CHAPTER ONE
INTRODUCTION

A. Background

Since the beginning of the 21st century, the world has witnessed such spectacular and severe cyber-attacks. These attacks include the attack on Estonia in 2007 as well as in Georgia in 2008. On 27 April of 2007, for weeks Estonia was hit by big cyber-attacks that taken down several online services with an internet traffic which disabled Estonian government bodies, banks, and media.[1] Furthermore, the attacks against Georgia took place in August 2008 and affected Georgian governmental web resources, mass media, forums and a lot of Georgian domains. It led to significant communication delays, as well as financial losses. The Russian Government denied the allegations that it was behind the attacks, saying that individuals in Russia were unfeasible that individuals in Russia or anywhere would be able to start the attacks.[2]

In 2018, the U.S. Justice Department reported a criminal complaint in Alexandria, Virginia, accusing a Russian national of her supposed role in a Russian plot to interfere with the U.S. political system, including the 2018 mid-term elections. Elena Alekseevna Khusyaynova has been accused of being an

[1] Damien McGunniess, "How a Cyber-attack Transformed Estonia", https://www.bbc.com/news/39655415, accessed on 3 March 2020 at 1:15 p.m.
[2] John Markoff, "Before the Gunfire, Cyberattacks", https://www.nytimes.com/2008/08/13/technology/13cyber.html, accessed on 3 March 2020 at 2:47 p.m.

alleged core member of the "Project Lakhta," a scheme aimed at interfering with the 2016 US presidential election. The project operated to create chaos and aggravate the political situation during the election by creating thousands fake social media account which were also posted so many messages before the election took place. [3]

The notion on cyber warfare cannot be separated with the discussion about the development of technology and the internet itself. Project Lakhta is in fact a result of the invention of the internet where in the late 1960s, the first workable Internet prototype came with the development of ARPANET, or the Advanced Research Projects Agency Network.[4] In 1969, the first demonstration was done through the ARPANET project which at that time Demonstrated University of California, Los Angeles (UCLA) communication with Stanford Research Institute through an integrated network now known as the Internet. [5] Actually, in a very early years of the emergence of the internet, it was invented for the military purposes, yet, with the rapid growth of the internet and the advent of the World Wide Web (WWW), the internet has grown quickly and exponentially across the world.

---

[3] U.S Department of Justice, "Russian National Charged with Interfering in U.S. Political System", https://www.justice.gov/opa/pr/russian-national-charged-interfering-us-political-system, accessed on 3 March 2020 at 5:15 p.m.

[4] Evan Andrews, "Who Invented the Internet?", https://www.history.com/news/who-invented-the-internet, accessed on 20 February 2020 at 7:17 p.m.

[5] Gregory Gromov, 2012, "History of Internet and World Wide Web - Roads and Crossroads of the Internet History", http://www.netvalley.com/, accessed on 20 February 2020 at 8:12 p.m.

All countries over the globe have becoming so dependent with computer and internet. Computerization happened everywhere and becoming a must in a modern life nowadays. It is widespread and used in every dimensions of life, such as politic, economic, social, culture, law, defense, and security. The internet's emergence and global expansion has proven to be the most successful and the fastest technological revolution in human history. Within a period of only18 years the number of active Internet users has increased from an estimated 1.9 billion in 2010 to over 3.9 billion in 2018.[6] Nowadays, we witness that states, businesses, academia, and individuals all are interconnected to a point never before imagined.

A very good example and a solid evidence is in 2018, the world has experienced on what so called the industrial revolution 4.0. This event marked the new era of not only how the industry works, but also many aspects of life work. The advancement of technology has pushed every sector of human life to develop and keep on developing. This development also happens in such a rapid state, which of course, the technology has to do with all these. At the beginning in industry 3.0, where computers were introduced, it was disruptive because of all the addition of an entirely new technology. Today, and in the future when Industry 4.0 occurs, when computers are linked and able to interact

[6] Statista, "Numbers of Internet Users Worldwide", https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ accessed on 20 February 2020 at 8:45 p.m.

with each other and make decisions without any human interference and influence, this is how these machines create and exchange knowledge resulting in Industry 4.0's true strength.[7]

In addition, to providing benefits to mankind, technology also raises a new threat that operates through cyber space. Over the past few years, many armed conflicts have been going on in some parts of the world, those armed conflict for example, situated in Iraq, the fight against ISIS. Everybody could easily acknowledge about these armed conflicts with such advanced information and communication technologies. The rapid advancement of technology around the world has tremendous consequences in all respects, including the war dimension, over time.[8]

War and technological growth have coexisted for centuries. Military operations rely heavily on computer systems and networks, opening up a "fifth" war-fighting environment in addition to generally recognized areas of land, sea, air and outer space.[9] For a very long time, states within their military operations has been seeking to develop weapons systems that will work more effectively and could minimize the risk for soldiers in order to decrease the casualties in battle.[10] Weapons systems are becoming more and more advanced, creating a

