Research report

BonaMUN

The First General Assembly

The prevention of cyber warfare

Ewoud Abspoel and Daksh Khanna

Introduction

Cyber warfare is becoming an increasing problem in the ever-digitalizing world. Cyber warfare is conducted against states or state-actors, but does not include the targeting of individuals, businesses or organizations. The first ever cyber warfare was conducted only as recent as 2007 on Estonia and was conducted by hackers of the Russian Federation.

Cyber warfare can be defined as 'computer- or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyber-espionage.' However, there has not yet been adapted one single international definition for cyber warfare by all Member States, which is crucial for the solving of the problem.

Cyber warfare is prominently classified in two categories: *cyber-espionage* and *cyber-sabotage,* often including cyber-attacks on the target. The first method is often used to obtain secret information from the targeted state. The second method is used to either temporarily disrupt or permanently damage computers or computer-controlled equipment.

The biggest difficulty faced in the solving of this issue is the tracking of (possible) attackers as it is quite easy to leave little to no trace on the internet.

Definition of Key Terms

Cyber-espionage: The obtaining of secret information from a targeted state through cyberspace.

Cyber-sabotage: Temporarily disrupting or permanently damaging computers or computer-controlled equipment through a cyber-attack.

Cyberspace: A term used to describe the virtual world, including the space where digital data is stored and all systems and devices connected to it.

Cyber warfare: Computer- or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyber-espionage.

Denial-of-service attack: A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Logic bomb: A piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met.

Rootkit: A collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that is not otherwise allowed.

Virus: A type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus.

General Overview

The prevention of cyber warfare is an issue that has just in the last decennium begun to become a problem to several countries. However, it is also an issue that is, together with technology, quickly evolving. What makes this problem so difficult to solve is that there are many ways a cyber attack can be carried out.

There are several attacks that can be put in to place to disrupt a system or device. For example a Denial-of-Service attack (DoS) can be easily planted, due to the low level of sophistication necessary for the implementation of such an attack. Furthermore there are viruses that replicate their own code into the device and hereby disrupt the system. Other malware that can be implemented is for example a rootkit or a logic bomb. Non-governmental attackers, as opposed to nations conducting cyber warfare, often use these methods. The methods of cyber-attacks conducted by states are often kept secret due to the controversial nature of these cyber attacks.

Although cyber warfare has not yet played a significant part in most conflicts, the danger of it must not be underestimated. Cyber warfare is just a recent development on the military field, but is quickly evolving and will become more and more important in conflicts to come. Therefore it is important to highlight the possible threats of cyber warfare and why it is so important to timely find a solution, before the issue escalates. Through cyber-espionage countries can obtain secret and sensitive information from another country and use it against them, without the countries knowledge. This might create unfair disadvantages for the subject of the attack. Cyber-sabotage would especially be harmful, as it effectively disrupts a system or device in place. In the modern-day world all big infrastructural systems are connected to an electronic device or system, creating the threat of a nationwide catastrophe if these systems are the subject of a cyber attack.

There comes a big uncertainty with the possibility of cyber attacks. Cyber warfare is comparatively easy to conduct, as one only needs a computer to carry out a cyber attack. This enlarges the inconsistency of the attacks. As a computer is easily accessible, any such attacks can be carried out whenever and wherever the attacker wants. What makes cyber warfare even more interesting for hackers is a low risk of getting caught. Due to the anonymity on the internet hackers can easily leave little to no traces after an attack. This presents difficulties for the possible tracking down of these attackers and the prevention of further attacks.

Major Parties Involved

China

China is rumored to have a ‘hacker army’, consisting of roughly 50.000-100.000 individuals. In 2009, China allegedly infiltrated the electrical grid in the U.S. and planted disruptive software. It has been accused of many more countries of the use of cyber-espionage and cyber-sabotage to obtain secret information, but the Chinese government has always denied those accusations. China itself is, compared to the USA, not subject to a lot of cyber attacks.

United States of America

The United States of America is the leading country in the prevention of cyber attacks, partially due to the fact that the United States of America is the country subject to most cyber attacks in the world. The National Security Agency (NSA) launched the United States Cyber Command (USCYBERCOM) in 2009 and is one of the ten unified commands of the United States Department of Defense.

