Research Report | XXVI Annual Session

General Assembly 1

The issue of state-sponsored cyber warfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Patrick Shepard
Fabianna Flores Sanchez

Forum	General Assembly 1
Issue:	The issue of state-sponsored cyber warfare
Student Officer:	Patrick Shepard
Position:	President of the General Assembly

Introduction

War has always been ongoing in our history varying in type and severity. During these wars spying has been implemented by many countries to cause damage and disruption as a tactic in these conflicts. The many conflicts throughout our history have been rather similar in the sense that there are distinct parties fighting each other; so this was seen as conventional warfare. As technology has adapted and changed so has warfare.

Now with the development in technology and cyberspace there is an ever growing issue with what is known as cyber warfare. This is on the rise, and is done very secretly, and because it is so new there have not been many attempts at solving this issue. There are no rules or regulations in the traditional and original conventions such as the Geneva Convention on this.

This is a highly controversial topic and is ever ongoing. In recent years there have been cases such as Edward Snowden revealing US state secrets. Edward Snowden claimed that the USA had been spying on other nations' government officials, even allies. Even though this is technically not warfare, it is important to understand there are many different areas and levels of this topic.

State sponsored cyberwarfare has been around in some form for quite some time actually; relevant trained people in World War 2 to hack communication links and decode coded messages. This is quite a primitive form of cyberwarfare. Cyberwarfare has changed dramatically since these times. Since then, what we call cyberspace has very much changed and it has molded; we are now capable of much more and cyber-attacks can implement much more damage, but it is also much more discrete and quiet.

There have been some attempts to solve the issue, but as stated earlier not many, there have however been academic reports written which just provide insight on some people's interpretations on the international law regarding cyberwarfare. As this is a new issue and member states cannot come to a consensus on what the regulations should be, these reports are purely informational and are not binding at this point. Some of the most famous reports are those regarding ‘jus ad bellum’ and ‘international humanitarian law’.

Definition of Key Terms

Cyberspace

Cyberspace is the virtual three dimensional realm where all online data is stored and through which users can move. Cyberspace is a way an area where information can be transferred without the need of a physical location. In more detail, to manipulate information the electromagnetic spectrum is often used.

Cyberwarfare

In this context it is when a sovereign nation penetrates another nations cyberspace or network in order to cause damage or disruption. This could be done for example to intercept military communications and learn the plan of an operation, or it could be to disable these communications to sabotage a mission. It could also be used for espionage, as a nation could spy on designs for new weapons to keep up to date information on potential threats.

Encrypted software

This is when data is converted from an electronic form to another one which is difficult to understand for outside parties and should only be able to be understood by authorized parties. An example for the use of encrypted software would be when sending messages, if there is a risk of a cyberattack in the sense of intercepting messages encrypted messages could be sent. This is to make it harder for the attacking part to interpret and understand the messages as they would have to first decode them.

Hacking

By definition a hacker is a computer expert, but in this context a hacker is essentially is someone who breaches another parties network to exploit their data. A hacker could be implemented to hack into the cyberspace of a government and retrieve files for example.

Virus

This is a piece of code that is secretly placed onto a computer and runs programs which can disrupt normal use. This could be done to slow down the progress of a specific operation being carried out.

Code

This is a system that programs a computer to carry out certain functions. Coding this these programs can be done by using a coding language such as C or python.

Computer

A computer is a device which can be programed to carry out mathematical functions and which can store data. In cyberwarfare computers can be the tool for attacks and they can also be the victim of attacks. The reason this is such a pressing issue is because computers are devices used for everything nowadays and hence attacks could have major impacts.

Hotline

A hotline in this context is a direct communication link to deal with a crisis situation or emergency. This communication link could be between to heads of government, or between different security teams in different governments. An example of this is the hotline between the White House and Moscow to deal with any rising issues quickly and securely.

General Overview

A large component of this issue is something called ‘internet sovereignty’, this is the issue of who actually owns the internet. This is one of the big issues that needs to be addressed first because if we do not know who has rights over their network and cyberspace how can we come up with regulations regarding the legal and illegal use of cyberspace for disrupting or damaging the other party.

Internet sovereignty

To evaluate who has control of certain parts of cyberspace we need to consider some different aspects of this question. There needs to be concrete rules to provide clarity in grey areas. Some of these grey areas include the issue of if a network is controlled and based in a specific country, does that give the country the right to claim ownership and control of all the data in the network? Another issue is something that has caused some controversy. If some information, traveling through cyberspace, passes over a country on route to its final destination would this give the country the right to monitor this data passing through? This links into a bigger issue called boomerang routing. This is when data is manipulated to travel over a country it was not originally destined to travel over, for the purpose of the monitoring the information. This has been done by countries such as the USA and they have claimed this is allowed due to their Patriots Act which allows them to intercept information if there are suspicions of terrorist activity.

