LEBANESE AMERICAN UNIVERSITY

Does Lebanon Possess the Capabilities to Defend Itself from Cyber-Threats? Learning from Estonia's Experience

By

Kristofas Barakat

A thesis

Submitted in partial fulfillment of the requirements

for the degree of Master of Arts in International Affairs

School of Arts and Sciences

April 2019

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS APPROVAL FORM

Student Name: Kristofas Barakat I.D. #: 201205971

Thesis Title: "Does Lebanon Possess the Capabilities to Defend Itself from Cyber-Threats? Learning from Estonia's Experience."

Program: MA in International Affairs

Department: Social Sciences

School: Arts and Sciences

The undersigned certify that they have examined the final electronic copy of this thesis and approved it in Partial Fulfillment of the requirements for the degree of:

MA in the major of International Aff[redacted]

Thesis Advisor's Name Dr. Makram Ouaiss	Signature [redacted]	DATE: 4 / 4 / 2019
Committee Member's Name Dr. Marwan Rowayheb	Signature [redacted]	DATE: 4 / 4 / 2019
Committee Member's Name Dr. Sami Baroudi	Signature [redacted]	DATE: 4 / 4 / 2019

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

THESIS COPYRIGHT RELEASE FORM

LEBANESE AMERICAN UNIVERSITY NON-EXCLUSIVE DISTRIBUTION LICENSE

By signing and submitting this license, you (the author(s) or copyright owner) grants the Lebanese American University (LAU) the non-exclusive right to reproduce, translate (as defined below), and/or distribute your submission (including the abstract) worldwide in print and electronic formats and in any medium, including but not limited to audio or video. You agree that LAU may, without changing the content, translate the submission to any medium or format for the purpose of preservation. You also agree that LAU may keep more than one copy of this submission for purposes of security, backup and preservation. You represent that the submission is your original work, and that you have the right to grant the rights contained in this license. You also represent that your submission does not, to the best of your knowledge, infringe upon anyone's copyright. If the submission contains material for which you do not hold copyright, you represent that you have obtained the unrestricted permission of the copyright owner to grant LAU the rights required by this license, and that such third-party owned material is clearly identified and acknowledged within the text or content of the submission. IF THE SUBMISSION IS BASED UPON WORK THAT HAS BEEN SPONSORED OR SUPPORTED BY AN AGENCY OR ORGANIZATION OTHER THAN LAU, YOU REPRESENT THAT YOU HAVE FULFILLED ANY RIGHT OF REVIEW OR OTHER OBLIGATIONS REQUIRED BY SUCH CONTRACT OR AGREEMENT. LAU will clearly identify your name(s) as the author(s) or owner(s) of the submission, and will not make any alteration, other than as allowed by this license, to your submission.

Name: Kristofas Barakat

Signature: [redacted]

Date: 11/4/2019

LAU
الجامعة اللبنانية الأميركية
Lebanese American University

PLAGIARISM POLICY COMPLIANCE STATEMENT

I certify that:

1. I have read and understood LAU's Plagiarism Policy.
2. I understand that failure to comply with this Policy can lead to academic and disciplinary actions against me.
3. This work is substantially my own, and to the extent that any part of this work is not my own I have indicated that by acknowledging its sources.

Name: Kristofas Barakat

Signature: [redacted]

Date: 11/04/2019

For my mother, father, brothers and my grandmothers.

In memory of my grandfather whose fingerprints graced our lives and shall never be forgotten.

In memory of my uncle and godfather, Gintautas, gone forever from us. Life is unfair taking you so early. The void you left in our lives will never be filled. I will make sure your memory lives on as long as I am alive. May our ancestors honor your arrival with a splendid feast.

For my beautiful Sanaa – always and forever.

Acknowledgments

I would like to express my deep and sincere gratitude to my research supervisor, Dr. Makram Ouaiss, for his advices, recommendations and guidance throughout this research. It was a great privilege and honor to work and study under his guidance. I would like to thank Dr. Marwan Rowayheb who trusted and encouraged me to enroll in the Master's degree in international affairs. I also thank Dr. Sami Baroudi for accepting to be part on the thesis committee.

I am extremely grateful to my father, Habib, and mother, Ingrida, for their love, caring and sacrifices for educating and preparing me for my future. No word can express how grateful I am to what you did, and still doing, for me and my siblings. I thank my entire family for their constant support during this journey. I would like to acknowledge the assistance I received from my uncle, Jihad, who shared great knowledge regarding the topic and my aunt, Hanane along with her husband, Tony, for constantly enquiring on the status of my thesis. To my brothers that began their own University-journey – thank you for always cheering and keeping up with me through the ups and downs. I also thank all my friends in Lithuania that kept motivating me and waiting for my return after a long absence.

Finally, I thank Sanaa Karam for all the encouragement and support that she gave me. I thank you for understanding and for putting up with me through the toughest moments. I thank fate for crossing our paths as you enlightened my life with your presence, love and kindness; always and forever.

Is Lebanon Capable of Protecting Itself from Cyber-Threats? Learning from Estonia's Experience

Kristofas Barakat

ABSTRACT

The growing danger of cyber-threats has forced many states to develop and strengthen their cyber-security capabilities. The complex nature of cyber-threats has a profound impact on traditional international relations, as many states today consider cyberspace as the greatest challenge to their national security. Research literature on cyberspace and cyber-threats is particularly limited in the case of Lebanon, despite Lebanon's interesting cyber-threats history. The domination of traditional security dilemmas have restricted Lebanon from developing a successful cyber-security. The lack of attention and development for cyber-security has made Lebanon an appealing target for various actors to conduct their cyber-operations. The objective of the thesis is to determine whether Lebanon has the ability to defend itself from cyber-threats in spite of a missing cyber-security policy. The thesis offers an analysis of Lebanon's current conditions with regard to cyber-security at various levels. The thesis employs the international legal framework on cybercrime, the Budapest Convention, in order to assess Lebanon's capabilities to counter cyber-threats. Furthermore, this study utilizes Estonia, a small Baltic nation considered as one of the leaders in the field, as a comparative case to further examine Lebanon's cyber-security and identify areas that would bolster Lebanon's capabilities.

Keyword: Budapest Convention, Cyberspace, Cyber-security, Cyber-threats, Lebanon, Estonia, Government, Strategy

Table of Contents

List of Tables

List of Figures

Abbreviations

BDL – Banque du Liban

CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence

CERT – Computer Emergency Response Team

CoE – Council of Europe

CSS – Cyber-Security Strategy

EU – European Union

EISA – Estonian Information System's Authority

GDGS - General Directorate of General Security

ICT – Information and Communication Technologies

ISF – Internal Security Forces

IT – Information Technology

ITU – International Telecommunication Union

NATO – North Atlantic Treaty Organization

NCSPG – National Cyber Security Policy Guidelines

NCSS – National Cyber Security Strategy

OECD – Organization for Economic Cooperation and Development

OMSAR – Office of the Minister of State for Administrative Reform

TRA – Telecommunication Regulatory Authority

UNODC – United Nations Office on Drugs and Crime

WTO – World Trade Organization

Chapter One

Introduction and Methodology

Never before has the world been more interconnected than it is today. The creation of the digital network, otherwise known as cyberspace, has allowed humans around the planet to access and retrieve information at a click of a button. From governments to businesses, from the military to individuals – most, if not all, conduct their business today via cyberspace. Despite the digital network providing opportunities never seen before, it has also become a technological weapon that can be utilized for harmful purposes.

While governments today remain occupied with defending their citizens from other states and even non-state actors, such as terrorist groups, the issues of cyber-security have become prominent concerns in the world. The rise of various cybercrimes, increasing cyber-espionage on states and corporations, concerns regarding terrorists exploiting digital networks to their own benefit and the proclamation of cyberspace becoming the fifth military domain[1] has made the subject of cyber-security a worldwide concern. In 2010, President Barak Obama declared that securing cyberspace has become a matter of national interest for the U.S (Peritz & Sechrist 2010: p.1). For the first time, securing cyberspace became an important matter for U.S. foreign policy. The aftermath resulted in the establishment of the U.S. Cyber Command which is responsible for protecting military and governmental activities on

[1] The other four military domains are the land, sea, air and space.

the digital platform (U.S. Department of Defense, 2010). Other states have also realized the advantages provided by cyberspace that can be utilized to meet their own interests. In 2007, Estonia, considered as one of the most advanced countries in the area of cyber-space policy, had its entire digital infrastructure crippled by powerful cyber-attacks that were allegedly conducted by Russia (Herzog, 2011: p.50-53). For a short time, the international community observed how cyber-attacks can be combined with sudden military attacks, also known as kinetic attacks. In 2008, Russia became the first country to combine cyber and kinetic attacks in its military operations during the Georgian-Russian war (Kozlowski, 2014: 238-240). China has also been heavily concerned with cyber-security. For China, cyberspace has become a double-edged sword. While China has engaged in active cyber-espionage activities that allowed it to obtain technological, political and military secrets from the West and neighboring countries, its government has been concerned with the information circulating on cyberspace that could threaten or affect its closed political system (Raud, 2016: 5).

While the big powers continue to harvest the variety of cyber-activities for their narrow interests, cyber-threats have proven to be more difficult to manage for other states. The aforementioned 2007 cyber-attacks on Estonia, which lasted for twenty-two days, managed to shut-down the websites of the President, the government, the parliament and some political parties, as well as damaging major Estonian banks, internet service providers and telecommunication companies (Ottis, 2008). Cyber-attacks have also had the ability to inflict physical harm on country's infrastructures. In 2009, Iran's nuclear program came to a halt as its nuclear plants centrifuges were ruined through the Stuxnet virus, developed by joint forces from the US and Israel (Sanger, 2012). In 2012, Saudi company Aramco saw its computers devastated by the

"Shamoon" virus, which erased critical information from the computers and forced the enterprise to disconnect its internal network (Perlroth, 2012). In more recent years, it has become apparent that even non-state actors can utilize cyberspace to their own advantage. The effective reach of the infamous Islamic Caliphate (ISIS) in the Middle-East region is attributed to cyberspace, as its members masterfully utilized the digital platform for their propaganda and managed to recruit radicals from all over the world (Sanger, 2016).

The issue of cyber-threats has become a global concern not only because of the damages it causes as just discussed, but also because of its ability to transcend all known physical and geographical obstacles. For instance, the difficulties in identifying the attacker behind cyber-attacks are well summarized in Romaniuk:

"*Firstly, it is difficult to identify the attacker. A cyber-attack in outer space has the characteristics of being long-range and anonymous, and the attacker is able to conduct a cyber- attack against space assets in or through foreign countries. Thus, it is critical to note in this regard that information, as a sort of weapon in and of itself, can flow across international borders while a nation's military, judicial and security agencies and institutions are restricted from carrying-out investigations in a foreign country at will. Second, producing evidence under such circumstance proves incredibly difficult, if not, impossible*." (Romaniuk, 2012, p.4)

In other words, tracking sophisticated cyber-attacks could be equal to mission impossible. As in the case of the cyber-attacks against Estonia in 2007, Russia was only allegedly blamed for the attacks, since the international community could not find any evidence that the cyber-attacks were conducted on behalf of Russian authorities

(Kozlowski, 2014; Herzcog, 2011). Even if we consider that a state can suddenly develop cyber-capabilities to identify perpetrators behind cyber-attacks, there are still legal issues as each country would have its own way of dealing with the cyber-criminals. As universal definitions regarding cyberspace, cyber-attacks, cyber-warfare or other type of cyber-crimes have not been reached, this leaves states, organizations and technical experts to interpret them differently (Hathaway & Crootof, 2012, p.822-832). For example, while The North Atlantic Treaty Organization (NATO) has set a variety of cyber-definitions, its members have developed their own interpretation for cyber-terms. NATO considers cyber-attack as:

"*Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself. Note: A computer network attack is a type of cyber-attack" (*NATO CCDCOE)

its members, for instance the United States defines it as:

"*An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information"* (NATO CCDCOE).

As cyber-attacks are not bound to a single jurisdiction, the sophistication of cyber-technology permits the attacks to be carried outside the territory of one state, this highlights jurisdiction concerns, as the attack could be carried out from country A, utilizing servers from country B and masking its internet address of country C in order to target country D. Unlike traditional crimes that are easy to pinpoint, cyber-crimes raise problems of jurisdictional claims (Cottim, 2010; Weissbrodt, 2013, p.366-368).

The complexity of cyber-attacks, the rising problems in finding a universal definition for cyber-terms and jurisdictional issues have indeed made cyber-threats an intangible weapon. As the situation internationally has become more complex and dangerous, the international community and many states have been striving to minimize, if not to solve, the dangers arising from cyber-threats. For instance, the 2007 cyber-attack on Estonia, despite having paralyzed the state for a short period of time, propelled the small Baltic nation to become one of the leaders in the cyberspace field, actively working on promoting cybersecurity issues in the international arena, including with the EU and NATO[2]. On the global arena, an increasing number of initiatives are aimed at combating cyber-crimes. In 2015, the United Nations Office on Drugs and Crime (UNODC) created a cybercrime repository, where states are able to access a database of legislation, case law and lessons learned on cybercrime that aims to assist countries around the world in their fight against cyber-threats[3]. Actions are also being taken on a global level. In 2012, the Tallinn Manual on International Law Applicable to Cyber Warfare, an initiative by the NATO Cooperative Cyber Defense Centre of Excellence, was published. Created by a group of experts, constituted from academics and practitioners, the Tallinn Manual is a non-binding document that offers comprehensive analysis on how current international law can be applied to cyber-warfare operations (ICRC, 2013; Kilovaty, 2014, p.96). Yet, the most important, and currently only binding document related to the cyber-crime is the

[2] As declared by Estonia's Ministry of Foreign Affairs, cybersecurity is vital for the nation's security. As such, the state has been actively involved in combating various cyber-crimes and creating frameworks for cyber-security. To see more http://vm.ee/en/cyber-security

[3] This database allows countries to easily access variety of procedural legislation on cybercrime of 181 countries. In addition, it will show successful records in cases against cybercrime, compilation of national practices and strategies initiated to combat cybercrime. See more at https://www.unodc.org/unodc/en/frontpage/2015/May/assisting-states-in-their-efforts-against-cybercrime.html

Council of Europe's Cyber Crime Treaty – the Budapest Convention. Originally drafted in 2001 by the European countries, the Budapest Convention permitted other states from different countries to also join the treaty[4]. Furthermore, the key importance of the treaty is that it is binding upon its members, unlike the Tallinn Manual, which forces the parties to cooperate in case of a cyber-crime that has been committed in the signatories' territories.[5] The Budapest Convention contains three main principles upon which all signatories agree once signing the treaty: 1) states that ratify the treaty must adopt cybercrime offenses into their national law, 2) defines procedures that states should adopt for cyber-crime investigation and 3) mechanisms that regulate international cooperation (Vatis 2013). Currently, the convention remains the single binding document that entitles its members to not only strengthen their domestic laws and procedures against cyber-crimes, but also to cooperate on an international level to combat cyber-threats. As such, the Budapest Convention will be considered as the pivotal treaty in combating cyber-crimes throughout this research paper.