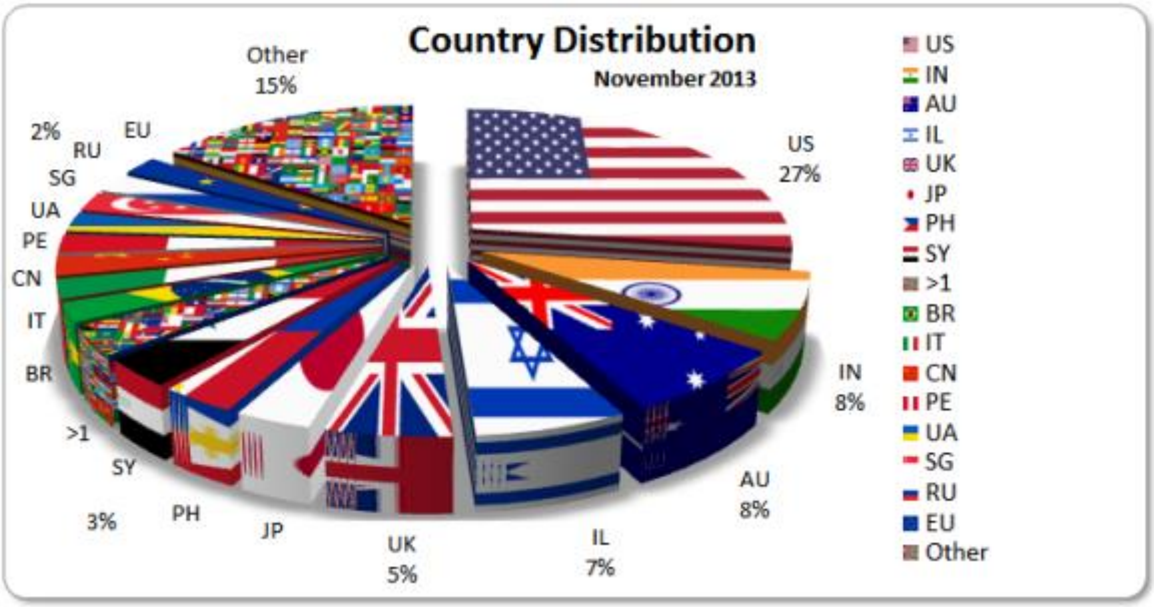
Estonia

As the first ever country to be subject to a cyber warfare attack, Estonia is now one of the leading experts in cyber defense. In 2010 Estonia created the National Cyber Defense League as a reaction to the earlier stated attacks. Furthermore it lead the proposition of the creation of the NATO Cooperative Cyber Defence Centre of Excellence, that plays a prominent part in the maintaining of cyber security around the world.

Russian Federation

The Russian Federation is infamous for having played a key role in several big cyber attacks, such as the first ever cyber attack on Estonian government servers, and maybe even more important, the alleged rigging of the 2016 U.S. Presidential election. Although it is rumored that the Russian Federation is behind a lot of cyber attacks, the country itself is not subject to a lot of cyber attacks compared to other major parties such as the United States.

Further countries that play a big role in this issue are Iran and North Korea.



This chart shows the distribution of received cyber-attacks per country in September 2013.

Timeline of Key Events

2007 – First ever cyber warfare-attack conducted on Estonia by Russian hackers

2010 – Stuxnet, a piece of malware, was found in Iran, leading to speculations that it was a cyber weapon aimed at the Iranian nuclear programme

2013 – First ever meeting of the NATO focused on cyber defense, and launches the NATO Computer Incident Response Capability (NCIRC) programme, as to better protect its networks against cyber attacks.

2016 – Alleged interference of Russian hackers in the 2016 U.S. elections

2018 – Secretary General Antonio Guterres calls for global rules to minimize the impact of cyber warfare on civilians

Previous Attempts to Resolve the Issue

As this is an issue that has just recently developed, there are not many previous attempts made to resolve the issue. However, this does make the solving of this issue all the more pressuring.

The NATO Cooperative Cyber Defense Centre of Excellence was founded in 2008, after being proposed as a concept by Estonia. It continues to be a world-leading center on the field of cyber defense and security. They carry out their mission through education, research and development, lessons learned and consultation. Their mission is to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence. The "Tallinn Manual

2.0 on the International Law Applicable to Cyber Operations", created by nineteen international law experts, is an influential resource, including a most comprehensive analysis on how the international laws created in a pre-cyber era apply to cyberspace.

