit new members and share their opinion all over the world, having an impact on world politics. They communicate secretly with each other and plan physical or cyber-attacks, they promote global terrorism and manipulate public opinion. The anonymity of internet lures many dangers such as extremism and destabilization. The origination of the attack and the identity of the hostile actor complicate the strategies of the countries and their defense plans. It is a new culture on military rather than implicating new norms and rules. Cyber terrorists or hackers may not use cyber-attacks to take control of important infrastructures, but concentrate on soft power actions, such as propaganda, espionage tactics to create mistrust and destabilization for a government. “The specific characteristics of cyberspace invite a plethora of opportunities and techniques to deceive the enemy with false information” (Nils Melzer, “Cyber Operations and jus in bello”, Disarmament Forum 2011, no 4, 2011, p. 17).

Data-controlling should be into the priorities for the international stage. Social networks with wide influence on the audience may cause severe damage, extremism and wreak havoc. Top-down regulations are crucial for the harmonization of policies and a government’s function. There many possible scenarios that cyber jihads may implicate, all at the same time. To avoid instability, complex regulations and technical systems, numerous teams should be avoided. Already cyberspace is a complex environment by itself, so power distribution should be well-organized and more accurate. International arena is familiar with the idea of diversity and creating common interests for the sake of national sovereignty.

For Sun Tzu, the use of intelligence is a necessary point in war. You must know your enemy, his men and its position. Through espionage you will learn the

vulnerabilities, the secrets and the power he may has. For cyberspace, information is a key factor for winning. You may not know the origination of the attack and what the exact motives are, but national mobilization is vital for ensuring the access to cyber professionals and evaluating the risks. Cyber experts will help promote defense mechanisms and ensure a safer cyberspace in important points that are relevant to the physical world. Politicians must serve civilian expectations and evaluate the cost and necessity of many strategies. If cyber jihads, terrorists or hackers steal confidential information and upload them to the internet, it is a matter of seconds that the secrets will be viewed by thousands of users. Government intervention should be well prepared to face these threats and secure its sovereignty. Social networks are a platform of getting informed, sharing ideas and leak data. States should be prepared to respond to these kind of threats, the wreak of havoc and extremism inside the country. The form of warfare is not limited to conventional but also to irregular methods. Cyber terrorists will not be restricted to the physical world, but they will use also cyberspace for their goals. Cyber infrastructure is composed of computers, servers, cables and other physical layers. The upcoming wars should be fought in all levels.

In the new future, soft power tools will be used more than ever. Adaptability and international cooperation will promote cyber security and eliminate cyber threats. If soft power is applied to all levels of country, and adapted to governance policies, then cyber terrorists' attacks will not cause wide-scale damages. "To respond rapidly to changes in cyberspace element priorities, strategic cyber defenses must be able to dynamically, seamlessly, and stealthily change to improve the defenses for the cyber elements and components that have the greatest value and importance at any given time" (Martin R. Stytz, Sheila B. Banks, "Toward Attaining Cyber Dominance", Strategic Studies Quarterly; winter 2013, Vol. 7 Issue 4, December 2013, p. 5).

Further information for Hybrid Warfare, Definitions - Examples

There are much more to be discovered for this modern warfare. Below there are presented some important definitions and examples of Hybrid Warfare that will help understand the potentials of this new type of war.

"Hybrid threat is a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat. Hybrid conflict and hybrid war are two specific categories whereby some hybrid tactics are used by a state to achieve its strategic ends." *"Hybrid conflict* is a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives." ("Understanding Hybrid Threats", European Parliamentary Research Service Blog, June 24, 2015)

"*Hybrid threats* are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives". ("NATO countering the hybrid threat", NATO ACT, 23 September 2011).

Examples of hybrid threats ***("Understanding Hybrid Threats", European Parliamentary Research Service Blog, June 24, 2015)***

Terrorism: terrorist organisations like Boko Haram, Al-Qaeda in the Arabian Peninsula (AQAP) and ISIL/Da'esh operate across the territories of many countries, and employ a variety of economic, military and technological tools to achieve their political goals.

Cybersecurity: the operations of state-affiliated hackers from Russia and China and the use of cyber-weapons are facilitated by difficulties with the attribution and the absence of norms of state behaviour in cyberspace.

Organised crime: armed criminal groups and drug cartels in Mexico resort to violence in the fight over territory and economic profits. Erosion of security, in turn, has a negative impact on the Mexican economy.

Maritime disputes: China is pursuing its aims in the South China Sea by combining economic and military pressure with extensive land reclamation projects in the Spratly archipelago.

Space: constraints on use of orbital space (and access to satellites) resulting from space debris – created, among other things, by anti-satellite missile tests.

Resource scarcity: resource-dependency between countries is increasingly used for political purposes. In 2010, China blocked exports of raw materials to Japan in response to the arrest of a Chinese fishing boat. In 2011, India's refusal to adopt a water-sharing agreement with Bangladesh put additional pressure on bilateral relations.

Covert operations: Russia's strategic use of special forces (i.e. 'green men') and information in Ukraine.

Conclusions of part B

The power of computing technologies has increased tremendously the last decade. The state system of 21st century, as well, has been affected from the latest technological evolutions. Modern warfare, cyber-attacks, cyber warriors, cyber weapons arsenal, new decision actors are few of the characteristics that set the new scene of national and international system. The expansion of globalization and hyper connectivity has influenced in powerful ways the society. Citizens explore every day the capabilities of virtual reality environments. Internet of Things, Big Data, Smart Cities are some examples of the future innovations in the way we live, we interact and work. Modern technologies involve all aspects of life and that means the state must act for a stable and secure digital environment. The digitalization of the conflicts has empowered cyber warriors to arise and cause severe damages to daily technological function with cyber-attacks, cyber espionage and sabotage. However, those actions may influence the national security and escalate into the international level. No one can know exactly the consequences of those cyber threats, or ignore their possible escalation. A 'global Renaissance' with new challenges and opportunities has already begun.

State continues to be the dominant actor in cyberspace and is responsible for national cyber security and political leadership. The management of hard and soft power will prepare governments to function despite the cyber-attacks and other cyber threats. Collaboration with private sector, innovative thinking and pluralism in decisions will enhance the stability and cyber security. "We expect that, in the short run, uneven patterns of cyber access will continue to reflect the distribution of power in the international system. Over time, the diffusion of cyber capabilities worldwide will expand political participation, enhance politicization of both idiom and action, and increase competition

for influence and control over the management of cyberspace" (Nazli Choucri, "Co-Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences", 2013, p. 11).

The militarization of the internet demands flexibility and robustness. Private companies cannot retaliate against actors funded from countries, modern threats such as hybrid warfare use irregular and conventional means, state should enforce its capabilities and a more organized strategy that will secure its infrastructure and national security. All cyber threats should be classified for purposes of immediate response. "Tactical cyber conflict is dominated by technological considerations; strategic cyber conflict is dominated by data, SA, and decision-making considerations" (Martin R. Stytz, Sheila B. Banks, "Toward Attaining Cyber Dominance", Strategic Studies Quarterly; winter 2013, Vol. 7 Issue 4, December 2013, p. 3).

Cyber security is impossible since cyberspace is a complex environment, with multiple cyber-attacks released simultaneously at different or same targets and various entry points. New decision actors threaten national stability, as anonymity in internet empowers individuals. As state is the major actor in international system, it must show adaptability in a constant changing environment, evaluate data and avoid classified information been uploaded to the internet. It is the virality of the news that will promote extremism and mistrust. To avoid escalation, a coordinated approach to cyber security must be designed analytically. Exploitation of penetrations, immediate recovery from cyber-attacks and response methods in physical and cyber level, and collaboration in international scale putting aside any obstacles are a few examples. The importance of threats and conflicts has not been yet great. States can still change the advantages that cyberspace offers in individuals and build a stable security.

PART C

Cyber Warfare, Cyber Terrorism and Cyber Crime

With the evolution of technology, the nature of warfare has changed a lot the last years. Threats in all levels of a country's structure have emerged, social media threats, government and business threats, and many more. The increasing importance of geopolitical matters requires operational analysts for further possibilities in cyberspace. Cyber Warfare is a silent war as state and non-state actors use cyber weapons to penetrate computers or networks for inserting or disrupting control systems. However, there is not a generally accepted definition. Although, the whole concept of this type of warfare is still controversial and ambiguous, it is an unavoidable element of discussion and research in the planning of policy strategies.

Adaptation is now typical and as major environmental theories of war have played a significant role and shaped many strategies (ex. Airpower – Douhet, Land power – Mackinder, Naval power – Mahan, Space power – Gray and Sloan), so they will continue to influence current perspectives in accordance with the technological advances, speed and scope. Cyber threats are a common phenomenon for states and national mobilization is structured accordingly to future cyber-attacks, for example a possible 'electronic Pearl Harbor'. Pre-emptive cyber-attacks and other preventive options such as testing national cyber defenses, roles and responsibilities, coordination and retaliation constitute national mobilization in cyberspace.

