Committee: Disarmament and National Security Committee

Issue: Counter-measures against Cyber Warfare

Student Officer: Harry Samakas

Position: Deputy Chair

INTRODUCTION

Nowadays, modern technology has come to dominate the world over, enabling us to reach information on countless topics, events, locations and anything in between, trade and communicate in a matter of seconds. However, knowledge is not the single benefit that contemporary networks provide us with. The most prevalent of these benefits is the internet. Although technological advancements do not reach all societies, a significant percentage of the world's population is connected to the internet, or any technological network for that matter. Nevertheless, what most people seem to ignore, is that this constant connection with modern means may not help the masses as much as it makes them vulnerable and leaves them exposed. Our data, which we all have submitted in one of those means, are always online, saved in a certain server and only a few clicks away from anyone who has basic knowledge on the technique needed to acquire these pieces of data. It is therefore apparent that the term digital privacy is, to a certain extent, an illusion.

This issue of privacy can be transferred to a global scale, since countries also suffer from this network vulnerability. They are mostly threatened by international organizations that aim to obtain sensitive data via various methods like computer viruses or denial-of-service attacks. These masses of data stored on the web are of crucial importance to states and they usually go to great lengths to protect them.

This very attempt of trying to counter the effects of Cyber-attacks is a problem that has risen only in the recent past since previous technologies didn't provide such a wide range of interconnectivity in order for the attackers to be able to acquire crucial info via them. Hence, it is an issue that is yet to be fully appreciated and resolved, due to its short existence as a problem.

DEFINITION OF KEY TERMS

Cyber-Warfare

There have been extensive discussions over a proper definition of the actions that compose Cyber Warfare and many different explanations to this term have been given by various bodies. There is also a debate on whether the term "cyber warfare" is accurate. For example, the Journal of Strategic Studies, a leading journal in that field, published an article by Thomas Rid, "Cyber War Will Not Take Place." An act of cyber war would have to be potentially lethal, instrumental, and political. Given that perspective not one single cyber offense on record constitutes an act of war on its own. Instead, all politically motivated cyber-attacks, Rid argued, are merely sophisticated versions of three activities that are as old as warfare itself: sabotage, espionage, and subversion.

(http://thomasrid.org/no-cyber-war)

Starting with the perspective of international Corporations, a definition has been given by one named RAND Corporation and it reads: "Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks."

(*As found in http://www.rand.org/topics/cyber-warfare.html , 26-6-2015)*

From a view of security expertise, U.S. government security expert Richard A. Clarke, in his book (*Cyber War, 2010*) defines cyber warfare as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." (*Clarke, Richard A. – Cyber War,* ISBN 9780061962233)

Espionage and national security breaches

Cyber espionage is the act or practice of obtaining secrets (sensitive, proprietary or classified information) from individuals, competitors, rivals, groups, governments and enemies for military, political, or economic advantage using illegal exploitation methods on the internet, networks, software and or computers. Classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world.[1]

[1] "Cyberwarfare." Wikipedia. Wikimedia Foundation, , *Accessed on 09-26-2015* <https://en.wikipedia.org/wiki/Cyberwarfare>.

Datum

Being the singular form of the word “data”, a datum is a piece of data which is a term widely used in the field of cyber-warfare.

Denial-of-service attack

Denial-of-service (DoS) is an attempt to make a machine or network resource unavailable to its intended users. A DoS attack generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.[2]

Computer and Data Networks

A computer network or data network is a telecommunications network which allows computers to exchange data. In computer networks, networked computing devices pass data to each other along network links (data connections).[3]

BACKGROUND INFORMATION

As repeatedly mentioned above, cyber-crime is a very recently-developed activity which makes it quite hard to look into as a historic phenomenon. Also, knowledge of cyber-warfare is intensely restricted as almost all information about these events becomes classified as soon as it is discovered. Nevertheless, focusing on the last three decades, as internet-based threats race up national security agendas, one can find signs of such activities, as well as numerous problems that rose after the cyber-warfare tactics were put into motion. It should also be made clear that, cyber–attackers do not exclusively focus on obtaining sensitive information and data from governments, but also from enterprises, banks and even individuals.

