Research Report I 30th Annual Session

First General Assembly

Fostering international cooperation to combat the growing threat of cyberwarfare

MODEL UNITED NATIONS
THE INTERNATIONAL SCHOOL OF THE HAGUE

Lina Sigmond

Forum:	1st General Assembly
Issue:	Fostering international cooperation to combat the growing threat of cyberwarfare
Student Officer:	Lina Sigmond
Position:	Deputy Chair

Introduction

In our world, which is increasingly dependent on the internet, cyber security has become a critically important part of our lives. We store and do everything online ranging from banking to attending classes through videocalls. With this increasing online activity comes an increase in online crimes as well. While this has been tackled relatively effectively, cyberwarfare has not. There have been incidents in the past that have been classified as cyberwarfare, yet international law has not yet been updated to encompass cyberwarfare yet. Countries by themselves often have legislation in place to tackle cybercrime, yet there had been little international cooperation handling this issue. Through increased international cooperation, this issue needs to be reviewed and handled to assure that cyberwarfare will not become an increasingly dangerous loophole for crime.

Definition of Key Terms

Cyberattack

The Tallinn Manual 2.0 states that: “A cyberattack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage and destruction to objects.”

Cyberwar

Actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption (Clarke, 14)

Cyberwarfare

Cyberwarfare are actions that may or may not imply a cyberwar, used by one nation to cause damage to another nation’s online presence and information.

Cyberspace

“A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” (CSRC)

Denial of Service Attacks (DoS)

A type of cyberattack that involves the target to be flooded with large amounts of traffic forcing the target to shut down. Can also occur through a crash attack, which employs bugs that exploit flaws in the target, causing it to crash.

Ransomware attacks

Type of cyberattack which shuts down or incapacitates parts of a computer, often blocking the user from accessing files. Demands ransom from the user in exchange for their files back.

.

.

General Overview

Cyberwarfare does not currently fit within the limitations of a war and therefore cannot be handled accordingly. Under the current system of International Humanitarian Law (IHL), cyberwarfare can only be seen and handled as an act of war if it triggers an armed, physical conflict or occurs during an armed, physical conflict. Therefore, it is necessary to repair this legislative loophole as quickly and effectively as possible. Cyber warfare is becoming more and more prominent and with our increasing reliance on the internet it is becoming more obvious how devastating cyberwarfare can prove to be.

While many countries have their own national research centres for cybersecurity and have implemented laws and legislation that penalises cybercrime, nations have rarely cooperated together to combat this issue. One example of an organisation which has achieved this is the CCDCOE, a NATO military organisation tasked with the research and preparation of countries against cyberthreats. This organisation is supported by 25 nations. While the organisation does promote cooperation against cyberthreats, it is a NATO organisation and is focused mainly on defence and military action. While the United Nation’s goal is to resolve problems with diplomacy before they happen. There is no UN organisation established yet tasked with cyberwarfare. The United Nations Office on Drugs and Crime has taken on the issue of cybercrime and deals with it as well, but there is no specified UN convention or sub-portion of an organisation specialised in this area.

For this issue to be combatted effectively, countries need to cooperate with each other. Previously many of the proposed solutions present in signed conventions such as the Budapest Cybercrime Convention, countries are usually urged to work within their own borders, increasing consequences of cybercrime as well as creating a generally more secure online environment. However, cyberwarfare does not focus on countries individually. The term itself implies that more than one country must be involved. For cyberwarfare to occur one country must attack another one. Therefore, this issue cannot stay within a country's borders. Possible ways to resolve this issue could have nations come together to create and ratify a treaty or some other binding form of agreement that prohibits the use of cyberwarfare and has severe consequences if the agreement is not respected. Additionally, before this can be done, definitions for each term involved in the issue have to be laid down as well to avoid any loopholes or confusion.

Major Parties Involved

USA, Russia, China, Iran

These countries have renowned cyber research centres. Additionally, many of them have taken part in or are implied to have taken part in cyberwarfare events. As this issue involves all nations, the most influential countries are also the most important concerning this issue.

CCDCOE

Established in 2008 as a response to the cyberattacks on Estonia in 2007, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) is an organisation tasked with research and preparation regarding cyberthreats. In October of 2008, it received the status of International Military Organisation. Supported by 25 nations, the organisation combines research and military as it prepares for cyberthreats. The CCDCOE are based in Tallinn, Estonia.

United Nations Office on Drugs and Crime (UNODC)

The United nations Office on Drugs and Crime (UNODC) is partly responsible for handling the issues surrounding cyberthreats and cybercrime. Previously they have held conferences to tackle cybercrime and cyberterrorism, as well as attempting to foster cooperation between countries to address these issues properly. However, to date, there is no solid signed agreement from the UNODC tackling cyberwarfare.

North Atlantic Treaty Organisation (NATO)

The NATO has previously recognized cyberwarfare as a major issue to security and aided in the creation of the CCDCOE which is tasked with handling cybercrime.

Timeline of Key Events

Timeline of openly reported cyberattack events.

