emun

ESSARP MODEL
UNITED NATIONS

2018

GA1 – Implementing measures to combat Cyberwarfare

Index

Forum: GA1

Issue: Implementing measures to combat Cyberwarfare

Student Officers: Serena Maquirriain – Nicolás Urdín

Position: Student Officer

Introduction

Worldwide, Internet access has grown substantially since the creation of the World Wide Web in 1991, with 3.58 billion users having been registered in 2017 as opposed to the 1.38 billion 10 years earlier, owing in great part to the facilitation of computer access and the growing availability of smartphones.[1]Yet as more users connect to the Internet, there is a greater and more serious risk for the vulnerabilities of network systems to be exploited for malicious aims. For instance, in October 2016, hundreds of thousands of personal devices were infected with malware used to launch a cyberattack on some of the world's most popular websites.[2]

Cyberwarfare is the use of such attacks in cyber space for the purpose of advancing the political aims of a nation or state. It generally refers to a confrontation between states, though agents outside of militaries and intelligence services, such as terrorists or hacktivists, can also be involved in the disruption of a country's activities or in cyberespionage. This has been especially highlighted since the devastation of September 11, 2001, with an increase in awareness about the possibility of terrorists exploiting information systems' vulnerabilities. These non-state actors pose a unique threat given their lack of regard for law enforcement

[1] https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

[2] https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault

and their little need to adhere to diplomatic conventions, which renders the measures for deterrence that are usually applicable to States practically useless. Part of the complexity of cyber warfare is its lack of subjection to geopolitical borders.[3]

A cyber arms race has begun to develop as states realize the inexpensiveness of acquiring cyber weaponry for defensive and offensive purposes relative to spending billions of dollars to enter the group of nuclear capable nations, for example. It is not just superpowers at the forefront of technological developments such as the United States, China or Russia that are leading this escalation, but it is rather the participation of countries as diverse as Estonia, Belarus and Argentina that turns cyberwarfare into a phenomenon worthy of global concern. The situation becomes more pressing when considering that adversaries such as India and Pakistan have also invested in the acquisition of these new technologies.[4] So far, around 29 countries have established distinct military units for the development of offensive cyber capabilities, 49 have acquired off-the-shelf hacking software, and 63 engage in national or international surveillance of cyberspace.[5] It is generally estimated that cyberwarfare will continue to grow in the future, although its impact is difficult to measure owing to the fact that it primarily affects the access and distribution of information unlike traditional forms of warfare that have measurable physical effects.

These Issues have caused organizations to become more preoccupied about cyber security. Many have begun to detect the pitfalls and vulnerabilities in their current technologies and strategies and have begun to question if they are adequate in preventing future cyber-attacks.As the need to secure information assets increases, it must be acknowledged that more than simply investing in new technologies needs to be done.

[3] https://searchsecurity.techtarget.com/definition/cyberwarfare
[4] http://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/
[5] https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710

Definition of key-terms

CyberSpace

The US Department of Defense defines cyber space as “one of five interdependent domains, the others being the physical domains of air, land, maritime, and space.”[6] It is a global network that allows for online communication and exchange of data. All activities carried out in the virtual world are conducted within cyberspace.[7]

CyberWarfare

A number of definitions of cyber warfare have been proposed, although no single one has been adopted in international legal convention. Richard A. Clarke has defined it as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".

Another definition proposes two types of cyber warfare: strategic and operational. Strategic being "a campaign of cyberattacks one entity carries out on another", whilst operational cyber warfare "involves the use of cyberattacks on the other side’s military in the context of a physical war."Other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations.

Some of the definitions provided by international and governmental organizations are the following:

- NATO (North Atlantic Treaty Organization) defines it as, “a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal”
- The NIPC (National Infrastructure Protection Center) defines it as, “A criminal act perpetrated by the use of computers and telecommunications capabilities resulting in violence, destruction, and/or disruption of services to create fear

[6] http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf
[7] https://www.techopedia.com/definition/2493/cyberspace

by causing confusion and uncertainty within a given population conform to a political, social, or ideological agent."

- Lastly, the FBI (Federal Bureau of Investigation) defines it as, "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents".

Cyberpeace

It is the achievement of sustainable cyber security and the reduction of conflict and espionage in cyberspace through global cooperation, rather than simply an absence of attacks and security breaches.[8]Measures associated to the securing of cyberpeace include the development of new rules and norms for warfare, the building of secure infrastructures, the promotion of open source,the establishment of cyber security centers, the disclosure of vulnerabilities, disarmament, defensive security strategies, decentralization, education and the application of relevant tools and infrastructures, encryption and other cyberdefenses.