Cyberspace is attractive for terrorists since it is cheaper and can communicate anonymously with other users without being traced. They can recruit new members, raise money, plan and support their operations and exploit the virality of social media. "Storage of sensitive information on networks has given birth to cyber espionage against governments and cyber economic warfare against businesses" (Andrew F. Krepinevich,

"Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary Assessments, 2012, p. 9). Cyber warriors or terrorists can develop linkages with trans-national criminals to support their objectives. Cyber criminals, on the other hand, can provide terrorists with cyber knowledge, profiting from this relationship. Both types of those actors can be empowered from the constant changes in cyberspace.

Terrorism is about the understanding of emotions, beliefs and psychological factors. The same procedure applies for cyber terrorism. The judgement of the attacks, the planning and the retaliation are common for evaluating terrorism in cyberspace. "There are many forms of terrorism on the Internet. Some are not dangerous enough to be deemed a simple spread of information instead of terrorism. They are simple show of sill and are harmless. Acts of cyber-crimes may involve stealing of money, company secrets, or attacking country's infrastructure and causing real damage" (Steve Saint-Claire, "Overview and Analysis on Cyber Terrorism", 2011, p. 1).

"Organized crime has been a major catalyst in the expansion of illicit cyber activity" (Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary Assessments, 2012, p. 65). *Cybercrime* is "criminal activity conducted using computers and the Internet, often financially motivated. Cybercrime includes identity theft, fraud, and internet scams, among other activities. Cybercrime is distinguished from other forms of malicious cyber activity, which have political, military, or espionage motivations" (Source: Compilation of Existing Cybersecurity and Information Security Related Defintions, Open Technology Institute New America - 2015 July).

For the academic community, there is still concern for the differences of those two definitions of cyber terrorism and cybercrime. Because of the constant emerging technologies, the efforts against terrorist groups are evolving into battles of intelligence. Anyone can 'play' with the internet weapons, and more specifically terrorists who seek out publicity as they can target a much wider audience.

Internet in the hands of terrorists can be very catastrophic for the states and the international community. Targeting national critical infrastructures, the risk of paralyzing every aspect of a government's organization is more than highly to become reality. Internet of Things, Big Data are widening the surface of cyber-attacks since the enormous number of entry points that can be affected. With wi-fi connection, any device or system can be hacked, as well as street surveillance cameras, or personal information and sensitive data to be stolen. "The last and often a neglected issue, has to do with the fact that security was not a main concern in the early phases of cyberspace development. The logic of its architecture was flexibility and openness and not security and reliability…. The promise of the Internet was to serve as a domain where individuals could interact, follow news, and share information and ideas freely" (Andrew Liaropoulos, "Reconceptualising Cyber Security" Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and Terrorism, Volume 6, Issue 2, April-June 2016, p. 34).

The use of social media from terrorists may cause chaos and spread paranoia. The virality of the news in internet is used as a propaganda machine, hurting the reputation of states. Cyber terrorists and cyber criminals are interested in keeping the internet working. What they cannot achieve militarily, they can achieve it through the free entrance points in internet and the information exchange.

Many are the possibilities for the cyber terrorists and many are the cyber threats for the governments. The role of the state is to safeguard its national security and prevent future cyber-attacks, or at least minimize the effect that may have. Governments should control information over cyberspace and the profile of users. That does not mean to become authoritarian regimes and control people's minds. With respect to human rights and privacy, states should focus on the leak of information and the security of critical infrastructures. Law enforcement for the protection of fundamental rights should be also a high priority for the international community.

"In their efforts to secure cyberspace, states are trapped in the classic security dilemma. This security dilemma arises from the situation of anarchy that exists in the international system" (Andrew Liaropoulos, "Reconceptualising Cyber Security" Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and Terrorism, Volume 6, Issue 2, April-June 2016, p. 34). There are many autonomous administrative domains that operate internationally, and if states want to secure cyberspace, then they should cooperate closely with each other and with the private sector. The size of information, the origination of the attacks and most importantly the persons who manage the information are a few examples of the difficulties in the modern technological era.

The dangers of the evolution of Cyber Warfare and Cyber Terrorism will continue to multiply. The approach of states has still many improvements to do and many ramifications to analyze. The control over the information and the profile of users must be exercised with a human-centric approach. Surveillance systems, sensors, and other technologies are not a panacea. Innovative thinking and adaptation will set a new agenda for the confrontation of modern warfare and terrorism.

Geopolitical and Geographical analysis

"Norms in particular are important given the current geopolitical information landscape, since they can "normalize the exercise of power in cyberspace," serving as a form of deterrent for aggressive cyber behaviour. Indeed, if complied with, norms can potentially channel, constrain and constitute action through inducement and coercion; moral pressure and persuasion; and social learning and habit. As noted at a recent meeting on Cybersecurity and Confidence Building Measures, CBMs can, on the other hand, serve to lay the foundation for agreeing on such norms and on measures to avoid miscalculation and escalation" (Camino Kavanagh, Daniel Stauffacher, "The Reach of Soft Power in Responding to Cybersecurity Challenges", ICT for Peace Foundation, p. 6).

Cyberspace is a domain made by human and needs more research to understand the possibilities that offers and the dangers that hides. Many researchers have compared cyber power with air power. Cyber power can be a destructive force and its technological nature can sometimes blur the lines of the war. However, as Douhet made a huge mistake with this comparison, that air bombing is a decisive method to win the war, so did the current researchers. You must know the limits of the battlefield to inhibit the enemy, or else he will return the attack with more power and pressure.

Dependence on science and technology, as well as internet, has grown a lot the last years, creating concerns for the vulnerabilities of the systems. Smart cities and home appliances, Big Data are a few examples of this phenomenon. "Terrorist use of cyberspace also has a geopolitical dimension in that efforts to raise money and recruit are geopolitically focused toward diasporas and co-religionists who have a geographic footprint" (John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters", published online: 03 November 2014, p. 5). Cyberspace is not just cables but

the realm of Internet of Things has already begun. Cyber terrorists take advantage of global networks to weaken governments focusing on rich countries all over the world threatening their national infrastructures. Networks are not limited geographically and a simple cyber-attack can have affects from one country to another, spreading the vulnerability and the fear of escalations. Countries are trying to limit the risk but many are the actions that should be done, and most importantly states must trust each other. Control of information and information access will be achieved with international cooperation and common response teams. National organisations, for example, are connected to the internet and can be hacked or have their data stolen. This should motivate governments to work closely and prevent future accidents such as electronic Pearl Harbor or multiple cyber Katrinas.

Distances have shortened and many countries "hire" cyber criminals to do the job. Cyber espionage is a method used by many governments to sabotage or damage the reputation of another state. Cyber criminals bring their laptops to the fight and try to exploit vulnerabilities in electronic systems and take control of it. Cyber espionage is used not only from countries but also from cyber terrorists. If governments want to limit the risk of been cyber attacked, then they must trust each other and eliminate any system vulnerabilities. However, the militarization of the internet depicts the incredulity that surrounds the international system. "States feel insecure about the motives and cyber capabilities of other actors and, therefore, develop offensive and defensive cyber-weapons. Since there is nothing to prevent states from trespassing the digital borders of other states, more insecurity is created" (Andrew Liaropoulos, "Reconceptualising Cyber Security" Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and Terrorism, Volume 6, Issue 2, April-June 2016, p. 34).

Offense and defense must be conceived in terms of technological innovation. A modern political agenda that depicts those changes will secure at the same time national stability and sovereignty. Geopolitical strategies underline how a state thinks and shapes its plans for control and influence. Geographic location still plays a key role to the structure of foreign policy and diplomacy. Coordination – Cooperation – Collaboration is a concept that will reinforce governments against cyber threats and set a new order in the international system. Cyberspace and cyber power are unique because they still influence traditional forms of power and they will continue to do it. The rise of space power has a significant role on the conduct of warfare and the character of diplomacy, policy and economy. "Whenever geopolitical rivalries and tensions are present and whenever the physical locus of power resides, cyber exchanges occur" (John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters", published online: 03 November 2014, p. 5).

Strategic behavior in Cyber Security and Cyber Risk Management

"Napoleon once said that 'war is 90% information" (Philippe VITEL (France), General Rapporteur, "The Future of Allied Airborne Intelligence, Surveillance and Reconnaissance", Draft General Report, NATO Parliamentary Assembly, Science and Technology Committee, 20 September 2016, p. 1). Current trends and threats have affected in a large scale the structure and the organization of states. Globalization has brought closely societies and has forced international system to re-evaluate policies and strategies for defending against cyber terrorists. Although the technological evolutions, the objectives of Strategy remain the same, but contingency plans, resilience strategies and consequence management initiatives will be adapted to the military capabilities that technology offers.

