Research Report

Leiden Model United Nations 2017
~ fresh ideas, new solutions ~

Forum:	*General Assembly First Committee*
Issue:	*Cyber warfare and Article 2.4 of the United Nations Charter*
Student Officer:	*Nika Engelen*
Position:	*Chair*

Introduction

As the use of technology and the internet have increased over the past few years, cyberwarfare is one of the most pressing rising issues at this time. Hacking groups, sometimes linked to governments, are suspected more and more of attacking sovereign states and companies, with informational or financial gain as a motive. This not only creates chaos, it also violates the territorial integrity and sovereignty of states, and therefore also the United Nations Charter, specifically article 2.4, which is a severe violation of international law.

Definition of Key Terms

Cyberwarfare
According to the Oxford Dictionary, cyberwarfare is defined as "*the use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.*[1]"

Article 2.4 of the United Nations Charter
The United Nations Charter is the foundational treaty of the UN and is made up of articles that all member states of the UN are bound to oblige to. Article 2.4 reads as follows:

"*All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*[2]"

In short, it says that member states cannot use force or threaten to use force against any other state, which includes types of warfare, such as cyberwarfare.

Territorial Integrity
Territorial integrity is the principle under international law that nation-states should not attempt to promote secessionist movements or to promote border changes in other states. It also states that imposition by force of a border change is an act of aggression.[3]

Political Independence
Political independence is defined as "*the right for sovereign governments to exercise freely the full range of power a state possesses under international law.*[4]"

General Overview

Cyberwarfare is considered a relatively new issue, as the internet has only become an efficient medium for global connection in the past few years. It's a type of warfare that very much differs from the traditional kind of warfare, with, for example, hacking of computer systems instead of attacking each other by bombings. This can be considered as less damaging than traditional warfare, however, cyberwarfare is still, in a way, a violation of the things mentioned in article 2.4.

It might not be very clear that cyberwarfare in the way it now exists is a real violation of the territorial integrity and political independence of states, but it does use or threatens to use force against the sovereignty of states, which is a violation of article 2.4. There are a several situations in which cyberwarfare can be seen as a violation of sovereignty, of which a few will be discussed in this section.

Firstly, cyberwarfare is often used to gain information from either governments or companies. An example of such an attack is Aurora which was discovered in 2010, for which China was accused of attacking multiple companies in the United States, such as Google. Likewise, in 2012 the United States and Israel were blamed for attacking Iran and other Middle-Eastern countries, with a programme called Flame.[5]

Attacks can also have financial gain as an objective. Such an example would be the Bangladesh Bank heist, when a hacking group linked to North Korea attacked the Bangladesh Central Bank's account at the Federal Reserve Bank of New York, in which $81 million was stolen.[6]

Major Parties Involved

United States of America
The United States have carried out several attacks in the past, such as Flame and Stuxnet, in which both the main target was the Iranian government. The country mostly operates alone, but has also often been working together with states such as Israel and the United Kingdom. It has also been attacked several times, both governmental organisations and private companies, such as during operation Aurora, when Chinese hackers attacked American companies, or when Russian officials tried to hack into government agencies in 2015.[7]

Israel
Israel mainly operates together with the United States on this topic. It has been blamed for the Flame attack, in which it hacked government systems of Iran and other Middle-Eastern states together with the United States. It's also known to have hacked into Kaspersky Lab systems, a Russian software company, when Russian officials were planning to attack United States government systems.

Russia
Russia has been blamed several times for attacks, for example Red October, in which it carried out surveillance on diplomats and scientists worldwide. It has also been accused of planning to hack into United States government agencies earlier, before Israel hacked into another Russian company and found out about the attack.

China
China has been accused of cyber-attacks such as operation Aurora, which was discovered in 2010, when it hacked into several United States companies, such as Google. The country is known to have powerful cyber capabilities and might form a threat for the future as well.

North Korea
North Korea is considered to be one of the states possessing the most powerful cyber force to launch an attack. This country is mostly known for its nuclear tests, but their cyberwarfare capabilities are very much underrated. It has been linked to some of the biggest cyber-attacks in history, including the Sony Hack and the Bangladesh Bank heist, which you can read about in the General Overview, and countless other attacks against South Korea and Japan and even U.S. interests.[8]

Timeline of Events

2009	Operation Aurora: China hacked several US companies
2012	Flame attack: USA and Israel attacked Iran and other Middle-Eastern countries
2015	Israel finds out about a planned attack by Russian officials to hack into United States government agencies
February 2016	Bangladesh Bank Heist: North Korea attacked Bangladesh Bank and stole $81 million

Previous Attempts to solve the issue

As this is a relatively new issue, no real previous attempts to solve the issue have yet been made.

Possible Solutions

There are several possible solutions that may do a good job in preventing future cyber-attacks. Firstly, international law concerning warfare should be updated. Right now, cyberwarfare is not considered a real act of war and it's seen as far less damaging than traditional warfare. It should be considered as a real act of war and the damage of cyberwarfare should be considered better. This gives international organisations and agencies, such as the United Nations Security Council, more power to prevent and condemn acts of cyberwarfare.

Secondly, there are more technical possible solutions. Companies and governments should use safe technology that can resist any cyber-attack. Making networks tighter and securing them better so it's harder for cyber-attacks to come through is also an effective possible solution. Lastly, governments and network operators should work together to secure the internet by, for example, rid network systems toxic viruses and other malicious software.

Useful documents

- United Nations Charter: http://www.un.org/en/charter-united-nations/ (Article 2.4 can be found under *Chapter I: Purposes and Principles*)

Appendix/Appendices

[1] "Cyberwarfare definition." English Oxford Dictionaries. *Oxford Dictionaries, n.d.* Web. https://en.oxforddictionaries.com/definition/us/cyberwarfare

[2] "Charter of the United Nations." United Nations. *United Nations, n.d.* Web. http://www.un.org/en/charter-united-nations/

[3] "Territorial Integrity." Wikipedia. *Wikimedia Foundation, n.d.* Web. https://en.wikipedia.org/wiki/Territorial_integrity

[4] "Independence." The Free Dictionary. *Farlex, n.d.* Web. http://legal-dictionary.thefreedictionary.com/independence

[5] Dunn, J. E. "The world's 10 most dangerous cyberwarfare attacks." Techworld. *IDG, 13 March 2015.* Web. https://www.techworld.com/security/worlds-10-most-dangerous-cyberwarfare-attacks-3601660/

[6] Shaikh, R. "US Accuses North Korea of $81 Million Bangladesh Theft – Sanctions Against Chinese Middlemen Expected." WCCFTECH. *WCCF PTE LTD, 23 March 2017.* Web. http://wccftech.com/us-north-korea-bangladesh-bank-heist/

[7] Perlroth, N. & Shane, S. "How Israel Caught Russian Hackers Scouring the World for U.S. Secrets." The New York Times. *The New York Times Company, 10 October 2017.* Web. https://www.nytimes.com/2017/10/10/technology/kaspersky-lab-israel-russia-hacking.html?rref=collection%2Ftimestopic%2FCyberwarfare&action=click&contentCollection=timestopics&region=stream&module=stream_unit&version=latest&contentPlacement=7&pgtype=collection

[8] Huminski, J. & Rogers, M. "North Korea threatens the world with cyberwarfare, not nuclear missiles." New York Daily News. *NYDailyNews.com, 19 July 2017.* Web. http://www.nydailynews.com/news/national/north-korea-threatens-world-cyberwarfare-not-nukes-article-1.3339250