[7] Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation for Anyone" https://www.forbes.com/sites/bernardmarr/2018/09/02/what-is-industry-4-0-heres-a-super-easy-explanation-for-anyone/#693793e9788a accessed on 20 February 2020 at 8:50 p.m.
[8] Ida Verkleij, 2016, *Autonomous Weapons Systems*, Tilburg, Tilburg University, p. 2.
[9] US Department of Defense, 2006, *The National Military Strategy for Cyberspace Operations*, p. 3
[10] Vincent Bernard, 2015, "Tactics, Techniques, Tragedies: A Humanitarian Perspective on the Changing Face of War", *International Review of the Red Cross*, Vol. 97

way for humans to move further away even are no longer needed to be directly and physically in the battlefield. As artificial intelligence advances in weapons systems, direct human involvement has become minimal.[11]

Information Technology and the internet have become a main units of a national power because on how they have grown and developed to such extent, cyber war has echoed as nation-states are preparing themselves for cyber battle space. Many states are already preparing themselves to engage in a cyber war with frightening frequency as they are not only conducting cyber espionage and reconnaissance, yet also developing national strategies and creating an offensive capabilities in cyberwar. Many Cyber-attacks and network infiltrations are widely documented, where this actions can be related to states and political goals. What possible is that more economic and human resources are expended on how to execute cyber warfare than on efforts to prevent it. Indeed, there is an amazing lack of international dialog and activity regarding cyberwar containment. This is such an unfortunate, because the cyber environment is a field where technological innovation and organizational art have far outstripped policy and strategy, and because cyberwarfare is, in theory, a phenomenon that must inevitably be controlled politically.[12]

[11] Geneva Academy of International Humanitarian Law and Human Rights, 2014, *Academy Briefing No. 8: Autonomous Weapons Systems under International Law*, Geneva, Geneva Academy, p. 3.
[12] Fred Schreier, 2015, *On Cyberwarfare, DCAF Horizon 2015 Working Paper No. 7*, Geneva, Geneva Centre for Democratic Control of Armed Force, p.7.

The case of Project Lakhta turns out to be one of the prime example on how these technological advancement could poses a serious threat. Where the Russian Nationals, Elena Alekseevna Khusyaynova is alleged to be the core member of the operation which intervened with United States Political System. Project Lakhta was designed to create and disseminate campaigns of misinformation on various issues, including misinformation on political candidates.[13] While it is clearly constitutes a breach of International Law and International customary law when it interferes with the domestic affairs of the United States, yet it raises questions whether these conduct could be connected with the Russian government because the perpetrator was a Russian and was committed on Russian soil. When it does, could the Russian government be held liable and the state responsibility could be given a rise. When a cyber-attack such Project Lakhta occurred, the issues on how to determine whether the attack has any connection to a particular state will face a difficulty. Since the attribution of cyber-attack is very difficult to do and pose some challenges because it brings new means of method and need a new way of approach.

Cyberwar is in turn part of the evolution of traditional warfare, which is also linked to broader social and political changes. It is now difficult to foresee any confrontation in a conflict where the elements of cyber-activity such as surveillance or sabotage are not involved. Whether the cyber war is real is not

[13] Criminal Complaint, 2018, United States *vs* Eleena Khusyaynova

as relevant as how we can focus on preserving and mitigating the threats posed by this computer technology. After all, a cyber-attack does not need to kill someone or even inflict significant material harm to be deemed dangerous.[14]

This trend raises the question of how far the prevailing international law can be used into the cyber domain. There is no doubt that the prevailing international law governs state activities wherever they might occur, with no exception as in cyberspace. Nonetheless, in a point of view from some specific characteristics of the technology in question, trying to apply some of these prevailing laws, principles and terminology to a brand new technology that brings somethings new could pose some difficulties.[15] One of the very challenging obstacle is pertaining on how is the state should be responsible when this cyber war ever occurred. According to International Law Commission Articles on Internationally Wrongful Acts, every internationally wrongful act of a State entails the international responsibility of that State. Looking at the Project Lakhta case, then how the Russian government is could bear liable and should be responsible for the cyber-attack in this case. Therefore this thesis will find out on how a state responsible for a cyber-attack under international law with special reference to the case of project Lakhta.

[14] Jarno Limnéll, Thomas Rid, 2014, "Is Cyberwar Real? Gauging the Threats", *Foreign Affairs*, Vol. 93, No. 2, p. 166-168.
[15] Rain Liivoja, 2015, "Technological Change and the Evolution of the Law of War", *International Review of the Red Cross*, Vo. 97

B. Research Problem

Based on the background that has been described, the problems to be discussed by the author are:

How is Responsibility of States towards the Issues of Cyberwarfare under International Law: With Special reference to the Case of Project Lakhta?

C. Research Objective

To find out how is Responsibility of States towards the Issues of Cyberwarfare under International Law: With Special reference to the Case of Project Lakhta.

D. Research Benefit

This research was conducted in the hope that it would provide several benefits:

1. Theoretical Benefit

   The research gives an understanding about the concept on how is Responsibility of States towards the Issues of Cyberwarfare under International Law: With Special reference to the Case of Project Lakhta.

2. Practical Benefit

The research provides a better understanding to implement the concept on how is Responsibility of States towards the Issues of Cyberwarfare under International Law: With Special reference to the Case of Project Lakhta for states, officials, academia, or any individuals.