Date	**Description of Event**
27 April 2007	Estonia was hit by a series of cyberattacks targeting Estonia's government sites as well as banking and media sites
20 July 2008	Georgia experienced cyberattacks during the Russo-Georgian war resulting in the overloading of several websites, including the website of the then-president and several news organisations
June 2009	A piece of malware named Stuxnet destroying centrifuges of the Iranian nuclear enrichment facility in Natanz
August 2012	Saudi Arabian firm *Saudi Aramco* was hit by a piece of malware named Shamoon that wiped three-quarters of its computers
December 2014	A group of North Korean hackers targeted Sony Pictures, leaking emails as well as unreleased films and wiping thousands of computers, leaving behind an extortion message demanding money and calling for the termination of the movie *The Interview*.
2015 - 2017	During the annexation of the Crimean peninsula, Russia caused a number of cyberattacks on the Ukraine resulting in blackouts and power outages, federal computers being hacked, and information deleted, and transportation systems being delayed.
May 2017	North Korean hackers created and released a ransomware worm named WannaCry. The worm shut down Chinese universities, Indian Police, and the British NHS, causing between $4 and $8 billion in damage.
June 2017	A piece of code called NotPetya, infected about 10% of Ukraine's computers, appearing as Petya ransomware, hence the name. The worm hot important infrastructure such as airports and hospitals, crippled banks and even affected the operation responsible for monitoring radiation levels at Chernobyl. The worm spread to infect international companies such as Maersk and spread back to Russia as well, infecting and wiping

computers. The worm is estimated to have cause $10 billion damage worldwide.

August 2017 Triton (or Trisis) was a piece of malware that attacked the Saudi Arabian firm Petro Rabigh, shutting down one of the firm's oil refineries.

Previous Attempts to Resolve the Issue

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), was established in 2008, in response to the cyberattacks on Estonia in 2007. The centre conducts conferences on research and response to cyberattacks and aims to aid countries in preparation and defence of cyberattacks. It is well-known for its publication of the Tallinn Manual, started in 2009, which gives a guide to how cybercrime fits in current international law. However, the CCDCOE is a NATO organisation, and not part of the United Nations. It focuses more and defence and preparation while the UN concerns itself with diplomacy and preventing cybercrimes rather than preparing them.

While there have been conferences, such as the Twelfth United Nations Congress on Crime Prevention and Criminal Justice held in Salvador, Brazil (12-19 April 2010), and signed agreements such as the Budapest Convention on Cybercrime (1 July 2004), neither have resulted in countries coming to an agreement on how to address cyberwarfare. The end-result of both of these was that countries should look at their own legislative systems and incorporate measures that apply to cybercrimes.

Possible Solutions

Taking inspiration from an organisation such as the CCDCOE, which had banded together nations to combat cybercrime, a possible solution to the threat of cyberwarfare would be to create something similar, an UN-based organisation tasked with dealing with cyberwarfare. In coordination with countries' own centres for research and cyber defence, such as the United Kingdom's National Cyber Security Centre (NSCS), this new organisation could collaborate internationally and promote the sharing of information. Additionally, a treaty could be created to protect countries from cyberattacks, defining certain actions as war crimes and drafting the consequences of these that would apply internationally and not rely on each country's own legal system and laws.

Bibliography

Bradshaw, Samantha. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*. Vol. 23, Chatham House, 2015.

"CCDCOE : About Us." *CCDCOE*, NATO, www.ccdcoe.org/about-us/.

Clarke, Richard A., and Robert K. Knake. *Cyber War: the next Threat to National Security and What and What to Do about It*. Ecco, 2010.

"Convention on Cybercrime." *European Treaty Series - No. 185*, 2001. *Council of Europe*, www.cicdr.pt/documents/57891/151968/Conv_Budapest.pdf/f561f77a-bb81-49ce-a8a6-8ba3733c0778.

"Fortifying Regional Disarmament and Security, Countering Potential Cyberwarfare, Misuse of Dual-Purpose Technologies, Focus of Debate in First Committee." *United Nations Meetings Coverage and Press Releases*, United Nations, 21 Oct. 2010, www.un.org/press/en/2010/gadis3419.doc.htm.

"Global Programme on Cybercrime." *United Nations Office on Drugs and Crime*, United Nations, www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html.

Greenberg, Andy. "Cyberwar: The Complete Guide." *Wired*, Conde Nast, 23 Aug. 2019, 7:00, www.wired.com/story/cyberwar-guide/.

ITU, International Telecommunication Union. *The Quest for Cyber Peace*. ITU, 2011.

Nakashima, Ellen. "Russian Military Was behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes." *The Washington Post*, WP Company, 13 Jan. 2018, 12:46, www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

Schmitt, Michael N., and Liis Vihul. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press, 2018.

Talihärm, Anna-Maria. "Towards Cyberpeace: Managing Cyberwar Through International Cooperation." *United Nations*, United Nations, www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation.

"Tallinn Manual 2.0." *CCDCOE*, NATO, www.ccdcoe.org/research/tallinn-manual/.

United Nations Office for Disarmament Affairs. *Cyberwarfare and Its Impact on International Security*. Vol. 19, UNODA Occasional Papers, 2009.

"The United Nations, Cyberspace and International Peace and Security Responding to Complexity in the 21st Century." *UNIDIR Resources*, UNIDIR, www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

United Nations Congress on Crime Prevention and Criminal Justice. *Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice**, UNODC, 2010. 12th Congress, report.

Appendices

Appendix A

Previous attempt to solve the issue: Budapest Convention on Cybercrime.

"Convention on Cybercrime." *European Treaty Series - No. 185*, 2001. *Council of Europe*, www.cicdr.pt/documents/57891/151968/Conv_Budapest.pdf/f561f77a-bb81-49ce-a8a6-8ba3733c0778.

Appendix B

Manual reviewing the application of international law on cybercrime.

"Tallinn Manual 2.0." *CCDCOE*, NATO, ccdcoe.org/research/tallinn-manual/.

Appendix C

Book on the issue and possible solutions to it.

Clarke, Richard A., and Robert K. Knake. *Cyber War: the next Threat to National Security and What and What to Do about It*. Ecco, 2010.