Hacktivism

Hacktivism involves the subversive use of computers and computer networks to promote a political or ideological agenda, and can potentially extend to attacks, theft and virtual sabotage that could be seen as cyberwarfare – or mistaken for it. Hacktivists use their knowledge and software tools to gain unauthorized access to computer systems they seek to manipulate or damage not for material gain or to cause widespread destruction, but to draw attention to their cause through well-publicized disruptions of select targets. Hacktivist groups are often portrayed in the media as cyber-terrorists, wreaking havoc by hacking websites, posting sensitive information about their victims, and threatening further attacks if their demands are not met.

[8] https://ndias.nd.edu/news-publications/ndias-quarterly/the-meaning-of-cyber-peace/

Deep/Dark Web

The term Deep Web refers to any and all information or data that is not accessible by conventional search engines such as Google and instead requires a specialized search engine such as TOR. Technically, the dark web is a series of interconnected systems, not indexed by search engines that can only be accessed by their creators or others with special privileges. This makes it the ideal terrain to become a cesspool for illegal acts and to harbor networks of criminal entities.

DoS and DDoS Attacks

In a Denial of Service Attack, the targeted system or network is overwhelmed by a heavy influx of online traffic that exceeds the amount of requests said platform can process, thus bringing it down. The difference between a DoS Attack and a Distributed Denial of Service (DDoS) Attack is that in the latter the attacker uses multiple computers (that have probably been infected with malware) to launch the offensive. The term "distributed" stems from the fact that they are using several computers for this purpose, rather than just one or two as in the case of the DoS Attack. They usually employ the use of botnets.[9]

BotNet Attacks

A Botnet is a network of computers that can be remotely controlled by an agent that has infected them with malware without their rightful owner's knowledge. This way, the command of computers performs identical operations that can be used to launch spam email campaigns, steal sensitive information and to carry forth DDoS attacks.[10]

[9] https://www.us-cert.gov/ncas/tips/ST04-015

[10] https://security.radware.com/ddos-knowledge-center/ddospedia/botnet/

General Overview

The cost of waging a cyber war

Cyber warfare continues to grow at an unprecedented level, and it is costly financially and diplomatically. In the United States, cyber attacks have increased by 27% in 2017 from the previous year. The cost associated with a cyber attack is largely dependent on the type of attack, the organization's size, its preparation and the country in which it is located (for instance, the cost of a breach in the US exceeds its cost in Brazil).[11]

The WannaCry cyber attack that disrupted over 300,000 computers in 150 countries and caused billions in losses is a prime example of the destructive potential of cyber weapons and of their misuse in particular. The United States has blamed North Korea for the attack given that it was traced back to a group of hackers sponsored by the North Korean government known as Lazarus Group, though it is suspected that the WannaCry worm was launched unintentionally while the code was being developed.

Escalation of conflict

The execution of a successful and proportional military response (whether in cyber or physical space) is a complex matter. It is generally agreed that retaliatory measures should be of equal impact to the original attack, though the intensity of cyberattacks is not so easily quantifiable or replicable. Another main problem arising from the growth of cyberspace as a platform for military and terrorist action is the difficulty in identifying the agent responsible for launching the offensive. Even if it is possible to trace the operation to a particular country, further evidence is needed to hold a national government accountable.Beyond that, cyberwarfare has far more unpredictable effects than other forms of conventional warfare. Even attacks designed to target specific, isolated networks can have unexpected consequences.

The aforementioned factors make the risk of war by miscalculation likely at an unprecedented level. The speed with which cyber attacks can be conducted creates an almost immediate need for a response. It is far easier to determine the culprit and intention behind an attack when a country is involved in a prolonged cyberwar with another State, yet

[11] https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2

overestimation of the threat, and the technological capabilities possessed by the offending agent can lead to States and other actors taking preemptive measures ranging from cyber attacks, to conventional and even nuclear warfare if the escalation allows it.

Impact on civilians

States often prefer Cyber warfare over direct military confrontation owing to the fact that it does not constitute such an overt declaration of war. It is perhaps less of a drastic method, as the physical destruction and loss of civilian life are significantly lower, but that is not to say that there is no collateral damage to such form of warfare. Common forms of cyber attacks, such as the targeting of enemy States' energy grids, have repercussions on civilians as electricity and IT systems are essential to keep the local infrastructure functioning. Besides, personal computers are also infected with malware during the process of conducting such a large-scale operation. This makes cyber warfare particularly problematic, as the laws of war indicate that collateral damage needs to be minimal relative to the attack and that non-combatant actors should not be targeted.

