Research Report | XXVII Annual Session

GA1 – International Security and Disarmament

Implementing Measure to combat cyber warfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Kieran Schmidt-Das
Ron van der Horst

Forum: General Assembly 1

Issue: Implementing Measure to combat cyber warfare

Student Officer: Kieran Schmidt-Das

Position: Chair

Introduction

The use of technology has significantly increased in the digital era. Around 40% of the world's population has internet connection, and in 2014 3 billion people used the internet in one day (*Scientific America, 2017*). Furthermore, most nations rely on computers or networks to run their military systems, financial systems and energy systems. However the response to the growing threat of cyberwarfare is only just beginning. Therefore in 2010 the International Institute for Strategic Studies warned "We are now, in relation to the problem of cyber-warfare, at the same stage of intellectual development as we were in the 1950s in relation to possible nuclear war" (*International Institute for Strategic Studies, 2010*).

Cyber warfare can be defined as internet-based conflict caused by actions of a nation-state, non-state actor, terrorist group or company to penetrate a nation's computers or networks for the purpose of causing damage or disruption, due to a politically motivated aim. It is important to note that cyberwarfare targets a nation rather than an individual or a company, however the entity that is conducting cyber warfare does not have to be a nation. Cyberwarfare can be split into two categories, cyber attacks, during which there is immediate damage or disruption to a network or computer, and cyber espionage, where classified information is stolen from a nation state.

There have been a number of high-profile instances of cyber warfare, such as in 2007 when massive waves of spam were sent by botnets, sending large amounts of automated online requests to online bank, media and government services in Estonia, leading to widespread confusion as well as the loss of tens of millions of dollars of equipment, showing the very real impact that cyber warfare can have on a nation. A main issue with cyber warfare is that it is very difficult to establish who orchestrated an attack, as it is possible to completely hide yourself on the internet.

Definition of Key Terms

Botnets

A network of private computers infected with malicious software and controlled as a group without the owner's knowledge. In the case of cyber warfare they are usually used to flood nation's servers with automated online requests, leading the servers to shut down. (*SearchSecurity, 2017)*

Cyberspace

A term used to describe the virtual world, includes the space where digital data is stored, as well as all devices and systems connected to it. Cyberspace is close to infinitely large, with billions of computers making it up and with many billions of gigabytes of information stored on it.

Cyber warfare

Internet-based conflict caused by actions of a nation-state, non-state actor, terrorist group or company to penetrate a nation's computers or networks for the purpose of causing damage or disruption, due to a politically motivated aim. (*SearchSecurity, 2017)*

General Overview

According to a study by the UN Institute for Disarmament Research conducted in 2013, more than 40 states have developed military cyber capabilities, of which 12 have developed offensive cyber warfare software. Furthermore the number of cyber attacks on nation states is on the rise, in 2004 India observed 20 security breaches of its systems, however this figure rose to over 13,000 in 2011 (*UN Institute for Disarmament Research, 2013*), showing the increase in cyber warfare that is occurring in the world.

Technological background information

It is important to understand the different forms cyber warfare can take. Cyber espionage works through entities gaining access to information, through hacking into secure networks and copying the information. There are many different forms of cyber attacks, the most common are Denial-of-service (DoS) attacks. These work by using a botnet to send a very large data packet to a network until the security measures drop due to the high influx of information. This renders the service unavailable for all users, and is the strategy employed

in Estonia in 2007. This method of attack is usually favoured by non-governmental organisations such as Anonymous, due to the low level of sophistication required for such an attack. However these attacks do not work as well against high security networks, such as military networks, therefore they are rarely used by nation states. The methods used by nation states on both offensive and defensive cyber warfare are shrouded in secrecy due the critical nature of these methods.