During the dawn of the cyber era, data hacking has been used as an expression of activism, focused on the limitless and open access to knowledge for the public. For example, WikiLeaks stood as a ground-braking platform that operated under such principles, by obtaining such confidential information and leaking them for the eyes and benefit of the public. This act was considered a criminal one and the US Government filed charges against

[2] < https://en.wikipedia.org/wiki/Denial-of-service_attack >, "Denial-of-service Attack." Wikipedia. Wikimedia Foundation, *Accessed on 09-26-2015*

[3] <https://en.wikipedia.org/wiki/Computer_network>, "Computer Network." Wikipedia. Wikimedia Foundation, *Accessed on 09-26-2015,*.

Julian Assange, founder of WikiLeaks. The question that may arise is, what differentiates the element of terrorism from that of plain activism.

To this end, the two following case studies elucidate, that Cyber-Warfare has been deeply adopted by both enterprises and governmental institutions. Hence, the issue that one should focus is not just the hacking itself – as it was in the past – but rather the fact that it has now become an element of the system per se.

Consequently and as it will be made clear through the cases themselves, Cyber Warfare attributes characteristics of both financial and terroristic nature.

Aramco Hack

The first case is the hack against the Aramco firm. Many claimed afterwards that this attack had a terroristic character.

In July 2013 Vanity Fair magazine published an article written by Gross M. J., who extensively described the story behind the cyber-attack in Aramco. [4]

Briefly put, in the headquarters of Saudi Aramco in eastern Saudi Arabia, a group of hackers known as the "Cutting Sword of Justice" executed in 2012 a full wipe of 30,000 Aramco personal computers and then projected an image of an American flag on fire on the screens of those PCs when the wipe was completed. The virus was called Shamoon and was used for cyber espionage in the energy sector.

The Aramco incident indicates the shift that has taken place in hacking; from a fashionable trend to a criminal mechanism. It should also be highlighted that Aramco is one of the world's largest oil companies, a fact that raises the eye for modern hackers' preferences as to their target firms. Keeping that in mind and in conjunction with the change of motives that the hacking sector has seen, there is no doubt that, however cyber, hacking surely shares a large part of its content with the physical world.

There is much more detail to the techniques and results that were revealed after the attack in Aramco, however the big picture is that this incident was a sign of what modern-day hackers are capable of doing in companies, people and above all, governments.

[4] (*Battlespace by Michael Joseph Gross, Accessed on 09-26-2015, http://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business).*

Ephemeral Security – Mosquito Program

The next case refers to the *mosquito program* which goes even deeper into the idea of hacking as a means of espionage and business strategy.

The Mosquito program involved two men, Brown and Scott, who had created a business called Ephemeral Security, which was hired by firms and banks to hack, steal their own information and then point out the flaws in the system in order to prevent other hackers from doing the same thing. What followed next, was a program named mosquito that the two of them created and was meant to gather information during penetration tests. However, this was more than a simple testing tool, as the two men's idea also stood as a revolutionary model for espionage. Such malware as mosquito proved useful for a handful of tricks. One could hack into one's microphone and record the machine's surroundings or look into architectural plans and design schematics, thus analyzing inner working of industrial installations. Other important applications consisted of the ability to take a screenshot of victims' computers, obtain passwords, record Skype conversations and force infected computers to connect via Bluetooth to any nearby devices thus spreading the virus even further.

Lastly, there's another noteworthy wave of cyber viruses that began in 2007. It was the time when the first versions of a computer worm were released. What differentiated them from the previous viruses was that they weren't meant to cause any digital harm to the targeted machinery; only physical damage.

What one should extract from the event is that, in this case, not only was hacking reincarnated into a business plan, but, in the essence, operated within the system as an integral part. Indeed, Cyber Warfare stands as an antagonizing "weapon" in a market-orientated combat.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

USA

The United States of America has acknowledged the issue of cyber-warfare and so recognizes it as a threat to national security. According to US officials, the use of a cyber-attack is to attack, degrade or disrupt communications, steal or hinder the flow of information. It should be noted that the elimination of the geographical factor that cyber-warfare indicates, is a crucial multiplier of this threat's gravity. Furthermore, the US perspective can be analyzed from both the position of the attacker and the attacked, thus making for a wider point of view. Financially speaking, the state has generously invested billions of dollars in major IT programs in hope of efficiently combating cyber-crimes by raising its defenses, but with little luck.[5]

In a rather more technical manner, the US has urged NATO to create a "cyber shield" in defense to any cyber-attacks on this transatlantic organization. According to the US's suggestion, the cyber defenses would consist of *Five Pillars.* In both*, Red Orbit* and *The Sunday Morning Herald,* articles published under the topic of cyber security[6] it is explained how this mechanism works. Briefly put, we can conclude to the above descriptions.