Classic Theorists like Sun Tzu still matter in cyberspace era. Cyber espionage, for example, is used for defense purposes. State actors, and even non-state actors, avoid the exposure threat, hack system networks, and steal data information. But it is not only about hacking and stealing information, they use surveillance methods to track their targets, learn their vulnerabilities and build their offense against the threat. An intelligence culture has arisen, and states should understand the security requirements to prevent cyber-attacks and escalation of the cyber threats.

Examples of cyber war show the destructiveness of this new modern of war. Hard power is still important, except that wars have become more sophisticated. "From a strictly theoretical perspective it cannot be excluded that even a small but organized group of hackers launching highly destructive cyber operations against a state's military network could trigger a non-international armed conflict" (Nils Melzer, "Cyber Operations and jus in bello", Disarmament Forum 2011, no 4, 2011, p. 12).

According to Sun Tzu, you must hit the enemy without being exposed, and that it the nature of cyber-attacks offers. “If he sends reinforcements everywhere, he will everywhere be weak” (Nils Melzer, “Cyber Operations and jus in bello”, Disarmament Forum 2011, no 4, 2011, p. 12). Still, in an information age, we do not know if the other side could be vulnerable in variable electronic positions. Technology has shown the innumerous possibilities that offers, if there can be simultaneous cyber-attacks, then a cyber defense can be programmed to automatically respond in different attacks at the same time.

For a coherent cyber strategy, policy makers, IT experts, psychologists, and strategists should work together to secure national sovereignty and stability, and build a new innovative cyber strategic behaviour and power. Policies and strategies must be reviewed, updated system networks and constant identification process of vulnerabilities are a few ideas. National parliaments have also responsibility to harmonize internal and external policies, create decision support systems and promote national and international cooperation with private sector.

National cyber security is a game of strategy. To avoid a strategic vacuum, policy makers must review their diplomatic relations. Cyber threats seem to alter power balance and affect international relations. Cyber operations should be re-planned on a constant basis and adapted to the ramifications of technology. Cyber terrorists want publicity and with the internet, they target a much wider audience. The threat of terrorist views going viral and controlling civilization is that disrupts the national system. The typology of cyber operations should include diverse types of data, possible targets of networks and possible scenarios of cyber threats.

A new counter cyber agenda should be adapted to the new global domain and the revolution in military affairs. Cyber terrorists always target a physical realm and try to cause chaos, as their identity is hidden and no one can know the origin of the cyber-attack. A battle that started in cyberspace, by hacking, controlling and destroying crucial data or system networks, may split in the physical structure of a government will grievous consequences, demanding the military to interfere for securing the nation's stability and sovereignty. The potentials of cyberspace have a profound effect on national power and the nation's behaviour. Non-state actors seem to benefit from these potentials, illustrating the importance for governments to rely on traditional strategists and theories as a basis for the new counter cyber agenda. The risk management should include not only policy makers but also opinions and ideas from the military, to preserve the internal and external security. The diffusion of power in non-state actors may cause more disaster than can anyone imagine.

Strategic analysis of Stuxnet and its importance in the new era of Interconnectivity

In 2010, the International Atomic Energy Agency visiting Iran, noticed that the enrichment procedure of uranium was failing and they did not know why. Five months later a Belarus security company in Iran had problems with its computers at they were crashing and rebooting and again they did not know the reason. The worm Stuxnet identified by the security company VirusBlokAda the same year although, it was inserted the summer or 2009. The worm Stuxnet was characterized as 'highly sophisticated' and marked a new era in cyberspace. The malware had successfully impacted on a considerable number of centrifuges and forced them to get out of control. The clandestine appearance and its unique function pointed at specific nations who had decided to stop the Iranian nuclear infrastructures, the USA and Israel.

The relations between the USA – Israel – Iran have not been very friendly the last years. Iran's extremist views and political strategies in combination with the idea of building nuclear development, made her a threat to Middle East and to her other international enemies. Despite the Stuxnet and the economic sanctions from EU and the USA, Iran did not stop enriching uranium and expanding its nuclear capabilities with clear motive, the reinforcement of national power and security.

Stuxnet is unique on several levels as "it is the first 'precision-guided' cyber weapon in that it focused on a specific target and it was designed to attack a particular kind of facility" (Andrew F. Krepinevich, Cyber Warfare "A Nuclear Option", Center for Strategic and Budgetary Assessments, 2012, p. 151). Its catastrophic ability and its sophisticated action aiming one specific target have marked a new era in cyber security,

as it was the first time that a cyber weapon had been used through internet and it was state-sponsored.

The Distributed Denial of Service attack spilled into the physical world and especially to physical infrastructures connected to the internet. The insertion of the Stuxnet was accomplished with a simple USB stick into a common computer. Prior cyber-attacks focused only on websites and other networks. The Stuxnet worm showed the danger of such sophisticated malware if they fall into the hands of cyber criminals or terrorists for their own purposes. It is important to note that a physical actor had entered the nuclear infrastructures and inserted the worm into the system network without being caught. For many cyber experts, what is extraordinary, is the function of the malware as a 'ghost file'. The information systems of Iran were not capable of tracing any hostile action or any alteration in the data. Stuxnet updated its data via internet and autonomously conducted the cyber-attack deceiving the operators and the electronic defense of the centrifuges.

As a tactical cyber-attack, Stuxnet have succeed its goal to delay the function of the Iran's nuclear program and damage effectively 1,000 centrifuges as well as reveal to the international community the secret nuclear enrichment that was threatening neighbor, and not only, countries. However, the ongoing nuclear procedure did not stop by Stuxnet and did not force the Iranian government to alter its plans or even come up with an agreement with EU and the USA, even if those countries imposed sanctions to Iran. Iranian government, though, was not discouraged to replace the damaged centrifuges and reinforce its efforts for the nuclear enrichment, or even expand their research to the new cyber tool that it was used to destroy their nuclear enrichment program. Stuxnet did not dissuade Iranians to develop their nuclear strategy and install new centrifuges.

Cyber-attacks, in an era of interconnectivity and internet of things, will be used as a strategic tool for getting 'control' over data and reinforcement of national sovereignty. It is crucial for states to secure their civilian cyberspace infrastructures (power grid, military and government offices) against cyber criminals and cyber terrorists, as it is highly potential that they will face cyber-attacks in the future. International cooperation will help states to protect their interconnected networks and strengthen their cyberspace security. As Stuxnet proved, the target of a hostile actor could be an important physical infrastructure in order to surprise and confuse the victim or create fear and chaos, or for a state-sponsor cyber actor to gain political influence by revealing secret weapons at the expense of other states.

Cyberspace is a fertile ground for offense actions and the intensifying of states activities prove that the weaponization of internet is a necessary element for the security of a government. Cyber-attacks, cyber espionage or sabotage are not overwhelming weapons of a cyber war rather than capabilities that offer in an actor opportunities to win many advantages and finally the battlefield. Many studies have shown that various countries have the capability to conduct cyber-attacks. "States intrude into each others' cyber systems in "preparation of the battlefield" for what could be future conflicts" (Joseph Nye and Cyber Power, Belfer Center, May 2010, p. 11).

Cyber-attacks offer many opportunities to the offender in a tactical level, while in the strategic level they may have failed to accomplish their goal. Those cyber-attacks or other cyber methods were designed to provide political advantage and influence, and most importantly control and power. Stuxnet was a wakeup call for the security of international community. It targeted high security infrastructure, imitated data and relied on the vulnerabilities of the system networks. It was a well-planned cyber-attack, specifically

designed for such networks, proving at the end how crucial tool was for the offender to achieve a specific strategic goal using also a trustworthy employee to spread the malware. Here also it should be mentioned that "Stuxnet infected computers in many countries, and it is not entirely clear how the worm was disseminated" (James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", 2011, p. 34). Because of the rise of cyber criminals and terrorists in combination with the anonymity in internet, Stuxnet maybe used as a platform for future cyber-attacks more sophisticated and capable of shutting down not only industrial infrastructures but also national and military networks. Smart devices could conduct such cyber threats as their capabilities have improved and they are more than a simple device. Cyber operations will be used as equalizers, and they constitute part of national security. Cyber proxy wars will be multiplied not only with cyber-attacks and with virality of classified data threatening a regime's stability. "A well-executed cyber attack offers the opportunity for sophisticated targeting. But if damage from cyber attacks can be quickly repaired, careful strategic thought is required in comparing the cost and benefits of cyber versus traditional military attack" (James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", 2011, p. 34).