State sponsoring

In many cases the parties funding cyberwarfare are governments, because these are the parties carrying out these cyberattacks in the first place. As of now there are no conventions and generally accepted legislatures, which means anything done can just argued as exercising their sovereign rights. To reduce the risk for the state itself, they will often hire organizations to do so for them. They will ask these organizations to relay information back to them as they receive them; and if carried out correctly, these hackers will infiltrate the servers and network of other nations and roam the cyberspace for months at a time without being detected. Alternatively, some states hire companies to help them protect their servers, network and cyberspace. These are people with advanced hackers to detect and remove any present parties which are committing a cyber-attack.

Direct government action

Governments often have their own organizations set up to do deal with cyber security. For example the United Kingdom has the Government Communications Headquarters (GCHQ). This is the organization that protects the UK from cyber-attacks and probably deal with cyber espionage. Whether or not they carry out cyber-attacks themselves is not confirmed, because they are not required to admit to this or abide by any regulates the scope of this could be widespread, which is further reason for regulation. The USA equivalent of this is the National Security Agency (NSA) who carry out similar tasks.

Consequences

It is important to note the consequences of cyber-attacks. Although this has luckily not happened yet a full out cyber-attack could be launched which could cripple all communications within a large nation such as the USA. If this was timed with an actual military attack, then it would be very difficult to react and deploy troops. Therefore, regulates and monitoring of what is being developed technologically so that independent bodies can constantly adapt and assess the situation.

Cyber-attacks in key countries in the world could have huge knock on effects. Say China suffered a cyberattack that wiped out all computer systems, its trade and economy would suffer hugely which would impact the rest of the world as many countries heavily rely on China for trade.

There are also many humanitarian impacts, especially in well developed countries. In developed countries there is huge infrastructure behind things like cleaning water for drinking, or sewage systems which are all heavily reliant on computers. A cyber-attack could heavily impact these basic services causing huge issues in health and normality of living.

Major Parties Involved and Their Views

China

There are many reports of China using cyber-attacks to further develop their military technology. This is done by cyberespionage which gains information about nuclear weapon designs and they gather this information by hacking into other nations' databases. They have also been monitoring USA weapon transfers to Taiwan, and have been keeping track of Chinese defectors. Currently what China and the USA agree on is that they will both respect cyberspace but will take necessary actions for self-defense.

The United States of America

The USA has very clearly expressed their views that they feel Cyberwarfare is just another weapon in the arsenal of a military and should be used like any other measure would be used. The NSA has a special branch to protect its cyber infrastructure which is called the USCYBERCOM. This has sparked some controversy but this is likely to do with it being a relatively new weapon. The media has questioned the ethics of such actions, but it is seen as necessary by many to stop the ever growing threat of terrorism.

Germany

Germany in 2013 revealed that they had a computer network operation team which consisted of 60 people to try and defend the governments cyberspace and hence contribute to national security. Germany reportedly gets 5 cyber-attacks a day on its government and these attacks reportedly originate from China. The maximum amount of internet traffic allowed to be monitored by law in Germany is 20%, and the German intelligence services were given a budget increase of 100 million Euros to do so.

The United Kingdom

The UK's cyber security section of Military Intelligence 6 (M.I.6) has indulged in cyber-attacks at terrorist organizations. It is said that they infiltrated Al- Qaeda's website and replace the recipe of how to make a bomb with the recipe of how to make cupcakes. This brings up another dynamic and a question that needs to be answered. Are cyber-attacks on terrorist groups allowed? Should this be differentiated from interstate cyberwarfare.

Iran

Iran are very big on cyber security. They have a section of their security forces which is called the ‘Cyber Defense Command’. They claim to be the 4th most capable state in the world when it comes to cyberwarfare. Iran has sufferance from various cyber-attacks as for example in June of 2010 Iran’s nuclear infrastructure was hacked, by a cyber weapon called ‘stuxnet’. This is believed to be a joint effort of both Israel and the United States of America and reportedly infected 60,000 computers with this virus.

The Netherlands

The Dutch secret service called the AIVD have successfully used cyberwarfare to counter terrorism. They set up a fake website for so called ISIS to use to communicate and managed to monitor any plans and prevent attacks, and also managed to pin down high value targets. This is an example of governmental use of cyberwarfare in a more discrete form.

Anonymous

Anonymous are a group of hackers that work independently for personal views. They can be very influential and their views do not always coincide with those of governments. They have decided to use their hacking skills to help combat so called ISIS and help disrupt them as much as possible.

Timeline of Events

The timeline will distinguish mainly technological advances, and key cyber-attacks in the past:

Date	Description of event
1882	The first computer was invented by Charles Babbage. It is important to note the first computers were not electronic they were mechanical computers that would carry out basic functions
1914	The Government Communication Headquarters was established in the United Kingdom. This shows that before computers were a wide used thing we still had monitorying of communcations and as communcation has developed into what we now know as cyberspace it has developed along with it. This is just an example of a security agency to combat any cyberthreats.

1980 Cyberattacks became more prominant at this time, and started to develop into sophicticated technique. This is when hackers as people began to develop into the type of hackers we know today.

