Received: 5 March 2012 Accepted: 6 April 2012 Published online: 15 June 2012
Available from www.defenceandstrategy.eu doi: 10.3849/1802-7199.12.2012.01.053-062

Jak citovat tento článek / How to Cite this Article

VASILESCU, Cezar. Cyber Attacks : Emerging Threats to the 21st Century Critical Information Infrastructures. Obrana a strategie: Defence & Strategy. 2012, roč. 12, č. 1, s. 53-62. ISSN 1802-7199. DOI: 10.3849/1802-7199.12.2012.01.053-062. Dostupné z: http://www.defenceandstrategy.eu/

Kybernetické útoky: nové hrozby pro kritickou informační infrastrukturu ve 21. století

Cyber Attacks: Emerging Threats to the 21st Century Critical Information Infrastructures

Cezar Vasilescu

Abstrakt

Příspěvek zkoumá pojem kybernetického útoku jako konceptu pro pochopení moderních konfliktů. Začíná zpracováním koncepčního teoretického rámce a zjištěním, že pokud jde o kybernetické útoky, kybernetickou válku a kybernetickou obranu, neexistují žádné mezinárodně uznávané definice těchto pojmů, a to zejména z důvodu jejich relativní novosti. Druhá část analyzuje počítačovou realitu posledních let, s důrazem na kybernetické útoky nejvíce medializované prostřednictvím mezinárodních sdělovacích prostředků: Estonsko (2007) a Gruzie (2008), přičemž se soustředí na dvě hlavní poučení – jak složité je definovat kybernetickou válku a jak je těžké se proti ní bránit. Zásadní důsledky pro země světa a roli NATO v zajišťování efektivní kolektivní kybernetické obrany jsou analyzovány ve třetí části. Dále je zkoumána potřeba rozvoje strategických dokumentů kybernetické obrany (např. Politika kybernetické obrany NATO, Strategická koncepce NATO). Předložený návrh předpokládá, že bude věnována zvláštní pozornosti vývoji postupů pro jasné rozlišení událostí (kybernetických útoků, kybernetické války, počítačové kriminality a kyberterorismu) a pro provádění operací legitimní národní vojenské / civilní kybernetické obrany.

Abstract

The paper explores the notion of cyber attack as a concept for understanding modern conflicts. It starts by elaborating a conceptual theoretical framework, observing that when it comes to cyber attacks, cyber war and cyber defense there are no internationally accepted definitions on the subject, mostly because of the relative recency of the terms. The second part analyzes the cyber realities of recent years, emphasizing the most advertised cyber attacks in the international mass media: Estonia (2007) and Georgia (2008), with a focus on two main lessons learned: how complicated is to define a cyber war and how difficult to defend against it. Crucial implications for world's countries and the role of NATO in assuring an effective collective cyber defense are analyzed in the third part. The need for the development of strategic cyber defense documents (e.g. NATO Cyber Defense Policy, NATO Strategic Concept) is further examined. It is suggested that particular attention should be paid to the development of a procedure for clearly discriminating between events (cyber attacks, cyber war, cyber crime, or cyber terrorism), and to a procedure for the conduct of nation's legitimate military/civil cyber response operations.

Klíčová slova

Kybernetické útoky; kybernetická obrana; Politika kybernetické obrany NATO; informační bezpečnost

Keywords

Cyber attacks; Cyber defense; NATO Cyber Defense Policy; Information security

INTRODUCTION

In present times we are the witnesses of an unprecedented and continuous growing of nations' dependence on Internet and computer networks for performing activities necessary for smooth functioning of the society. The technological progress and the tendency to automate every aspect of our lives brought us not only freedom from manual and repetitive activities, significantly improving the citizens' quality of life, but also various security risks.

The history shows that conflicts are embedded in human nature. During the first ages of human existence the race for vital resources took the form of local fights between groups or tribes competing for land, resources or social status. Lately, during medieval times the battles expanded until they reached the magnitude of nation against nation or alliance against alliance. The territory where the wars were conducted varied from the size of a country to continental or even global battlefields.

