Research Report

General Assembly
First Committee (International Security and Disarmament)

Measures to prevent cyber warfare attacks and information warfare

MUNISH

Please think about the environment and do not print this research report unless absolutely

Forum	GA1
Issue:	Measures to prevent cyber warfare attacks and information warfare
Student Officer:	Philipp Hälsig
Position:	Chair

Introduction

In 2013, cyber warfare is regarded as a bigger threat to the United States of America (USA) than terrorist organization such as Al-Qaeda by many intelligence officials. This is the highest ranking cyber warfare has ever received in the USA and is also considered a big threat for every other country. Many millions of documents are stored digitally by governments. However, this kind of storage is not entirely safe and unlike real physical storages, the geographical obstacle for enemies which are trying to obtain access to the data is gone. This is known to all nations. While all of them try to find new security systems to seal their information as well as possible, most of them are also trying to find new ways how to bypass these security measures of other countries to collect information.

India observed a little more than 20 security breaches in 2004 but in 2011 there were more than 13,000. Cyber warfare is already going on and it's not always performed by governments but also by hackers or non-state actors, which is an additional problem for governments as the amount of people that know how to hack other networks is very high and steadily increasing. The only tool required is a computer which billions of people have. Just recently, large systems by the USA and the United Kingdom (UK) have been exposed which have the objective of spying millions of people by hacking into communication networks. The question has been raised to what amount such activities are still in order and when it can be called cyber or information warfare. The problem of cyber warfare and information warfare is one of today's world problems and has already started and therefore security measures should be taken as fast as possible.

Definition of Key Terms

Cyber warfare

The term describes any conflict between two entities which takes place in the cyberspace and involves hacking. It includes any political motivated attacks on technical devices where (classified) data is stolen, altered or deleted, websites are disabled or essential systems and services are disabled or corrupted. This can go as far as to manipulate the power grid of a region and possibly even disable it. Cyber warfare does not necessarily have to be a state vs. state conflict, but can also be started by non-state actors. However, an international definition still has to be agreed on.

Information Warfare

Information warfare (IW) is very similar to psychological warfare and involves the pursuit of collecting or manipulating information and using this to gain an advantage over the enemy. It includes propaganda, the manipulation of media in favor of oneself, hacking enemy communication networks or even changing numbers in stock markets. Information warfare is very similar to psychological warfare, only with the specific manipulation of information. This concept has been established and is mainly used by the United States. If IW is combined with a heavy use of technology, it can extend to cyber warfare. A term used more often by other nations is information operation, which is broader and focuses more on human related information instead military or other classified information.

Cyberspace

Cyberspace is a term for the virtual world, the space where all digital data is stored and basically refers to the internet and all devices and systems adjacent to it, which makes it a very large network.

Computer Crimes

Crimes which happen in the cyberspace or with the use of the cyberspace are regarded as computer crimes (also referred to as cybercrimes). They include mainly crimes performed by individuals or groups such as hacking, phishing, frauds or spam. Cyber warfare and information warfare however, can also be regarded as computer crimes though this has not been defined yet.

General Overview

Cyber warfare and information warfare does not particularly mean war between two countries. One country might just want to steal data because they need information on certain citizens, organization or something else which the government doesn't want to hand over. On the other hand, a country can also inflict great damage with the same resources by hacking and manipulating the correct structures. All states should be very careful with cyber attacks as they can lead to greater conflicts. At the same time, all states should take measures to prevent these attacks in first place. But in order to establish effective measures, one has to understand the reason and methods of cyber attacks first.

Information warfare

Information warfare is, as the name already says, based on the use of information against the enemy. In case of a conflict, whether it is just a pre-conflict situation or a war, it is obvious that states try to steal information of the enemy concerning whatever the conflict is about. This can include information on military bases or other numbers which can be of good use when trying to imagine how strong the enemy is and what he is capable of. Another likely case is that a state manipulates information which is given to the enemy or has altered its own data and numbers so in case the enemy tries to steal information they will only get wrong information.