Cyber-attacks have begun important political methods to gain power in a tactical level and will target decision makers and not so much society. They are ideal for influencing politicians and gaining political advantage rather than causing instability in a strategic level. This should not appease governments that cyber terrorists will be limited to such attacks, but they still need to reinforce their cyber security and design a modern cyber strategy capable enough of preventing any havoc in military, governmental and civilian systems.

The political motives of cyber-attacks

Stuxnet proved to be a sophisticated cyber-attack and unusual tool for that era. The effects that the specific malware had were not only restricted to the Iranian infrastructures, they also expanded to the international community and how the states could develop their cyber power. With high political and strategic importance, Stuxnet is the junction between cybercrime and state actors. Attribution is a matter that creates innumerous problems to the governments and tracing the location of the attack. States should keep in mind a famous phrase for cyber-attacks, "Perceive that which cannot be seen with the eye" (Miyamoto Musashi, "The Book of Five Rings", 1645).

Many have supported the idea that cyber-attacks can be used as a governmental tool to shape foreign policy and support their strategies. "Cyber can nevertheless be a tool to discredit, destabilise and weaken the authority of adversarial regimes" (James P. Farwell & Rafal Rohozinski, "Stuxnet and the Future of Cyber War", 2011, p. 35). Cyberspace, technological evolution and interconnectivity have affected not only daily life but also the structure of governments. States use cyber-attack methods to weaken an enemy, destabilize a regime or prevent any hostile actor. However, we should keep in mind that it is very difficult to translate a cyber-attack into political strategy and name an actor or a state responsible for the attack. Below there are presented some prominent cyber-attacks that have drew attention of states, causing a cyber weapons arsenal and design of more sophisticated networks.

- 2007: Estonia, disable of websites, DDoS
- 2008: Georgia, disable of websites, DDoS
- 2009: American websites
- 2009: Google in China under cyber-attack

- 2010: Two sided-battle between Indian and Pakistani hackers
- 2010: Stuxnet, Iran, target: nuclear infrastructure
- 2012: "Red October", a worldwide cyber-attack, target: countries in Eastern Europe, the former USSR and Central Asia

Sources: NATO REVIEW magazine, "The history of cyber attacks - a timeline" and "Cyber Warfare: Concepts and Strategic Trends", Shmuel Even & David Siman-Tov, Memorandum No. 117, Tel Aviv: Institute for National Security Studies, May 2012.

Sophisticated cyber-attacks acquire a lot of money, not to be executed, but for the offender to hide its identity and build a defense wall. Governments have the capability to design defense mechanisms and if they execute a cyber-attack, then they can protect their "position" in cyberspace. Because of the anonymity in cyberspace and the rise of criminal activity, state actors do not risk being exposed and thus they hire cyber criminals and hackers to "do the job". Such criminals are triggered by the difficulty of those nature of targets (military or national networks, national infrastructures), or they just simply bribe their freedom due to the crimes they have committed working as mercenaries. The escalation of cyber-attacks by extremist policy makers having effective capabilities to design cyber-threats could create significant problems. It may be proved that the governments are more vulnerable than they have imagined and unable to cooperate with such advanced attacks.

An underground war has begun in cyberspace hiding many secret weapons and cyber offense and defense methods, criminals and terrorists, or even classified information for states. The wide scale of the Dark Net or Dark Web has established a fear for the unknown and the consequences it may have on an international scale. The lack of security awareness is another crucial factor for the countries to consider.

"Win victory before the first battle" (Sun Tzu, "The Art of War", 514 B.C.). Cyber-attacks as a tool of foreign policy will be used to win territorial control and diplomatic power and to protect national interests. Globally, we are depended more on information networks than ever before, and national security will be undertaken not only by countries alone, but also with the help of civilians having awareness of networks vulnerabilities and how easy they can become targets by cyber terrorists. In an independence age, each state's prosperity and sovereignty depends on the actions of other states too. Cyber evolution has brought significant changes in all levels of a nation. Therefore, it is unavoidable that a state will attack another country in cyber infrastructures preventing actions that will threaten her sovereignty and cyber national power, pointing out that security dilemma exists also in cyberspace. The key it not technical attribution, but national responsibility.

Conclusions of part C

Cyberspace has embedded in all aspects of our life and our independence on internet grows every day. National security strategy should include all these technological changes and re-evaluate the status of each country in international system. The involvement of government in cyberspace ranks the importance and the risk for national security the frequent cyber threats. State readiness is a high priority for governments and the cooperation with private sector should promoted as soon as possible. It is widely known that private companies own most of cyberspace and control vast amounts of data. The rise of cyber criminals and cyber terrorists has brought significant changes into the structure of a cyber national security and forced the international community to interact closely. The fight against cyber criminals and terrorists is a battle of intelligence. It is noteworthy for the governments to clarify the differences between cyber criminals and cyber terrorists. Terrorism is an international phenomenon, crime exists mainly into societies. Though, in a cyber era the nature of terrorists has changed and they will need a computer and an internet connection to destroy a target.

The surface of cyber-attacks is widening with the technological advances threating not only civilians, but also national infrastructures. Emerging technologies have given the capability to hostile actors to use surveillance methods, cyber espionage or cyber sabotage to shut down national system networks and spread havoc. Transnational terrorists can share ideas, knowledge or recruit new members without being exposed. The size of information, the enormous number of entry points and the anonymity in cyberspace are benefiting the attackers. Internet as a tool for terrorists may have devastating results. National infrastructures are crucial for a country because of their geographical and geopolitical importance. If they are under attack, thy will lose security credibility and

national power. Therefore, the attacker wins the battle in cyberspace and in the physical layer.

The fight against cyber jihads and extremists demands national mobilization and a coherent strategic behaviour, or else national power will be affected and limited. Harmonization of response teams, collaboration and quick response will preserve the national stability. Electronic systems have numerous vulnerabilities, and as people are connected with each other with smart applications and internet, the threats are global. Typology of cyber operations and frequent electronic monitoring will prevent or minimize the risk of the threat being spread to other areas. National territories should be secured in depth, because if they cannot retaliate and defend themselves they will be paralyze and destabilized. Apart from the cyber criminals and terrorists, many states have the capability to hack other countries internationally. A cyber weapons arsenal has already begun changing the current status quo. Preventive options such as research, development, resilience and pre-emptive cyber-attacks have taken their position in the international arena. However, "States are also [re]claiming their sovereignty in cyberspace through the promotion of international regimes" (John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters", published online: 03 November 2014, p. 4).

High-technology advanced countries are more likely to become targets. In the case of Iran with the worm Stuxnet was designed to control the centrifuges of nuclear program to get of control. Some opponent countries felt that the enrichment of uranium by Iran was a threat for their national sovereignty and security and the international stability, thus designing a weaponized malware specifically for the Iranian infrastructure. Attribution is still a weakness for this worm. Iranians scant the evidence and had some thoughts for who the attacker could be. Given the geopolitical tensions in the region and the diplomatic

relations, with some states, the USA and Israel are the possible actors, reflecting that policy-interests continue in cyberspace.

In an interconnected age, technology influences traditional instruments of power. Customized malware as weapon against states that are threats for others will be a common phenomenon in cyberspace. Stuxnet was an industrial cyber-attack, and no one can exclude the fact that it may be used as a platform for future more sophisticated attacks who will challenge sovereignty, stability and neutrality. Adversarial regimes are now a target. Regimes that depend on technology become threats for other nations that are not so technological advanced. Every government claims its independence in cyberspace by seeking cyber power and dominance, knowledge and sophisticated capabilities. Cyberspace is already a war-fighting domain with many escalations to follow. Countries seek to reinforce their offensive capabilities with advanced technology and personnel as they are the key for retaliation. A defense against states, cyber criminals and terrorists and state-sponsored attackers.

Global governance, consequence management initiatives, cyber army for each nation, resilience strategies and 'traffic management' programs are some innovative policies for the transition of traditional national power to cyber one. Malwares in the future may designed not only for specific networks, but for various electronic systems without being exposed. Cyberspace has no boundaries. "In many ways, it feels as though we are in a situation similar to that which existed prior to World War I: no government desires war, but the structural conditions of the situation lead to it regardless" (Ronald J. Deibert, "Bounding Cyber Power: Escalation and Restraint in Global Cyberspace", Internet Governance Papers, Paper No. 6, October 2013, p. 7).

PART D

The scenario of a possible electronic Pearl Harbor

In 1941 a military attack, known as the Battle of Pearl Harbor, by the Japanese Navy against U.S. surprised the American army and destroyed their base in the Pacific. Outstanding was that the Japanese military attack destroyed the U.S. Battleship Force in less than two hours ensuring that the Americans will not interfere with retaliation plans. From 1990, it is widely discussed the scenario of 'electronic Pearl Harbor' or 'Cyber Pearl Harbor', that a similar attack would emerge in cyberspace. It is an electronic Pearl Harbor because cables, and not simply cyber, applications and programs provide or connect devices, people and networks to the internet, to the wider meaning of internet, cyberspace. "Cyberspace is highly interconnected, not just within itself, but with other systems on which it depends, or which depend on it" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p.18). Due to this interconnectivity, policy makers and analysts assume that a cyber-attack would paralyze and shock nations.