- First Pillar: Overlaps the elements of the battlespace to those of cyberspace.
- Second Pillar: Provides proactive defenses as opposed to passive defense.
- Third Pillar: Consists of critical infrastructure protection (CIP) to ensure protection of critical infrastructure.
- Fourth Pillar: Provides use of collective defense in order to offer early detection.
- Fifth Pillar: Focuses on enhancement & maintenance (e.g. increasing all capabilities)

Taking in consideration the *Pillars'* operations, one may realize that cyber warfare is almost identical to conventional warfare. It is therefore rational for one to question whether or not the importance and casualties of conventional warfare is one of those elements that are transferred into the cyber era.

There have also been several allegations of the US acting as a cyber-attacker, mainly against China and Iran. The US has also published numerous statements as to their position concerning cyber-attacks as an act of war, many of which were expressed by the White House and can be viewed from its official website.[7]

China

China's position on this matter, however different than those of the other states, can be viewed more clearly through the lens of its combat with the United States. When it comes to cyber-attacks, those two nations probably have the longest, most intense "cyber-feud" ever recorded in history. For instance, the breach of the Office of Personnel

[5] *"Reports: Air Force's troubled technology projects cost millions:, John Nolan, Dayton Daily News, Ohio, <http://www.stripes.com/news/us/reports-air-force-s-troubled-technology-projects-cost-millions-1.180564>*

[6] *The Sunday Morning Herald, "US urges NATO to build 'cyber shield'" http://www.smh.com.au/technology/us-urges-nato-to-build-cyber-shield-20100915-15d27.html, Red Orbit, "ssavage", "Official: NATO Should Build A 'Cyber Shield'" <http://www.redorbit.com/news/technology/1918102/official_nato_should_build_a_cyber_shield/>*

[7] *Launching the U.S. International Strategy for Cyberspace, Howard A. Schmidt, <https://www.whitehouse.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace>*

Management that occurred during this year's spring. The attack cost to the US the exposure of over 21 million deferral employees, contractors and others.

Furthermore, over 70% of America's corporate property theft is considered to be originated from China. Many believe that this aggressive behavior from the Chinese state was a result of the fact that the nation couldn't compete with the US in military terms and therefore needed a new source to stabilize this imbalance of power; in other words by using corporate espionage. According to an article[8] published by Alexander Abad-Santos, Chinese hackers are in control of "*Pentagon's most sophisticated weapons systems*" thus leaving the US on the defensive side of cyber warfare diplomacy. After acquiring such crucial Intel as those of the Pentagon, China has somewhat eliminated the advantage that once stood next to the US.

Politically speaking, China has denied any cyber-warfare-related accusations by the US, while striking back with counter-accusations of similar nature against the United States, which in turn are denied by the US government.

Although, for some, the facts may speak for themselves it should be bravely highlighted that the nature of cyber-warfare is ideal for an environment of secrecy, as it is nearly impossible for one to be certain about the source of a cyber-attack. Therefore, all of the above are based only on allegations and up until today we have no definitive case against any nation.

India

India is one of the most emerging superpowers in the technological and telecommunications field. Despite that fact, Cyber warfare against India has mostly been identified with minor breaches like websites defacements and hacking into e-mail accounts. It's a fact that India is belated to realize the need for a strengthened cyber security, however it has drawn up a national cyber security policy of 2013 (NCSP 2013). It must be noted that India has no cyber warfare policy until now.

NATO

Just like the majority of countries and organizations, the North Atlantic Treaty Organization has acknowledged, the rapidly increasing scale of cyber-attacks, as well as their effect on national and international security and, hence, it considers the protection from such harm as a crucial task. The transatlantic organization officially approved its first cyber

[8] *"China Is Winning the Cyber War Because They Hacked U.S. Plans for Real War", Alexander Abad-Santos, The Wire,* http://www.thewire.com/global/2013/05/china-hackers-pentagon/65628/

defense policy on January 2008 in the event of the famous cyber-attacks that occurred in Estonia during the same time period.

What is worth mentioning is that, in these exact words and as published in NATO's official web page, *"nations are and remain responsible for the security of their communication networks which need to be compatible with NATO's and with each other's".*[9] In that spirit, it is of crucial importance that NATO chose to be undoubtedly specific as to the protection and defense policies that it provides and the responsibilities it requests.