But IW includes much more than just stealing or manipulating important information. It is also about the use of information in order to demoralize the enemy or their civilians. This is very similar to psychological warfare which involves using the media to influence a certain target group very subtly. A conflict is always driven by something, a source of power or strength which makes both sides fight each other. This source can be everything such as simple hate against the other country. If one side achieves to destroy the motivation of the enemy, then the conflict can be ended quite quickly. The correct use of IW or psychological warfare can achieve exactly this but IW also has the power to make the civilians of the enemy stand up against their government or leaders. For example, if one side somehow obtains classified information from the other side, not necessarily having anything to do with the conflict, which can be harmful, shocking or very controversial, they could choose to publish it (anonymously) and might cause unrest in the country of the enemy. This would weaken the country and give a huge advantage to the other country. And this is only one example on how to use IW to manipulate a conflict and to weaken the enemy.

Cyber warfare

For many years cyber warfare has been a possible threat but it still hasn’t caused or played an important role in a conflict. Others say cyber warfare is not part of a conflict but a competition which has already started. This might be due to the fact there hasn’t been any major conflicts between powerful nations but it is more likely due to the fact that it can stay hidden if done correctly. Because in contrary to physically stealing information, with the help of computer and the internet you can simply look at any document from the other side of the world and make copies without leaving any traces. And even though cyber attacks, once spotted, can be traced back, hackers often hijack computers of civilians remotely from which they then launch the attack. Or in other cases governments may have paid cyber criminals to perform these attacks in order to destroy any possibility it could be trace back to them. One way to prevent these attacks or rather use them against whoever tries to steal the information has first been demonstrated in 1982. Soviet spies stole software from a Canadian firm which regulates oil pipelines. The Central Intelligence Agency (CIA) had manipulated the software however, which would lead to overpressure after a few years. The CIA and the Canadian firm were aware of this and knew that they would have to reset the program. In Siberia though, it lead to a huge explosion which was only indirectly caused by the USA but is the result of cyber attacks by the Soviet Union. These are called logic bombs and can be very effective and dangerous.

Other cyber attacks are aimed at causing disorder and chaos, which is very similar to cyber terrorism. Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, which send a very large number of data packets to the victim until the security measures drop, are used to make certain networks or websites unavailable for their intended users or not at all. Such attacks are of coursed intended to receive attention by the media or government and are often used by non-state actors, such as the organization Anonymous, which want to send a message or express their opinion about a certain topic. Another method of cyber warfare which can cause serious damage, possibly even deaths, and will very likely lead to a very serious conflict is sabotaging or manipulating important infrastructural networks. This could be the electrical grid, banks, stock exchange market and even small things like traffic lights. Because they are all organized by automated computer programs, it is also possible to hack them and alter them. The consequences would be catastrophic. Many specialists also expect a cyber war much more disastrous than many previous wars. The loss of lives might be less at first, though a long term disabled electrical grid and communication network will lead to chaos and might lead to great problems for the civilians and the manipulation of nuclear reactors or oil pipelines can also lead to a giant loss of innocent civilian’s lives. Because the geographical limitations have been overcome a cyber war can start very fast or, if the enemy is unprepared, cause a lot of damage in a few hours or even less. The possibilities are endless and fearsome and can be regarded as one of the most damaging and catastrophic kind of war after a nuclear war.

Major Parties Involved and Their Views

United States of America

The United States are one of the most advanced countries regarding technology but also in regards of measures to prevent cyber attacks. In 2009 they have established United States Cyber Command which is aims to not only prevent any attacks against the USA but also to research all possibilities of cyberspace and in a few cases also commit cyber attacks against other governments or networks. It is reported that the USA has used cyber warfare and information warfare in Afghanistan in order to gain an advantage but there have also been other reports about cyber attacks against China, Iran and possibly many more countries. The government of the USA has warned companies and agencies in 2010 about the threat of cyber attacks mainly originating from China and Obama stated that one trillion dollars were lost in 2009 to cyber attacks.