National infrastructures, banks, financial sector, private companies and many more are vivid examples of organisations and sectors that are connected to the internet and have adapted to IT services. Globalization has affected governmental infrastructures as well who have adapted the technological evolution. The international community cooperates with global networks and not only national ones. All countries use same systems maybe with a few differences. Sensitive data and classified information are stored online, causing much trouble to governments and their security strategies.

"Storage of sensitive information on networks has given birth to cyber espionage against governments and cyber economic warfare against businesses" (Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary

Assessments, 2012, p. 8). Cyber espionage and sabotage will be a common phenomenon for the states. Exploitation of computer networks provide to hostile actors essential information for their attacks and the destabilization of the enemy. Cyber espionage is a type of silent war that will benefit the attacker in combination with the system's vulnerabilities and will have huge impacts on the victims. Silent battles in cyberspace will multiply every day and increase the risks that states will face.

Global governance is a new concept for states, for the securitization of cyberspace and the fight against cyber terrorism. The absence of legal framework causes severe problems to the international community, and to the private companies also. Not only governmental infrastructures are at high-risk but private companies as well who cooperate with governments and manage national data, websites.

"Senior leaders in the United States and abroad have expressed concern that the risks of a cyber 'Pearl Harbor' are growing. Some even have likened cyber weapons' potential to inflict damage to that of nuclear weapons" (Andrew F. Krepinevich, "Cyber Warfare: A 'Nuclear Option'?", Center for Strategic and Budgetary Assessments, 2012, p. 8). The military escalation of cyberspace and the digital arsenal depicts the dangerous possibilities for states and the looming cyber terrorist attacks. The concept of electronic Pearl Harbor is attacks at important national infrastructures and the spread of it in domains of a nation or even multiple nations. Are states willing to ignore such threat? Maybe it is not even possible to become reality, but who can risk putting in danger a nation or the whole international community? Many researchers assume that the electronic Pearl Harbor attack will come at the grid if financial sector. It will be a coordinated intrusion attack at IT infrastructures and related services, it will be only a threat for the financial and grid sector. The metaphor with the surprise military attack by

the Japanese Navy against U.S. in December 1941 tries to emphasize the significance of this historical event and how it had affected the Americans then and after the war. Was or not a devastating attack for the American army? It destroyed the American base and Japan won the Battle of Pearl Harbor. Nevertheless, the U.S. had not large scale damage and could recover from this attack. The metaphor in cyberspace attempts to signify the cyber weapon arsenal and how catastrophic can be an electronic attack. The audience of the cyber era is much wider than before. Cyber-attacks work silently into the networks, there are not momentary attacks but permanent ones and longer-lasting.

The number of online devices is increasing and cyber-attacks may be launched by such devices. Internet of Things, Artificial Intelligence, digital governance are a few examples of the evolution of societies and at the same time they have become vulnerabilities that will give terrorists opportunities to control, destabilize or paralyze a nation. The scenario of electronic Pearl Harbor should be studied and analyzed thoroughly by policy makers, IT experts, and many more. It is a scenario of national emergency level. The victim country will discover after a long time the intrusion with huge impacts on national security. No major attacks happened yet but the concept of deterrence and the concept of national security should include such far-fetched scenarios and be adaptive constantly to new technological evolutions and cyber threats.

There are no rules in cyberspace and no barriers for cyber terrorists, and even for small actors who have the capacity to cause cyber-attacks with large scale effectiveness. Multiple local failures will lead to global failures. This is the structure of electronic Pearl Harbor. Through the interconnectivity of devices and services, an intrusion into a less important network will spread in a national and international level threating security and stability. The increasing coupling of politics, economy, society and military with internet

has created in cyberspace a character of aggressiveness for cyber power and control over internet. The metastasis of cyber terrorism can be much easier than before, malware can travel from one country to another, from one continent to another leaving behind enormous damages.

The loss of IT services can affect government and business infrastructures, dismantling a nation's power. Cyber-attacks can paralyze physical destruction and shock the nation. Cyberwarfare is a war for anyone who can play smart and is quick-thinker. As Leon Panetta claims the information in computers is more important than surveilling emails. The 2007 cyber-attack in Estonia was a small example of what cyber terrorists can do, or countries as payback attacks. As airpower secured the domain with multiple methods, so must cyber power do.

A sudden cyber-attack targeting water supply, electrical grid will cause chaos in a government and spread panic. Cyber terrorists will have the ability to take down natural infrastructures and demand or threat more power, more control. As many countries use similar networks or share experience and knowledge, could be easily targets for extremists who seek power. The Dark Web hides many secrets and many terrorist actors who have such targets. Countries should cooperate and build retaliation methods for such threats. It is important to deter the offender to attack again.

An electronic Pearl Harbor could escalate from a national to international level. If a nation cannot protect its water (water contamination: Saudi Aramco), electrical grid or financial sector, then society will be easily in the hands of terrorist actors. Through the phrase of electronic Pearl Harbor someone can understand the significance of cyber era and how many vulnerabilities countries should fight. Governments are still not ready to deter a crash in national infrastructures and prevent this threat to escalate from hysteria to

full scale paralysis. More technological advances will come and many more sophisticated cyber-attacks will rise. The dependence on IT devices and services is yet rising but in the upcoming years, it will grow more. Smart Cities, Artificial Intelligence and IoT have made clear their presence, but the adaption in the everyday life and the solution of technologic problems that they have need more time and research. A scenario of an electronic Pearl Harbor is more than possible and capable of causing huge and severe damages nationally and internationally and with permanent effects. Many experts have been speaking for this scenario twenty years now, and still it has not happened. The dependence on smart devices is still on early stage. Cyber terrorists will motivate themselves if this dependence continue to grow, making states vulnerable to cyber-attacks. Electronic Pearl Harbor will take advantage of the systems' vulnerabilities, creating physical destruction and the virality of the new causing hysteria and panic. Experts and policy makers should have in mind a wider meaning and action of electronic Pearl Harbor, that can affect less important targets and continue the metastasis in more crucial domains, taking control of systems and domains. The militarization of cyberspace will continue to escalate and threaten with various cyber tools the stability and security. Governments should prevent this escalation or plan an adaptive deterrence strategy to recover from such attack in shorter time and with less damage, limit the attack and secure the nation.

Domino Effect

"With growing reliance on the internet, the volume of the shocks will likewise multiply" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p. 7). The use of similar devices and networks, globalization and interconnectivity have brought people closely in many ways. Incidents, problems or other events will influence the international community in unusual ways for each country in brief time. Cybersecurity Domino effect is when an event sets off a chain of similar events in cyberspace. This chain action is much easier in cyberspace as networks are connected with each other and a cyber-attack in a private company or another domain will have an effect on other domains too causing chain action problems. Many researchers point out the threat of a cyber-attack causing considerable damage at the national economy, having an impact at the larger economy.

"A number of shocks could cascade completely out of control, or multiple shocks might cascade and reinforce one another. Sometimes the initial incident is catastrophe enough, other times this sparks a cascading failure, or else the problem might be insidious and not obvious until it has quietly become a crisis" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p. 23). The hyper connectivity of cyber era creates interdependent networks and commitment to the internet. The monoculture of cyberspace hides many dangers for the governments, silent threats that will have major consequences at all national and international domains.

The models of cyber-attacks are constantly changing and states must adapt their security strategies in accordance with these alterations. IT experts, analysts and many more should cooperate closely for defending against such attacks and design a coherent plan of resilience and retaliation. However, the information warfare is a type of silent war

meaning that the intrusion will not leave traces or will not be visible to the experts despite the networks' updates. Networks will continue to have vulnerabilities as they become more sophisticated.

"A significant chain of disruptions to an interconnected system that only a few, if any, fully understand, could bring it all crashing down" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p. 9). A coordinated sophisticated attack will not be eliminated in a network or a domain, but it will spread national and international disruption. The escalation of a threat is easier to become than ever before. "The potential for human tragedy is enormous, and it is likely to increase with our growing dependence on computer-controlled systems to sustain our daily lives" (Nils Melzer, "Cyber Operations and jus in bello", Disarmament Forum 2011, no 4, p. 20).

The scenario of an electronic Pearl Harbor is more possible with the interconnections and the commitment to cyberspace. Ramifications of similar attacks are about to come with national significance. Critical sectors of nations are in danger and can be affected as the hostile actors are multiplying. It is crucial for each government to expand its multi-national corporations and influence, securing with this way national data. Political collaborations will provide to countries experience, knowledge and expertise over cyberspace, building a stronger wall against cyber threats. The risk of electronic Pearl Harbor will not disappear but the effects it may have, they can be restricted. The possibility of widespread disruption depicts that domino effect can threaten cyber security and that intelligence has gained more importance in cyber era.

