Research Report | XXVIII Annual Session

Disarmament Committee

Combating the growing threat of cyber warfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Fede Everts
Paloma Mauries

Forum: Disarmament Committee

Issue: Combating the growing threat of cyber warfare

Student Officer: Fede Everts and Paloma Mauries

Position: President of Disarmament Committee

Introduction

Cyber attacks are a form of non-kinetic warfare that focuses on destabilizing countries through targeting civilian commercial entities. There was never a way to target such groups until the rise of technological advancements in the 20th and 21st century. Now with the help of technology this is far more prevalent and is an efficient way of sending a political statement or destabilizing a country. As technology and this specific form of warfare did not exist before there are fewer guidelines in place for such attacks.

Through the institution of protocols and other legal works the pressing issue of cyber warfare can be tackled. Focusing on ways to prevent cyber warfare from happening, reducing vulnerability to cyber attacks and minimizing damage after a cyber attack. These goals need to be addressed in order to deal with this issue. It is also important to highlight the importance of tackling the issue from the root cause, cyber attacks are made for reasons: military, civil, political etc. Ignoring the root cause of the problem will just cause the attack to take another form.

There have been several high profile cases of cyber attacks that have caused a lot of media coverage and hindered the attacked party. For example, in 2007 there were botnets that were sent that caused a massive wave of spam to an online bank and government related websites in Estonia. This caused a lot of confusion and eventually the loss of millions of dollars of equipment, this shows the terrible effect that cyber attacks can a have on a nation.

Definition of Key Terms

Cyber Warfare

Cyber warfare is the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information system for strategic or military purposes.

Cyber espionage

Cyber espionage is the use of computer networks to ultimately gain access or spy on confidential information, usually held by a government or other organization. These attacks are often subtle and hard to track. These attacks can result in damaged reputations, stolen data, which includes personal as well as private information.

Computer Crime

A computer crime is an act performed by a knowledgeable computer user, also known as a hacker, who browses or steals from company's or individuals private information. In some cases, this hacker will destroy or otherwise corrupt the computer or data files. Examples of such computer crimes could be considered fraud, espionage, phishing, scamming and many more.

Firewall

A firewall is hardware of software that is ultimately designed to prevent unwelcome or unauthorised access to a computer or network from another computer or network. Firewalls are created to keeps things at. For instance, the great firewall of China was made to control everything that is roaming through in the Internet in China.

Virus

A computer virus is created to continuously replicate itself, to cause immense damage to a computer or hard drive. Once a virus has been successfully downloads, the virus will not begin acting unless it has been activated. These viruses can be spread through email or text attachments, Internet downloads and many more. These viruses are highly dangerous and can cause serious damage.

Cyberspace

Cyberspace ultimately refers to the entire virtual computer world, and more specifically an electronic medium used to create a global network to allow for online

communication. Cyberspace allows anyone to share information, interact with one another, and swap ideas as well as many others in a global network.

General Overview

Cyber warfare are operations made to disrupt certain organizations or states in order to communicate a message or cause inconveniences. This can take up many forms, from cyber espionage, sabotage and propaganda. As the attack is targeting civil commercial entities the largest effect the attacks can cause is disruption to the system, however, it is an effective way of spreading propaganda and other messages. These attacks are made for a purpose, mostly to send a message or to protest certain things, which is effectively done through technological devices as it reaches wide audiences and had a more global effect on the target.

Cyber attacks have a strong tie with regards to the military; they often are paired with a military attack to destabilize the opposition more, or are done because of a military incentive. The Russian military operation in Georgia in 2008 in South Ossetia for example happened during a cyber attack on their government website. These attacks are used to destabilize a country even more, allowing them to make a more effective attack on the country.

Cyber warfare also has another face, that of “Hacktivism”. Organizations or groups to spread information use this form of computer crime; it is a form of activism. This means that there is no widespread destruction caused by this incentive of cyber warfare but do draw attention to the well-publicized targets of the disruption. This is where their activism comes forward. Even though this does not cause as much damage to software systems and other, it is a factor to keep in mind when addressing the issue of cyber safety.

