National Defence Défense nationale

Canadian Forces College
Collège des Forces Canadiennes

CYBER WARFARE NEW THREAT TO GLOBAL SECURITY IN SAME OPERATIONAL ENVIRONMENTS

Maj Jose Angel Soriano Chavez

JCSP 44	PCEMI 44
Exercise *Solo Flight*	Exercice *Solo Flight*

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE – COLLÈGE DES FORCES CANADIENNES
JCSP 44 – PCEMI 44
2017 – 2018

EXERCISE *SOLO FLIGHT* – EXERCICE *SOLO FLIGHT*

CYBER WARFARE NEW THREAT TO GLOBAL SECURITY IN SAME OPERATIONAL ENVIRONMENTS

Maj Jose Angel Soriano Chavez

"This paper was written by a student attending the Canadian Forces College in fulfilment of one of the requirements of the Course of Studies. The paper is a scholastic document, and thus contains facts and opinions, which the author alone considered appropriate and correct for the subject. It does not necessarily reflect the policy or the opinion of any agency, including the Government of Canada and the Canadian Department of National Defence. This paper may not be released, quoted or copied, except with the express permission of the Canadian Department of National Defence."

Word Count: 3160

"La présente étude a été rédigée par un stagiaire du Collège des Forces canadiennes pour satisfaire à l'une des exigences du cours. L'étude est un document qui se rapporte au cours et contient donc des faits et des opinions que seul l'auteur considère appropriés et convenables au sujet. Elle ne reflète pas nécessairement la politique ou l'opinion d'un organisme quelconque, y compris le gouvernement du Canada et le ministère de la Défense nationale du Canada. Il est défendu de diffuser, de citer ou de reproduire cette étude sans la permission expresse du ministère de la Défense nationale."

Compte de mots: 3160

CYBER WARFARE NEW THREAT TO GLOBAL SECURITY
IN SAME OPERATIONAL ENVIRONMENTS

INTRODUCTION

The current threats against global security have evolved over time, as part of the technological development as a starting point for the terrorist attacks of September 11, 2001 against the United States of America, since those days the methods to confront terrorism, irregular war and cyber war have changed, but the operational scenarios are repeated. So is necessary that armed forces to update their procedures and the creation of new doctrine to effectively face these threats considering complex environments and Battlefields.

Nowadays we live in a complex environment and computer development, however in parallel some people are developing malware programs which are malicious software that aims to infiltrate and damage computer systems, operating systems and internet networks, which are Trojan horses and spyware that "can perform a variety of functions, including stealing, encrypting or deleting sensitive data, altering or hijacking core computing functions and monitoring users' computer activity without their permission."[1] The impact and consequences of cyber attacks cause economic, social, political and military destabilization, putting at risk the infrastructure and national security of any country, through a "dirty war" that consists in the use of technological and informative tools, being the challenge to know with certainty the attribution or the author of the cyber attack. One of three legal issues about Cyber warfare is that "it may be very difficult to determine what person, organization, or country is ultimately responsible for any

[1] Malware (malicious software), https://searchsecurity.techtarget.com/definition/malware. November 2016.

given cyber intrusion."[2] There are some definitions of Cyber warfare but the U.S. Department of Defense has prepared a formal definition of this new warfighting domain, and inspired by the writings of Sun Tzu: "Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood."[3] In this order of ideas, the Cyber warfare is the conflict without deployment troops neither physical combat, using computer programs as weapons with approval or not from public opinion. Likewise "a cyber attack is a cyber operation, whether offensive or defensive that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[4]

In this context the most attractive objectives of cyber warfare are developed countries that use technology in their financial, industrial, commercial systems and in the field of national security, representing a risk from outside and inside with regard to cybercrime.

This paper will demonstrate that there is a need to adapt the military doctrine to increase the capabilities of the armed forces to face cyber warfare in effective way and technological threats to reduce the risks in national security of countries as well as global security.

The United States is considered a frame of reference and an important example of lessons learned in the field of cyber warfare, which has extensive experience in this new form of hybrid war, highlighting its ability to adapt its military doctrine and response procedures to face threats. current cyber attacks.

[2] Kramer Franklin D. *"Cyber power and National Security"* Center of technology and National Security Police, National Defense University Press, Unites States of America 2016. p 525.

[3] Carr, Jeffrey. *"Mapping the cyber underworld Inside Cyber Warfare"* O' Reilly Media, United States of America 2010. p 2.

[4] Schmitt, Michael N. *"Tallinn Manual on The International Law applicable to Cyber Warfare"* prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States of America 2013. p 91.