While cyber-attacks and their implications on a state's security are growing exponentially, not all states are actively involved in securing their cyberspace. Lebanon, a small state in the Middle-East that borders Israel, Syria and the Mediterranean, has become a victim of a variety of cyber-attacks over the years. Despite the looming threats of cyberspace on its security, Lebanon's stance in its cyber-security is defined by its Telecommunications Regulatory Authority which has openly posted on its website an assessment stating that:

[4] It is stated in the Preamble of the Budapest Convention. See more at https://rm.coe.int/1680081561
[5] Article 45 binds all parties to seek settlement of dispute through negotiations or other means agreed by parties. See more at https://rm.coe.int/1680081561

"Lebanon has not yet developed a vision and a strategy for cybersecurity as there is no government entity to deal with cybersecurity issues; Lebanon has not yet established legislations related to cybersecurity; Lebanon lacks effective integral cybersecurity awareness plans and dedicated campaigns"[6]

Since the state itself openly declares its lack of means to defend its own cyberspace, one should not be surprised for the lack of academic literature regarding Lebanon and issues related to cyber-security. Hussin Hejase, Ale Hejase and Jose Hejase (2015) have conducted a survey study which indicated that even the educated community of Lebanon lacks awareness on cyber-threats and cybersecurity. In Hasan Al-Rizzo (2008) article Lebanon has become a battleground not only for conventional warfare between Hezbollah[7] and Israel, but also for the intensive cyber-warfare between those two sides. Piotrowski (2015) mentions Lebanon in the affairs of cyber-warfare only from the perspective of Hezbollah, and not from the Lebanese state's standpoint. While the problem of cyber-threats in Walid Tohme et al. (2015) work is considered from a state's perspective, their suggested strategic approach to combat these threats is offered for the countries of the Middle-East as a whole and not specifically for Lebanon. Apart from the academic literature, other sources, such as magazines and newspapers, have been by far more attentive to cyber-issues related to Lebanon. In 2012, a virus dubbed "Gauss" that aimed at stealing information from banks in the Middle-East region, mainly targeting Lebanese banks, was discovered (Gjelten, 2012; Williams, 2012). In 2017, Lebanon's Central Bank systems were

[6] See more at http://www.tra.gov.lb/Cybersecurity-in-Lebanon

[7] Hezbollah, specifically its military wing, is listed as a Foreign Terrorist Organization by the US. Department of State and the European Union. See more at https://www.state.gov/j/ct/rls/other/des/123085.htm and http://www.reuters.com/article/us-eu-hezbollah/eu-adds-hezbollahs-military-wing-to-terrorism-list-idUSBRE96K0DA20130722

cyber-attacked, however, it succeeded in foiling those attacks, despite having some of its online services interrupted (Xuequan, 2017; "Lebanon's Central Bank thwarts cyberattack", 2017). While some Lebanese businesses, such as the banking sector, were praised for investing in cyber-security, the Lebanese government is yet to create a platform where individuals and companies could report cyber-breaches to the security authorities (El-Amine 2017). Unfortunately, the general state of cyber-security in Lebanon is dismal, as the country lacks cyber-experts, there are no set budgets for issues related to cyber-security and the general public awareness for cyber-threats remains limited (Schellen, 2017).

While it is apparent that Lebanon has been the victim of cyber-attacks for the past several years, academic literature examining Lebanon's cyber-capabilities remains mostly inexistent.

1.2 Research Question

While a small state such as Estonia has been receiving international acclamation as being a model for its cyber-strategies and combating cyber-threats, Lebanon's capabilities in this domain have yet to be explored. Until today, there has been a lack of attention to cyber-threats implications to Lebanon's security, prosperity and stability. Given Lebanon's frail cyber-security policy framework and lack of research on its cyber-capabilities, this thesis asks the following question:

"Does Lebanon possess the capabilities to defend itself from cyber-threats ?"

The importance of this question stems, as stated above, from the fact that cyber-security and cyber-threats have received limited academic attention in contrast to other

traditional security issues in Lebanon. In fact, due to lack of scholarly literature, Lebanon's cyber-capabilities at all levels cannot be evaluated. Since the danger posed by cyber-threats to Lebanon is too real to be ignored, it is hoped that by answering this question, the research will highlight the gaps in the literature on this subject and evaluate the current capabilities of Lebanon in the area of cyber-security, taking into account the country's weaknesses and possible ways to strengthen its defenses.

1.3 Research Methodology

The research approach in this thesis is a qualitative study where a variety of cyber-activities conducted against Lebanon will be studied. It aims to examine the cyber-capabilities Lebanon possess and whether they are sufficient to counter cyber-threats. To achieve this goal, this research will first establish the fact that Lebanon is under imminent danger of cyber-threats and needs to be protected. Due to the lack of extensive scientific literature on Lebanon and cyber-threats, this thesis will rely on newspaper articles and reports conducted by cyber-security companies.

Having established the fact of impending threats to Lebanon's cyberspace, this research will next assess the state's current cyber-capabilities to counter such threats. Currently, the academic literature is very limited on such topic. Thus, the assessment will be conducted using the following tools: available policy documents, reports and self-assessments by the Lebanese government and its agencies, current Lebanese legislation related to cyber-crimes and newspaper articles on this topic. Finally, WikiLeaks documents will also be reviewed, to determine if classified information leaked reveal unpublished material on the topic by the Lebanese authorities. This

assessment will help us determine if Lebanon is part of any international agreement that contributes to cyber-security by providing expertise and support against cyber-threats.

Having examined Lebanon's cyber-capabilities, the research will then compare Lebanese to international standards for cyber-security. The research determined that the Budapest Convention on Cybercrime is the only binding international agreement that addresses crimes over cyberspace. It must be noted that the Convention only covers issues related to cyber-crimes and child prostitution on the internet. Yet, the elements laid by the Budapest Convention serve as a foundation that help states eventually resist other forms of cyber-threats. In that sense, the Convention's key mechanisms will be examined in order to discover if Lebanon's current cyber-capabilities comply with them.

Finally, to better evaluate Lebanon's cyber-security, the research uses Estonia as a comparative case study. The decision to choose Estonia as a comparison case stems from the fact that it is a small state with limited resources, and yet, has managed to succeed in becoming one of the leaders in the area of cyber-security. The study of the small Baltic state is also important for two reasons: 1) it holds similar geopolitical traits as Lebanon and 2) represents a success model for any small state. In the first case, Estonia and Lebanon share the following traits: a) categorized as small states; b) located in unstable geopolitical regions; c) small populations; d) Lebanon has a long history of sectarian issues, while Estonia with Russian minorities; e) both countries began a new chapter in their history in the early 1990's. The examination of Estonia's case will be done through reviewing Estonia's cyber-security before the 2007 cyber-

attacks and after. The examination of Estonia's cyber-security will allow this thesis to better identify flaws in Lebanon's cyber-security. The research will draw on the rich academic literature regarding Estonia's cyber-security experience, Estonian governmental policies and reports, and cyber-attack incidents reports. Estonia's case will lastly be used in the concluding section, to highlight the areas of the Lebanese government shortcomings and that could be addressed to significantly strengthen its cyber-security.

Throughout the research the author draws on another important source of information namely five expert interviews. Interviewing experts was chosen as scientific literature on the topic of Lebanon and cyber-security is lacking. The interviews supplement the assessment of Lebanon's cyber-capabilities. Two types of interview participants were included. The first, comprised two academics with direct knowledge of the current condition of Lebanon's cyber-security. The second, comprised three private sector experts in developing cyber-security systems. Before beginning the interviews, all certifications and approvals were received from the Institutional Research Bureau. Semi-structured and open-ended interviews were used in order to gather detailed information about the topic[8].

Chapter three will review the scientific literature on cyber-security in the following four areas: definitions and impacts of cyber-threats, cyber-security in international relations, Estonia and cyber-security, Lebanon and cyber-security

Chapter four contextualizes Lebanon's cyber-security current position. It reviews cyber-attacks that have targeted the country. Examines the current policies

[8] A copy of the questionnaire used can be found in the appendix.

and initiatives undertaken by the Lebanese authorities and reviews their effectiveness. The evaluation of Lebanon's cyber-capabilities will be conducted basing itself on the Budapest Convention. The Budapest Convention document is examined to determine the key elements and mechanisms that make the international agreement relevant to Lebanon's cyber-security.

Chapter five studies Estonia's case and achievements in the field of cyber-security. The chapter reviews the steps that Estonian authorities undertook up till the 2007 cyber-attacks, and the changes that have taken place since.

Chapter six will proceed to analyze Lebanon's cyber-security using Estonia as a reference point. This chapter will further identify Lebanon's weaknesses with regard to cyber-security and present the lessons that the Lebanese government could take in order to enhance its cyber-security in the future.

Finally, chapter seven concludes by summarizing the research findings and the highlighting the contribution made to the literature on this topic. The chapter examines the limitations and difficulties faced by the research. This thesis will indirectly provide recommendations on how Lebanese policy-makers can improve cyber-security conditions along with identifying areas for future research.

Chapter Two

Literature Review

2.1 Overview

While many articles, reports and papers can be found regarding cyber-threats and Estonia's initiatives in cyberspace, the same cannot be said about Lebanon. This literature review chapter consists of four main sections: definitions of cyberspace and cyber-threats, a description of cyberspace threats and their implications on international relations, Estonia's cyberspace strategy and a review of the limited literature regarding Lebanon's cyberspace policies and threats.

The conclusion of this literature review reveals the limited amount of existing literature regarding the topic of this research. To be more precise, a very limited number of academic articles cover cyber-security and cyber-threats from Lebanon's perspective as a state. Unfortunately, the rest of available scholarly literature simply mentions Lebanon as a territory or battleground that is used by numerous actors in their cyber-operations.

2.2 Definitions and Impact of Cyber-Threats

In recent years, the topic of cyberspace has become one of the most discussed and debated issues in the world, yet scholars and policymakers have not managed to agree on a universal definition of this concept. As a result, various organizations have

described cyberspace in their own way (DoD, 2010; Fourkas, 2012; Godwin et al. 2014: p. 17; NATO CCDCOE n.d.). Due to its unique characteristics, cyberspace has been embraced as it allows humans to bypass the traditional geographical barriers of the physical world. As cyberspace allows information to be processed and disseminated at a tremendous speed, it has positively impacted a variety of actors, such as businesses, organizations and governments (Manyika and Roxburgh 2011). Nevertheless, cyberspace has also attracted actors that utilize its unique characteristics, to transcend state borders and access information with ease, as a weapon to inflict damage on others (ibid.). Cyber-attacks have become major threats on cyberspace. Like cyberspace, cyber-attacks have no common definition (NATO CCDCOE n.d.). While a variety of cyber-attacks types exist, they are grouped in mainly three ways: 1) cyber-espionage, 2) cyber-terrorism and 3) cyber-warfare. Unfortunately, like the terms "cyberspace" and "cyber-attack", the main forms of cyber-attacks have yet to receive a universal definition, leaving a variety of actors, either states, organizations or others, to define them as they see fit (Jarvis and McDonald 2014; Schreier 2015; NATO CCDCOE n.d.).

Another part of literature highlights the danger that cyber-threats pose to states. In his article, Lewis (2002) highlights the fact that cyber-threats are "weapons of mass annoyance" as a state's critical infrastructure could be endangered or disrupted, terrorists can utilize them as means of publicizing and spreading fear. In 2007, the world was shocked as Estonia, one of the most advanced nations in cyberspace, was heavily cyber-attacked affecting all government websites, two major bank operations, political parties and disabling the email server of the Parliament (Herzog 2011). In the following years, it became apparent that cyber-threats can not only be utilized

alongside conventional military warfare to blind the enemy and limit one sides' casualties, but also to inflict physical damage to critical infrastructure, including nuclear plants. (Farwell & Rohozinski 2011, p.23-25; Kelic, Warren & Phillips, 2008). It has been recognized that cyber-threats can inflict tremendous costs on a state's economy, as its military and local corporate secrets can be stolen, sensitive information on individuals can be acquired and the operations of private sectors can be affected, due to theft of intellectual property (Lewis, 2012; The Economic Impact of Cybercrime and Cyber-Espionage, 2013; Watkins, 2014).

2.3 Cyber-Security in International Relations

The threats emerging from cyberspace have profound implications on today's international relations. Unlike any other technology, cyberspace's sophisticated nature allows it to transcend geographical boundaries. Kissinger (2014) explains that cyberspace poses a great challenge to states, unlike other technologies, the internet has outpaced most rules, regulations and doctrines. As cyber-attacks are easier to be conducted, rather than defended against, it encourages actors to take an offensive stance and build offensive capabilities. In addition, individuals are able to act in ways that have global consequences right from their laptops. According to Kissinger, the problem compounded considering that there is no international agreement that regulates cyberspace Kissinger states that a framework for cyberspace is needed, as the absence of agreements on acceptable rules and limits could lead to a crisis that would strain the concept of international order. The slow progress on dealing with cyber-security globally is further elaborated by Lewis (2018) who states that

negotiations for international cybersecurity norms are being outpaced by the development of offensive cyber-capabilities. Lewis warns that this issue is straining international norms and is endangering the West and its values.

Cyberspace has been challenging the traditional notions of international relations. The traditional international system focused on the state and its interactions with others. However, cyber-innovations have made the private sector a dominant feature in the IR system, as cyberspace depends on the integrity and effectiveness of their performance (Vaishnav et al. 2013). Furthermore, cyber-threats have rendered states unable to fully defend themselves and poses challenges to their national security, as even non-state actors can threaten the State. Unlike traditional historical conflicts, where the identity of contenders were known, conflicts on cyberspace can be caused within states by unknown culprits. As cyberspace has been evolving rapidly, a big gap has appeared between 21st century cyber-innovations and the international relations of the 20th century. Thus, Vaishnav et al. (2013) conclude that there is a need to combine cyberspace and international relations into "Cyber International Relations", where engineering systems are integrated in social sciences.