Also the weapons were continuously improved, usually the research for military purposes being in the forefront of science and technology. As a consequence, most inventions were used also for destructive purposes and the Internet did not constitute an exception. Worldwide with an increasing percentage of each nation's people, services provided by computer assisted technologies or based on information infrastructures became a day by day life style: emails have mostly replaced paper based letters, mobile phones are a must for most teenagers and not only for them, interactions mediated by social networks like Facebook, Twitter or Google+ substitute and speed up normal human interactions, online shopping and online financial payments have become prevalent.

The race for new technologies, new usage of computers and new functions / features of existing high tech environment did not take into consideration the security related issues. Consequently, with functionality as a primary demand, security mechanisms were overlooked, neglected or not taken into account at all. Without having the security features built-in, the software used in computers (operating systems, browsers, utility programs) and the services/mechanisms that provide network connectivity (such as DNS, software based firewalls) are vulnerable to cyber attacks and thus require a constant surveillance of network/security administrators and almost daily updates provided by commercial software companies.

But what is a cyber attack? Who are the actors involved in the process and what impact might it have? The answer to those questions will be provided in the following paragraphs.

THEORETICAL FRAMEWORK

Computer based attacks were executed during last decades at lower scales and with a lesser degree of magnitude. The concern for security in general (and for computer security in particular) had a great importance for both military and civilian specialists. In 2011, NATO Standardization Agency defined the term computer network attack as 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*" and remarked that *"a computer network attack is a type of cyber attack."*[1]

Such definition put forward well known and agreed elements of hostile computer based activities against localized/limited information infrastructures. When it comes to cyber attacks, cyber defense and cyber security there are no internationally accepted definitions on the subject, mostly because of the

[1] *NATO Glossary of Terms and Definitions of military significance for use in NATO*. Allied Administrative Publication AAP-6 (2011), NATO Standardization Agency, March 22, 2010. Available from http://nsa.nato.int/nsa/zpublic/_branchinfo/terminology_public/non-classified%20nato%20glossaries/aap-6%282011%29.pdf

recency of such terms. In the last decade cyberspace (admirably defined by Ottis and Lorents as "*a time-dependent set of interconnected information systems and the human users that interact with these systems*"[2]) became a more dangerous place, due to the fact that states rely on systems based on computer networks for communication, economic/financial transfers and information storage. The sum of those "*interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy*"[3] represents critical information infrastructures. Starting from this definition, that is to say, targeting a nation's critical information infrastructure (CII) in the 21st century is an act of war.

The absolute distinction between words such as cyber attacks, cyber war and cyber crime is not yet accomplished. What one nation considers a cyber attack might appear more like a cyber war to another or even a simple cyber crime to a third one[4], simply because cyber threats have different forms and can originate from individuals, governments or even nonstate actors, such as terrorist organizations. The author of the book named "Law of Cyber Space"[5] partially clarifies the terms. He incrementally defines:

- cyber attack as a "*computer network related mischief, such as defacing websites or releasing a virus or a worm, without necessarily causing any serious disruption or widespread panic or terror for the general population*";
- cyber warfare as "*the deliberate use of information warfare by a state, using weapons such as electro-magnetic pulse waves, viruses, worms, Trojan horses, etc., which target the electronic devices and networks of any enemy state*"; and
- cyber terrorism as "*attacks and threats of attack against computers, networks, and the information stored therein, with the objective of intimidating or coercing a government or its people in furtherance of political or social objectives*".

We can see that the definitions can be discriminated only by using the classification of the conspirator (state or nonstate) as differentiation criterion.