BACKGROUND CYBER WARFARE

As antecedent or historical data of the creation of malwares and computer viruses highlights the first hacker prosecuted for spreading computer virus “Robert Tappan Morris was a Harvard graduate and Cornell graduate student when he developed the first widely spread Internet “worm Morris.”[5] He released it on Nov. 2, 1988.” This event resulted in an economic loss for the United States because “The cost in removing the worm from each computer or network system ranged from $200 to more than $53,000” also was a great damage on the computers field because “according to estimates by the U.S. General Accounting Office, between $100,000 and $10 million was lost due to lack of access to the Internet.”[6] This event shows that human intelligence and cybernetic knowledge maliciously applied can get catastrophic consequences for the security and economy of any country.

As a comparison of the first internal cyber attack in U.S. mentioned in the previous paragraph, nowadays the economic consequences of a cyber attack are counted in millions of dollars, for example according with U.S’ Council of Economic Advisers report malicious “cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016. The report details the range of threats that U.S. entities face from actors, including corporations and countries such as Russia, China, Iran and North Korea,”[7] countries that are the main actors of the cyber-wars adding to the United Kingdom.

[5] “On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus” http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html. date Jul 26, 2011.

[6] Ibid.

[7] “The Cost of Cyber Attacks to U.S. Economy.” By Jennifer Epstein and Shelly Hagan, February 20, 2018. https://www.insurancejournal.com/news/national/2018/02/20/481121.htm

With the computers and networks' development the threats against global security have changed "Cyber operations began to draw the attention of the international legal community in the late 1990s. Most significantly, in 1999 the United States Naval War College convened the first major legal conference on the subject."[8] As a historical event of cyber attacks is "The first internet "war" has already taken place in April 2007 between Russian and Estonian hackers; the initiation of the conflict was blamed on the Russian government,"[9] This aggression showed how easy it is for a hostile country to take advantage of potential tensions and technological capabilities within a society to cause damage. In this war the activating incident was Estonia's relocation of the statue "The Bronze Soldier of Tallinn," dedicated to soldiers of the former Soviet Union who had died in Battle. The resulting massive Distributed Denial of Service (DDoS) attacks took down Estonian web sites belonging to banks, parliament, ministries and communication outlets.[10]

CYBER WARFARE NOWADAYS

Today the economies of the countries and the complex global economy are based on the infrastructure of Internet and computers networks, this dependence on technology represents dangerous threats that most of the time the users do not know. The need for inter connectivity of computer networks in commercial, financial companies as well as security systems represents a

[8] Schmitt, Michael N. *"Tallinn Manual on The International Law applicable to Cyber Warfare"* prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States of America 2013. p 16.

[9] Karatzogianni, Athina. *"Cyber conflict and global politics"* Taylor and Francis group, United States of America 2009. p 29.

[10] Carr, Jeffrey. *"Mapping the cyber underworld Inside Cyber Warfare"* O' Reilly Media, United States of America 2010. p 3.

permanent external and internal risks for the information stored in computer terminals. “The world faces unprecedented risks across the internet in what has become known as “The 21st Century’s Wild West,” where attacks on computer systems and networks are generally conducted with the complete anonymity and impunity for those perpetrating these acts,”[11] an example are Distributed Denial of Service (DDoS) attacks when the server is attacked from many computers sending them an excessive volume of "junk" information, blocking certain web pages or the entire computer system.

However also the role played by the academic preparation of computer science in the educational field focus in interconnectivity has been an important factor to increase the risks in terms of computer security and possibilities of cyber attacks, because "for over 40 years universities have taugh courses on designing and writing computer coding. As the interconnectivity of the Internet evolved, few people realized the inherent flaws and lack of sound security measures in legacy systems.”[12] So educational field is an important factor and learning about computer systems and networks applied in a malicious way, bring risks of computer insecurity and cyber attacks. For example “today, Chinese students top of International science and math challenges. In a 2003 math, science and reading assessment involving 250,000 students from 41 countries, China ranked #1 in science and #3 in math,”[13] so it is possible that these students later become hackers and carry out cyber attacks.

[11] Lowther, Adam B. *“Conflict and cooperation in Cyberspace, The challenge to National Security”* Taylor and Francis group, United States of America 2014. p 9.

[12] Ibid.

[13] Carr, Jeffrey. *“Mapping the cyber underworld Inside Cyber Warfare”* O’ Reilly Media, United States of America 2010. p 172.