Cyber warfare is a topic of research by many countries; since 2013 120 countries have done research into ways that they can develop tools to use the Internet as a weapon. Targeting financial markets, government websites and utilities. This is a growing problem that is becoming a lot more present, and pressing with the rise of electronics and the Internet. Even though there are organization sin place, such as Cyber peace, which attempts to resolve this issue there is still a long way to go. Surveillance technology to prevent the militarization of cyber technology is being put in place, without clear legal infrastructure no advancement can be made on this topic. This is a pressing issue that must be addressed, creating proper infrastructure and methods to deal with the issue of cyber warfare.

This complex issue can have major side effects economically and socially. The damage that it wreaks on infrastructure and economically are pressing and in developing countries especially, can be devastating. This is why such an important issue should be tackled in the disarmament committee. The attack can cause very costly damage, and the need for security to safeguard online databases can also be very expensive. For example on a cyber attack on Target in 2013, the company lost almost 70 million wroth of customers credit card information and other data. This also meant that target lost US$890 million in market value (Palmquist). Target, being a big company, could deal with the attack and put in place security improvements to stop it from happening again. But smaller companies and governmental organisations that are not as wealthy as Target, will suffer greatly economically. These organisations will not be able to recover as well as larger companies, like target, and they will also be less likely to be able to afford security measures. Following the attack Target spent $100 million dollars on improving their IT and security measures to prevent cyber attacks from happening again. This is not only Target but other companies as well. Annually $445 billion is spent on cybercrime (Palmquist). Many small organisations and businesses will simply not be able to afford this and will therefore be a lot more vulnerable.

Cyber attacks also have a large effect on countries' and organisations' infrastructure. For example an attack made on Ukraine in December of 2015 caused a power outage for up to six hours in some areas (Campbell). Sensitive data and information is not the only thing at stake with cyber crime, but infrastructure and the physical world of organisations are affected as well. Not only does cyber crime have a great effect economically but socially and politically these attacks can be destabilising and serious. This is why cyber attacks are often used for political incentive. This is a problem that the disarmament committee need to take care of in order to prevent devastating effects on organisations and companies that damage them both economically and politically.

Major Parties Involved

United States

In the past, the United States has been one of the main parties involved cyber warfare. As a major economy has been developed in the United States, the nation highly depends on the Internet, leading to the possibility of cyber attacks. The United States has invested large amounts of money in developing not just systems against cyber warfare attacks as well as their offensive techniques. In 2010, the United States began to step up its

focus on cyber warfare. The United States now openly announced the existence of their own cyber in their own national military.

China

In the past, China has had the biggest cyber military in the world and continues to add to this army. The “Chinese Information Operations and Information Warfare” includes this idea of “cyber warfare” which roughly has a hacker army of 50,000 to 100,000. In the past, large amounts of Western countries have accused China of cyber espionage. Nonetheless, The Chinese government continues to deny cyber warfare attacks. Tracking such affairs is nearly impossible due to the difficulty in tracking true identities in the cyberspace (Breene).

Israel

Israel continues to emerge as a cyber-powerhouse. Since the early days of Israel being a nation, technology has played a large role in the national security. In the past few years of technological advancements, cyber warfare continues to become more of a problem in the nation of Israel. It has grown to the point of becoming the nations biggest threat. To respond to this growing problem, Jerusalem must continue to revise the cyber security of the nation of Israel to avoid attacks as well as stay one of the more superior cyber nations around the globe. To this day, Israel is recognized as the globes leader in cyber abilities.

Russia

Alongside China and the United States, Russia is one of the most advanced and involved nations in cyber warfare. Similar to China, Russia denies all hacker attacks. Furthermore, in the past, Russia has used cyber attacks for offensive purposes. For instance, in 2014, the “Cyber Snake” program, which attacked the nation of Ukraine, coincidentally came from Russian origin.

Timeline of Key Events

Timeline of events in reverse chronological order leading up to present day.