TIMELINE OF EVENTS

January 2008	NATO first officially approved its first cyber defense policy on January 2008. In the same period a famous cyber-attack occurred in Estonia.
26 November 2010	The cyber-attacking group Indian Cyber Army attacked the webpages of the Pakistan Army and on several other official webpages and government ministries, such as the Ministry of Foreign Affairs, the Ministry of Education, the Ministry of Finance, the Pakistani Computer Bureau, as well as the Council of Islamic Ideology. The attack was considered a response to the Mumbai terrorist attacks.
4 December 2010	The Pakistan Cyber Army hacked the webpage of India's Central Bureau of Investigation (CBI).
July 2011	The South Korean corporations SK Communications was attacked, resulting in the theft of the personal data of up to 35 million people.
August 2011	McAffe, an internet security company, reported Operation Shady RAT. The operation started in 2006 and it included attacks on at least 72 organizations including governments and defense contractors.
August 2012	An organization called the "Cutting Sword of Justice" hacked into 30,000 Saudi Aramco computers. The virus, Shamoon, was planted in other energy companies as well.

UN INVOLVEMENT: RELEVANT RESOLUTIONS, TREATIES AND EVENTS

[9] "Cyber security", North Atlantic Treaty Organization, Accessed at 09-26-2015 http://www.nato.int/cps/en/natohq/topics_78170.htm

The UN has acknowledged the threat that comes from the scale that cyber-attacks have grown to. The United Nations has posted an article on this topic where it describes an event held by the Economic and Social Council called "Cybersecurity and Development", organized by UNDESA (United Nations Department of Economic and Social Affairs) and the International Telecommunications Union (ITU)[10]. The discussion led to the following key-goals:

- Raising awareness on the issue by providing ECOSOC members with a picture of cyber-security's challenges and its ties to future development.
- Identifying a mass of policies and initiatives, on a global scale, and creating a cyber-security culture.
- Discovering new ways to respond to the constantly expanding act of cyber-crime.

Under the category of "Developments in the field of Information and Telecommunications in the context of International Security"[11] the UN has provided extensive reports on all the developments that this field has seen during the course of the last decades.

The issue of information security, which is directly linked to that of cyber-security, was first introduced by a resolution submitted by the Russian Federation which was accepted and adopted without a vote.[12] Being one of the first resolutions ever to deal with this issue, the majority of the clauses aimed at encouraging other countries to express their own views and positions on this topic, thus engaging in an era of further diplomatic cooperation on this newly introduced subject.

All in all, the UN has been active on this matter for almost two decades, with numerous resolutions that constantly elaborate in greater depth on the issues, views and points that are being expressed by its member states[13]. However, the resolution coded "69/28"[14] could be considered as a sum of all previous resolutions, as it refers to the fulfillment of some

[10] "Cybersecurity: A global issue demanding a global approach", United Nations Department of Economic and Social Affairs, United Nations, Accessed on 09-26-2015, <http://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html>

[11] GGE INFORMATION SECURITY, UNODA, < http://www.un.org/disarmament/topics/informationsecurity/> , Accessed on 09-26-2015

[12] http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/53/70 , A/RES/53/70

[13] e.g. 53/70 of 4 December 1998, 54/49 of 1 December 1999, 55/28 of 20 November 2000, 56/19 of 29 November 2001, 57/53 of 22 November 2002, 58/32 of 8 December 2003, 59/61 of 3 December 2004, 60/45 of 8 December 2005, 61/54, of 6 December 2006, 62/17 of 5 December 2007, 63/37 of 2 December 2008, 64/25 of 2 December 2009, 65/41 of 8 December 2010, 66/24 of 2 December 2011, 67/27 of 3 December 2012 and 68/243 of 27 December 2013.

[14] https://ccdcoe.org/sites/default/files/documents/UN-141202-ITIS.pdf , A/Res/98/28

individual resolutions,[15] while also recalling the purposes, goals and conclusions of past resolutions altogether.[16] Among other points, it is worth nothing that Res "98/28" also promoted and supported the research of the *Group of* Governmental *Experts* to "*to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security* […] (and) *the issues of the use of information and communications technologies in conflicts…*".[17]

Nevertheless, in recent years the wider debate has intensified over the development of possible norms of behavior or a set of confidence-building measures[18] in the cybersecurity domain. It should not be forgotten that most of the pressing issues and challenges in areas related to cybersecurity have roots in the adoption and review of national legislation and the implementation of multilaterally agreed upon principles.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The majority of modern cyber-attacks are combated with the aid of cyber counter-intelligence.