China

China is said to have the biggest cyber army in the world with many more additional hackers that can be hired. The goal of the Chinese government is to win cyber and information warfare halfway around the 21st century. It is also reported that most cyber attacks against other countries, news agencies or other companies in the recent years have originated from China even though the Chinese government has always denied to have played any role in such events. But also China is victim of an increasing number of cyber attacks especially because of their very large networks such as the network of the University of Beijing which is a gateway to many other smaller networks.

Timeline of Events

Date	Description of event
1998	The US hacked into the Serbian Air Defence System and disabled it in order to bom Serbian targets.

April 2007

A botnet in Estiona infected thousands of computers and caused many websites to malfunction as well as banks or ministries. The attack mainly originated from Russia and might be motivated by the tensions between the countries.

February 16th 2010 The United States launched Cyber ShockWave, an experiment simulating a possible cyber war in order to evaluate whether the US could withstand such an attack.

September 2010 The Stutnex malware (software programmed to harm or sabotage other software) infiltrated many facilities in Iran, also the nuclear enchrichment facilities. It is the most advanced malware discovered until today which is why it is believed that the attack was supported by a government.

March 2013 The probably biggest cyber attack in history took place against a company called Spamhaus. They have been victim of a DDoS attack, six times larger than normal attacks against banks which even could've succesfully disable government security measures, with the result of the entire internet slowing down.

Evaluation of Previous Attempts to Resolve the Issue

There have been several attempts to take effective measures against cyber attacks but none have been successful on international base. For example, in 2011 the Shanghai Cooperation Organization proposed to the UN the "International code of conduct for information security" which did not pass because it enabled to much internet censorship according to many western countries. Another measure taken by the US and Russia is the establishment of a cyberwar-hotline which should be used in ciris situation to prevent an accidential cyberwar. This might not prevent any cyber attacks but it is certainly an important step because as mentioned, cyber attacks can be commited through other computers which could lead to tensions between to countries caused by someone else.

In order to effectively prepare for a possible cyberwar the USA has launched a simulation called Cyber ShockWave in 2010 which simulate the situation as realistic as possible. The results were shocking and showed that the USA isn't prepared for such attacks, especially not if they would be attacked by surprise. Similar simulations have been conducted before by the USA. They have proved very efficient as it showed in which aspects the USA was unprepared and in which aspects they were.

Possible Solutions

Because the whole issue of cyberspace and the problems and damage it can cause is quite new and is still on the rise, many things have not yet been internationally agreed on and many states take different measures. Cyber attacks can be prevented with two different types of measures: The first type intending to prevent states from carrying out cyber attacks and the second type being measures to increase security of the networks which have the highest risked of being attacked. Most states have laws regulating computer crimes done by individuals or non-state actors to hopefully prevent any cyber attacks but other states are not bound to any rules yet. They would only have to be aware of the reaction of the attacked country. Besides definitions of cyber warfare and information warfare and other important terms, an internationally agreed list of computer crimes or rules should therefore be established, maybe in combination with an organization monitoring the cyberspace, with large and serious consequences against states violating these rules.

Each state should increase its own security measures against cyber attacks. In order to do this as effectively as possible governments should establish, if not yet done so, an agency whose solely focus is on the cyberspace and cyber attacks. Moreover they should follow the example of the USA and conduct simulations on a regular basis, maybe even in cooperation with other countries, in order to analyze their current security measures. Once they have done that, they will have a bigger insight into the strength of their security measures and should try to strengthen the most vulnerable parts. It is important to notice, that many internet networks are all connected to a big network which is like the gateway to the whole internet. These are in most cases not managed by the governments but by large technological companies or universities. Governments should hence support these companies and organizations financially to protect their network as well as possible. If these gateways are protected well, then a large number of cyber attacks can be stopped and the government, banks, companies and all other entities threatned could handle the few remaining attacks more easily. However, the strength of a security system is not always the most important part as the potential strength of attacks is steadily growing, sometimes it’s more important to take different measures. Two very controversial ideas are the kill switch and the electrical wall. The kill switch could shut down the internet of certain areas, whether it is only concerning a company, a city or a whole country, in case of serious cyber attacks. The electrical wall intends to inspect every data package coming into the country’s network and compare it to known signatures and in case of a match do not let them through. Both these ideas can be very useful and even save lives, however, if used by the wrong person or government, they can violate basic human rights by censoring certain parts of the internet.