Evaluation of Electronic Pearl Harbor

Leon Panetta was the first who pointed out the risk of a 'cyber Pearl Harbor' almost twenty years ago, and how catastrophic could be not only for the USA but for the entire globe. Yet, there is not any government that has faced such an attack. It is very difficult to understand cyberspace and the ramifications that has. Coordinated and sophisticated cyber-attacks will have a much wider set of targets that are crucial to states. The interactions across the borders will be more frequent and vivid. A new global order has already begun threating the national security and sovereignty.

"Failures may start as cyber shocks but will be quickly transmitted to the physical world and become 'shocks' without the 'cyber' modifier" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p. 18). The coupling of all levels of a state with other countries depicts the changes that globalization and internet have brought. The battles in cyberspace will be for smart and adaptive players. An electronic Pearl Harbor is not far from reality. Leaders will be able to secure their state with adaptive and evolutional strategies, equipped with personnel and cyber weapons. Deterrence is a matter of perspective and preparation against a sophisticated cyber-attack that can disrupt and destabilize a nation. "With so much complexity (and for the other reasons explained here) cyberspace might face such a phase transition, initiated by a single sudden shock analogous to the failure of Lehman Brothers" (Atlantic Council, "Risk Nexus, beyond data breaches: global interconnections of cyber risk", April 2014, p. 17).

If an electronic Pearl Harbor attack occur in one country, it will metastasize in all states simultaneously of after a while. The consequences will be fatal to all international community as global shocks need global response. The problem is that nations should

realize that the importance of an electronic Pearl Harbor is not that it can paralyze only one domain or national critical infrastructure, but everyone and everything that is interconnected. The offender will not be found and the malware will continue to spread globally. Cyberspace and information warfare benefits offense and this is the reason that nations should cooperate, to resist against a common enemy – ghost.

Internet has connected real life with cyberspace and governments should raise awareness to the civilians for the dangers that cyber threats hiding. Local failures may cause widespread shocks. The thousand loosely electronic mechanisms allow cyber terrorists to spread panic and destabilize nations due to the absence of a global governance, a global control. The emerging information society faces crucial risks capable of destabilizing in a few minutes systems and countries. States such as the USA, Russia, China and Israel who have power plants, federal generators, energy and power companies that cooperate with sophisticated system networks are high at risk. “To assess the potential threat of cyberterrorism, experts such as Denning suggest that two questions be asked: Are there targets that are vulnerable to cyberattacks? And are there actors with the capability and motivation to carry out such attacks?” (Gabriel Weinmann, “Cyberterrorism: The Sum of All Fears?”, Studies in Conflict & Terrorism, Routledge, Taylor & Francis Group, 2005, p. 16). For the future generation of cyber terrorists, it will be easier to take control of federal systems, spread fear and gain power. They are already making wide use of internet exploring all the potentials it can offer. The invisible threat of electronic Pearl Harbor has become a potential danger in the cyber era where information and internet rule all layers of structure.

CONCLUSION

In a world where everything and everyone is interconnected, it is impossible to avoid evolution in all aspects of life. Cyberspace has grown significantly and has taken a crucial role to the structure of governments given ability to state and non-state actors to interact. Equal resources have been given to those actors to start or join a Cyber Warfare. Hard power has given space to soft power evolving into cyber power. Globalization and cyberspace have brought the world closely creating a status of monoculture and interdependence on internet and social media. From this game, cyber terrorism cannot be excluded. Cyber policies against this threat are beginning to develop but more are needed to deter the escalation and the prevention of terrorists from spreading chaos.

In a new digital age, the meaning of state sovereignty and national power has taken a different meaning. Virtual reality, megacities, urbanization and IoT are a few examples of the technological evolution that states should be adapted to. The traditional meaning of government and national borders will be shaped according to the evolution of internet and cyberspace. Even if this new framework in international community includes new actors, new threats and new possibilities, state remains the dominant actor. As cyberspace cannot be disarmed, governments should follow the cyber revolution and adapt to the latest technological advances. IoT or Surveillance methods for defense purposes may become the Achilles heel of a state. Soon, cyber shocks will multiply and destabilize the function of countries in a national and international level with terrible consequences that may not be visible in the actual time.

In cyber security, political leadership is an outstanding characteristic for the design and implementation of offense and defense measures. Future smart cities will continue to have more security vulnerabilities than now as threats are easier to spread in a more connected environment. Cyber security is a game of strategy, a game where the cleverest

actor will win the battle. Considerable damage could be done with a click of a button in vital infrastructures. This information warfare demands abilities of crisis management and political decision makers that can be adapted in every situation. Manipulation of the opponent is a traditional characteristic of policy actors based on psychology.

Cyberspace can be approached with the help of social sciences to discover how effective can be into the real world. Collaboration with private sector will reinforce city's security capabilities and design a whole different approach for cyber security, innovative ideas and coherent strategies. Private companies will help governments to isolate cyber-attacks into a 'dead zone network' and study their structure. Mutual trust between countries and private companies is obligatory for a coherent cyber strategy. Cyber weapons arsenal has already begun and each country tries to strengthen its capabilities with a cyber army by recruiting cyber hackers seeking cyber dominance. Cyber defense is hard to implement into cyberspace.

The digitalization of war has benefited asymmetrical threats and escalation of intelligence proxy wars. Hybrid Warfare is a new type of war using irregular and conventional methods escalating security crises in the international system. Because of the information warfare, this term tries to describe the evolution in military affairs and how hybrid warfare operations are likely to be exercised. The traditional theoretical approaches of war have taken a different shape (political, strategic, operational, tactical), though the international community cannot define specifically this term. A new military approach will consist of high tech capabilities and soft power skills. Cyber armies are shaped to defend national infrastructures and protect democracy, armies consisted of hackers, IT experts and policy makers. Conflicts internationally will evolve into cyber proxy wars targeting vital infrastructures and networks. Cyber warriors against threats

will consist of senior military analysts, policy makers and junior academics or experts simply because they have grown in a technological society, experiencing the capabilities of internet and global communication. Multicultural cyber armies will be able to analyze, combine and develop revolutionary counter measure policies by also decoding terrorists' communication.

The hidden nature of cyber-attacks benefits the offender and especially in the case of cyberspace, cyber terrorists. With the rise of cyber criminals and cyber terrorists, non-states actors have strengthened and obtained threatening capabilities for nations. Internet is a tool that promotes fear, chaos and extremist ideas, and can break civilian's morale. "It's a valuable tool for them", Freese told NewsFactor, "so they don't want to disrupt the flow of the Web; rather, they target specific companies that are working with or are sympathetic to their enemies" (Steve Saint-Claire, "Overview and Analysis on Cyber Terrorism", 2011, p. 11). The virality of social media offers to cyber terrorists many opportunities to spread their ideas, recruit new members and threaten with live terrorist attacks (mass killing, paralyze of national networks, murder) policy actors. It is a matter of social revolution that policy makers should re-evaluate and realize the high importance of this transformation for the stability of nations. Traditional strategies will help develop and set new policies for cyber security and cyberspace in general.

Stuxnet, in 2010, was an example of malware that shocked the international community for its adaptivity and how it replicated itself. It was a customized digital weapon, working silently and designed especially for the nuclear program of Iran in Natanz, a highly-secured infrastructure. Its main purpose was to shut down the centrifuges and stop the enrichment procedure. Though it may have slowed the procedure, it failed to stop the Iranian program as the government restored the damaged centrifuges and

continued the initial plan of nuclear enrichment. The fact that the Stuxnet worm was specifically designed for the Iranian infrastructure, it is still a surprise for all governments. Many cyber terrorists can use this malware as a platform for future cyber-attacks or military espionage. The matter of attribution is still a weakness for the IT experts as well as states, complicating more the whole strategic analysis of Stuxnet. Such tactical cyber-attacks hide political motives for promoting multi-national cooperation. Iran, the USA and Israel have no formal diplomatic relations, and the Iranian enrichment procedure of uranium posed a threat for the American and Israeli governments. Many analysts claim that the Stuxnet attack came from Americans and Israelis as a tool to stop the threat in the Persian region. However, it is difficult to translate a cyber-attack into political motives.

In a virtual and interconnected world, cyber-attacks will become a frequent tool of foreign policy and gaining power in cyberspace. The evolution of malwares, smart cities, Artificial Intelligence and IoT constitute the future society. The power of internet and the possibilities that has, threaten the stability and the neutrality of international community. Many scenarios have been discussed upon academics and strategists, and most commonly the scenario of electronic Pearl Harbor. The rapid change of technology sets difficult for governments to prepare themselves for a massive cyber threat that could have an impact on all levels of state's structure with terrible consequences, making difficult for them to trace the attackers.