The second definition states that cyber attacks "*incorporated the potential to degrade national economic systems and communications networks as a means of breaking the enemy's will to resist and inflicting military and political defeat, at low cost and without the need to occupy territory, achieving disruption without destruction.*"[6]

Even if the definitions add a certain rigor to this new uncharted domain, it generates some new strategic issues to be solved by the information security analysts, such as:

- Identification. Because the battlefield is the cyberspace, the ways to pinpoint the enemy and to certainly identify the attacker are quite ambiguous. If a certain number of computers from a certain country were participating in a cyber attack, can we definitely prove that the government of that country is the attacker? Or can we assume that the government is responsible for the cyber attacks

[2] OTTIS R., LORENTS P. *Cyberspace: Definition and Implications*. The 5th International Conference on Information-Warfare & Security, Air Force Institute of Technology, Ohio, USA, 8-9 April 2010, pp. 267-271. Available from http://www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf

[3] *Glossary of Terms*. European Network and information Security Agency (ENISA). Available from www.enisa.europa.eu/act/res/files/glossary

[4] PEEGLISSE Pilk. *Estonia and NATO Article Five, Glance at the Mirror*. Estonian Ministry of Foreign Affairs, 2008, p. 47. Available from http://web-static.vm.ee/static/failid/238/NATO_art5.pdf

[5] KAMAL A. *The Law of Cyber-Space*. United Nations Institute for Training and Research, New York, 2005, p. 81. Available from www.un.int/kamal/thelawofcyberspace/The%20Law%20of%20Cyber-Space.pdf

[6] JOYNAL, P. M. *The Brave New World of the 5 Day War: Russia-Georgia Cyberwar, Where Cyber and Military Might combine for War Fighting Advantage*. Available from www.nationalstrategies.com

launched by malicious users? Under conventional conflicts, the enemy's identification was relatively easy, but in cyber world a precise identification is hard to get.

- Distrust. In cyber based environments we can "trust" the content of the databases and computer systems' integrity until a certain point. Evolving capacities of viruses, Trojan horses and malware to spoof and deceive the most effective antivirus and firewall systems made the verification of information security highly uncertain. Moreover, in 2008 the MD5 encryption algorithm (used by all Internet web browsers) was compromised[7], which allows the forging of certificates trusted by web browsers. This security breach provides a way for attackers to conduct phishing attacks that are virtually undetectable. Once you got a false Certification Authority (CA) certificate, this will be accepted as valid and trusted by browsers that will display phishing web sites as "secure" and the connection as "https".
- Symmetry. The broad definition of an asymmetric warfare states that a weaker party is applying unconventional attack methods against stronger (in terms of military capabilities) but more vulnerable forces. The reality tells us that the asymmetry concept is unlikely to be applied in cyber attacks. Hackers attacked countries like Estonia and Georgia (cyber strong against cyber weak), Arab Sunni and Iranian Shiite hackers or Indian and Pakistani patriotic hackers carry on hostile cyber attacks against each other (cyber weak against cyber weak). Moreover, as the chairman of the White House Homeland Security subcommittee on emerging threats and cyber security stated in 2008, we will "*Never see again major warfare without a strong cyber component executed as part of it.*"[8]
- Deterrence. From the Latin author Publius Flavius Vegetius Renatus remained the immortal phrase "*Si vis pacem, para bellum*", translated in English as "*If you want peace you should prepare for war.*"[9] In other words a well-equipped and strong nation is less likely to be attacked by adversaries - this is the essence of the deterrence models developed during the Cold War. In cyber related domains, the old core U.S. Cyber Policy (2003) "deterrence by denial" failed to measurably affect the motivations and discourage the actions of cyber attackers.[10] The new US Cyberspace Policy Review and also the Cyber Security Strategy for Germany shift the focus from passive, defensive and post factum cyber defense actions to global awareness and a much more preemptive approach.

In case of conventional wars, the victim state has the right to self-defense with conventional military means. But what actions a nation should take in case of a cyber attack (other than cyber defensive)? Should conventional weapons be involved, against whom and in what progression? In traditional conflicts until now, the military strategy takes into consideration the following escalation rule generally accepted by all players: to respond against an attack with equivalent means (conventional to conventional, nuclear to nuclear, chemical weapon against chemical weapon) or to produce a similar / equivalent damage. In case of cyber attacks or cyber warfare it is difficult to quantify the damages and respond in accordance with the aforementioned rule.