Nowadays, the countries' governments are more concerned about the damages that can be caused by cyber attacks than by conventional war or nuclear war, because a single personnel with sufficient technology and knowledge of information technology is capable of causing severe damage to infrastructure. of a country in the economic, social and security fields. "Cyber operations by "hacktivists against Estonia in 2007 and against Georgia during its war with the Russians Federation in 2008, as well as cyber incidents like the targeting of the Iranian nuclear facilities with the Stuxnet worm in 2010."[14] These events worried some States about the cyber warfare issue, forcing them to update on this subject, such as: United Kingdom with its 2010 security strategy where cyber attacks are included, Canada with its Cyber Security Strategy and Russia who published the cyber concept regarding the activities of its Armed Forces.[15]

Cyberwarfare has relation with media and information technology (IT) which are pillars of the interaction of societies and States, impacting on the rapid access to information of the civilian population in the face of events that affect stability, such as Syria, Iran, Venezuela and diplomatic relations of countries like the United States, North Korea, Russia, Iran and China that as a whole could affect global security. However the power of the information is dangerous "due to ease in which propaganda, involving valid information, mixed with dis-information, mis-information and excessive information (coupled with mis- or dis-interpretation of that information) can be disseminated and utilized globally on the Internet ."[16] In addition the informational's power of nowadays, megacities and their economic, industrial, political, security

[14] Schmitt, Michael N. *"Tallinn Manual on The International Law applicable to Cyber Warfare"* prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States of America 2013. p 16.

[15] Ibid. p 17.

[16] Karatzogianni, Athina. *"Cyber conflict and global politics"* Taylor and Francis group, United States of America 2009. p 13.

and military infrastructure represent a very attractive target for hackers who carry out cyber attacks.

A recent example of cyber attack was the one that appeared in banks in Mexico on April 30, 2018 where a newspaper from Mexico "El Financiero" reported on the delay of electronic banking transactions as a result of "The “attempt"of cyber attack that suffered some financial institutions affected its process of connection with the Interbank Electronic Payment System (SPEI), which led several banks operate under a "contingency" program, which generates a delay in electronic transfers.”[17] With this event, not only were the transactions delayed, also represented a risk to confidence of foreign investors in Mexico.

LEGAL ASPECTS OF CYBER WARFARE

First of all it is necessary to mention that "the law of war is divided in two principal areas, “jus ad bellum” and “jus in bello.” Jus ad bellum , also know as the law of conflict management, is the legal regime governing the transition from peace to war. Jus in bello, also know as the law of armed conflict, governs the actual use of force during war."[18] In this case the cyber warfare and specifically “whether states can respond to cyber attacks with active defenses predominantly falls under “jus ad bellum.”[19] The regulation or establishment of laws to reduce and punish cyber attacks are ambiguous, “the nature of cyber operations raises difficulties for the criminal law approaches to accountability used in ad hoc tribunals and the International Criminal

[17] Alleged 'hacking' of Banxico's payment system hits operation, Date April 30, 2018. http://www.elfinanciero.com.mx/economia/pagos-electronicos-presentarian-lentitud-tras-ciberataque-bancos.

[18] Carr, Jeffrey. *“Mapping the cyber underworld Inside Cyber Warfare”* O’ Reilly Media, United States of America 2010. p 48.

[19] Ibid.

Court (ICC)."[20] NATO, during the Prague conference in 2002, decided to launch a global program to coordinate cyberdefense, with the aim of strengthening the capabilities of the Alliance and fighting computer attacks. It was not until after the events in Estonia (2007), when it was decided to work with the aim of defining a new strategic concept of cyber defense policy, which was the result of the Lisbon Summit (2010). "NATO acknowledged the new threat in its 2010 Strategic Concept , wherein it committed itself to develop further our ability to prevent, detect, defend against and recover from cyber attacks, including by using NATO planning process."[21]

The cyber war presents a new field for the Laws of armed conflicts (LOAC), due to the complexity that this type of war represents. However it is worrisome in the "ideal world" to convince the leaders of the States and authorities that have an influence on this issue to raise awareness of the human, material and economic damages represented by employing these new cyber threats.

U.S. CYBER WARFARE ENVIRONMENT

United States of America has high risk of being a victim of cyber attacks because it is the world's leading power, taking into account that technology is developing at an amazing rate and "new generations of products are being released every six to nine months. Several things, however, are clear: information systems are steadily becoming a more critical aspect of the

[20] Reveron, Derek S. *"Cyber space and National Security"* Threats, Opportunities and power in a virtual world. Georgetown University Press, United States of America 2012. p 82.