The attack on Pearl Harbor in 1941 was a historical trauma for the American navy and how effective was. The metaphor of this attack in cyberspace tries to draw attention for the possibilities of internet, the non-state actors and how cyber terrorists can benefit from exploring networks. The scenario of electronic Pearl Harbor emphasizes the effect of a surprise attack on critical networks and infrastructures, taken under the control of

terrorists. A live streaming electronic Pearl Harbor could have significant impact not only on nations' security and stability but also on the international society by spreading the fear of terror. This domino effect due to interconnected global networks empowers non-state armed groups to fulfil their goals.

Cyber terrorists are spread globally and interact with each other with encrypted messages. As they have grown in different countries, they have influenced by the culture and the way people think. In an information warfare, they use such information for their own advantage, for multiple and simultaneous attacks. Cyber terrorism is now global and with many hidden cores, they can approach targets that before were unassailable. Terrorism in contemporary society has been affected by the rapid change of technology and how important is information for states. The internet is the ideal tool for cyber terrorists to spread their ideas, wreak havoc and explore vulnerabilities in national critical infrastructures. Global terrorist networks can be more efficient than bombs. Physical destructions will not be eliminated due to cyber-attacks, but they will be multiplied and forwarded from a small country to a bigger one. Software holes offer to cyber terrorists innumerous possibilities to take the control of bank networks, transportation systems and water supply infrastructures. In an uprising information society, the actual and potential damage from cyber-attacks has not been yet explored.

Cyber blackmail, cyber ransom for sensitive information are a few examples of how cyberspace threats will evolve and what counter measures should be implied. Cyber security professionals should analyze and develop coherent counter measures against cyber terrorists, prevent network vulnerabilities and eliminate the danger of the cyber domino effect. "Changes in information have always had an important impact on power, but the cyber domain is both a new and a volatile manmade environment", "while leaving

governments the strongest actors, the cyber domain is likely to increase the diffusion of power to non-state actors, and illustrates the importance of networks as a key dimension of power in the 21st century" (Joseph Nye and Cyber Power, Belfer Center, May 2010, p. 19).

Bibliography

1. Brian Solis, “Social Media is About Social Science Not Technology”, March 14, 2012,http://www.briansolis.com/2012/03/social-media-is-about-social-science-not-technology/

2. Gabriel Weinmann, “Cyberterrorism, How Real is the Threat?” United States Institute of Peace, Special Report 119, December 2004.

3. Martin C. Libicki, “Cyberdeterrence and Cyberwar”, THE RAND, 2009.

4. Graig B. Greathouse, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” 2014.

5. Myriam Dunn Cavelty, “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities”, September 2014.

6. Atlantic Council, “Risk Nexus, beyond data breaches: global interconnections of cyber risk”, April 2014.

7. Nicholas Tsagourias, “Chapter 2: The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II – The Use of Force”, Yearbook of International Humanitarian Law/ Volume 15/ December 2012, pp 19 – 43.

8. Ronald J. Deibert, “Bounding Cyber Power: Escalation and Restraint in Global Cyberspace”, Internet Governance Papers, paper no.6 – October 2013.

9. John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters”, published online: 03 November 2014.

10. James A. Lewis, Simon Hansen, “China’s cyberpower, International and domestic priorities”, Australian Strategic Policy Institute, November 2014.

11. Tremayne Gibson, “2015 a Pivotal Year for China’s Cyber Armies”, The Diplomat December 17, 2015.

12. P. W. Singer, “How the United States Can Win the Cyberwar of the Future”, December 18, 2015.

13. Pardis Moslemzadeh Tehrani, Nazura Abdul Manap, Hossein Taji, “Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”, Computer Law & Security Review 29 (2013) 207-215.

14. T. Spyridopoulos, G. Karanikas, T. Tryfonas, G. Oikonomou, “A game theoretic defence framework against DoS/ DDoS cyber-attacks”, Computers & Security 38 (2013) 39–50.

15. The RAND Corporation, “Interdependence Day: Contending with a New Global Order”, August 21, 2015.

16. Lara Schmidt, “Perspective on 2015 DoD Cyber Strategy”, The RAND Corporation, September 29, 2015.

17. Benjamin Brake, “Strategic Risks of Ambiguity in Cyberspace”, Council on foreign Relations, Center for Preventive Action, May 2015.

18. Andrew Liaropoulos, “On Cyber-terrorism: Redefining Terror in Cyberspace, Politics and Public Administration Association, The University of Hong Kong.

19. James A. Lewis, “Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats”, Center for Strategic and International Studies, December 2002.

20. Catherine A. Theohary, Specialist in National Security Policy and Information Operations, John W. Rollins, Specialist in Terrorism and National Security, “Cyberwarfare and Cyberterrorism: In Brief”, Congressional Research Service March 27, 2015.

21. Andrea Manciulli (Italy), Rapporteur, “Terrorism and Surrounding Instability: The Dimensions of the Daesh Threat”, NATO Parliamentary Assembly, Mediterranean and Middle East Special Group Draft Report, October 2016.

22. Joelle GARRIAUD-MAYLAM (France), General Rapporteur, “Enhancing Euro-Atlantic Counter-Terrorism Capabilities and Cooperation”, NATO Parliamentary Assembly, Committee on the Civil Dimension of Security, 20 October 2016,

23. Philippe VITEL (France), General Rapporteur, “The Future of Allied Airborne Intelligence, Surveillance and Reconnaissance”, Draft General Report, NATO Parliamentary Assembly, Science and Technology Committee, 20 September 2016,

24. Martin C. Libicki, “Cyberdeterrence and Cyberwar”, Published 2009 by Rand Corporation, Project Air Force.

25. Robert Jervis, “Deterrence and Perception”, International Security, JSTOR, Vol. 7, No. 3. (Winter, 1982-1983), pp. 3-30.

26. James P. Farwell & Rafal Rohozinski, “Stuxnet and the Future of Cyber War”, 2011, http://dx.doi.org/10.1080/00396338.2011.555586.

27. Edited by Andrew Liaropoulos and George Tsihrintzis “Proceedings of the 13th European Conference on Cyber Warfare and Security”, The University of Piraeus, Greece, 3-4 July 2014.

28. Andrew Liaropoulos for ISN, “Cyberspace, Sovereignty and International Order”, 30 January 2014.

29. Andrew Liaropoulos, “Exercising State Sovereignty in Cyberspace: An Introduction Cyber-Order under Construction?”, Journal of Information Warfare, Volume 12, Issue 2, ISSN 1445 – 3347 (On Line Journal), July 2013.

30. Andrew Liaropoulos, “A Human-Centric Approach to Cybersecurity: Securing the Human in the Era of Cyberphobia”, Journal of Information Warfare, Volume 14, Issue 4, ISSN 1445-3347 (On Line Journal) Fall 2015.

31. Andrew Liaropoulos, “Power and Security in Cyberspace: Implications for the Westphalian State System”, PANORAMA of global security environment, Centre for European and North Atlantic Affairs (CENAA), Bratislava 2011.

32. Andrew Liaropoulos, “Exploring the Puzzle of Cyberspace Governance, Proceedings of the 15th European Conference on Cyber Warfare and Security, Bundeswehr University, Munich Germany, 7-8 July 2016.

33. Andrew Liaropoulos, “Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?”, Proceedings of the 8th International Conference on Information Warfare and Security, Regis University, Denver, Colorado, USA, 25-26 March 2013.

34. Andrew Liaropoulos, “Great Power Politics in Cyberspace: U.S. and China are drawing the lines between Confrontation and Cooperation”, PANORAMA of global security environment, Centre for European and Atlantic Affairs, Bratislava 2013.

35. Andrew Liaropoulos, “Reconceptualising Cyber Security” Safeguarding Human Rights in the Era of Cyber Surveillance, International Journal of Cyber Warfare and Terrorism, Volume 6, Issue 2, April-June 2016.

36. A Wikistrat Crowdsourced Simulation, “Crime, Terror, and the Internet of Things”, November 2016.

37. Andrew Liaropoulos, “Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi-stakeholderism, and Power Politics”, Journal of Information Warfare Volume 15, Issue 4, Fall 2016.

38. 1st Lt Robert M. Lee, USAF, “The Interim Years of Cyberspace”, Air & Space Power Journal, January–February 2013.

39. Graig B. Greathouse, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?”, 2014.

40. Martin R. Stytz, Sheila B. Banks, “Toward Attaining Cyber Dominance, Strategic Studies Quarterly; winter 2013, Vol. 7 Issue 4”, December 2013,

41. Myriam Dunn Cavelty, “Breaking the Cyber – Security Dilemma: Aligning Security Needs and Removing Vulnerabilities”, Received: 21 November 2013 / Accepted: 13 April 2014 Springer Science+Business Media Dordrecht 2014.