In order to prepare the right means to successfully react in case of a cyber aggression, clear definitions and understanding of terms is needed, especially to avoid possible escalation of cyber conflicts to conventional warfare.

[7] NARAINE R. *SSL Broken! Hackers Create Rogue CA Certificate Using MD5 Collisions*. ZDNet News, December 30, 2008. Available from http://blogs.zdnet.com/security/?p=2339

[8] LANGEVIN, J. *U.S. Urged to Go on Offense in Cyberwar*. Washington Times, September 29, 2008. Available from www.washingtontimes.com/news/2008/sep/29/us-urged-to-go-on-offense-in-cyberwar

[9] CLARKE J. *The Military Institutions of the Romans (De Re Militari)*, translation from Latin, Publius Flavius Vegetius Renatus. Digital Attic 2.0. Available from http://www.pvv.ntnu.no/~madsb/home/war/vegetius/

[10] *The National Strategy to Secure Cyberspace*. Department of Homeland Security, Washington, DC, 2003. Available from http://www.dhs.gov/files/publications/editorial_0329.shtm

REALITIES

Once we discuss the theory implied by the cyber-related domain, it is time to see what the real world prepares for us. In the recent years' literature (ranging from scientific articles to press releases) the number of topics containing the word "cyber" was constantly growing, denoting the interest of the subject for authors and the worldwide public.

There were two major cyber attacks that galvanized the information security community, politicians and military analysts: the cyber attacks against Estonia (April 2007) and Georgia (2008). Because both attacks were relatively close in time and successful, it emphasizes the unsatisfactory level of preparedness when it comes to cyber defense measures.

Chronologically, those attacks did not indicate the start of the cyber war age, simply because they were not the first cases. Other states possessed cyber capabilities and have been vaguely accused of launching similar attacks. China is the state presumably to be one of the most active and most interested in such things, along with Israel, India, Pakistan and the United States. Attacks emanating from China have been targeting the computer systems of the Pentagon as well as major European government agencies.

Some specialists in information security suggest that China will not limit itself to the attempt to compete with other states in terms of military expenditures to create strong military capabilities that could be used for propaganda purposes. It would be much easier to "*wage war directly against the American population by attacking its digital and physical infrastructure, its confidence and morale?*"[11]

The running order of Estonia's critical information infrastructures was threatened and hence Estonia's national security was jeopardized in 2007 when almost the entire electronic infrastructure was blocked by a Distributed Denial of Service (DDOS) type of attack. Even if the intent of such an attack is not to damage CII, having in mind that for an attack to be successful it only has to cause disruption to a significant number of citizens, the state's security and credibility were severely affected.

The situation was aggravated by the heavy reliance of Estonia (or "E-stonia" as the country was nicked) on information technology and network communications. All the Estonian IT security specialists could do was to try to block the outside connections to country's servers, waiting for the cyber attacks to come to a standstill. Personal relations among worldwide Internet Service Providers of three world-renowned IT specialists that happened to be at the right place at the right time (in Estonia) helped on the cyber defense measures of blocking Internet Protocol (IP) addresses that were sending harmful traffic to Estonia's international connections.[12]

The Estonian case was the most advertised by the international mass media because it was the first cyber attack against an entire country's information infrastructure that pointed out the inappropriate level of international laws regarding such situations. The identification of the cyber attacker is mostly vague and because the attack was distributed (based on millions of compromised computers from multiple geographical locations - a botnet army), it is hard to blame a certain state of being behind the aggression.