Kshetri (2016) adds that current existing international standards are insufficient in combating cyber-threats. If in the past traditional warfare and issues related to nuclear wars were the main focus, today, cyber-attacks have become a center of international relations as a nontraditional security issue. Kshetri highlights that due to the asymmetric nature of cyber-attacks, it has given rogue or less developed economic states the capabilities to launch cyber-warfare operations with the possibility of avoiding sanctions or retaliations.

Attempts at analyzing cyber-threats from traditional IR theories were also reviewed. Petallides (2012) analyzes cyber-terrorism through realism, liberalism and constructivism. Petallides admits that the internet with it threats perfectly ticks the boxes of realism, as cyberspace is an anarchic system without a governing body and forces states, alone or with allies, to develop cyber-capabilities to counter threats. In addition, offensive and defensive realists support the idea of striking first the enemy of the state. However, Petallides argues that such view has two weaknesses: 1) realists completely disregard non-state actors who also can conduct damaging cyber-operations; and 2) the nature of the internet renders the state blind, as it is impossible to predict or anticipate a cyber-attack before time. Therefore, Petallides suggest that the combination of neoliberal and constructivist, with some risks, could be a potential solution. He argues that a neoliberal approach would tackle the security dilemma through the creation of international institutions, composed from states and non-state actors, which would maintain global cyber security. The weakness of such perspective is the fact that actors would require to share information, risking of revealing more than they would wish. Petallides also suggest that as constructivism builds on symbols, ideas and their meanings, such perspective is relevant in today's digital age. For instance, the (in)famous group Anonymous is comprised of various people from around the globe with the aim of protecting internet neutrality and having an impact on the real world. Therefore Petallides suggest that in today's era of cyberspace, the relations between states and non-state actors must evolve to adapt to the internet culture.

In contrast, Isnarti (2016) claims that neorealism is the IR theory that provides the best explanation for cyber-war. According to him, liberalism's view is insufficient,

as no powerful existing institution could manage the behavior on cyberspace. Isnarti offers a positive note on constructivism, as in his opinion this IR theory suggests that in order to secure cyberspace, various actors would need to interact and come to an understanding about their different identities and interests. Interestingly, Isnarti concludes however that neorealism is the most appropriate theory as it explains the reason behind cyber-war. According to him, realism regards states as the major actor in cyberspace, and the anarchy surrounding them dictates their behavior in both, physical and cyberspace in order to protect their national security.

2.4 Estonia and Cyber-Security

Estonia has widely become a reference when it comes to topics related to cyber-threats and cybersecurity. The infamous cyber-attacks on Estonia in 2007 could be considered as the pivotal incident that not only led the world to turn its attention to matters regarding cyber-threats, but forced the Baltic nation to proceed in strengthening its cyber-security to avoid such attacks in the future. Herzog (2011) identifies the 2007 cyber-attacks on Estonia as the "wake-up call" for the international community to increase its involvement in combating cyber-threats. Herzog shows us that while the main aim of cyber-attacks was to cripple Estonia's digital infrastructure, the ending result was the international community getting involved, as NATO, the European Union and even Israel, would send their experts to not only help Estonia restore its cyberspace, but also to gather data on the attacks. As it became obvious that Estonia's digital network has also become a target for future cyber-attacks, the government moved on to strengthen the state's cyber-security. As Pernik and Tuoahy (2013) mention in 2008 Estonia became one of the few countries to launch a

cybersecurity strategy that aimes to increase the defense of its digital infrastructure. According to Pernik and Tuoahy the cybersecurity strategy was launched for the period of 2008-2013 and clearly indicated the objectives it wanted to achieve: 1) applying multi-level security measures on a large scale, 2) increasing the level of expertise and awareness on cyber-security, 3) developing and enacting national legislation to secure the usage of information systems, 4) fortifying Estonia's position as one of the leading nations in international cooperation on cyber-security and 5) raising the awareness of cyber-security within the general public. Pernik and Tuoahy highlight that the first and fourth objectives of the national cyber-security strategy were completely achieved and while the other three were not fully achieved, most of the actions and projects related to them were completed. As a result, Pernik and Tuoahy remark that despite Estonia being a small state with limited resources, it has achieved remarkable progress in terms of cyber-security as: 1) the NATO Cooperative Cyber Defense Centre of Excellence is hosted in Tallinn, 2) the "Tallinn Manual" published in 2009 has clearly improved rules governing cyber-conflicts and 3) Estonia has been one of the leading countries in promoting initiatives to improve cyber-security in such international organizations such as EU, NATO, United Nations and others. James Andrew Lewis (2016) hails Estonia in four particular areas: 1) the cyber-culture of the nation, 2) education, 3) enacted legislation and its 4) international cooperation. Lewis reports that Estonia has become a leader in e-governance, as its sophisticated cyber-security technology allows citizens to access systems for internet voting, e-prescriptions, online tax returns and even online health records. As Lewis shows education has been playing a pivotal role in Estonia's cyber-security initiatives, as training programs and awareness campaigns for cyber-security begin when children enter their pre-schools, where other educational

programs target elementary, middle-school and college levels. Lewis also praises Estonia's legal and regulatory frameworks as they have been extensively developed, particularly highlighting the Emergency Act of 2009. The Act requires the private sector to be responsible for vital service provisions to report any cyber incidents to the Estonian Information System Authority after damaged systems are restored. As international cooperation plays a crucial part in Estonia's attempt to secure its cyberspace, Lewis notes that the Baltic State, after its lessons of the 2007 cyber-attacks, will become the first country in the world to create virtual embassies that will be hosted in servers based in Estonia and other friendly countries, as it would allow the state to continue providing e-services in the event of a physical attack that could disrupt the government's functions in the traditional sense. In 2012, Estonia became the first country in the world to recognize internet as a human right by adopting the United Nations General Assembly Resolution 20/8, which states that 'the same rights that people have offline must also be protected online' (Kaljarand 2016: 120-123). In other words, the same rights that apply to Estonian citizens in the real world are applicable on cyberspace.

Jeffrey Carr (p.247) notes that in addition to the establishment of the NATO Center of Excellence, Estonia has established the Cyber Defense League (CDL) which is comprised of volunteers. According to Carr, these volunteers are cyber-security professionals from both public and private sectors and in case of conflict would perform their duties under military command. Furthermore, Carr writes that these volunteers have regular weekend exercises that would allow them to prepare for cyber incidents. Shardon Cardash, Frank Cilluffo and Rain Ottis (2013) note that while it is difficult to assess the current capabilities and effectiveness of the Cyber Defense

League, due to lack of serious cyber-attacks since its establishment, yet high expectations are given to this concept. For instance, Cardash, Cillufo and Ottis marked that the CDL is engaged in raising cyber-security awareness as well as improving the level of expertise of specialists in cyber-security field and assisting in the protection of critical information infrastructure. Cardash, Cillufo and Ottis further demonstrate the advantages of the CDL by emphasizing that the volunteers participate in tactical military exercises and were able to create a suitable environment for the state to host international exercises "for the price of coffee", which otherwise would have cost enormous amounts of money.

2.5 Lebanon and Cyberspace

In the case of Lebanon securing its cyberspace, the available academic literature has proven to be very limited. As a matter of fact, the literature relating the state of Lebanon to cyberspace is barely existent. An exploratory research conducted by Ale Hejase, Husin Jose Hejase and Jose Hejase (2015) revealed that the Lebanese, particularly the educated community, are not prepared to face the cyber-threats and have yet to realize the actual danger of cyber-attacks. The fact that Lebanon has become a target by various actors in today's cyberspace has been announced by Kaspersky Lab[9] which discovered that the infamous "Gauss" virus, was specifically created to target the Lebanese banks with the aim of infecting computers and transmitting various transaction data to other parties (Zarate 2015).

[9] Kaspersky Lab is a software company based in Moscow which specializes in analyzing various cyber-threats and developing security software to combat these threats.

More interestingly, most of the available literature pertaining to Lebanon and events related to cyberspace are connected to the activities conducted by the Hezbollah group that is based in Lebanon. For instance, Hasan M. Al-Rizzo (2010) and Stephane Bernard Azan et al. (n.d) mention Lebanon in the cyber-warfare conflict between the Hezbollah group and Israel, during the 2006 military conflict between the two sides. Al-Rizzo (2010) states that while Lebanon did not declare or participate in the war as a state, Hezbollah's success in gaining popularity and the support of the Lebanese population in the military conflict could be attributed to its skillful utilization of cyberspace. While the Lebanese government has yet to develop a strategy or legislations relating to cyberspace, Hezbollah has integrated a cyber-unit within its organization since the beginning of the 21st century (Jean-Loup 2015: 297). In short, a non-state actor such as Hezbollah has fully involved itself in cyberspace activities, while the state of Lebanon has yet to take an active stance.

Chapter Three

Lebanon's Case Study

3.1 Political Background

Having a total area of 10,452 square km [10] and a population of around 6 million people[11], Lebanon is one of the smallest states in the Middle-East region which borders Syria, Israel and the Mediterranean Sea. Despite its size, Lebanon has always been considered not only as an important commercial place, but also as the center of Middle-Eastern conflicts[12].

Since gaining its independence from the French in 1943, Lebanon's modern history could be described as turbulent. Once known as the "Switzerland of the Middle-East" with a booming economy, Lebanon fell into a 15-year civil war from 1975 until 1990 which devastated the country.

The major reasons behind Lebanon's turbulent history are the complex sectarian problems and foreign interference. Lebanon's Independence was built on the National Pact of 1943 which was a power-sharing agreement made between the Christians and the Muslims (Karam 2017, p.2). As a result, since its independence Lebanon's political life has been dominated by sectarianism which was

[10] Data retrieved from the US Central Intelligence Agency (CIA) at https://www.cia.gov/library/publications/the-world-factbook/geos/le.html
[11] *Ibid.*;
The World Bank Population Data can be seen at https://data.worldbank.org/indicator/SP.POP.TOTL?locations=LB
[12] "Lebanon country profile," *BBC*, Dec. 6, 2017. Accessed 25 March, 2018 at See more at http://www.bbc.com/news/world-middle-east-14647308

institutionalized by the country's elite to serve their interests. The National Pact itself was an unwritten agreement between the Christian and Muslim communities which specified the appointments to major positions[13] and the parliamentary seats division.

The first turmoil in the independent Lebanon occurred in 1958. This was the result of internal and external events: the rising tensions between Christians and Muslims internally, the turmoil occurring in the Middle-East region with the establishment of the state of Israel, the rise of Egypt's leader Jamal Abdul Nasser, rising Arab nationalism, the struggle for influence in the region between the United States and the Soviet Union, and the eventual U.S. military intervention in Lebanon (Sorby 2000). Thus, the first crisis occurred as a result of both sectarianism and the events happening between regional and major powers of the world.

Eventually, the combination of heating rivalry during the Cold War between the United States and the Soviet Union in the region, the Arab-Israeli conflict, souring relations between Arab states and rising sectarian tensions internally led Lebanon to the disastrous Civil War. The Civil War that lasted for 15 years witnessed the consolidation of Palestinian guerillas' power within the state and their clashes against the Lebanese right-leaning Christian parties. Israel's invasion in 1982, militia groups' control over areas of the country, the collapse of state institutions, the crash of the economy and the complete division of the Lebanese population along sectarian lines further weakened Lebanon and was the source of new political tensions and conflicts (Makdisi and al-Khalil 2013, p.22-23). The end of the Lebanese Civil War came with

[13] According to the National Pact, the President must be a Maronite representative, the Prime Minister – a Sunni representative, the Speaker of the Parliament – a Shia representative.

the Ta'if Agreement of 1989 which restored Lebanon's consociational democratic system under Syrian military tutelage.[14]

While the Ta'if agreement temporarily froze the sectarian conflict that enraged the country, it did not permanently bring peace and harmony to the state. From 1990 onward, Lebanon witnessed political assassinations and periods of civil unrest[15], paralyzed governments[16] and spillages of Middle-East conflicts[17] that continue to affect Lebanon's integrity and stability.

In general, Lebanon's unfortunate position in the Middle-East region is best depicted by Sorby (2000, p.84):

"*Indeed Lebanon was a mirror which reflected Arab rivalries and activities. When the Arabs were at peace with each other, generally Lebanon too was at peace with itself and with its neighbours. But when the Arab countries were engaged in intrigue and plotting against each other, Lebanon, because of its circumstances, was bound to be involved."*

Alas, this depiction still applies today. Lebanon's security is constantly being threatened by conflicts and rivalries in the Middle-East in parallel to the fluctuating sectarian tensions within the state. While traditional security problems continue to pester Lebanon, it must now direct its attention to the newest set of global hazards namely: cyber-threats.

---

[14] The Ta'if agreement is an agreement that brought the warring parties in Lebanon into a consensus to end the Civil War and restore peace. It was designated to restore Lebanon's sovereignty and aimed at abolishing the political sectarianism. However, the latter subject has yet to be fulfilled. More can be found at https://peacemaker.un.org/lebanon-taifaccords89

[15] DeFraia, Daniel, "Lebanon's assassinations: A timeline", *Agence France-Presse,* 26 March, 2018. https://www.pri.org/stories/2012-10-22/lebanons-assassinations-timeline

[16] Perry, Tom, "Lebanon government denounces Hezbollah "coup" in Beirut", *Reuters,* 26 March, 2018. https://www.reuters.com/article/us-lebanon-conflict-idUSL0742599820080509?sp=true

[17] Daragahi, Borzou, "Middle East: Three nations, one conflict", *Financial Times,* 26 March, 2018. https://www.ft.com/content/b6f93e4e-e584-11e3-8b90-00144feabdc0

Since cyber-threats have so far been ignored in Lebanon's security agenda, the next section will presentthe fact that these threats have been looming around the state longer than one could expect. Truly, Lebanon has been dragged into the contemporary cyber-operations, while somehow its cyberspace and attacks on it have been overlooked not only by its own authorities, but by the international community as well.

3.2 Cyber-Threats against Lebanon

Although cyber-attacks against Estonia were labelled the first ever cyber-war, Lebanon could challenge Estonia for this title. Astonishingly, while the awareness and strategies regarding Lebanon's cyber-security are relatively low and slow to progress, the state was already exposed to cyber-war even before the infamous cyber-attacks in Estonia.