Threats faced by cyber warfare

So far, cyber warfare has not played a significant part in most conflicts, whilst it has been used many times the overall loss of life or infrastructure from cyber warfare has remained low. However this should not downplay the significant threat that could occur due to cyber warfare. A first threat that can arise from cyber warfare, is that the nation that has been targeted may not be aware that it has been attacked. This would occur from cyber espionage, and would allow an entity to obtain sensitive information. Secondly, nations can remain anonymous when carrying out cyber attacks or cyber espionage due to the many options faced by entities willing to commit cyber warfare are endless. They could remotely take control of a civilian computer and use that to attack a nation, or they could pay cyber criminals to perform attacks which would not be able to be traced back to the original perpetrator. Thirdly, cyber warfare is especially dangerous due to the potential to sabotage or manipulate critical infrastructure of a country, as automated computer programs which can be hacked, mainly run them. Consequences from a sabotage of infrastructure could be catastrophic, for example a disabled electric grid or communications network would cause chaos in a nation and prevent it from operating. Whilst this would result in a direct loss of life, over the long term such an attack could potentially be fatal. Lastly, the speed and origin of a cyber attack is unpredictable. Seeing as all you need for a cyber attack is a computer, the origin and timing of a cyber attack would be impossible to predict, especially if a nation is not prepared to counter a cyber attack.

Historic Events in Cyber Warfare

Since the digital era begun in the early 1970's nations have been interested in stealing information stored in cyberspace through cyber warfare. The first cyber attack was considered to be in 1982, when the US altered software to cause a pipeline to explode, which was stolen by the Soviet Union and hence exploded it's Trans-Siberian Pipeline (*Infoplease, 2017*). The first major incident relating to cyber warfare came in 1998 during the Kosovo War between the Federal Republic of Yugoslavia and the Kosovo Liberation Army. The United States of America supported the Kosovo Liberation Army during this war, with airstrikes. To make the airstrikes more effective the US hacked into the Yugoslavian Air

Defence System and disabled it, allowing them to bomb major cities in Yugoslavia without the fear of any defensive attacks. This bombing campaign resulted in an estimated 1500 civilian casualties. However the US could have chosen to attack Yugoslavia with greater force, they had the capability to take down its national economy, however refrained from doing this due to their fear of breaching human rights. Some critics suggest that the US was actually afraid of its enemies stealing their cyber warfare technology if they used it openly. The second major incident that has occurred in cyberwarfare is the attack on Estonia, which is believed to have been perpetrated by the Russians, however this was never proven. A distributed-denial-of-service-attack compromised Estonia for 22 days. The president's office, parliament, law enforcement officials and Estonia's two biggest banks were targeted in these attacks. As mentioned before, the attack caused the loss of huge amounts of infrastructure and assets, leading to an overall predicted loss of tens of millions of dollars. These are the two largest incidents involving cyber warfare, and the two incidents where the perpetrators are believed to be known with a degree of certainty. There have been countless other incidents of cyber attacks and cyber espionage, however they are too long to list. Various governments such as North Korea, as well as non-governmental groups such as Anonymous carried out these attacks.

Major Parties Involved

United States of America

The United States of America is at the forefront of technology including the prevention of cyber attacks. It has simulated the effect of a cyber attack multiple times, including the 2010 Cyber ShockWave simulation, which demonstrated the lack of awareness and defensive capability the US would have in case of a cyber attack. Furthermore, it also established the United States Cyber Command in 2009, which aims to prevent any attacks against the US and is currently expanding that program to 6500 people by 2018, made up of military, civilian and contract workers. This is in response to the rising threat of cyber warfare, as acknowledged by President Barack Obama when he stated that around 1 trillion dollars was lost to cyber attacks in the US in the year 2015.

China

China is looking to be a major player in the digital era and especially in regards to cyber warfare. It is said to have the biggest cyber army in the world, which work with the military to combat cyber threats. There have been many accusations by western countries, complaining of Chinese hackers hacking into their networks and stealing information, however these have all been denied by the Chinese government.

Anonymous

Anonymous is a hacking group founded in 2003, which whilst not adhering to a strict philosophy seem to be united in their opposition to censorship. They have attacked governments, corporations and religious websites.