In Estonia's case a student was found guilty and fined with around 1000 USD for posting downloadable root-kits on public websites with instructions on how to join in the cyber attack. The same technique was used one year later in Georgia's case, during the short Georgian-Russian conflict. A commentary of an Internet journalist investigating the issue is suggestive for this unspecific type of attacks: "*All I needed to do was to save a copy of a certain web page to my hard drive and ... voilà: my*

[11] PETERS, R. *The Counterrevolution in Military Affairs - Fashionable thinking about defense ignores the great threats of our time*. The Weekly Standard, July 2, 2006, volume 011, issue 20, p. 3. Available from http://www.weeklystandard.com/Content/Public/Articles/000/000/006/649qrsob.asp?page=1

[12] LAASME, H. *Estonia: Cyber Window into the Future of NATO*. Joint Force Quarterly, issue 63, 4th quarter 2011

browser was now sending thousands of queries to the most important Georgian sites, helping to overload them. In less than an hour, I had become an Internet soldier."[13]

One of the main lessons learned from cyber attacks against Georgia and Estonia was that it is complicated to define a cyber war and it is extremely difficult to defend against it. In Georgia it was a cyber attack (that precedes the conventional ground attack) targeting military communication system to create confusion among Georgian troops, disrupt their plans, cut their communications, and throw them off balance.[14]

Another example of cyber attack was the December 2008 terrorist attack in Mumbai, India. The strike underlined the creativity of attack teams to assemble an integrate command and control capability using cable television, BlackBerry phones, Google Earth imagery, and global positioning system information to achieve a "low-cost information superiority". Incidents such as Mumbai demonstrate that nonstate actors "*do not fear network-centric warfare because they have already mastered it.*"[15]

THE ROLE OF NATO IN ASSURING AN EFFECTIVE COLLECTIVE CYBER DEFENSE

Since its creation, the North Atlantic alliance has pursued the goal of protecting its communications and information systems against unauthorized access and information based attacks. Nonetheless, until 2007 when the Estonian cyber attack occurred, NATO had mainly concentrated on traditional aspects of information security such as the confidentiality, integrity and availability of the main operational information systems. Suddenly, because an ally was under attack and somebody should offer assistance, the Alliance realized that it also should assist its members in protecting theirs critical information infrastructures. As a result NATO changed its common security trajectory by extending the development of cyber defense capabilities also to its individual Allies.[16]

In the drafting phases of the new NATO Strategic Concept, a group of experts chaired by Madeleine Albright recommended that: "*NATO must accelerate efforts to respond to the danger of cyber attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defense capabilities aimed at effective detection and deterrence.*"[17]

Estonia had a great role in defining cyber attacks in official NATO documents as significant threats to global security and also underlined the inadequacy of the current cyberspace concepts for defending NATO. The technology advances faster than global policies and laws, usually being an approximately one decade lag between them. That determines the impossibility to apply technologically feasible means to secure the cyber domain because of the limitation determined by policies.

In the analyzed case, NATO as a military alliance could not intervene due to the fact that Estonia (NATO member since 2004) could not invoke Article 5 of the treaty:

- There was no identifiable enemy to retaliate against;
- The war had a different dimension (virtual cyber war); and
- Cyber attacks were not considered (at that time) among cases when the collective self-defense principle is automatically activated.

[13] MOROZOV, E. *An Army of Ones and Zeroes - How I became a soldier in the Georgia- Russia Cyberwar.* Slate.com, August 14, 2008. Available from www.slate.com/id/2197514

[14] MILLER, R. A. and KUEHL D. T. *Cyberspace and the "First Battle" in 21st-century War.* Defense Horizons, no. 68, Center for Technology and National Security Policy, National Defense University, September 2009

[15] PETERS, ref. 11, p. 1.

[16] NATO, *Defending Against Cyber Attacks: How Did the Policy Evolve?* January 29, 2009. Available from www.nato.int/issues/cyber_defence/index.html

[17] *NATO 2020: Assured Security; Dynamic Engagement.* Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO, 17 May, 2010. Available from http://www.nato.int/cps/en/natolive/official_texts_63654.htm

To address the issue, in 2008 the NATO Cyber Defense Policy was ratified and a Cyber Defense Management Authority was created, bringing together key actors in NATO's Cyber-Defense activities. Its aim is to manage and support all NATO communication and information networked systems and individually allies upon request. NATO finally realized that some form of common strategy had to be developed for defending the electronic infrastructures of its member states.