Despite the Internet's original purpose of fostering access to information and acting as a democratizing tool, weaponization of cyberspace is causing political instability, and manipulation of elections. The use of targeted propaganda, hacks against prominent political figures, the planting of malware and Trojans and cyber espionage are some of the most commonly employed methods of cyber warfare to influence political opinion and disrupt the actions of foreign governments. Russia is known for leading some of the largest scale destabilizing campaigns against its adversaries.Russia's first cyber offensive to influence political opinion was its cyber attacks against Estonia in 2007, following clashes over the relocation of a war memorial. Parliament, government departments, media broadcasters and financial institutions were brought down. Further attacks against German political institutions have been traced back to Russia since 2015. It is NATO and European Union members that are most commonly targeted by Russian cyber attacks whose influence on the politics of Western democracies is increasing.[12]

[12] https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/

Major parties involved and their views

United States of America

The USA is arguably the world's top superpower in terms of investment and development of defensive and offensive cyberwarfare capabilities. It is credited with counting with the most sophisticated and complex techniques in the realm of cyberwarfare.

It is accused of having destroyed Iranian power plants through the use of the Stuxnet worm in 2010. It has been made responsible for the surveillance of EU officers in 2010. It is also suspected of having attacked Gemalto, an European enterprise, in 2011.

China

China is known for using large-scale attacks that have the capability of inflicting great damage on their targets, though they are not especially notorious for doing so. It has been accused of data theft from Google Inc. in 2009, and of other American companies in 2013. It was further blamed for attacks on Britain and South Korea in 2010 and 2011 respectively. The official position of the Chinese government is of support towards cyber security and of opposition to militarization of cyberspace.[13] China has opposed the early classification of cyber weapons.[14]

Russia

Russia is known for employing both complex malware and simple techniques such as phishing. It develops its own software and acquires off the shelf cyber weapons as well. It has targeted Estonia in 2007, Georgia in 2008, and most recently Ukraine in 2015. The Russian government denies conducting any cyber attacks against other States and its official position is of support towards a legally binding UN convention on cyber security. It in has accepted the introduction of UN regulations to cyberspace.

[13] https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710

[14] https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

Israel

Israel possesses one of the world’s most developed cyber espionage agencies. It participated in the Stuxnet attack towards Iranian nuclear facilities in 2010 and subsequently continued to spy on its nuclear programme as far as 2015.

North Korea

North Korea is not as much of a threat in terms of technical capabilities as it is regarding its willingness to escalate tensions and destroy foreign information systems. It denies involvement in incidents such as the 2017 WannaCry cyber attack and considers accusations to be part of a smear campaign.

Iran

Iran’s government claims to count with cyber espionage capabilities. It poses a threat to cyber peace worldwide because of its offensive capabilities and willingness to utilize them. Its targets include Saudi Arabia in 2012 and the United States in 2013, when financial institutions were targeted via DoS attacks.

Timeline of important events/Documents

Events

- 1998: Moonlight Maze becomes the first state-sponsored case of cyber espionage after American government documents were found to have been stolen by a foreign agent (possibly Russia)[15]
- 1998: The Morris worm spreads across US information technology infrastructure. Robert Tapan Morris becomes the first person to be convicted under the US computer fraud and abuse act
- 2006: Spyware is found in the IT systems of the China Aerospace Science & Industry Corporation. Wikileaks is launched
- 2007: Estonian government services are temporarily shut down by DoS attacks following a row with Russia
- 2008:
  - Unknown foreign intruders hack the Republican and Democratic presidential campaigns in the United States of America
  - Georgia’s government websites are targeted by cyber attackers in apparent coordination with Russian military exercises
  - The State Bank of India is targeted by Pakistani hackers
- 2009: Israel suffers cyberattacks at the time of the Gaza Strip military offensive and blames Hamas or Hezbollah for ordering the hacks
- 2010: Iran and Indonesia are found to have been infected with Stuxnet by a foreign government possibly targeting the Iranian nuclear programme
- 2011: The Canadian and US governments are cyber attacked
- 2012: “Red October” is discovered to have been affecting European, Central Asian and North American governments since 2007
- 2013:

[15] http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/The%20United%20States%E2%80%99%20Cyber%20Warfare%20History%20Implications%20on.pdf

  - North Korea is accused of hacking South Korean financial and media services
  - NATO holds its first meeting dedicated to cyber security[16]
- 2014: An unidentified state-sponsored actor hacks 500 million Yahoo accounts
- 2015: Russian cyberattacks against Ukraine
- 2016: Russia’s hack and publication of Democratic National Committee emails influences the outcome of the US presidential election[17]
- 2017:
  - WannaCry ransomware attacks target private companies and government institutions worldwide by exploiting vulnerabilities leaked by a group of hackers[18]
  - NotPeya ransomware attack causes billions of dollars in damages. The USA and UK later blame Russia
- 2018: Trails against Facebook & Cambridge Analytica for leaking and selling personal information of users