[21] Schmitt, Michael N. *"Tallinn Manual on The International Law applicable to Cyber Warfare"* prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States of America 2013. p 17.

American economy, government, and national security at every level,"[22] also by the capacity that the United States has in the manufacturing in military technological development and in the field of National Aeronautics and Space Administration (NASA) which is US government agency responsible for the civil space program, as well as aeronautical and aerospace research.

The need of United States to deter cyber warfare has increased as technology advances and the economic and military power of this country is confirmed as a center of gravity, tools that the US uses to establish its hegemony in comparison with other countries and public opinion, "cyber warfare is a major avenue of attack against the United States and has done significant damage to its national security interests, to the interests of allies, as well as to other states in international politics."[23] Some of cyber attacks on United States Defense Department focus on military computers system to obtain sensitive military information and produce serious damage were "launched from are training centers operated by governments, including Russia, China and Iraq. One example was a computer virus that invaded U.S. Marine Headquarters PCs on October 21, 1999."[24] Cyber warfare is here to stay and today is a new challenge to improve the response capabilities not only to United States, this new form of war represents an element of conflict to all countries especially those with technological development as well as power economic, political and military.

[22] Cordesman, Anthony H. *"Cyber-threats, Information warfare, and critical infrastructure protection"* Defending the U.S. Homeland, Center for Strategic and International Studies, Washington, D.C. Taylor and Francis group, United States of America 2002. p 2.

[23] Mazanec, Brian M. *"Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace"* Palgrave Mac MIllan, United States of America 2015. p 5.

[24] Dunnigan, James F. *"The Next War Zone"* Confronting the Global Threat of Cyberterrorism, Kensington Publishing Corp., United States of America 2002. p 86.

The current American perspective is that "over the last few years, US policymakers have become increasingly concerned about US vulnerability to cyber attacks. In 2009 President Obama warned of cyber threats to US national security and described cyber attacks that crippled Georgia during its conflict with Russia."[25] In 2010 Dennis Blair, US Director of National Intelligence, listed cyber attacks as a threats before than terrorism or even the wars in Iraq and Afghanistan, So, "in response to these growing threats, the Department of Defense created US Cyber Command in 2011, a military command on par with the regional combat commands,"[26] Its mission is the use of computer techniques with the objective of ensuring United States' interests or his allies. This includes the direct protection of computer systems, rapid response actions against attacks or even execute attacks to protect their interests.

It is interesting to mention that the experience of the United States in the field of cyber warfare is the result of a need for change and adaptability to face the threats of cyber attacks that can shake and destabilize its infrastructure and power. Representing this change in first term as a reaction to cyber danger and later as a proactive and anticipatory procedure to take advantage of the cybernetic enemy.

MILITARY'S ROLE IN CYBER WARFARE

The constant changes in the operating environments and learn lessons through the wars have motivated the armed forces to make modifications to their military doctrine, "foreign nations have begun to include information warfare in their military doctrine, as well as their war college curricula, with respect to both defensive and offensive applications. They are developing

[25] Reveron, Derek S. *"Cyber space and National Security"* Threats, Opportunities and power in a virtual world. Georgetown University Press, United States of America 2012. p 89.

[26] Ibid p. 90.

strategies and tools to conduct information attacks."[27] Mainly the Armed Forces of Russia, China and the United States have included the cyber war in their military doctrine; however of these countries Russia "has been the most active country in its implementation of cyber attacks against its adversaries, which include Chechnya, Kyrgyzstan, Estonia, Lithuania, Georgia, and Ingushetia."[28] Russia started its cybernetic activities in the 1980s and has carried out a variety of cyber attacks as they are logic bombs, viruses, microchipping and other ways of weaponized malware.[29]

Based on its experience and, United States is the country that has produced more information on how the cybernetic war is conducted, the cyberspace domain "was originally defined by the U.S. Department of Defense in 2000 as the notional environment in which digitized information is communicated over computer networks,"[30] however, the increase in technology applied to all areas has led to the updating of doctrine, so the new military definition of cyberspace is "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including internet, telecommunications networks, computer systems, and embedded processes and controllers,"[31] this concept includes smartphones, tablets, internet services and computer resources that today are part of our life routine.

[27] Carr, Jeffrey. *"Mapping the cyber underworld Inside Cyber Warfare"* O' Reilly Media, United States of America 2010. p 161.

[28] Ibid.

[29] Ibid.

[30] Mazanec, Brian M. *"Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace"* Palgrave Mac MIllan, United States of America 2015. p 13.

[31] Mazanec, Brian M. *"Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace"* Palgrave Mac MIllan, United States of America 2015. p 13.