The 2006 Summer War which took place in Lebanon witnessed clashes between the Israeli forces and the Hezbollah militia group[18]. While the battles resulted in casualties on both sides and destroyed buildings and other infrastructures, this war was in a way different. Al-Rizzo (2008, p.400) notes that while both sides engaged in conventional war, intense battles were simultaneously being fought on the internet. As Al-Rizzo (2008, p.400) explains, the war on internet, or what he calls the cyber information war, was heavily utilized by both sides to inflict psychological pressure on each other and to legitimize their own actions. The actions undertaken by both resulted in thousands

[18] The 2006 Summer War was a war that occurred between Israel and the Hezbollah group on Lebanon's ground. The war began when Hezbollah group kidnapped two Israeli soldiers and in retaliation Israel sent its ground forces to Lebanon. To see the timeline of the war, see more at https://web.archive.org/web/20060928081123/http://www.dailystar.com.lb/July_War06.asp

of websites being hacked that spread false information, communication networks being overtaken by each other and other information channels being penetrated. While Lebanon as a state was not a participant, its cyberspace was still utilized by the Hezbollah militia group during the war. Piatowski (2015) states that as long as Iran's cyber-capabilities will continue to augment, it should be expected that Hezbollah will accordingly improve its own cyber-operations. Since Hezbollah is based in Lebanon, it can be indirectly assumed that the state's cyberspace will be utilized or that Lebanon will be again dragged into a cyber-war as long as the militia group continues to develop its cyber-capabilities and conduct cyber-operations. Since Lebanon's cyberspace was utilized in a cyber-war in 2006, there is a high possibility that such attacks may be repeated.

One might argue that the battle on the internet that occurred between Hezbollah and Israel cannot be considered as a cyber-war with Lebanon, as the state itself did not conduct any cyber-operations and Israel's cyber-attacks were directed at Hezbollah. However, the following cyber-attacks events will prove that these attacks were focused and aimed on the state itself. In 2017, it was reported that despite the Central Bank of Lebanon's success in thwarting a cyber-attack that targeted its email systems, it had to suspend some of its online services as a safety measure (Xuequan, 2017; "Lebanon's Central Bank thwarts cyberattack", 2017). The same year, it was reported that Iranian hackers attempted a large scale hack into the emails of high ranking Lebanese officials and institutions such as President Michel Aoun, Prime Minister Saad Hariri, the ministers of Justice, in the army and at some Lebanese banks[19]. If the cyber-attacks on

[19] Saint-Paul, Patrick, "Téhéran sponsor d'un piratage massif contre le gouvernement d'Hariri", *Le Figaro*, Nov. 26, 2017.

Estonia in 2007 received international scrutiny, then the 2012 cyber-attack on Lebanon should have also received some of the attention, yet somehow it was disregarded. In 2012, a virus dubbed "Gauss", which had the ability to track financial transactions of people,[20] was discovered in the Middle-East region, specifically in the territories of Lebanon, Israel and Palestine. More interestingly, Goldman (2012) reported that out of the 2,500 reported incidents related to the Gauss virus, 1,600 of them were found in Lebanon. After further investigations and decoding of the virus, it became evident that the creation of "Gauss" was sponsored by an unidentified nation-state to specifically target Lebanese banks in order to obtain and transmit various data transactions (Zarate, 2015). It must be noted that the price tag of creating such a virus is extremely high. According to some reports, the Gauss virus could have cost several millions dollars due to its sophistication[21]. These events support the belief of some of the interviewees for this thesis that one of the main threats to Lebanon's cyber-security are foreign states[22]. It leaves us to contemplate why another nation-state would sponsor such an expensive project to target Lebanon. Whether it was to retrieve financial information on government members or people affiliated with the Hezbollah military group remains a mystery. While foreign states are the biggest threat, non-state actors, must not be overlooked as they can also collect and misuse financial and political information[23]. In addition, Lebanon should not overlook individual hackers as they also

[20] "Virus found in Middle East that can spy on finance transactions", *Reuters*, Aug. 9, 2012.
In addition, all five interviewees mentioned the Gauss virus and its implication.
[21] Gilbert, David, "Cost of Developing Cyber Weapons Drops from $100M Stuxnet to $10K IceFog", *International Business Times*, Feb. 6, 2014.
[22] Khalife, Joseph. Personal interview. 15 Jun, 2018;
Khayrallah, Jean. Personal interview. 29 Jun, 2018.
[23] Khayrallah, Jean. Personal interview. 29 Jun, 2018.

pose a threat to the state's cyber-security[24]. The recorded cyber-attacks along with the statements of interviewees confirm that Lebanon, as a state, has been exploited by cyber-attacks by different actors, whether nation-states, non-state actors or individual hackers.

From the aforementioned information, few specific concerns emerge related to Lebanon and cyber-attacks – how many have not been traced up till today, and how many have been hidden from the public. The first concern is related to the technical aspect of cyber-attacks. It is a well-known fact that cyber-attacks, in some cases, are hard to be detected and can remain in a breached system for a while until detected, especially if the threat is relatively new and has not been seen before (Raiyn 2014, p. 252). It becomes even worse when considering Lebanon's situation with cyber-security. The second matter is related to the Lebanese authorities' transparency. Lebanon's institutions are known for extensive corruption and lack of transparency to citizens (Salem, 2017; Freedom House Lebanon Report, 2017). Thus, a high possibility remains that cyber-attacks, especially those that succeeded in their original mission, are hidden from the public. For instance, for the month of March 2018, the Kaspersky Real-Time Map has identified more than 100,000 cyber-attacks and infections in Lebanon[25]. However, such numbers of cyber-attacks are unknown to the

[24] Barakat, Jihad. Personal interview. 5 Jul, 2018;
Karam, Marie-Line. Personal interview. 5 Jul, 2018

[25] The Kaspersky Real-Time Map shows real-time cyber-attacks that are happening in the world. They are identified only if the Kaspersky anti-virus systems are installed on individuals, businesses, or governmental institutions computers. For the month of March of 2018, more than 100,000 cyber-attacks and infections were recorded for Lebanon. It must be noted that every day at 00.00 GMT time, the detection system is reset to 0. See more at
https://cybermap.kaspersky.com/stats#country=34&type=oas&period=m

majority of the citizens, as the Lebanese authorities have not reported nor published such information.

The above information confirms one major point – Lebanon's cyberspace is constantly bombarded by cyber-attackers and deserves to receive national and international attention for that matter. Like Estonia's 2007 cyber-attacks that became the cornerstone to many academic and policy researchers in the field of cyber-security, Lebanon could serve as a case study of how a state faces contemporary and sophisticated cyber-threats with no proper cyber-security mechanisms. Cyber-threats should become an important topic on Lebanon's security agenda. The following part will discuss the Cybercrime bureau which had high expectations in defending Lebanon's cyberspace from cyber-threats.

3.3 Initiatives, Strategies, and Regulations for Cyberspace

When it comes to regulations and strategies, Lebanon has a long way to go to catch up to Estonia. If the latter is known for declaring cyberspace as an important factor for its existence, Lebanon is known as a state that openly states its lack of vision or strategy when it comes to cyberspace[26]. Lebanon's critical condition in cyber-security strategies has been noticed in the world. According to the International Telecommunication Union Global Cybersecurity Index (ITU GCI) 2017, Lebanon has been marked as a state in the initiating stage in cybersecurity which means that the state is only aware or only started making commitments in developing initiatives. At

[26] Check chapter one for the official statement found on the Telecommunications Regulatory Authority of Republic of Lebanon.

the global level, Lebanon is ranked in the 119th position on the global rank in cybersecurity, while in the Arab region it is ranked 15th out of 22 countries.[27]

Although Lebanon has no cyber-strategy, it cannot be said that the state did not attempt to deal with the issue. In 2012, the Presidency of the Council of Ministers (PCM) created the National Cyber Security Committee to produce a national strategy that would defend governmental websites[28]. The committee contained members from different public institutions that were tasked to prepare cyber-security policy guidelines that could be adopted by all public agencies[29]. Eventually, with the recommendation of the National Cyber Security Committee, in 2015 National Cyber Security Policy Guidelines (NCSPG) were prepared by the Office of the Minister of State for Administrate Reform (OMSAR) that set a minimum level of cyber-practices consistent with international security standards to be adopted and incorporated in all public institutions[30]. This first initiative by the Lebanese government to increase the security practices in cyberspace was aimed as a starting point for public agencies to build cyber-security. However, studying the concept NCSPG more carefully it becomes evident that the Lebanese government somehow managed to make this initiative illogical and paradoxical. Plenty of irrationalities can be noticed in the cyber-initiative: the members that were behind its creation, its name which encompasses the word "national" and finally the statement that underlines to whom it was created.

[27] Information retrieved from the International Telecommunication Union Global Cybersecurity Index 2017 report p.53-54. See more at https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
[28] The creation of National Cyber Security Committee came with the issued decision number 32 on 25th July 2012. See more at http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Pages/NationalCyberSecurityPolicyGuidelines.aspx
[29] *Ibid*.
[30] *Ibid*.

While the word "national" should cover the entire state, the NCSPG aims to outline guidelines for public institutions, as such not including the private sector. Furthermore, the National Cyber Security committee had members from OMSAR, the Ministry of Interior and Municipality, the Ministry of Economy and Trade, the Ministry of Defense, the Ministry of Telecom and the Central Bank of Lebanon (Lebanese National Cyber Security Policy Guidelines 2015, p.4); yet, the expertise and the opinion of the private sector was not taken into account, since no representative from the latter could be found on the committee. This comes surprisingly as countries formulating "national" initiatives usually include the private sector in creating policies, strategies or other frameworks. For instance, leaving aside Estonia, states like the United States, Singapore, France and others stress on the importance of the private sector's participation in developing cyber-security to counter cyber-threats[31]. Thus, Lebanon somehow attempted to create a "National" framework without incorporating the private sector. Furthermore, the attempt to unify all ministries under one cyber-defense umbrella ended up as a failure, as each one remained separate from the other[32].

The second problem of the NCSPG is its framework being completely outdated from the modern reality of cyber-security and cyber-threats. If analyzed carefully, throughout the NCSPG document the word "cyber" is not utilized. This is confusing as the initiative is called National Cyber Security Policy Guidelines, yet no words

[31] The national cyber strategies of the United States, Singapore and France state the importance of private sector's partnership in creating and developing cyber-security on all levels. The US view on private sector can be found at https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf p.3-4; Singapore's view - https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf p.4,29; France's - https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/information-systems-defence-and-security-frances-strategy p.3

[32] Chebat, Khaled. Personal interview. 1 Sep, 2018.

related to cyber is found. Furthermore, when it comes to general security the policy seems to be more concentrated on providing minimal guidelines for the individual and physical security of the assets through which cyberspace flows. For instance, the entire Part 2 of the NCSPG is dedicated to "*Accountability and Access Control"*, which aims to protect the Lebanese government data and access to IT assets. After proper examination it appears to be simply dedicated to individuals with recommendations regarding passwords, authorized access to specific programs and accountability in tracking user's actions on the computer (Lebanese National Cyber Security Policy Guidelines 2015, p.17-23). Another section that could be related to security is the "*Physical and Environmental Security*". Yet again, this part of security merely suggested safe locations for the IT installations, protection from environmental threats, assets that should not be left unattended or secure disposal of equipment (Lebanese National Cyber Security Policy Guidelines 2015, p.32-41). These security guidelines completely fail to address even the basic cyber-threats. It seems as if the Lebanese government perceives threats to its data and IT information from a physical interaction perspective as when someone obtains a civil servant password, obtains important information from an office or simply damages a hardware that contains data. This indicates that the Lebanese government is completely out of touch with cyber-reality, since today accessing and stealing information is done remotely through the internet without the need of the culprit to be physically in the location. Cyber-threats are not adequately identified and nor are the steps to counter them. While the Lebanese government released a set of cyber-security guidelines, their impact was limited as few beneficial recommendations were proposed on what to do in case of cyber-attacks. While the NCSPG is the only strategic framework that is connected to cyber-security,

it was not the sole initiative. In 2006, the Lebanese Internal Security Forces launched the Cybercrime Combating Bureau to combat cyber-threats. This initiative will be discussed separately later on.

Other than measures taken to improve cyber-security, there were attempts to create an accessible and safer cyberspace environment through e-government and e-commerce laws. In the e-government case, the matter took many years till it finally saw the light. The first strategy relating to e-government was released in 2002 with the vision of providing public services online to citizens, reducing the time of citizens in filling required documents through traditional means, making the government's ability to communicate and notify citizens easier and facilitating information exchange between government institutions (E-Government Strategy for Lebanon 2002, p.4). While such strategy was released nearly two decades ago, the e-government still has a long way to go and is still not fully operational. E-governmental services have taken a long period of time to develop: the e-taxation system for public use was released in 2011; services for civil servants and their medical compensation automated system was initiated in 2010; a website and a hotline connected to the Tourism police for tourists' complaints in Lebanon was launched in 2011; and, Water Evaluation and Planning electronic system was launched in 2011 (Choueiri et al. 2013, p.54-55). It also took almost a decade for many governmental services to actually be digitalized and some have yet to be fully effective and functional. In their limited scope study of e-government services and public trust, Alaaraj and Ibrahim (2014) found that the e-administration is not trusted by the public as most of its procedures are still conducted manually and have yet to be digitized. While the e-government services took time to develop and some have still to become fully operational, it is obvious that it is

progressing steadily. It has yet to be seen if Lebanon can harness the opportunities and benefits of e-government by fully digitizing its services.

Another important proposition that did not materialize up till now has been the e-commerce laws. Despite e-commerce being on the rise in Lebanon, there continues to be a lack of e-commerce laws along with legal frameworks for e-transactions[33]. This is surprising as the Ministry of Economy & Trade has stated the importance of e-commerce back in 2002 and actually worked on its legal and regulatory framework[34]. In addition, as Fayad and Kazzi state (2015, p.40-41), Lebanon's attempt to incorporate electronic evidence and electronic signature to its Code of Civil Procedure was attempted back in the year 2000, when the bill was approved by the Council of Ministers, but not endorsed by the Parliament. Once again, an initiative undertaken by the Lebanese government was not realized and undermines Lebanon's commerce in the region. For instance, Chelala and Ghalayini (n.d.) highlight four negative effects due to the absence of e-commerce laws:

1. Competition with regional countries – international or local firms will choose to launch online services in neighboring countries (where e-commerce laws are available);
2. Online payment and security – people will continue paying in cash, rather than online due to the lack of trust in the level of security and protection of personal data;
3. Consumer trust – consumers are avoiding using Lebanese payment gateways due to the absence of e-commerce laws; and,

[33] Retrieved from the International Trade Administration. U.S. Department of Commerce. See more at https://www.export.gov/article?id=Lebanon-ecommerce. Accessed

[34] E-commerce was seen as a tool that can enhance Lebanon's economy in the world. Development of e-commerce laws was being conducted through EU funded project. See more at http://www.economy.gov.lb/en/projects/e-commerce

4. E-Signature – global third party online payment processors, such as PayPal, are reluctant to enter the Lebanese market.