April 2007 The Estonian networks were harrased, there was denial from all parties and noone was held accountable. The harrasment followed a dsipute with Russia about the removal of a war memorial.

January 2009 The Israeli internet infrastructure was hacked an disrupted. This occured during a time of attack on the Gaza strip.

January 2011 The Canadian government suffered attacks on many agencies.

October 2013 NATO invested 58 million euros into upgrading cyber defences.

UN involvement, Relevant Resolutions, Treaties and Events

There has only been very recent United Nations involvement. The issue of cyberwarfare has just come onto the agenda for debate in the first commission of the General Assembly. Here they have been debating on regulations and how important it is they regulate this now before cyber weapons get so advanced they could completely destroy infrastructures.

Evaluation of Previous Attempts to Resolve the Issue

At this point in time, the measure taken to solve cyberwarfare has been implement by countries in their own county. No one has really discussed the legality of cyberwarfare to a great enough extent to see if it is actually allowed under international law, and that is where the problem comes in; if we cannot decide what is legal and what is not how can we tell if cyberwarfare sponsored by the state is allowed. Furthermore, as warfare starts to migrate from what we know as traditional, conventional warfare, we may need to put in place some conventions, in the context of 'war rules' to provide a structure, and a guideline to this issue.

There are however some Non-Governmental Organizations (NGOs) that have developed with the issue. For example, there is the 'Rand Cooperation'; this cooperation gives advice to military and civilian parties on how to increase their cyber defense to prevent attacks. They have helped many big countries and organizations.

Possible Solutions

Possible solutions vary as there are many different aspects which must be solved. Potentially a central body should be put in place to come up with a treaty and some international laws on this issue specifically. These laws would have to tackle the issue of internet sovereignty, state involvement, rules of engagement, and if cyberwarfare is legal at all. Once clarity has been provided on things like boomerang routing, courts can subsequently come up with suitable penalties regarding the violation of privacy and other offences. A convention would also provide strict guidelines on what is allowed in terms of cyberwarfare in a conflict so that any governments disregarding these could be brought to justice.

Communication is also of vital importance, so maybe there should be conferences every 6 months specifically on this issue where every government sends a delegation to represent their views and where they can communicate any issues such as new regulations required for developing technology. Here they could also raise any concerns and learn from each other on cyber defense. This is also to provide a place where less technologically developed countries could still stay up to date with this threat. This is because in another environment smaller countries may be neglected and be less aware and less prepared for this threat. Furthermore, there need to rules on when engagement of cyberwarfare is permitted under international law

Also once guidelines have been set as to what is allowed and what is not allowed, there should be a task force set up to ensure that no one is violating these terms and if so they should be held accountable with suitable sanctions. If agreed upon reports may be required to monitor any advances. To encourage cooperation these reports could be kept secret as to not interfere with any legal cyberwarfare.

Potentially a specific court could be put in place to evaluate the legality of cyber actions to bring justice to those breaking any regulations. This does however mean that first regulations are needed to provide clear rules on what is and is not allowed.

This issue also needs resolutions which propose explicit laws to be passed by the Security Council to actually make some progress in the short term.

Bibliography

"About GCHQ Scarborough." *GCHQ Site*. N.p., n.d. Web. 15 Aug. 2016. https://www.gchq.gov.uk/features/about-gchq-scarborough

"Cyber Warfare: The Newest Battlefield." *Cyber Warfare: The Newest Battlefield*. N.p., n.d. Web. 15 Aug. 2016. http://www.cs.wustl.edu/~jain/cse571-11/ftp/cyberwar/

"Cyberwarfare in Iran." *Wikipedia*. Wikimedia Foundation, n.d. Web. 15 Aug. 2016. https://en.wikipedia.org/wiki/Cyberwarfare_in_Iran

"Government Communications Headquarters." *Wikipedia*. Wikimedia Foundation, n.d. Web. 15 Aug. 2016. https://en.wikipedia.org/wiki/Government_Communications_Headquarters

N.p., n.d. Web. http://www.un.org/press/en/2014/gadis3512.doc.htm

"Patriot Act." *Wikipedia*. Wikimedia Foundation, n.d. Web. 15 Aug. 2016. https://en.wikipedia.org/wiki/Patriot_Act

"State-Sponsored Cyber Attacks." *MWR InfoSecurity*. N.p., n.d. Web. 15 Aug. 2016. https://www.mwrinfosecurity.com/our-thinking/state-sponsored-cyber-attacks/

"State-Sponsored Cyber Attacks." *MWR InfoSecurity*. N.p., n.d. Web. 15 Aug. 2016. https://www.mwrinfosecurity.com/our-thinking/state-sponsored-cyber-attacks/

Wikipedia. Wikimedia Foundation, n.d. Web. 15 Aug. 2016. https://en.wikipedia.org/wiki/Cyberwarfare#Cyberwarfare_in_the_United_States

Wikipedia. Wikimedia Foundation, n.d. Web. 15 Aug. 2016. https://en.wikipedia.org/wiki/Cyberwarfare#Legality.2C_rules