Documents

- 2003: A/RES/57/239 “Creation of a global culture of cybersecurity”
- 2004: A/RES/58/199 “Creation of a global culture of cybersecurity and the protection of critical information infrastructures”

[16] https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm

[17] https://www.wired.com/2016/12/years-biggest-hacks-yahoo-dnc/

[18] https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html

UN involvement

The Global Cybersecurity Agenda (GCA) of the International Telecommunications Union (ITU) was launched with the objective of promoting cooperation and security in IT.[19] The UN has also introduced the Global Cybersecurity Index with the aim of quantifying countries' commitment to cyber security and raising awareness of the dangers to critical infrastructure posed by not addressing vulnerabilities in critical IT systems. It ranks countries according in terms of Legal Measures, Technical Measures, Organizational Measures and Capacity Building and Cooperation.[20]

The UN coordinated a summit with experts from the permanent members of the Security Council and 10 other cyberpowers in which it was agreed that all principles of international law are applicable in cyberspace, including the principles of State responsibility, territorial sovereignty and restriction to the use of force.[21]

The UN has been trying to implement meaningful guidelines on international cybersecurity for the better part of the last 15 years. There were two token resolutions passed in 2003 and 2004. Resolution 57/239 of 2003 calls for more awareness and responsibility by capable nations to prevent, detect, and respond to cybersecurity threats. Resolution 58/199 of 2004 invites member nations with national cybersecurity strategies to share and assist other member nations in their efforts to establish similar strategies. These resolutions are certainly optimistic, though it is unlikely that cyber warfare superpowers would assist their perceived enemies in bettering their cybersecurity infrastructure.

[19] https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

[20] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx

[21] https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

Possible Solutions

As mentioned above, the two resolutions presented in 2003 (A/RES/57/239) and again in 2004 (A/RES/58/199) took huge strides towards better security measures to prevent cyber attacks from happening, but still, there is much ground to cover.

Recommendations that can help both governmental and private actors abound. Most of these are directed at building defenses around their IT systems to minimize or eliminate damage inflicted by cyber attackers. Capacitating incident response teams is one of the most sensible defensive measures, as the costs and losses of a cyber attack are minimized with a faster response. The use of security analytics and cooperation and sharing of data on security breaches and vulnerabilities with other organizations can serve to make each other aware of possible threats. Segmenting networks is another viable cautionary measure given that in the event of a cyber attack against a centralized network, all data would be compromised.

Regarding security measures that can be undertaken by countries to propel their defenses individually, both state and non-state actors commonlyrecruitwhite hat hackers and programmers to break into their secure systems and "perfect" their software to avoid future breaks in. It would be advisable for international organizations to aid vulnerable states in the development of appropriate response systems.

A crucial solution would be the establishment of a universally accepted legal framework to regulate cyber warfare, given that no sufficiently specific international regulations are currently in place. Defining what constitutes cyber crime and terrorism, among other measures, would facilitate the prosecution of offending parties. Measures to prevent the proliferation of offensive cyber weapons should also be introduced.

Further operations against criminal networks in the deep web would be an advisable though ambitious feat.

List of Sources

- https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
- https://www.theguardian.com/technology/2016/oct/22/cyber-attack-hackers-weaponised-everyday-devices-with-malware-to-mount-assault
- https://searchsecurity.techtarget.com/definition/cyberwarfare
- http://foreignpolicy.com/2016/11/03/the-internet-of-things-is-a-cyber-war-nightmare/
- https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710
- http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12R.pdf
- https://www.techopedia.com/definition/2493/cyberspace
- https://security.radware.com/ddos-knowledge-center/ddospedia/botnet/
- https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710
- https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity
- http://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/The%20United%20States%E2%80%99%20Cyber%20Warfare%20History%20Implications%20on.pdf
- https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm
- https://www.wired.com/2016/12/years-biggest-hacks-yahoo-dnc/
- https://www.csoonline.com/article/3237324/cyber-attacks-espionage/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html
- https://www.reuters.com/article/us-usa-cyber-northkorea/u-s-blames-north-korea-for-wannacry-cyber-attack-idUSKBN1ED00Q
- https://www.ft.com/content/56dae748-af79-11e7-8076-0a4bdda92ca2
- https://www.weforum.org/agenda/2017/07/why-cyberattacks-could-be-war-crimes/
- https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/
- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/United-Nations-Launches-Global-Cybersecurity-Index.aspx
- https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Recommended Reading

- In-depth chronology of cyber warfare related incidents:
  - https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity

  - https://www.nato.int/docu/review/2013/Cyber/timeline/EN/index.htm
- Member state stances and actions:
  - https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710