The conditions of air superiority and defense system with electronically controlled missiles are users of technology for effective and successful missions, "this utilization of cyberpower enhances our hard power capabilities and defines the attributes of the network to support these operations."[32] As well as in expeditionary operations, especially in stabilization operations against insurgent and terrorist groups, military personnel are exposed to cyber risks in their communication systems, combat aircraft and defense systems controlled through computer systems and networks. It is necessary to adopt measures that reduce these risks, which can be the acquisition of defensive software for cyber attacks and that the staff knows how to use them effectively.

CONCLUSIONS

Nowadays cyber attacks represent one of the greatest threats to global security taking into account that the damage caused by these attacks have the same magnitudes as conventional weapons, but one difference that cyber weapons can be manipulated by only one person from a computer. Based on the nature of these attacks and considering the difficulty in pointing out the perpetrators of cyber attacks, it would be an extraordinary solution for States to work together within International organizations and through diplomatic relations establish prohibitions and sanctions to those who make use of cyber warfare. In other words cyber needs to be analyzed and reviewed with an International framework and International consequences in mind.

[32] Kramer Franklin D. *"Cyber power and National Security"* Center of technology and National Security Police, National Defense University Press, Unites States of America 2016. p 307.

The educational field is important in the cyber war, because the students graduates of universities in computer's science who got a lot of knowledge in the field of networks and computer systems, is possible that they will be recruited by groups of hackers as technical experts in computing, is for this reason that level of cyber warfare will get high level.

Taking into account the evolution of technology, it is necessary for the Armed Forces to be updated and have enough capability to adapt in defensive cyber technological resources and apply in land, air and sea military power focus on tactical and operational levels to reduce risks of cyber attacks, as well as to train permanently at all command levels on this subject. On the other hand, the States and agencies responsible for the administration of a country should consider in their budget resources to face cyber war through defensive actions supported by updated software and protected from malwares and computer viruses, to reduce and avoid cyber attacks on their industrial, commercial, financial infrastructure and defense systems, as well as its Armed Forces.

Computer malwares and viruses are bought and sold as tools and weapons of cyber attacks. So it is vital to carry out military intelligence and information operations in coordination with civil security departments to reduce and neutralize these activities, establishing as main objective to focus on knowing the location of the places where viruses and malwares are created as well as their destruction before they are distributed.

BIBLIOGRAPHY

Carr, Jeffrey. “Mapping the cyber underworld Inside Cyber Warfare” O’ Reilly Media, United States of America 2010.

Cordesman, Anthony H. “Cyber-threats, Information warfare, and critical infrastructure protection” Defending the U.S. Homeland, Center for Strategic and International Studies, Washington, D.C. Taylor and Francis group, United States of America 2002.

Dunnigan, James F. “The Next War Zone” Confronting the Global Threat of Cyberterrorism, Kensington Publishing Corp., United States of America 2002.

Karatzogianni, Athina. “Cyber conflict and global politics” Taylor and Francis group, United States of America 2009.

Kramer Franklin D. “Cyber power and National Security” Center of technology and National Security Police, National Defense University Press, Unites States of America 2016.

Lowther, Adam B. “Conflict and cooperation in Cyberspace, The challenge to National Security” Taylor and Francis group, United States of America 2014.

Mazanec, Brian M. “Deterring Cyber Warfare: Bolstering Strategic Stability in Cyberspace” Palgrave Mac MIllan, United States of America 2015.

Reveron, Derek S. “Cyber space and National Security” Threats, Opportunities and power in a virtual world. Georgetown University Press, United States of America 2012.

Schmitt, Michael N. “Tallinn Manual on The International Law applicable to Cyber Warfare” prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, United States of America 2013.

Alleged 'hacking' of Banxico's payment system hits operation, Date April 30, 2018. http://www.elfinanciero.com.mx/economia/pagos-electronicos-presentarian-lentitud-tras-ciberataque-bancos.

Malware (malicious software), https://searchsecurity.techtarget.com/definition/malware. November 2016.

“On This Day: Robert Tappan Morris Becomes First Hacker Prosecuted for Spreading Virus.” http://www.findingdulcinea.com/news/on-this-day/July-August-08/On-this-Day--Robert-Morris-Becomes-First-Hacker-Prosecuted-For-Spreading-Virus.html. date Jul 26, 2011.

“The Cost of Cyber Attacks to U.S. Economy.” By Jennifer Epstein and Shelly Hagan, February 20, 2018. https://www.insurancejournal.com/news/national/2018/02/20/481121.htm