Pentagon's Cyber-strategy

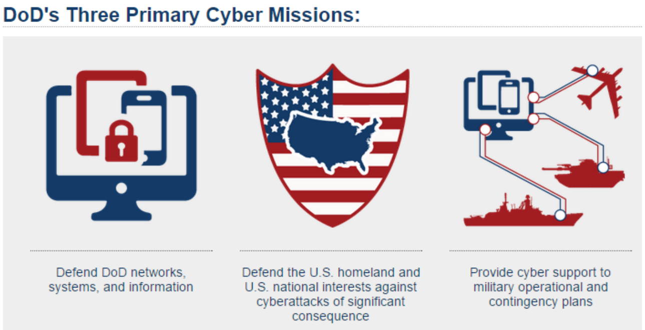
DoD's Three Primary Cyber Missions:
Defend DoD networks, systems, and information
Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence
Provide cyber support to military operational and contingency plans

Fig. 1. Courtesy of U.S. Department of Defense, http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy

According to an article issued on DefenseNews website, earlier this year – the 23th of April – the Pentagon released their new plan concerning their aims and ideas on the concept of cyber-intelligence.[19] It is the newest official development on the Pentagon's action plan, since their previous update that was released in 2011. In general, the Pentagon sheds light upon three basic categories that considers top priority:

- Defend the Department of Defense's (DoD) networks and systems and information.

[15] Ibid., par. 15, A/Res/98/28

[16] Ibid., par 1 & par 12, A/Res/98/28

[17] Clause #4, A/Res/98/28, UN, 2 December 2014, Accessed on 09-26-2015, <https://ccdcoe.org/sites/default/files/documents/UN-141202-ITIS.pdf

[18] As seen on Clause 4 of Res 98/28

[19] Aaron Mehta, "Cyber Strategy Relies on Deterrence, Industry", April 26, 2015, < http://www.defensenews.com/story/defense/policy-budget/budget/2015/04/26/pentagon-new-cyber-strategy-deterrence-industry/26298913/>

- Defend, in the event of cyber-assaults, what the DoD refers to as "*significant consequence*".[20] Provide integrated cyber capabilities to military operations.[21]

NATO Policy on Cyber Defense

NATO's action plan against cyber-attacks was endorsed by Allies at NATO's Wales Summit in September 2014. Through this policy, the Alliance recognizes cyber-defense as a fundamental aspect of its task of collective defense and also confirms that international law applies in cyberspace. It has also prioritized on the top of its list the protection of the communication systems owned and operated by the Alliance.

Furthermore, NATO's policy underlines and elaborates on the assistance of Allied countries in cyberspace through a *streamlined cyber defense governance*.[22]

In technical terms, the tool that NATO has created in order to maintain its security is the NATO Computer Incident Response Capability (NCIRC) which ought to protect NATO's networks via a full-proof cyber-defense support on various NATO sites.[23]

Issue of "Attribution"

A very common aspect that differentiates and exclusively characterizes every attack or assault of cyber nature, is the problem of Attribution; thus the deficiency of tracking the cyber-attackers' source.

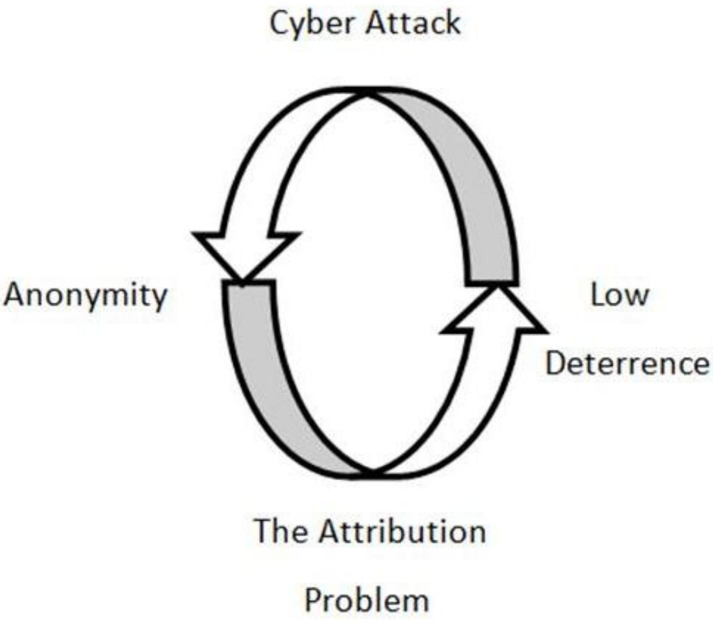

Fig. 2, Courtesy of ENFOSEC Institute, "The Attribution Problem in Cyber Attacks", http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/