Lebanon's inability to act swiftly and implement measures that would be up-to-date is costing the state not only in terms of its security, but also in terms of its economy.

The above stated facts lead to a puzzling conclusion. While efforts were made to improve, to a certain degree, Lebanon's cyberspace many of the initiatives failed to materialize. Although some strategies were released, many were left incomplete. It remains difficult to explain why the Lebanese government is so inconsistent in developing a complete cyber-initiative. One possible answer could be that the Lebanese political elites are not informed and lack general knowledge on cyber-threats and cyber-security[35]. Another explanation could be related to the lack of pro-active planning and long-term strategy building by the Lebanese government[36].

The following section will present the only available governmental agency, the Lebanese Cyber Crime Bureau, which possess the capabilities to counter cyber-threats directed to Lebanon.

3.4 Lebanon's Cyber Crime Bureau

One initiative related to Lebanon's cyber-security deserves particular attention. In 2006, the Internal Security Forces (ISF) established the Cybercrime and Intellectual Property Rights Bureau, commonly referred to as the Cybercrime Bureau[37], to combat

[35] Khalife, Joseph. Personal interview. 15 Jun, 2018;
Khayrallah, Jean. Personal interview. 29 Jun, 2018.
[36] Chebat, Khaled. Personal interview. 1 Sep, 2018.
[37] Hereinafter the Cybercrime Bureau will be referred simply as the Bureau.

online crimes such as identity theft, money laundering and child pornography[38]. Again, Lebanon could be categorized as one of the earliest states to take such measures in securing cyberspace. However, being one of the earliest does not necessarily mean being one of the most efficient and effective. Since its creation in 2006, the Cybercrime Bureau has been controversial in its activities. In fact, even the creation of such a unit has been questioned. The Bureau was established through a Service Memorandum 204/609 and not a legislative decree which puts in question according to some the legitimacy of such an entity (Frangieh 2014). From a legal perspective, such an issue undermines the Bureau's authority to participate in law enforcement tasks or obtaining assistance from international and local parties.

Leaving aside the legality of the Bureau, another aspect that drew major criticism is its activities. Established for the purpose of combating cyber-crimes, the Bureau has earned a reputation of repressing opinions in cyberspace rather than combating cybercrime. In 2010, the Bureau attracted attention by detaining a student that criticized the ex-president of Lebanon, Michel Sleiman, over the internet.[39] In 2011, a Lebanese musician, Zeid Hamdan, was detained for a song "General Soleiman", which criticized Lebanon's politicians and warlords[40]. The peculiarity of this detention was that the song was posted 18 months prior to his detention. In 2014, Karim Hawwa, 21 years old, was detained for sharing a Facebook article that accused

[38] "FACTs on Anti-Cybercrime and Intellectual Property Rights Bureau", *The Daily Star*, Dec. 07, 2016. Accessed 25 March, 2018 at http://www.dailystar.com.lb/News/Lebanon-News/2016/Dec-07/384401-facts-on-anti-cybercrime-and-intellectual-property-rights-bureau.ashx

[39] Adrian Blomfield, "Man Arrested for 'insulting Lebanese President on Facebook," *The Telgraph*, Jul 28. 2010. Accessed April 1, 2018 at https://www.telegraph.co.uk/news/worldnews/middleeast/lebanon/7914474/Man-arrested-for-insulting-Lebanese-president-on-Facebook.html

[40] "'General Suleiman' Song Lands Musician in Jail," *Al-Naharnet*, Jul. 27, 2011. Accessed April 1, 2018 at http://www.naharnet.com/stories/en/11364.

Nouhad al-Machnouk, the Interior Minister, of outsourcing to a company related to Israel[41]. In 2017, a Lebanese journalist was interrogated about his blog were he criticized the President of Lebanon, the Foreign Minister and other officials for their corruption and the deaths of refugees in the army's custody[42]. The Bureau has also been criticized for applying double standards as those online commentators without any political connection are being detained, yet those affiliated to political members or groups are left untouched[43]. These reported events match the affirmation of all the interviewees for this research that the Cybercrime Bureau has been transformed into a political tool to surveil, monitor and control information over cyberspace[44].

However, recent scandals related to the Cybercrime Bureau eclipse the acts of the latter against individuals. The most recent, and currently ongoing scandal is related to the former chief of the Cybercrime Bureau, Suzan El-Hajj. It was reported that the former head of the Bureau was arrested and accused for falsifying charges against Ziad Itani, prominent Lebanese actor, for collaboration with Israel[45]. It is believed that the ex-chief of the Bureau cooperated with a hacker to frame the Lebanese actor. While the outcome of this investigation has yet to be seen, it is clear that the high-level

[41] "Cybercrime Bureau's ever-growing powers threatening freedoms in Lebanon," *Al-Akhbar*, Nov. 22, 2014. Accessed April 1, 2018 at https://english.al-akhbar.com/node/22605
[42] Chehayeb, Kareem. "Cybercrime Bureau interrogates journalist," *The Daily Star*, Jul. 11, 2017. Accessed April 1, 2018 at http://www.dailystar.com.lb/News/Lebanon-News/2017/Jul-11/412330-cybercrime-bureau-interrogates-journalist.ashx
[43] Khatib, Lina and Bassem Deaibess. "Lebanon's cybercrime arrests threaten state's credibility," *Middle East Eye*, Jan. 13, 2017. Accessed April 1, 2018 at http://www.middleeasteye.net/columns/lebanons-cybercrime-arrests-threaten-states-credibility-625803839
[44] All five interviewees have agreed that the Bureau has become a surveillance institution that monitors the Lebanese population activities over cyberspace.
[45] "Lebanese ex-colonel 'faked' charges against actor accused of spying for Israel", Al-Arabiya English, Mar. 3, 2018. Accessed April 1, 2018 at http://english.alarabiya.net/en/News/middle-east/2018/03/03/Lebanese-ex-colonel-faked-charges-against-actor-accused-of-spying-for-Israel.html; "Ziad Itani Freed as Arrest Warrant Issued for Suzanne al-Hajj," *Naharnet*, Mar. 13, 2018. Accessed April 1, 2018 at http://www.naharnet.com/stories/en/243425

officials and politicians are exploiting the Cybercrime Bureau for their own interests, rather than utilizing it for its original purpose – combating cyber-crime[46]. The biggest scandal, which could be called as unexpected and shocking knowing Lebanon's instability is related to a report related to digital mass surveillance. In 2015, Citizen Lab reported that the General Directorate of General Security (GDGS) and the ISF were utilizing "FinFisher" malicious software for surveillance operations within Lebanon[47]. While there was no direct mention of the Cybercrime Bureau in this report, one could easily guess, according to various sources, that it played a role in this surveillance incident since it is equipped with up-to-date technologies. In another instance, WikiLeaks database exposed the Bureau's attempt to obtain a new software for spying. In 2015, WikiLeaks e-mails showed that Bureau contacted an Italian malware surveillance company, Hacking Team, to gather information on the GALILEO Remote Control System software, which is utilized to hack smartphones[48]. Further leads revealed that the demonstration of this software was probably carried out in Beirut[49] and that a contract to hack 50 individuals was being negotiated with the Hacking Team for a sum of €450,000[50]. The Bureau's controversial activities do not end here. In early 2018, the Electronic Frontier Foundation and Lookout reported to

[46] While the case is ongoing, many new charges were put forward against the ex-chief of the Bureau. See more at https://aawsat.com/english/home/article/1200336/lebanon-suzan-hajj-suspected-hacking-government-security-websites. Accessed Nov 25, 2018.
[47] Information was retrieved from the Citizen Lab, which is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto. More information can be found at https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/
[48] E-mail conversation can be found https://wikileaks.org/hackingteam/emails/emailid/131690. Accessed Apr. 1, 2018
[49] More information can be found at https://wikileaks.org/hackingteam/emails/emailid/11959. Accessed Apr. 1, 2018
[50] Quino, Zalfa. "#HackingTeam Leaks: Lebanon's Cybercrime Bureau Exploited Angry Birds to Surveil Citizens' Mobile Devices," *Global Voices Advocacy*, Jul. 28, 2015. Accessed April 1, 2018 at https://advox.globalvoices.org/2015/07/28/hackingteam-leaks-lebanons-cybercrime-bureau-exploited-angry-birds-to-surveil-citizens-mobile-devices/

have uncovered a global cyber-espionage campaign, Dark Caracal that targeted Android phone users around the world[51]. It was stated that people in the U.S., Canada, Germany, Lebanon and France have been infected with the virus. Further investigations on the malware left many specialists astonished. After the Dark Caracal was disseminated, the cyber-espionage malware that targeted Android cellphones data was traced back to the headquarters of Lebanese General Security Directorate in Beirut (Dark Caracal Cyber-espionage at a Global Scale 2018). One could assume that the Cybercrime Bureau had a part in this global spying campaign, due to its technical abilities. If not, then the Bureau was supposed to but failed to protect the Lebanese citizens that were drawn into this incident, as this cyber-espionage attack was stealing all kind of information found in the user's Android phone. It should be considered that the culprit of cyber-espionage, the GDGS, was within the national boundaries. It should not come as a surprise that Lebanon has launched a cyber-espionage campaign. Despite the fact that the state's cyber-security is in a jeopardy, Lebanon has produced experts in cyberspace that are recognized in major tech-companies[52]. The problem in utilizing such experts is the lack of an institutional body that could utilize such experts in a proper and beneficial way[53].

Originally, the Cybercrime Bureau was an initiative that was aimed at combating cyber-threats, including cyber-espionage. Yet, the revelations made in this section clearly assert that this entity was instrumentalized to conduct cyber-espionage

[51] Gebhart, Gennie. "Dark Caracal: Good News and Bad News," Electronic Frontier Foundation, Jan. 19, 2018. Accessed April 1, 2018 at https://www.eff.org/deeplinks/2018/01/dark-caracal-good-news-and-bad-news
[52] Khalife, Joseph. Personal interview. 15 Jun, 2018.
[53] *Ibid.;*
Chebat, Khaled. Personal interview. 2 September, 2018.

activities and to consolidate the power of higher Lebanese authorities over the internet. The allegations involving Lebanese security intelligences in the Dark Caracal incident allows us to assert that Lebanon as a nation-state has become capable in participating in international espionage. Yet, this capability can have profound implications on Lebanon from a legal standpoint and honoring international agreements regarding privacy and freedom of speech. The Bureau's involvements in spying indicates it has disregarded the privacy rights of the Lebanese citizens. As it stands, Lebanon's cyber-security raises many concerns. The lack of complete policies by the Lebanese authorities restrains the tools that Lebanon could use to combat cyber-threats. Furthermore, the actions undertaken by the only technologically equipped governmental agency to combat cyber-threats, the Bureau, are perturbing. As such, this study will proceed to examine the Budapest Convention and how it could inform the ailing cyber-security of Lebanon.

3.5 The Budapest Convention

To understand how the Budapest Convention can aid Lebanon, one must understand the mechanisms of the treaty against cybercrimes. While, the Budapest Convention is by no means a permanent solution to the constantly evolving cyber-threats, it lays down the fundamental elements for a cybersecurity strategy that should be adopted by Lebanon and utilized for future cyber-security development.

This international treaty against cybercrimes is currently the only binding convention in the world with regard to cyberspace. The reason behind it being a sole binding international agreement is the difficulty in achieving an international

consensus on the rules of cyberspace given the differing national interests by states and their perception of use of the digital landscape[54]. Some states simply refuse to join the Budapest Convention as they were not parties in the formation of the international document[55]. Nevertheless, the Budapest Convention is an important international treaty that is in existence and is designed to facilitate international cooperation in combating computer crimes. The Convention framework is built on three key elements: 1) provision of cyber-crimes definitions and their adoption into a country's domestic legislation, 2) defining procedures and rules for investigating cyber-crimes and 3) establishing mechanisms that facilitates international cooperation (Holdorf 2015). It must be noted, that the Budapest Convention focuses on cyber-security pertaining cyber-crimes, rather than from a political-military sense. Nevertheless, its foundation can be utilized to develop a more advanced cyber-security system at later stages.

As such, the research will proceed in analyzing whether Lebanon's current cyber-capabilities comply with the framework of the Budapest Convention.

3.5.1 Lebanon in Light of the Budapest Convention

As mentioned before, the convention is built around three main principles: adoption of cybercrime offenses into a country's national law, defining procedures that

[54] Alexander Seger, Executive Secretary Cybercrime Convention Committee of Council of Europe, discusses the reasons behind the lack of a universal agreement for cyberspace. His list of reasons are related to India and its uncertainty in joining the Budapest Convention. However, same reasons apply to all other states. The report by Seger was a contribution to the India Conference on Cyber Security and Internet Governance 2016. More can be seen at https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/. Accessed November 17, 2018.
[55] *Ibid.*

states should adopt for cyber-crime investigation and establishing mechanisms that regulate international cooperation. How can these principles help a state like Lebanon?

To begin with the first part of the Budapest Convention lays down four separate categories of offenses: 1) "*offences against the confidentiality, integrity and availability of computer data and systems*"; 2) "*computer-related offences*"; 3) "*content-related offences*" and 4) "*offences related to infringements of copyright and related rights*" on computer systems (CoE Convention 2001). Furthermore, the Budapest Convention sets down definitions for variety of offenses under different categories. There are five offenses defined under the first category:

1. Illegal access – concerned with internationally accessing computer systems without the right to do so (Art. 2 of the CoE Convention);
2. Illegal interception – related to violation of privacy, where data is tapped, recorded or transmitted without the consent of the party (Art.3 of the CoE Convention);
3. Data interference – damaging, deteriorating or deleting computer data that could affect the integrity or the information content (Art. 4 of the CoE Convention);
4. System interference – the intentional sabotaging of computer and its data (Art. 5 of the CoE Convention);
5. Misuse of devices - defines criminal offences of specific conducts that are aimed for accessing devices and use them for illegal purposes (Art. 6 of the CoE Convention).