In May 2008 the **NATO's Cooperative Cyber Defense Centre of Excellence (NATO CCD** COE) was established in Tallin, Estonia. The creation of CCD COE had the aim to enhance the Allies' capabilities and interoperability in cyber defense by emphasizing doctrine and concept development, awareness and training, research and development, analysis and lessons learned, and consultations. Currently there are ten sponsoring nations participating in the activities of this international military organization: Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Slovakia, Spain, Poland, and the U.S.A. (joined in 2011), and the Netherlands (joined in 2012).

Since 2008, CCD COE organized several cyber defense conferences and training courses on information security. The focus was on both legislative / theoretical aspects and practical ones. For example, at 2009's conference the following topics were discussed: 1) an analysis on GhostNet (China's intelligence collection network), which presumably infiltrated high-level computers in more than 100 countries; 2) measuring techniques of distributed denial-of-service attacks; 3) the concept of borders in cyberspace; and 4) botnet countermeasures.

Also, CCD COE organized an annual Cyber Defense Exercise in which "players" have to deal with various fictive geo-political computer crisis scenarios that could happen in a real world (a threat to the energy sector, viruses and general malicious codes, etc.). The need for training in this domain was emphasized once more by the 2011 participation involving 23 NATO nations and six partners (e.g. New Zealand and Australia).

In 2010, the NATO Strategic Concept[18] finally included cyber attacks as a significant threat to Euro-Atlantic security, that might require consultations under Article 4 ("*The parties will consult together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened*"[19]) and even collective defense measures under Article 5, if necessary.

A revised NATO Policy on Cyber Defense was approved in 2011. It is the overarching policy that sets out:

- A clear vision for cyber defense initiatives throughout NATO;
- The framework for how NATO will assist its Allies in their own cyber defense efforts and clarifies political and operational mechanisms of NATO's response to cyber attacks;
- The principles of NATO's cyber defense cooperation with partner countries, international organizations, private sector and academia; and
- Integration of the cyber defense into NATO's Defense Planning Process (NDPP).

The Policy offers a coordinated approach to cyber defense, focusing on preventing cyber attacks, building resilience capabilities, and its aim is to optimize information sharing and situational awareness, collaboration and secure interoperability based on NATO agreed standards.[20] To ensure the policy's timely and effective implementation an Action Plan was also adopted.

[18] *NATO New Strategic Concept: Active Engagement, Modern Defence*, November 19, 2010, p. 4. Available from www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

[19] *The North Atlantic Treaty*. NATO Basic Texts, NATO on-line library. Washington D.C., 4 April 1949. Available from http://www.au.af.mil/au/awc/awcgate/kosovoaa/northatlantictreaty/treaty.htm

[20] CALOPĂREANU, G. *Security Implications of NATO and EU enlargement in the Black Sea Region*. Impact Strategic, no. 38(1), 2011, ISSN 1841-5784, p. 65.

Apart from that, but in accordance with NATO policy on Cyber Defense, the U.S.A. establish their own military cyber capabilities and structures, such as the U.S. Cyber Command (CYBERCOM), which became fully operational in 2010. The command is located in Fort Meade, Maryland, is co-located with the National Security Agency (NSA) and is reporting to the U.S. Strategic Command. The commander of the U.S. Cyber Command is also the director of the National Security Agency.

The declared main role of CYBERCOM is to protect critical infrastructures in order to ensure continuity of government in a crisis and to achieve a greater cyber situational awareness.[21] It is also responsible for directing all cyber activities, to operate and defend Department of Defense (DoD) networks, to build offensive and defensive military cyber capabilities, to develop a suitable workforce and to provide support to combatant commanders.