Date	Description of Event
1979	The first hacker forum emerges, this is done through the medium of a crude electronic messaging board
1994	Vladimir Lenin leads a group of hackers, stealing millions of dollars from Citibank through tits dial-up wire transfer service

March 1999	Serbian hackers attack NATO systems after NATO's military intervention in Kosovo
May 1999	NATO accidentally bombs the Chinese embassy in Belgrade, this causes a large amount of cyber attacks to be directed to the US government websites from Chinese hackers
2003	A series of assaults are launched on US government computer systems that last years. This attack is code named Titan Rain and is eventually traced back to China.
April – May 2007	Hackers linked to the Russian government hack websites that are linked to Estonia's parliament, ministries, banks, broadcasters and newspapers.
June – July 2008	Hundred of government and corporate websites in Lithuania are hacked. The nature of the hacking denotes Russian nationalist hackers.
August 2008	Hackers hijack Georgia government and commercial websites during a military conflict with Russia.
January 2009	Half of Kyrgyzstan's internet servers are shut down due to hackers, after political disputes with Russia and Kyrgyzstan's political parties.
April 2009	A popular news website is closed down due to attack on Kazakhstan.
October 2009	The new US cyber command is scheduled to begin overseeing the protection of military networks from cyber threats.

Previous Attempts to Resolve the Issue

In the past, many attempts have been made to stop cyber warfare as whole, however, none have been as successful as needed. For instance, in December of 2010, the United Nations created a resolution which called for the, "technical assistance and training States to improve national legislation and build the capacity of national authorities in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms, and to enhance the security of computer networks". This resolution has given a good bases for nations to work on and build off of, however, not all nations are sticking to these principles.

Furthermore, in 2011 "the Shanghai Cooperation Organization" proposed a new code of conduct, which called for more Internet censorship and secrecy. Many western nations

turned against this planning ultimately making it fail. Nonetheless, many nations such as Germany are opting to lean towards “cyber peace”. For example, the German civil rights panel runs a campaign for cyber peace.

Possible Solutions

In the past, the United Nations has no set definition of what cyber warfare truly is. By defining such a term, nations would understand what cyber warfare truly is. Once the UN expresses cyber war to be on the same level as standard war, the UN will be able to take the necessary actions to end the threat of cyber war. To tackle such an issue, the entire United Nations as well as the globe must understand that such an issue is pressing and must be dealt with sooner rather than later, as it could lead to many countries to be destabilized and larger audiences being affected more easily.

Throughout this process, own member nations must call to increase their own security measures against such cyber attacks. Delegates could encourage governments to establish agencies with the main focus of to protect the nation against said cyber attacks. Furthermore, nations should meet routinely to discuss cyber warfare and keep each other up to date. These summits will lead to change, change that needs to be made. Ironically, the worst offenders of cyber warfare are permanent members in the United Nations Security Council, making it hard to make change. Many of the powerful nations in today’s world, such as the P5, continue to work on their own cyber security, however, continue to place their own attacks. Nonetheless, a creation of an emergency response team who would quickly detect acts of cyber attacks and report these to the correct correspondence would easily improve awareness and response to the problem of cyber attacks. This team could start the creation of an international black list with past and current major hackers and attackers. Although these are merely small ideas, the problem still lingers today and as the Internet continues to grow, it will not go away any time soon.

Bibliography

Baram, Gil. “Israeli Defense in the Age of Cyber War.” *Middle East Forum*, 1 Jan. 2017, www.meforum.org/articles/2016/israeli-defense-in-the-age-of-cyber-war.

Breene, Keith. "Who Are the Cyberwar Superpowers?" *World Economic Forum*, 4 May 2016, www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/.

"Cyberwarfare in China." *Wikipedia*, Wikimedia Foundation, 12 June 2018, en.wikipedia.org/wiki/Cyberwarfare_in_China.

"DefinedTerm: Cyber Security Key Words and Search Terms." *Defined Term*, definedterm.com/cyber_security_key_words_and_search_terms.

"Hacker Wallpaper." *Celebs Wallpaper*, Celebswallpaper, 2018, celebwallpapers.net/wp-content/uploads/2017/11/hacker-wallpaper-download-hacker-hd-x-wallpapers-of-hacker-wallpaper.png.

"What Is a Computer Virus?" *What Is A Computer Virus?*, us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html.

"What Is Computer Crime?" *Computer Hope*, 1 Apr. 2018, www.computerhope.com/jargon/c/compcrim.htm.

"What Is Cyberspace? - Definition from Techopedia." *Techopedia.com*, www.techopedia.com/definition/2493/cyberspace.