Former UN Secretary General Ban-Ki Moon issued a report on the developments in the field of information and telecommunications in the context of international security in 2013. It was written to carry out a mandate from the General Assembly to "study possible cooperative measures in addressing existing and potential threats" related to the use electronic devices. It recommended the implementation of international laws regulating the behavior of countries in cyberspace. This forms an important milestone in the combat against cyber warfare, as it forces the UN to recognize the ever-growing threat of cyber warfare. However, this report does not implement binding agreements and forms only guidelines for the Member States how to behave in cyberspace.

Possible Solutions

To find any possible solutions for his problem, one must look at the problem from two points. First, one has to avoid a cyber attack by preventing the carrying out of such an attack. Second, if such an attack is carried out, the necessary security measures need to be taken in order to minimize the effect of the attack.

But before this problem can be solved, all Member States need to reach a common definition of 'cyber warfare', in order to effectively prevent it.

To prevent cyber warfare between nations, international laws need to be put in place. Furthermore sanctions can be placed on a country found guilty of cyber warfare and the UN can put an international tribunal in place to carry out the legal process of convicting countries of cyber crimes. Furthermore it is useful to put a database in place in which all detected hackers and cyber attacks are registered, so the monitoring and possible tracking of hackers is easier, and it is easier to prevent a next attack. Catalog all the tools, techniques and methods of attack used by hackers in previous campaigns and use this information to guard against future attacks. If you want to know how a hacker thinks, use an ethical hacker, either hired or trained by the government, to easily detect an attack and what specific attack is carried out. There needs to come a binding treaty for all Member States stating rules and guidelines for behavior in cyber space. This can only be obtained through international cooperation.

Appendices

- https://ccdcoe.org
- https://www.un.org/press/en/2014/gadis3512.doc.htm
- https://www.un.org/press/en/2018/sgsm18900.doc.htm
- https://gra.com/united-nations-cyber-warfare/

- https://www.cfr.org/blog/un-secretary-generals-call-regulating-cyberwar-raises-more-questions-answers

Bibliography

- Silverman, Jacob. “Could Hackers Devastate the U.S. Economy?” HowStuffWorks, HowStuffWorks, 25 June 2007, computer.howstuffworks.com/die-hard-hacker1.htm.
- Rouse, Margaret. “What Is Cyberwarfare? - Definition from WhatIs.com.” SearchSecurity, TechTarget, 20 May 2010, searchsecurity.techtarget.com/definition/cyberwarfare.
- “What Is Cyber Espionage? | Cyber Espionage Definition.” Carbon Black, Carbon Black, www.carbonblack.com/resources/definitions/what-is-cyber-espionage/.
- ““WHAT IS A DENIAL OF SERVICE ATTACK (DoS)?” What Is Cybersecurity? - Palo Alto Networks, Palo Alto Networks, www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos.
- Armendariz, Tommy. “What Is a Logic Bomb?” Lifewire, Lifewire, 23 June 2018, www.lifewire.com/what-is-a-logic-bomb-153072.
- Rootkit: What Is a Rootkit?” Veracode, Veracode, 26 Jan. 2018, www.veracode.com/security/rootkit.
- Li, Zoe. “What We Know about China's Shadowy Army Unit 61398.” CNN, Cable News Network, 20 May 2014, edition.cnn.com/2014/05/20/world/asia/china-unit-61398/index.html.
- NATO. “The History of Cyber Attacks - a Timeline.” NATO, NATO, www.nato.int/docu/review/2013/cyber/timeline/en/index.htm.
- Khalip, Andrei. “U.N. Chief Urges Global Rules for Cyber Warfare.” Reuters, Thomson Reuters, 19 Feb. 2018, www.reuters.com/article/us-un-guterres-cyber/u-n-chief-urges-global-rules-for-cyber-warfare-idUSKCN1G31Q4.
- “Arms Control Today.” Nonproliferation Benefits of India Deal Remain Elusive | Arms Control Association, 4 Sept. 2013, www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity.
- Mars, Santa. “September 2013 Cyber Attacks Statistics.” 2012 Cyber Attacks Statistics, cyber-imformation.blogspot.com/2013/11/september-2013-cyber-attacks-statistics.html.
- Harding, Luke. “What We Know about Russia's Interference in the US Election.” The Guardian, Guardian News and Media, 16 Dec. 2016, www.theguardian.com/us-news/2016/dec/16/qa-russian-hackers-vladimir-putin-donald-trump-us-presidential-election.