In conclusion, even if some may ask if it is NATO's role to intervene in case of a cyber conflict that targets one of its members, the NATO Policy on Cyber Defense adopted in 2011 shows that the Alliance's interest is expanding also in this field and NATO's policies are reaching beyond the boundaries of "conventional" military threats. Another important conclusion is that each country's cyber defense and cyber policies vary form almost nil to extended ones, depending on the development of information infrastructures and the reliance level on them for civil / military types of activities. This finding should indicate that NATO is as vulnerable to cyber attacks as the weakest link in the chain (the weakest, most exposed country from this point of view).

Conclusions

One of the foundations of the 21st century world is the fact that computers are involved in most of the operational activities of our infrastructure. The increasing dependence on cyber tools that improve the comfort of people or the efficiency of the world's economies means also that critical infrastructures must be dependable, reliable, strong and secure, impenetrable for external / internal cyber attacks that pursue data manipulation, denial of service or identity theft.

Based on the information presented so far, I would like to offer a few key take-aways.

First, the finding that NATO's Strategic Concept recognizes that the security of the Alliance's information and communication systems is highly dependent on the protective measures against the more and more sophisticated cyber attacks. Therefore, security issues must be treated before they potentially become dangerous, thus, we should allocate resources for security instruments dedicated to:

- Intruder identification and client authentication;
- Achieving network resiliency;
- Cyber intelligence, surveillance, and reconnaissance; and
- Cyber early warning and response.

Additionally, explicit procedures should be defined for dealing with consequences, as part of the cyber prevention and cyber defense process. Also, an insurmountable (until now) obstacle to obtain a bullet proof cyber defense was to find means for nations to assure more effective cyber protection capabilities of privately owned (civil) critical infrastructures. It is recommendable that stakeholders from the public and private sectors try to find workable ways to collaborate together in order to lean on each other's strengths and share their expertise and knowledge.

The most important issue still to be solved (beside the cyber defense itself) is the lack of a globally recognized legal body for cyber conflict resolution. But there is a problem of law enforcement even in a better recognized area of cyber crimes. What evidence could be gathered and provided for legal analysis, when most of the times the source of cyber attacks is hidden, cyber conflicts took hours or days and the evidences can be deleted? Another question still to be answered is what should be the

[21] WALKER, M. B. *Gen. Alexander: CYBERCOM structure will ensure seamless response to cyber crisis*, February 23, 2011. Available from http://www.fiercegovernmentit.com/story/gen-alexander-cybercom-structure-will-ensure-seamless-response-cyber-crisis/2011-02-23

framework of such a body? Every nation has a different approach on how to translate international (if any) laws that cover different actions in the cyber space into local ones. In this respect, international laws remain underdeveloped in determining the threshold when a cyber attack transforms into a cyber war and if it should trigger the use of military force.

Consequently, a lighter (and more feasible) approach is the establishment of an international code of conduct carried by an international organization (such as the United Nations General Assembly). Such an ongoing international initiative already took place in September 2011 when a group of four countries presented a draft resolution for an "International Code of Conduct for Information Security" at the UN General Assembly.[22] But the creation of a global culture of cyber security is useful only for preventing or discouraging cyber conflicts, while during cyber conflicts it would be of no use.

Second, there is a need for a procedure for clearly discriminating between events like cyber attacks, cyber war, cyber crime or cyber terrorism, and a procedure for the conduct of legitimate military/civil cyber operations of states or alliances of nations. We mentioned here "civil cyber operations", because in the future military-on-military cyber actions may become an exception.

Finally, for a cyber crisis situation, the governing bodies of all nations should develop (and when needed activate) an effective decision-making and execution framework (below the cabinet level) for coordinating the state's response to a cyber event and facilitate a quick recovery of the affected critical information infrastructures.

[22] Draft resolution for an "*International Code of Conduct for Information Security"*. Ministry of Foreign Affairs of the People's Republic of China. Available from http://www.fmprc.gov.cn/eng/wjdt/wshd/t858978.htm