The second category includes two traditional offences, forgery and fraud, which can be committed over computer:

1. Computer-related forgery – relates to unauthorized creation or disruption of stored data to create inauthentic data that could be considered or acted upon as authentic (Art. 7 of the CoE Convention);
2. Computer-related fraud – criminalizes manipulation, such as alteration or deletion of computer data and intrusion of computer systems (Art. 8 of the CoE Convention).

The third category mandates a State Party to adopt legislation related to offenses that include a variety of acts related to child pornography. It aims to strengthen protection for children against sexual exploitation and offenses that can be conducted through computer systems (Art. 9 of the CoE Convention).

The offences involved in the fourth category aims to protect the intellectual property rights. It criminalizes any reproduction or dissemination of a piece of work on cyberspace, without the approval of the copyright holder (Art. 10 of the CoE Convention). These crimes are among the most committed and cause considerable damage to the copyright holders that work on cyberspace. In comparison, the NSCPG of Lebanon, the only available document that attempted to tackle matter related to cyber-security, fails to define cyber-crimes. Its definitions are mostly vague and fails to address the cyber-realities of today. Thus, the framework of NSCPG, if kept, should be readjusted to meet the definitions set in the Budapest Convention.

Continuing on, the second principle of the Budapest Convention is procedural powers that aims to define investigative powers and techniques related to cyber-

crimes. These procedural aspects and scopes are covered in Articles 14 to 21 of the Convention. In this matter, the Convention seeks either to adopt some of the traditional procedural measures or to create new measures to remain effective in a constantly changing cyberspace environment (Csonka 2016). The key element in the Budapest Convention is Article 15, which requires the State Parties of the Convention to fulfill their obligation of protecting people from cybercrimes while respecting their fundamental rights during investigations. Another key requirement is that States must adhere to certain principles found in Article 15 which "includes standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments" (Explanatory Report to the Convention on Cybercrime 2001). This means that by adopting the Budapest Convention, the Lebanese state would have to fulfill the obligations of Article 15 as a result of the following:

1) Lebanon is not only a signatory to the Universal Declaration of Human Rights (UDHR), but it was on the drafting Committee[56], and it has ratified the International Convent on Civil and Political Rights (ICCPR)[57];
2) The preamble of the Lebanese Constitutions states that "*Lebanon is also a founding and active member of the United Nations Organization and abides by its covenants and by the Universal Declaration of Human Rights.*

[56] More about Lebanon's contribution to the UDHR can be found at https://web.archive.org/web/20130927221000/http://unyearbook.un.org/1948-49YUN/1948-49_P1_CH5.pdf. Accessed 8 April, 2018.
[57] See more at https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=IV-4&chapter=4&clang=_en. Accessed 8 April, 2018

The Government shall embody these principles in all fields and areas without exception"[58]

The Budapest Convention, supported by other international agreements, would force a state to respect individual's rights during any investigation related to cyber-crimes. In this situation, Lebanon is a puzzling case. Although Lebanon is not part of the Convention, it has adopted other international agreements that relate to the second principle of protecting people from cyber-crimes while defending their individual rights during investigations. Interestingly, as highlighted in the above sections, the Lebanese security agencies have breached all the international agreements that are related to the second principle of the Budapest Convention, as they conducted cyber-espionage not only internally, but globally without justifications, in addition to detaining individuals for their comments. This causes a dilemma, as if Lebanon applied for the Convention, the first action its authorities would need to undertake is to interfere and modify the Bureau. Currently, Lebanon is not protecting its citizens, as they are being detained due to their comments on the internet, retained from their rights of freedom of expression. As such, its current actions clash with the procedural requirements of the second principle of the Budapest Convention.

The final element of the international treaty, international cooperation, is seen as the most important part (Chernenko et al. 2018; Csonka 2006). This is a reasonable view as cyber-crimes are transnational threats that bypasses traditional state boundaries. As such, the Convention establishes important principles to facilitate international cooperation among states, which could be in the interest of Lebanon. The

[58] Part one of the Lebanese Constitution, Preamble B. Retrieved from http://www.wipo.int/edocs/lexdocs/laws/en/lb/lb018en.pdf. Accessed 8 April, 2018

first principle requires states to mutually assist in the "widest extent possible" in investigations related to cyber-crimes (Art. 25 CoE of the Convention). In addition, the Convention obliges Parties to "accept and respond to" requests made by "expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication," but may demand "formal confirmation to follow" (Art. 25, 3) Obviously, in case of a restriction under its domestic law or by applicable mutual assistance treaties, the State is allowed to refuse cooperation in the matter (Art. 25, 4). The provision also sets guidelines in case two Parties have no mutual legal assistance treaty or any other formal arrangement. For instance, Art. 25 of the Convention implies the two Parties to create a central authority that would be responsible for "sending and answering requests for mutual assistance". Furthermore, the requests would be executed according to the procedures set by the requesting state, except if it violates the laws of the requested state (Art 27, 2). The Convention also sets provisions related to real-time collection of traffic data where it requires two Parties to assist each other in case of criminal offense or in tracking the source of a cyber-attack[59]. The fundamental objective of such cooperation in sharing data is to establish a legal entity that could rapidly respond to cyber-crimes. The Convention requires a Party to create a point of contact, known as "24/7 Network", that could ensure the facilitation of mutual assistance requests concerning cyber-crimes[60]. In addition, the Budapest Convention requires the "24/7 Network" to be trained and equipped in order to carry-out the aforementioned procedures[61].

[59] Convention on Cybercrime, Art. 33(1), Art. 33 (2) and Art. 34. See more at http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. Accessed April 5, 2018.
[60] Ibid., Art. 35(1).
[61] Ibid., Art. 35(3).

Regrettably, Lebanon has no official agreement regarding cooperation in emergency situations of cyber-threats. To make matters worse, the Bureau, if considered currently as a "24/7 Network", meets only the following criteria: trained and equipped. However, as mentioned before, the Bureau has been dealing with illegal cyber-espionage activities. Such actions are completely opposite to the ones that are required by a "24/7 Network" of the Convention. In this situation, the Bureau, instead of interfering and assisting against cyber-crimes, is the one performing them internally and globally.

Unfortunately, an analysis of Lebanon's levels of preparedness based on the literature, review, the review of legal documents, agency reports and interviews conducted for this research shows that Lebanon is completely out of sync with the basic foundation of the Budapest Convention. This can be better understood from the following table:

Lebanon's Compliance to the Budapest Convention's Key Mechanisms			
Convention's Key Mechanisms	Comply	Not Comply	Implication
Harmonizing cyber-crimes with domestic legislation		X	Unavailability of definiti of cyber-crimes in Leba legislation restrain any possible steps the state's authorities could against cyber-threats
Procedures and rules against cyber-crimes		X	Lack of legal tools that Lebanese authorities cou utilize against criminals conduct crimes through cyberspace.

International cooperation (24/7 Network)		X	No official and legal too available for Lebanon to request international sup in case of a major cyber- crime. This absence of a Network, CERT in this c severely hardens the issu no agency is available to monitor, react and conta assistance in case of a cy crime

Since Lebanon has no national laws regarding crimes committed over the internet, it could adopt the cyber-crimes and their definitions laid down by the Budapest Convention. These laws would serve as the starting point for the Lebanese legislation that could be improved and modified at a later stage. For instance, while it has ratified the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography in 2004[62], till today Lebanon has no legislation against such crimes over the internet due to absence of laws in its national legislation. Adopting the Budapest Convention could solve the gap regarding online child-pornography in the Lebanese legislation.

Adhering to these provisions would benefit Lebanon in many ways. Firstly, it could contact and request another state's assistance in case of a cyber-crime having a legal ground. Secondly, Lebanon would be required to create a "24/7 Network" that would be constantly collecting and investigating evidence related to cyber-attacks. Such unit would be completely different from the Cybercrime Bureau, as its creation would have a legal basis and would not be an intelligence property and would be less

[62] Other treaties signed and ratified by Lebanon can be found at http://www.ilo.org/ipec/Regionsandcountries/arab-states/lebanon/WCMS_201535/lang--en/index.htm. Accessed April, 2018.

likely to be accused of illegal and unethical activities. In general, CERT's and other incident reporting teams cooperate on various levels in tracking, reporting and sharing data on cyber-attacks (Nye 2014, p.6).

It must be clear that the Budapest Convention alone does not result in an effective and enhanced cyber-security. On the one hand, the Convention has received many criticism, such as being outdated or not having cyber-warfare and cyber-terrorism in its agenda (Marion 2010; Bucaj 2017, p. 145-146). For Lebanon, nevertheless, it would help it acquire the fundamental elements that are urgently required in combating cyber-crimes. Establishing domestic laws related to cyber-crimes, setting guidelines for investigations, legal entities to participate in tracking cyber-attacks and participating in international cooperation are all foundational components of a state's cybersecurity.

As Lebanon's cyber-capabilities, from policy and technical perspective, are behind the realities of today's cyber-threats, this thesis will proceed to the Estonia's case. The following chapter will provide a different version of cyber-security in contrast to Lebanon's, which will further identify the latter's weaknesses and policy needs.

Chapter Four

Estonia's Case

4.1 Estonia's Political Background

As a consequence of the infamous Molotov-Ribbentrop Pact of 23 August 1939, Estonia was occupied by the Soviet Union and felt under the dominion of Moscow[63]. In 1990, after being occupied for half a century, Estonia along with the other Baltic States, Lithuania and Latvia, regained its freedom from the Soviet Union. After the restoration of its independence, Estonia swiftly began its post-communist transition in order to break with its Soviet totalitarian past.

Today, with a population of 1,300,000 and area of 45,227 km^2 [64], Estonia is the smallest state in the Baltic region that borders the Baltic Sea, Finland, Latvia and Russia. Despite bordering Russia, which has shown a desire to reclaim its former superpower status and influence over the regions that were once under the Soviet Rule, Estonia is now arguably more secure than ever. The small Baltic state has succeeded in integrating itself into major Western institutions such as the North Atlantic Treaty Organization (NATO), World Trade Organization (WTO), and the Organization for Economic Cooperation and Development (OECD)[65]. As of 2004, it became a member

[63] Lobjakas, Ahto, "Molotov-Ribbentrop Pact Still Divides Europe", *Radio Free Europe Radio Liberty*, 17 October, 2009. Accessed 10 April, 2018. https://www.rferl.org/a/MolotovRibbentrop_Pact_Still_Divides_Europe/1854113.html

[64] Information retrieved from the official Republic of Estonia government's website. See more at https://www.eesti.ee/en/republic-of-estonia/republic-of-estonia/information-about-estonia/ .Accessed 10 April, 2018.

[65] See more about Estonia's membership in international organizations at http://vm.ee/en/international-organisations . Accessed 10 April, 2018.

of the European Union (EU)[66] and most importantly, it has been a key supporter of the sole binding agreement against cyber-crimes in the world – the Budapest Convention[67].

While Estonia succeeded in integrating itself into the Western world, the true success of the small Baltic nation lies in the decisive strategy it took in the early 1990's regarding cyberspace. The collapse of the communist system left Estonia in a dire situation where the state had limited resources and required radical reforms to transition itself towards the democratic and open-market systems of the Western world. Being small with limited resources, the government of Estonia decided that the best way forward was to invest in information and communication technologies (ICT) ("Agenda 2030" 2017, p.27). Today, despite its size, Estonia is considered as one of the leading nations in cyberspace as well as a digital powerhouse.

4.2 Estonia in the Field of Cyberspace

In the field of cyberspace, Estonia has achieved remarkable achievements. Despite its size and limited resources, Estonia has been stated as being "the most advanced digital society in the world"[68]. This status was not earned in one day, nor in one year. The root of this success began under the "Tiger Leap" initiative set by the Estonian government in the late 1990's that paved the way for the state to become a digital power. As a result, today Estonia is highly regarded in many key areas of

[66] *Ibid*.
[67] Estonia's ex-Minister of Foreign Affairs, Urmas Paet, explanation about Estonia's support to the Budapest Convention. See more about the statement at http://vm.ee/en/news/estonia-supports-council-europes-fight-against-cybercrime . Accessed 10 April, 2018
[68] See more at https://e-estonia.com/ . Accessed 10 April, 2018.

cyberspace such as e-governance, e-services, x-road, digital ID, online banking and cyber-security. Before progressing towards the lessons learned from Estonia's successful experience, this paper will briefly explain the importance of the "Tiger Leap" strategy.

4.3 The "Tiger Leap" Project

Due to the half-century of occupation and the collapse of the Soviet Union, Estonia found itself being economically and technologically inferior to the West. In 1996, the Estonian government released the "Tiger Leap Program" in which the main aim was to develop and expand computers and network infrastructure in the state with particular focus on education. In 1997, the "Tiger Leap Foundation" was a government-backed body through which the state supported massive investments in technology in order to increase the quality and integration of Estonia's education system with information and communication technology (Sillaots and Maadvere 2012). The first step of the "Tiger Leap Foundation" was to connect all of Estonia's schools to the Internet and to provide basic ICT courses for teachers. By the end of 1997, 97% of Estonian schools had access to the Internet and 4,000 teachers had received basic training on ICT[69]. In early 2000, the "Tiger Leap Plus"[70], the continuation of the "Tiger Leap Program" was launched with the aim of improving the competences of students, teachers and educational staff on ICT. The initiative led to

[69] Data retrived from the Information Technology Foundation for Education (HITSA) of Estonia. See more at http://www.hitsa.ee/about-us/historical-overview/1997-2000 Accessed 23 February, 2018.
[70] Continuation of the "Tiger Leap Program".

the creation of electronic educational materials and a digital platform for teachers to exchange ideas and opinions. In the latter years, the "Tiger Leap Plus" continued developing the students' and teachers' ICT competencies, making e-learning a natural part of education, improving the quality of Estonia's education system and implementing a variety of programs and projects for students to compete and improve their skills through various competitions[71]. Today, the "Tiger Leap Program" is widely considered as the main element that transformed Estonia into one of the leaders of cyberspace (Gaskell 2017; Kouremetis 2015). Even today, the small Baltic nation maintains its objective of improving its ICT capabilities through the continuation of initiatives. In 2012, the "ProgeTiger" program was launched with the aim of integrating computer programing into school curriculums of students from grade 1 to 12 which would in turn allow them to succeed in future careers (Delaney 2017). The whole idea is to teach children basic programming from the moment they enter primary school, as at early age they are able to rapidly learn various materials the same way they grasp foreign languages.