[20] Ibid.
[21] Department of Defense
[22] "NATO Rapid Reaction Team to fight cyber-attack", NATO, 13 Mar. 2012, Accessed on 09-26-2015, <http://www.nato.int/cps/en/natolive/news_85161.htm>
[23] Ibid.

There's a great deal of info and theoretical background surrounding this idea (e.g. "State and Non-state actors", "Anonymity", "Sanctuary state" and many other principles outlined both in law texts and numerous articles or stories,[24]) but what one should essentially extract from such info, is that this advantage of constant interconnectivity, is the very reason why it is difficult to identify the source of an attack.

It is this very characteristic of cyberspace that may be the key to the embodiment of *modern warfare:* the ideality and perfection in the borders of which cyberspace was crafted; it is the weapon to which no machinery may ever become immune.

POSSIBLE SOLUTIONS

First of all, when talking about cyberspace, there is always room for improvement, meaning that anti-virus programs (in both a private-sector and government-scaled perspective) can always be constantly updated, thus increasing their efficiency in terms of overall security. However, this might turn out to be a never-ending circle, since the cyber-attackers can also improve their methods and techniques as the cyber-defenses mature as well. Therefore, although this continuous cyber upgrades may be of some assistance, it should always be kept in mind that the core of this issue will remain the same as the attackers always progress along with the defenders.

Moreover, a solution may be found if one looks away from the means and focuses on the goal; the motivation. For instance, Hacktivism is a form of cyber warfare that is strictly politically motivated. Hacktivists undertake acts such as Web site defacements, URL redirection, denial-of-service attacks, information theft and dumping, web site parodies, typosquatting, and virtual sabotage. With that in mind, a possible solution to this issue may be found on the reason why cyber attackers put their criminal activities in motion in the first place. Furthermore, states should collaborate in order to improve transparency, so as to avoid cases of inter-state cyber-warfare.

[24] *The Attribution Problem in Cyber Attacks, INFOSEC Institute, Hacking, <http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/>*

Last but not least, after having explained possible key-elements on the sector of software updates and the variation of the attackers' motives, it is also equally crucial for governments to maintain and upgrade the hardware of all their machinery and equipment. This action will not only reinforce each state's network powerhouse, but also make it harder for a data-thief to catch up with the updated technologies to which only the governments may be granted access.

BIBLIOGRAPHY

Info, Statistics, Articles

The sources stated bellow were all checked in 30th of June 2015.

U.S. Department of Defense, Jim Garamone, "*Lynn Explains U.S. Cybersecurity*",

<http://www.defense.gov/news/newsarticle.aspx?id=60869>

The Daily Beast, "*China reveals its cyber war secrets*",

<http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.html>

The Joining Operating Environment,

<http://wayback.archive.org/web/20130810043238/http://www.jfcom.mil/newslink/storyarchive/2010/JOE_2010_o.pdf>

Stars and Stripes, John Nolan, "*Reports: Air Force's troubled technology projects cost millions*",

<http://www.stripes.com/news/us/reports-air-force-s-troubled-technology-projects-cost-millions-1.180564>

Forbes, Loren Thompson, "*Five Things The Government's Cybersecurity Providers Should Have -- And Usually Don't*",

<http://www.forbes.com/sites/lorenthompson/2012/06/18/five-things-the-governments-cybersecurity-providers-should-have-and-usually-dont/>

POGO Blog, Bryan Rahja, "*The Cost of Contractor Computer Engineering Services*",

<http://pogoblog.typepad.com/pogo/2012/06/occupational-education-6-the-cost-of-contractor-computer-engineering-services-.html>

Redorbit, "*NATO Should Build A 'Cyber Shield'*",

<http://www.redorbit.com/news/technology/1918102/official_nato_should_build_a_cyber_shield/>

Financial Times, James Blitz, "*A huge challenge for China, Russia and organized crime*",