42. Vincent Joubert, “Five Years after Estonia’s cyber-attacks: lessons learned for NATO?” Research Division – NATO Defense College, Rome – No. 76 – May 2012.

43. Robert J. Butler, “Testimony before the House Foreign Affairs Committee Cyber War: Definitions, Deterrence, and Foreign Policy”, Center for a New American Security, September 30, 2015,

44. Jason Healey “Beyond data breaches: global interconnections of cyber risk”, Risk Nexus, Atlantic Council, April 2014.

45. Nils Melzer, “Cyber Operations and jus in bello”, Disarmament Forum 2011, no 4 (2011).

46. Tobias Feakin, “Enter the Cyber Dragon, Understanding Chinese intelligence agencies’ cyber capabilities”, Australian Strategic Policy Institute, June 2013 — Issue 50.

47. Mathew J. Burrows, “Global Risks 2035: The Search for a New Normal”, Foreword by Brent Scowcroft, Atlantic Council Strategy Papers, September 2016.

48. Jason Healey, Leendert von Bochoven, “NATO’s Cyber Capabilities: Yesterday, Today, and Tomorrow”, SMARTER ALLIANCE INITIATIVE, Atlantic Council, February 2012.

49. Les Bloom and John E. Savage, “On Cyber Peace”, Issue Brief, Atlantic Council, August 2011.

50. Jason Healey, “Pursuing Cyber Statecraft”, Atlantic Council, Cyber Statecraft Initiative, August 2011.

51. GAO, “Agencies Need to Improve Cyber Incident Response Practices”, United States Government Accountability Office, Information Security, April 2014.

52. Shmuel Even & David Siman-Tov, “Cyber Warfare: Concepts and Strategic Trends”, Memorandum No. 117, Tel Aviv: Institute for National Security Studies, May 2012.

53. Andrew Nagorski, “Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway”, EastWest Institute, 2010.

54. James A. Lewis, “Cyberspace and armed forces, The rationale for offensive cyber capabilities”, Australian Strategic Policy Institute, May 2016.

55. Irving Lachow, “Active Cyber Defense, A Framework for Policymakers”, Center for a New American Security, February 2013.

56. Security & Defense Agenda, “Where cyber-security is heading”, January 2013.

57. Andrew F. Krepinevich, “Cyber Warfare: A ‘Nuclear Option’?” Center for Strategic and Budgetary Assessments, 2012.

58. Michael Kassner “Gender Gap: Why Information security needs more women”, in IT Security, November 4, 2013.

59. John B. Sheldon, “Geopolitics and Cyber Power: Why Geography Still Matters”, Taylor & Francis Online, November 2014.

60. Nazli Chouchri, “Co – Evolution of Cyberspace and International Relations: New Challenges for the Social Sciences”, Prepared for World Social Science Forum (WSSF) 2013 Montreal, Canada.

61. Daniel Goldsmith, Michael Siegel, “Cyber Politics: Understanding the use of Social Media for Dissident Movements in a Integrated State Stability Framework”, IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (2012).

62. “Empirical Studies of Bottom – up Internet Governance”, Jesse H. Sowell, Mar 2012, SSRN Electronic Journal.

63. Gabriel Weinmann, “Cyberterrorism, How Real is the Threat?” UNITED STATES INSTITUTE OF PEACE, Special Report 119, December 2004.

64. ”, Rabiah Ahmad, Zahri Shahrin Sahib, Mariana Yusoff, “Perception on Cyber Terrorism: A Focus Group Discussion Approach Journal of Information Security, 2012, 3, 231-237).

65. Sarah Gordon, Senior Research Fellow Symantec Security Response, and Richard Ford, Ph.D. Independent Consultant, Symantec Security Response “Cyberterrorism?”.

66. Gabriel Weinmann, “Cyberterrorism: The Sum of All Fears?” Studies in Conflict & Terrorism, Routledge, Taylor & Francis Group, 2005.

67. Imrav Awan “Debating The Term Cyber-Terrorism: Issues and Problems”, Internet Journal of Criminology, ISSN 2045 6743 (online), 2014.

68. Wolff Heintschel in Heinegg, “Territorial Sovereignty and Neutrality in Cyberspace”, Volume 89, International Law Studies, US Naval War College, 2013.

69. Noel Cox, Auckland Uni. Of Technology, New Zealand, “The Regulation of Cyberspace and the Loss of National Sovereignty”, Article in Information & Communications Technology Law, August 2003.

70. David P. Fidler, “Introduction: The Internet and the Sovereign State: The Role and Impact on Cyberspace on National and Global Governance Symposium”, Indiana Journal of Global Legal Studies, spring 1998.

71. Pal Wrange, Professor of International Law, Stockholm University, Director, the Stockholm Center for International Law and Justice, “Intervention in national and private cyberspace and international law”, 2014.

72. Lieutenant Colonel Patrick W. Franzese, “Sovereignty in Cyberspace: Can it Exist?”, https://www.law.upenn.edu/live/files/3473-franzese-p-sovereignty-in-cyberspace-can-it-exist

73. Oren K. Upton, “Asserting National Sovereignty in Cyberspace: The case for Internet Border Inspection”, Monterey, California, Naval Postgraduate School, Thesis, June 2003.

74. Jackson Adams, Mohamad Albakajai, “Cyberspace: A New Threat to the Sovereignty of the State”, University of Essex, Colchester, UK, Volume 4, No. 6, 256 -265, Management Studies, Nov. – Dec. 2016.

75. James A. Lewis, Senior Fellow, “Sovereignty and the Role of Government in Cyberspace”, Center for Strategic and International Studies, Volume XVI, Issue II, Spring/ Summer 2010.

76. Eric Talbot Jensen, “Cyber Sovereignty: The Way Ahead”, Texas International Law Journal, Volume 50, Symposium Issue 2.

77. Kerstin Vignard, Editor in Chief, Ross McRae, Jason Powers, Editors, “Confronting cyberconflict”, disarmament forum, United Nations for Disarmament Research, 2011.

78. Jones, Ken M., “Cyber war: the next frontier for NATO”, California: Naval Postgraduate School, Calhoun: The NPS Institutional Archive, Monterey, 2015-03.

79. John E. Savage, Brown University, Bruce W. McConnell, EastWest Institute, “Exploring Multi-Stakeholder Internet Governance”, cybersummit 2014.

80. MADELINE CARR, “Public–private partnerships in national cyber-security strategies”,https://www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

81. Alexander Klimburg, “National Cyber Security, Framework Manual”, NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Tallinn 2012.

82. Malcolm N. Shaw, “International Law”, sixth edition, Cambridge University Press, 2008.

83. Article 2, paragraph 1 of the Charter of the United Nations states: "The Organization is based on the principle of the sovereign equality of all its Members."

84. Emilio Iasiello, “Cyber Attack: A Dull Tool to Shape Foreign Policy”, NATO CCD COE Publications, Tallinn, 2013.

85. European Commission, “Fourth progress report towards an effective and genuine Security Union”, COM (2017) 41 final, Brussels, 25.1.2017.

86. Stamatis Karnouskos, “Stuxnet Worm Impact on Industrial Cyber-Physical System Security”, SAP Research, Germany.

87. Pankaj Ghemawat, “Even in a Digital World, Globalization Is Not Inevitable”, Harvard Business Review, February 1, 2017.

88. Judith H. Germano, “Cybersecurity Partnerships: A New Era of Public-Private Collaboration”, The Center on Law and Security, October 2014.

89. European Parliamentary Research Service Blog, “Understanding Hybrid Threats”, June 24, 2015.

90. Michael Kofman and Matthew Rojansky, “A Closer look at Russia’s ‘Hybrid War”, Kennan Cable, No. 7, April 2015.

91. Julio MIRANDA CALHA (Portugal), “Hybrid Warfare: NATO’s New Strategic Challenge?”, Defence and Security Committee, General Rapporteur, 7 April 2015.

92. Bettina Renz and Hanna Smith, “Russia and Hybrid Warfare – Going Beyond the Label”, Aleksanteri Papers, 1/2016.

93. Maria Snegovaya, “Putin’s Information Warfare in Ukraine, Soviet Origins of Russia’s Hybrid Warfare”, Russia Report 1, Institute of the Study of War, September 2015.

94. Frank G. Hoffman, “Hybrid Warfare and Challenges”, issue 52, 1st quarter 2009 / JFQ.

95. Daniel Runde, “Soft Power and Security”, Global Forecast 2016.

96. Camino Kavanagh, Daniel Stauffacher, “The Reach of Soft Power in Responding to Cybersecurity Challenges”, ICT for Peace Foundation.

97. Steve Saint-Claire, “Overview and Analysis on Cyber Terrorism”, 2011.