Therefore such measures have to be evaluated very carefully and include certain restrictions. In general all states should consider their possibilities with care as the internet is a symbol for freedom and a state interfering with the internet could lead to protest of the civilians. Because the internet connects everyone worldwide, each state is equally affected. Cooperations between countries and international agreements could therefore prove very useful leaving only non-state actors as a possible cyber threat.

Bibliography

"Cyberwarfare." *Wikipedia*. Wikimedia Foundation, Web. 30 June 2013. <https://en.wikipedia.org/wiki/Cyberwarfare>.

"USCYBERCOM." *USCYBERCOM*. Web. 30 June 2013. http://www.arcyber.army.mil/org-uscc.html

"Cyberspace." *Wikipedia*. Wikimedia Foundation, Web. 30 June 2013. https://en.wikipedia.org/wiki/Cyberspace

Dilanian, Ken. "Cyber-attacks a Bigger Threat than Al Qaeda, Officials Say." ***Los Angeles Times*****. Los Angeles Times, 12 Mar. 2013. Web. 30 June 2013. http://articles.latimes.com/2013/mar/12/world/la-fg-worldwide-threats-20130313**

"Computer Crime." *Wikipedia*. Wikimedia Foundation, Web. 30 June 2013. https://en.wikipedia.org/wiki/Computer_crime

"Cyberwar - The Threat from the Internet." ***The Economist*****. 1 July 2010. Web. 30 June 2013. http://www.economist.com/node/16481504**

"War in the Fifth Domain." ***The Economist*****. 1 July 2010. Web. 30 June 2013. http://www.economist.com/node/16478792**

McCullagh, Declan. "U.S. Military Cyberwar: What's Off-limits?" *CNET News*. CBS Interactive, 29 July 2010. Web. 30 June 2013. http://news.cnet.com/8301-31921_3-20012121-281.html

"Cyber ShockWave." *Wikipedia*. Wikimedia Foundation, Web. 30 June 2013. https://en.wikipedia.org/wiki/Cyber_ShockWave

"Cyberwarfare." *What Is ?* Web. 30 June 2013. http://searchsecurity.techtarget.com/definition/cyberwarfare

"Information Warfare." *Wikipedia*. Wikimedia Foundation, Web. 30 June 2013. http://en.wikipedia.org/wiki/Information_warfare

"5 Ways to Fight Back against Chinese Cyber Attacks." *The Week*. Web. 30 June 2013. http://theweek.com/article/index/243112/5-ways-to-fight-back-against-chinese-cyber-attacks

"Masters of the Cyber-universe." *The Economist*. 6 Apr. 2013. Web. 30 June 2013. http://www.economist.com/news/special-report/21574636-chinas-state-sponsored-hackers-are-ubiquitousand-totally-unabashed-masters

"Washington Free Beacon." *Washington Free Beacon Cyber War Details Revealed Comments*. Web. 30 June 2013. http://freebeacon.com/cyber-war-details-revealed/

US News. U.S.News & World Report, Web. 30 June 2013. http://www.usnews.com/debate-club/should-there-be-an-international-treaty-on-cyberwarfare

Lee, Dave. "Global Internet Slows after 'biggest Attack in History'" *BBC News*. BBC, 27 Mar. 2013. Web. 30 June 2013. <http://www.bbc.co.uk/news/technology-21954636>

Appendices

I. "Cyber Attacks: Prevention and Proactive Responses." *Practice Note*. Practical Law Company, 2011. Web. 30 June 2013. http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2-849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97-9f4fb1f58b36/CyberAttacksPreventionandProactiveResponses.pdf

This document focuses on possible prevention methods and how to react to cyber attacks. It has a focus on companies but the ideas and solutions given can also be used by states.

II. "Preventing and Defending against Cyber Attacks." George Washington University, Oct. 2011. Web. 30 June 2013. http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-057.pdf

Another document, similar to the first Appendix, with some more solutions and ideas on how to prevent cyber attacks created by the George Washington University.