<http://www.paconsulting.com/introducing-pas-media-site/highlighting-pas-expertise-in-the-media/articles-quoting-pa-experts/financial-times-security-a-huge-challenge-from-china-russia-and-organised-crime-1-november-2011/>

Philpapers, Jojn Arquilla, "*Can information warfare ever be just?*"

<http://philpapers.org/rec/ARQCIW>

Academia.edu, Seas Collins, Stephen McCombie, "*Stuxnet: the emergence of a new cyber weapon and its implications*",

<https://www.academia.edu/4155240/Stuxnet_the_emergence_of_a_new_cyber_weapon_and_its_implications>

GSN, Andrew Ginter, "*Critical infrastructure to attack, warns cyber security expert*",

<http://www.gsnmagazine.com/article/40042/critical_infrastructure_vulnerable_attack_warns_cy>

Digital Threat, Jago Maniscalchi, "*What is Cyberwar?*"

<http://www.digitalthreat.net/2011/09/what-is-cyberwar/>

WindsOfChange.net, Joe Katzam, "*4GW: What is 4th Generation Warfare?*"

<http://www.windsofchange.net/archives/002736.html>

Global Dashboard, Alex Evans, "*Playing with fire in the Ukraine",*

<http://www.globaldashboard.org/2014/05/14/playing-fire-ukraine/>

Oxford Dictionaries, "datum", <http://www.oxforddictionaries.com/definition/english/datum>

Bloomberg Business, anonymous writer, "*Hackers Linked to China's Army Seen From EU to D.C.",*

<http://www.bloomberg.com/news/articles/2012-07-26/china-hackers-hit-eu-point-man-and-d-c-with-byzantine-candor>

Dailymail.co.uk, "*NSA whistleblower Edward Snowden says U.S. government has been hacking Chinese universities, businesses and politicians for FOUR YEARS as he finally breaks cover*",

<http://www.dailymail.co.uk/news/article-2340295/Im-traitor-hero-Im-American-NSA-whistleblower-Edward-Snowden-speaks-Chinese-newspaper.html>

The Japan Times, The Washington Post, AP, "*Snowden says U.S. hacking targets Chine; NSA points to thwarted attacks",*

<http://www.japantimes.co.jp/news/2013/06/14/world/u-s-hacking-effort-targets-china-snowden/>

Perry4Law, PTLB, "Perry4Law, PTLB, "*Cyber Warfare Against India and Its Defenses",* <http://perry4law.org/blog/?p=585>

Perry4Law, International Legal Issues of Cyber Attacks, Cyber Terrorism, Cyber Espionage, Cyber Warfare and Cyber Crimes, <http://perry4law.co.in/cyber_security/>

Perry4Law, Critical Infrastructure Protection in India: The Problems, Challenges and Solutions,

<http://ptlb.in/csrdci/wp-content/uploads/2014/01/Critical-Infrastructure-Protection-In-India-The-Problems-Challenges-And-Solutions.pdf>

The Express Tribune, non-listed writer, "*36 government sites hacked by 'Indian Cyber Army'",*

<http://tribune.com.pk/story/83967/36-government-websites-hacked-by-indian-cyber-army/>

CBS News, CBSNEWS, "*Pentagon Bill To Fix Cyber Attacks: $100",*

<http://www.cbsnews.com/news/pentagon-bill-to-fix-cyber-attacks-100m/>

Npr.org, Tom Gjelten, *"Seeing the internet as an 'information weapon'",*

<http://www.npr.org/templates/story/story.php?storyId=130052701>

The Wall Street Journal, Siobhan Gorman, "*U.S. Backs Talks on Cyber Warfare",*

<http://www.wsj.com/articles/SB10001424052748703340904575284964215965730>

Ars technical, Seann Gallagher, "*us, Russia to install 'cyber-hotline' to prevent accidental cyberwar",*

<http://arstechnica.com/information-technology/2013/06/us-russia-to-install-cyber-hotline-to-prevent-accidental-cyberwar/>

UN Chronicle, "*Towards Cyberspace: Managing Cyberwar Through International Cooperation",*

<http://unchronicle.un.org/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation/>

Graphs, Images

Google Books, Ngram Viewer, (the word "network" must be added manually due to different individual URLs),

<https://books.google.com/ngrams>

United States Department of Defense, DoD's Three Primary Cyber Missions,

< http://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy>

The Attribution Problem in Cyber Attacks, INFOSEC Institute, Hacking,

<http://resources.infosecinstitute.com/attribution-problem-in-cyber-attacks/>