In summary, the continuation of initiatives that began from the "Tiger Leap Program" allowed the Estonian government to increase its citizens' capabilities in cyberspace. It has played a pivotal role in achieving the vision of e-Estonia throughout the decade and achieving the status of a digital powerhouse. Today, Estonia is highly regarded in e-government, e-services, x-road and digital ID, online banking and cyber-security which will be further discussed in the following part of this paper.

[71] The Tiger Leap Plus program aimed to combine ICT with daily educational activities. See more at http://www.hitsa.ee/about-us/historical-overview/2006-2012 . Accessed 24 February, 2018.

4.4 E-government and E-services

The World Bank defines e-government, or e-governance, as "*the use by government agencies of information technologies (such as Wide Area Networks, the Internet, and mobile computing) that have the ability to transform relations with citizens, businesses, and other arms of government. These technologies can serve a variety of different ends: better delivery of government services to citizens, improved interactions with business and industry, citizen empowerment through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, revenue growth, and/or cost reduction"*[72]. In other words, e-governance allows the government to provide its citizens with an effective and wide variety of services at a higher pace. As of today, Estonia's e-governance provides 99% of public services with only marriages, divorces and real estate transactions being excluded[73]. The digitalization of Estonia's government provided services has facilitated the communication between the government and Estonian citizens. In addition, the Estonian authorities are able to provide services more effectively and efficiently than through traditional methods that are time-consuming.

[72] The complete and entire definition can be found on the official website of World Bank http://www.worldbank.org/en/topic/ict/brief/e-government

[73] The full Estonia's e-governance provided services can be found at https://e-estonia.com/solutions/e-governance/ Accessed 26 February, 2018.

4.5 X-Road System and Digital ID

To ensure a secure, effective and efficient communication and exchange of information system between governmental institutions, the Estonian authorities had to come up with a method that could accomplish this task. Their solution was the creation of X-Road system[74] and encouraging people to switch to digital identity cards.

Vassil (2016) defines X-Road as "a secure internet-based data exchange layer that enables state's different information systems to communicate and exchange data with each other". Basically, it is a platform where secure data exchange occurs between residents, public institutions and private companies. This eventually allows data exchange between different state institution computer systems. For example, instead of a police officer physically checking a person's car registry documents, he can access different state systems that contain separate information in a matter of seconds which would in turn efficiently save time.

[74] The initiative to create this system appeared in the 1990's and was eventually launched in 2001. Estonia is the first state to have created such system. See more at https://cyber.ee/en/e-government/x-road/ . Accessed 1 March, 2018

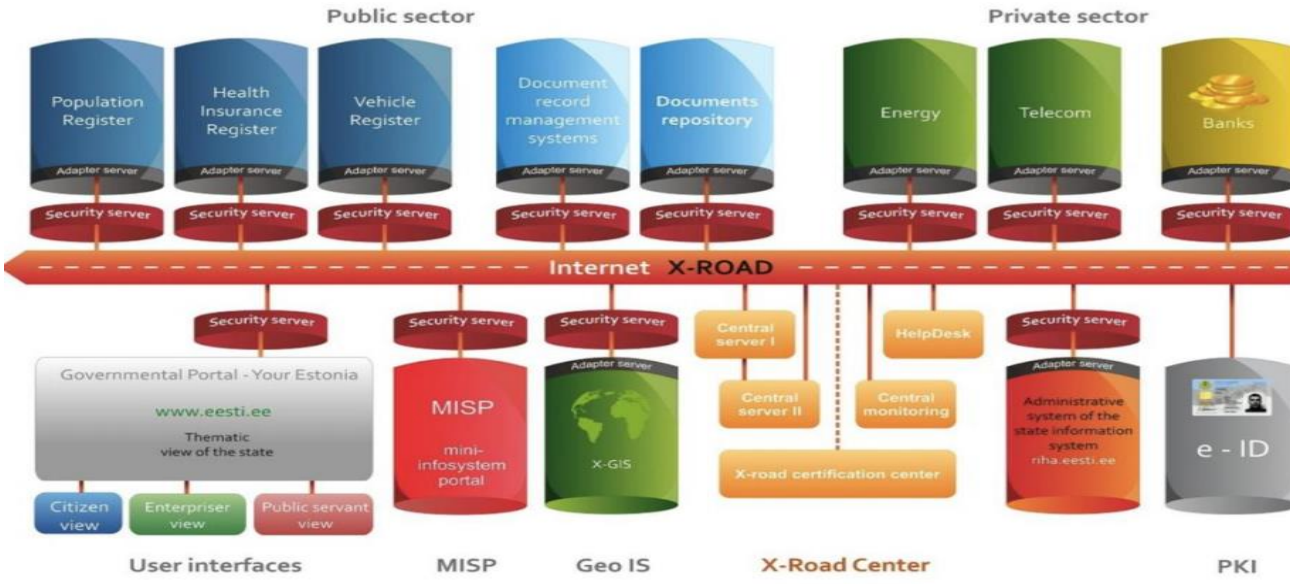

Figure 1: Estonia's X-Road System Schematic (Vassil, 2015)

Another defining feature of the X-Road system is its decentralized nature. When connected to the X-Road system, institutions are able to maintain ownership of their information, share it with others if required and access other institutions' information if necessary. This allows a joining institution to avoid collecting repetitive data on a client since it can access previously stored information of other institutions. As Vassil (2016, p.12) explains, the advantage of data exchange allows institutions to develop more convenient services than they would have done on their own which leads to better user experience and ultimately creates a relationship where individuals seek such convenient services and drives state institutions to continue upgrading their e-services. Eventually, the X-Road allows institutions and citizens to save time in comparison to procedures that would require physical interaction.

Estonia's ID card is not a typical identification document. In 2001, Estonia released a digital ID-card that contains a special chip with embedded files on it[75]. This ID-card allows an Estonian citizen to utilize it as a physical identification document and at the same time provides access to e-services of the government. The special chip that is placed on the card contains the following features: digital identification, authentication, digital signatures, encryption and decryption (Pedak 2013, p.9). The digital ID-card is issued with two important pins. As Vassil (2016, p.4) explains the first pin-code contains personal authentication information which allows the person to identify themselves and permits the e-services to recognize the user. The second pin, according to Vassil (2016, p4) carries a digital signature which allows the user to complete transactions and sign officially documents online. In 2005, Estonia became the first country to introduce voting over the Internet, i-Voting, which allowed Estonian citizens around the globe to vote in nationwide elections[76]. Part of the success of i-Voting in Estonia was credited to the digital ID-card, as its sophisticated security technology allows the citizen to be identified on the i-Voting system from any internet-connected computer in the world and maintain privacy over his/her voting choice (Vinkel 2012; Morgan & Parsov 2017). As such, voters instead of marching to traditional polling stations can save time and vote through the internet due to the digital ID-card.

As of 2007, Mobile-ID was introduced in Estonia. The concept Mobile-ID allows people to utilize their mobile phones as a digital-ID to access various e-services without requiring the user to have usernames and passwords, password cards or any

[75] More details about the embedded files can be found at https://e-estonia.com/solutions/e-identity/id-card/ . Accessed 1 March, 2018
[76] See more at https://e-estonia.com/solutions/e-governance/i-voting/ Accessed 1 March, 2018

other type of identification with them[77]. In order to have a Mobile-ID, a person must request a special SIM card that is provided by a mobile phone operator[78]. In other words, the Mobile-ID became an extension of digital-ID in a mobile phone.

4.6 Online Banking

Internet banking is another area which Estonia managed to digitize. Due to digital ID-Cards, most of Estonia's transactions are being conducted over the Internet. It is currently stated that 99% of all banking transactions are performed online[79]. This performance was achieved due to the banking sector as they encouraged Estonians to switch to digital ID-Cards in order to benefit from high-level banking services. E-banking has allowed banks to cut costs on online transactions, to improve people perception about them and to react faster to customer demands (Kerem 2003). The online banking in Estonia has shown to have positive economic impact on the state. Since Estonians could perform any banking related activity from their houses or offices, they could save time that they would otherwise lose to reach a bank office and stand in queues (Lustsik 2003). Obviously, the online banking system's huge success was the result of Estonia's Government strategies that aimed at popularizing the internet within the population. As of 2016, the internet penetration in Estonia was reported to be 88%[80]. Thus, the population's increased accessibility to the internet

[77] More about the Mobile-ID can be found at https://www.gsma.com/identity/wp-content/uploads/2013/07/GSMA-Mobile-Identity_Estonia_Case_Study_June-2013.pdf Accessed 1 March, 2018.
[78] *Ibid*, p.10
[79] Data retrieved from https://e-estonia.com/solutions/business-and-finance/e-banking/. Accessed 23 February, 2018
[80] Data retrieved from Freedom House at https://freedomhouse.org/report/freedom-net/2016/estonia . . Accessed 26 February, 2018.

made not only e-banking, but also other e-services to be effective and efficient, which in turn became popular in Estonia.

4.7 Cybersecurity Before 2007

The Estonian government realized that their investment in cyberspace must also be protected. As a result, in parallel to the previously mentioned initiatives, the state authorities began enforcing cyber-security measures in order to preserve their investments. On the framework level, the launching of Estonia's cybersecurity initiatives began with the Principles of the Estonian Information Policy which came into force in 1998[81]. This document simply defined the concept of information society with the objectives of seeking a friendly environment where businesses could flourish, bureaucratic mechanisms could be simplified and the private sector's involvement in creating legislations regarding the internet could become possible.

In 2003, Estonia ratified the European Convention on Cybercrime which came into force in 2004[82]. It became the first international agreement that Estonia incorporated into its legislation regarding matters of cyber-security.

In 2004, the government elaborated and approved the Principles of the Estonian Information Policy 2004-2006. While the document retained most of the principles formulated in 1998, it also defined the aim of increasing the cooperation of all parties

[81] Document can be seen at https://www.riigiteataja.ee/akt/75308 Accessed 1 March, 2018.
[82] Estonia is one of the 56 member states that have ratified the treaty. See more at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=false Accessed 2 March, 2018.

in developing the Information Society by improving e-services, e-security and e-education[83].

In 2006, the Estonian government approved the "Estonian Information Strategy 2013" which was approved on the basis of it being "conceived as a sectoral development plan, setting out the general framework, objectives and respective action fields for the broad use of ICT in the development of knowledge-based society and economy in Estonia for the period 2007-2013" (European Commission 2007, p.7). This document focused more on involving and increasing citizens' capabilities in utilizing the internet and harnessing its opportunities. The previous documents focused more on developing ICT technology and infrastructure in the state.

Systematically, the Estonian authorities were working on the organizational level as well. In 1996, the Estonian Government created the Estonian Informatics Centre which was mainly responsible to provide suggestions and advice on drafting principles for enhancing ICT development (Turlea and Bogdanowicz 2007, p.126). In 2011, the Estonian Informatics Centre was transformed into the Estonian Information System's Authority (EISA). This organization is responsible for providing assistance to the public and private sectors in cybersecurity[84].

In 2001, nine influential companies in Estonia began the initiative "Look@World" which in turn increased the usage and popularity of the internet within the Estonian

[83] More elaborated principles can be found at http://vm.ee/sites/default/files/content-editors/web-static/261/Information_society.pdf Accessed 2 March, 2018

[84] More about Estonia's Information System Authority can be found at https://www.ria.ee/en/the-estonian-informatics-centre-became-the-estonian-information-systems-authority.html Accessed 2 March, 2018.

population[85]. It was one of the first Estonian private sector involvement in such a matter. In 2006, a public-private partnership was formed between the "Look@World" foundation and the ministry of economic affairs and communications. The two sides launched the "Computer Protection 2009" initiative which aimed at making Estonia's information society the most secure in the world by focusing on investments in cyber-security and user awareness and encouraging the citizens to utilize their digital ID-card (European Network and Information Security Agency 2014). This partnership could also be considered as a step taken to focus on improving the skills and knowledge of Estonians, on the individual level, in the field of cyber-security. It was reported that the initiative provided "basic computer and internet training to 100,000 people, development and implementation of the eSchool environment, and opening nearly 500 public internet access points across Estonia" (Estonia Country Study Guide 2013, p.148)

In 2006, the Estonian Computer Emergency Response Team (CERT-EE) was established becoming the first organization in Estonia responsible for ensuring cooperation between various parties and providing assistance against cyber-threats (NATO CCDCOE 2013, p.7). The Estonian CERT's primary responsibilities are handling cyber-incidents, warning and notifying about vulnerabilities discovered in systems and applications, providing assistance for agencies and internet service providers and raising awareness about information security.[86]

[85] The nine companies were Swedbank, SED, Elion, EMT, MicroLink, BCS, IT Grupp, Starman, IBM and Oracle. More can be seen at http://www.vaatamaailma.ee/about-us Accessed 2 March, 2018
[86] Estonia's CERT webpage https://www.ria.ee/ee/cert.html. Accessed 2 March, 2018.

4.8 Estonia During 2007 Cyber-Attacks

In 2007, Estonia along with the rest of the world witnessed for the first time the tremendous damages that cyber-attacks can cause. That year, Estonia was cyber-assaulted which resulted in the paralyses of the state's entire digital infrastructure for almost a month. The cyber-attacks came shortly after Estonia's Government decision to relocate the Bronze Soldier statue from the center of Tallinn to another place (Herzog 2011; Goodman 2010; Kozlowski 2014). For Estonians, the removal of the statue was a celebrated act since the statue symbolized the Soviet Union's half-century occupation over Estonians. The Russian minorities saw the decision as an act of disrespect for the Red Army soldiers who died in the battles of WWII and on the hands of the German Nazis.

Shortly, what seemed as a minor malfunction in internet services at the beginning, turned into a full scale cyber-attack. The government was unable to communicate with its citizens properly, websites of presidential, governmental and banking institutions were being shut down, e-mails of some political parties were hacked, and damage to major Estonian banks, internet service providers and telecommunication companies was also caused (Ottis, 2008). While allegedly Russia was considered behind these attacks, all allegations were idle since no actual evidence was found to connect Russian authorities to the cyber-attacks. (Kozlowski, 2014; Herczog, 2011).