Timeline of Key Events

Date	Description of Event
December 1969	Advanced Research Projects Agency goes online in the U.S. connecting four universities. It is the first communications network set up in the event that a military attack destroys conventional communications systems.
June 1982	Soviets steal software from Canadian company to build its Trans-Siberian Pipeline, however software had been designed to blow up the pipeline by the CIA. This is considered the first cyber attack.
November 1988	An Internet worm temporarily shuts down 10% of the world's Internet servers, it is the first internet worm to have been recorded.
1998	US military hacks yugoslavian air defence systems to allow US military to bomb key strategic location uninterrupted.
April-May 2007	Estonia's governmental systems are compromised for 22 days by distributed-denial-of-service-attacks believed to be perpetrated by Russia
July 2008	Weeks before the war between Russia and Georgia, Georgia is hit a by distributed-denial-of-service-attack disabling governmental computer networks as well as media and transportation companies.
9th June 2013	Report commissioned by UN Secretary General Ban Ki-moon is published on "possible cooperative measures in addressing existing and potential threats"

UN involvement, Relevant Resolutions, Treaties and Events

The UN has not drawn up many resolutions regarding Cyber warfare. Most of the resolutions have been in regards to exploring the risks that cyber warfare poses. There are no binding treaties on how States should act in cyberspace, which is one issue that needs to be addressed in any resolution.

- Combating the criminal misuse of information technologies, January 2001, **(55/63)**
- Combating the criminal misuse of information technologies, January 2002, **(56/121)**
- Creation of a global culture of cybersecurity, January 2003, **(57/239)**
- Creation of a global culture of cybersecurity and the protection of critical information infrastructures, January 2004, **(58,199)**
- Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, March 2010, **(64/211)**

The Previous Attempts to Resolve the Issue

On the Developments in the Field of Information and telecommunications in the Context of International Security.

This was a report commissioned by the UN Secretary General Ban Ki-moon, released on August 9th 2013. It was written by 15 experts from the five permanent members of the UN Security Council plus Argentina, Australia (the chair), Belarus, Canada, Egypt, Estonia, Germany, India, Indonesia, and Japan to carry out a mandate from the UN General Assembly to "study possible cooperative measures in addressing existing and potential threats" related to the use of communications technology ICTs. The report recommends fully applying international law to state behavior in cyberspace, extending traditional transparency and confidence-building measures and international cooperation to make infrastructure more secure around the world. Whilst this is an important step for the United Nations to recognise the growing threat of cyber warfare, this report does little in the way of binding agreements combatting cyber warfare. However it is an important groundwork from which resolutions to combat this issue can be formed.

There have not been many attempts to resolve this situation, which is why it is a most pressing issue.

Possible Solutions

When looking at the possible solutions to this issues, there are two ways that it can be addressed. Either cyber attacks and espionage is stopped, or security against these activities is stopped. Both of these issues need to be addressed in any resolution combatting cyber warfare.

Currently there is no international binding treaty on how States should act in cyberspace. This ambiguity has been exploited by States to spy on each other. One way of solving this issue is to push for a special conference on this topic, or to clearly define what

states are and are not allowed to do in cyberspace. This would need to be reinforced by preventative measures.

A big issue with cyber warfare is the anonymity granted in cyberspace, through the taking control of other computers or through hiding your identity. This gives States the freedom to do whatever they want, without the fear of repercussions. Finding a way to reduce anonymity and increase transparency in cyberspace, would also help in identifying non-governmental actors that are pursuing illegal aims.

As with most issues, the most important step to solving this issue, is through increased international cooperation.

Bibliography

"Arms Control Today." *The UN Takes a Big Step Forward on Cybersecurity | Arms Control Association*. Arms Control, n.d. Web. 20 June 2017.

Borger, Julian. "Pentagon Kept the Lid on Cyberwar in Kosovo." *The Guardian*. Guardian News and Media, 08 Nov. 1999. Web. 20 June 2017.

"Cyberwar Timeline." *Infoplease*. Infoplease, n.d. Web. 20 June 2017.

"Cyberwarfare." *Wikipedia*. Wikimedia Foundation, 19 June 2017. Web. 20 June 2017.

"Here's What a Cyber Warfare Arsenal Might Look like." *Scientific America*. Scientific America, n.d. Web. 19 June 2017.

"Kosovo War." *Wikipedia*. Wikimedia Foundation, 15 June 2017. Web. 20 June 2017.

McGuinness, Damien. "How a Cyber Attack Transformed Estonia." *BBC News*. BBC, 27 Apr. 2017. Web. 20 June 2017.

Tisdall, Simon. "Cyber-warfare 'is Growing Threat'." *The Guardian*. Guardian News and Media, 03 Feb. 2010. Web. 20 June 2017.

"What Is Cyberwarfare? - Definition from WhatIs.com." *SearchSecurity*. SearchSecurity, n.d. Web. 20 June 2017.