Despite all the problems Estonia faced, it managed to rapidly respond to these attacks. First, the banking sector, most notably the Swedbank in Estonia, had already witnessed cyber-attacks prior to the 2007 event (Lindau 2012, p.47). Since it already had the experience against attacks carried through cyberspace, Swedbank managed to resume

its work after a few hours of the 2007 cyber-attacks in Estonia. Secondly, the security community in Estonia were already preparing for the up-coming cyber-attacks as they detected online messages on Russian based websites that called for cyber-attacks on the small Baltic nation. Furthermore, Estonia amassed nation-wide experts from various institutions, such as the Department of Commerce and Communication, the military, the intelligence community, the telecommunication companies, banks and others, that were led by the CERT-EE to combat the cyber-attacks (Schmidt 2014). When the cyber-attacks intensified, Estonia gathered international cooperation to counter these attacks. Estonia's security experts were collaborating with the global Internet security operations community, Finland's CERT, Germany's CERT, Slovenia's CERT and even some individual experts from Russia (Herzog 2011, p.54). This international collaboration provided assistance with monitoring the cyber-attacks, filtering internet traffic, providing information regarding the scope, nature and technicality of the cyber-attacks and supplementing hardware and bandwidth to combat the attacks.

Estonia requested Russia's cooperation and assistance in identifying the culprit on the basis of the Agreement on Mutual Legal Assistance, however, Moscow denied the request (Goodman 2010, p.111). Eventually, in the early 2008, a 20-year old student Dmitri Galuskevits was charged for carrying cyber-attacks against political parties in Estonia[87]. However, this situation revealed the challenge that occurs as a result of a cyber-attack conducted beyond the state's borders. Estonia was able to convict the student only because the attacks were committed from within the state,

[87] "Estonia fines man for 'cyber war' ", *BBC News*, Jan 25, 2008. Accessed 19 May, 2018. http://news.bbc.co.uk/2/hi/technology/7208511.stm

thus, allowing it to collect sufficient evidences for charges. Yet, on a transnational scale, Estonia hit a dead end as Russia refused to cooperate in identifying the culprits. While the agreement on Mutual Legal Assistance which was signed between Estonia and Russia in 1993 required the party who received a request for mutual legal assistance to cooperate with the other party, the Russians simply refused to provide assistance. Estonia's, NATO's and the European Commission's technical experts all failed to gather sufficient evidence that would prove the Russian authorities' direct involvement in the cyber-attacks. Yet, the timing and facts related to the incident led the international community to believe Russia's government involvement: the cyber-attacks paralleled the tensions that were sparking between Estonians and the Russian minorities due to the Bronze Soldier decision and the Russian government's unwillingness to collaborate. In addition, while the cyber-attacks were conducted from thousands of different IP addresses, some were traced to Russian IPs and Russian government computers (Goodman 2010; Haataja 2017; Kozlowski 2014). Unfortunately, even tracing back cyber-attacks to some IP addresses was not enough, due to the sophistication of cyber-attacks, the computers with Russian IP addresses could have been hacked by another party and configured to attack Estonia.

While this incident was named as the first cyber-war in history, Estonia capitalized on it. It quickly went off to strengthen its cyber-security on all levels. The following section will discuss Estonia's actions taken after the 2007 cyber-attacks.

4.9 Estonia's Cyber-Security Development After 2007 Cyber-Attacks

After the 2007 cyber-attacks, Howard Schmidt, former White House cyber-security advisor, stated that "Estonia has built their future on having a high-tech government and economy, and they've basically been brought to their knees because of these attacks"[88]. While it is true that the cyber-attacks did affect Estonia, "brought to their knees" is definitely an overstatement. In fact, the Estonian government capitalized on these cyber-attacks and utilized them as an opportunity to further strengthen its position as a leading nation in cyberspace. Major changes occurred on four major levels related to cybersecurity: national , legal, structural and educational. Since it is not the scope of the paper to review or examine these changes, only vital developments will be overviewed.

4.9.1 National Framework

Before the 2007 cyber-attacks, Estonia's strategies and policies could be summarized as attempts to create a society well educated and trained in utilizing cyberspace. As large scale cyber-attacks had never been witnessed before, the concept of cyber-security was not considered seriously . This view was completely altered once the cyber-attacks showed how they could affect the entire state's functioning.

The first major policy development came with the adoption of the Cyber Security Strategy (CSS) in 2008 that aimed to strengthen Estonia's cyberspace. The CSS highlights five key objectives that would improve the country's cybersecurity:

[88] Quoted from Stephen Herzog article "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses" 2011, p.52.

"1. The development and large-scale implementation of a system of security measures;

2. Increasing competence in cyber security;

3. Improvement of the legal framework for supporting cyber security;

4. Bolstering international co-operation;

5. Raising awareness on cyber security"[89]

It is clear that according to the above mentioned objectives that the CSS calls for active cooperation on various levels. It highlights the need for Estonia to actively promote cyber-security issues at the global level and engage strongly in international cooperation to compete with the rising threats. At the national level, the CSS recommends developments on organizational, technical and legal levels (Czosseck, Ottis and Taliharm 2011). In 2008, Estonia became one of the first countries to release such a strategy and consequently became an example for other states in developing cyber-security strategies (Jackson 2013, p.10). In 2014, the Cyber Security Strategy for 2014-2017 was approved by the Estonian Government which concentrated on raising the awareness of cyber-threats within the population and continuously increasing the state's role and capabilities in cyber-security[90]. Adopting and updating the Cyber-Security Strategy allows Estonia to re-evaluate its development in cyber-security, assess new threats, maintain public-private sector cooperation in combating cyber-threats and raise awareness both within its population and throughout the international community.

[89] The original document can only be found in Estonian language at https://www.ria.ee/en/documents.html. A summary of the document in English version can be see at http://www.circleid.com/posts/estonian_cyber_security_strategy/

[90] More about the Cyber-Security Strategy 2014-2017 can be found at https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/estonia-cyber-security-strategy-2014-2017-now-available Accessed 27 February, 2018

Another vital development was the approval of the updated National Security Concept in 2010 which sets the objectives, directions and principles in safeguarding Estonia's sovereignty and security. In this strategy, the Estonian government includes cyber-crime and cyber-security as elements that affect its reliance on ICT (The Government of Estonia 2010, p.17-18). The National Security Concept recognizes cyber-threats as a security issue that causes problems on both the national and international level. To combat cyber-crime, the National Security Concept affirms that "the state guarantees sustainability in fighting cyber-crime, along with the required technical means and availability of know-how", while strengthening cyber-security requires "legal framework, high awareness of information security and close international co-operation" (The Government of Estonia 2010, p.17-18).

The Cyber-Security Strategy and National Security Concept became the cornerstone of Estonia's cyber-security as it established objectives for the small state to pursue in order to enhance its capabilities to combat cyber-threats.

4.9.2 Legal Development

After the 2007 attacks and following the objectives declared in the Cyber Security Strategy, the Estonian legislation underwent major changes in areas related to cyber security. The first amendments were made in Estonia's Penal Code. These initiatives were taken for a few reasons. The first reason was to make Estonia's Penal Code compatible with the Budapest Convention against cyber-crimes and the Council Framework Decision 2005/222/JHA on conducted attacks against information systems (Kaska et al.). These changes were a must in order for Estonia to adhere to international agreements and to enhance its capabilities to combat cyber-crime from a legal

perspective. The second motive was the need to broaden legislation in the field of cyber-security. Czosseck (2011, p.60) notes that amendments made to the legislation "widened the scope of specific computer crime provisions, added a new offence of the preparation of cyber-crimes, modified the provision concerning acts of terrorism, and filled an important gap in the Penal Code by enabling differentiation between cyber-attacks against critical infrastructure and ordinary computer crime". The provisions made in the Penal Code meant that attacks conducted through cyberspace with the aim to damage any vital structure of the state would be considered as a terrorist act. By widening the scope of cyber-crimes in its legislation, Estonia expanded its legal arsenal to combat criminals in cyberspace.

Another important development in the legislation area came with the passing of the Emergency Act 2009. The new legislation was aimed to check the state's readiness to respond to emergency situations and its emergency management structure, including emergencies related to cyber-threats (Czosseck et al. 2011; Kaska et al. 2010). For instance, if a major incident occurs to the state, including cyber-incidents, the Emergency Act delegates crisis management power to the Prime Minister who not only becomes the chief authority of the state during the crisis but also receives the power to restrict rights and freedom if deemed necessary to protect the country (Collier 2016, p.6-7). Furthermore, the legislation increases the responsibility of the private sector as well. With the new legislation, the vital service providers became obliged to report cyber-attacks to the Estonian Information System Authority once the systems are secured from the threats (Inter-American Development Bank 2016, p.16). The Estonian private sector is expected to reveal any cyber-attacks that inflicted damage to critical infrastructure to state's authorities. For instance, while Estonia is constantly

bombarded by various cyber-threats, the authorities record almost 300 cyber-incidents each month[91]. This legislation is important as it not only requires harmonious public-private sector cooperation, but also mutual sharing of confidential and sensitive information. Some states still have problems in reaching this harmony, as their private sector is reluctant to cooperate with state authorities, due to the belief that sharing such information could affect their reputation, or that it will invite more governmental control (Jagasia 2017).

The implemented amendments improved Estonia's legal and regulatory framework. It managed to broaden the scope of cyber-security in the legislation, assert responsibilities in times of crisis and harshen punishments related to cyber-crimes. Furthermore, it allowed Estonia to adhere to its international obligations by harmonizing national laws with the aforementioned treaties. Finally, Estonia managed even from a legal perspective to bring the public and private sectors to cooperate in cases related to cyber-incidents in the hope of improving the state's security.

4.9.3 Structural Development

After the cyber-attacks, Estonia drastically improved its structures to combat cyber-threats. The first major development came with the creation of the Cyber Security Council as a result of the Cyber Security Strategy. The Council was established in 2009 with the main aim of overviewing the implementation of the Cyber

[91] As stated by Klaid Magi, the head of the Incident Response Department (CERT-EE). Retrieved from https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/

Security Strategy goals and to facilitate the cooperation between various public institutions in Estonia in matters related to cyber-security.[92]

In 2011, the Estonian Informatics Centre was re-organized into Estonian Information System's Authority (EISA or RIA) and became the main cyber-security body in the state with government agency status. According to the NATO CCDCOE (2015, p.7-8) "RIA is responsible for the development and administration of state information systems, as well as drafting related policies and strategies, coordinating the implementation of security standards, organizing activities related to cyber security, and handling security incidents either previously reported or currently occurring on Estonian networks". In order to protect critical information infrastructures, RIA conducts risk analysis and sets security measures, which allows the institution to impose fines on parties that violate the security requirements[93]. In 2010, the Critical Information Infrastructure Protection (CIIP) at RIA was established with the aim to secure public and private information systems that were deemed critical to the state (Cyber Security Strategy 2014-2017, p.2)

During the cyber-attacks, Estonia's CERT was assisted by volunteers that were skilled in cyber-security (Jackson 2013). In 2011, a Cyber Defense Unit was added to the Estonian Defence League with the aim of protecting "Estonia's high-tech way of life by protecting information infrastructure and supporting the broader objectives of

[92] The Cyber Security Council reports directly to the Government Security Committee. It is chaired by the Secretary General of the Ministry of Economic Affairs and Communications. See more at https://www.mkm.ee/en/objectives-activities/information-society/cyber-security Accessed 25 March, 2018

[93] RIA's entire capabilities and powers are highlighted in the Emergency Act 2009. See more at https://www.riigiteataja.ee/en/eli/517122014005/consolide . Accessed 25 March, 2018

national defence"[94]. This Cyber Unit is comprised of experts in cyber-security or matters related to it, individual IT specialists and even youth with interest to cyber-security[95]. The aim of such unit was to gather dedicated experts and volunteers from public and private sectors to cooperate and ensure the effectiveness of Estonia's cyber-security. In addition, by formalizing this unit, the Estonian government succeeded in directing the desire of the volunteers to assist their state in a comprehensive and constructive mode.

In 2008, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn was established. While the idea of such center had been circulating since 2003, the momentum did not appear till the 2007 cyber-attacks. Today, CCDCOE is defined as "a NATO-accredited research and training facility dealing with education, consultation, lessons learned, research and development in the field of cyber security"[96]. It must be noted that CCDCOE is neither a cyber-force nor a cyber-control center that would be aimed at sending or countering cyber-threats. In fact, CCDCOE is a consortium were specialists related to cyberspace are constantly engaged in research and publications to provide effective cyber-security practices (Kaiser 2014, p.16). While many countries have contributed to CCDCOE, the key founder of it is none other than Estonia, which proposed the concept of such a center in 2004 after joining NATO[97]. As of today, experts in CCDCOE have created the "Tallinn Manual" which is considered as the most advanced guide for the applications

[94] Estonia's Defence League is a voluntary militarily organized organization operating under the command of the Ministry of Defence. See more at http://www.kaitseliit.ee/en/edl. Accessed 2 March, 2018.
[95] See more at http://www.kaitseliit.ee/en/cyber-unit. Accessed 28 February, 2018.
[96] Definition taken from the official NATO CCDCOE website http://www.ccdcoe.org/about-us.html. Accessed 28 February, 2018
[97] History of NATO CCDCOE at https://ccdcoe.org/history.html

of international law on cyber-activities[98]. Furthermore, the CCDCOE has been conducting simulation trainings to maintain and raise the skills of the personnel to combat threats in cyberspace (Crandall and Allan 2015, p.357). This allows experts to continuously evolve in the field of cyber-security through theoretical and practical trainings.

In short, the examination of Estonia's case highlighted the procedures and steps that were undertaken to develop such a high-level cyber-security. It has demonstrated the two different stages of the state's cyber-security development – before and after the 2007 cyber-attacks. The next chapter will focus on the lessons from the Estonian case that can inform the Lebanese authorities' work in developing the capabilities of Lebanon's cyber-security.

[98] More about the Tallinn Manual can be found at https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html

Chapter Five

Estonia's Relevance to the Lebanese Case

5.1 Comparing Lebanon to Estonia

As set out in chapter five, Estonia has become an international example of how a state should proceed in developing its cyber-security. In contrast, chapter four has revealed the negligence of Lebanese authorities in developing its cyber-capabilities. The table below provides a better picture of the compliances of both states to the Budapest Convention.

Table 1. Estonia's and Lebanon's Compliance to the Budapest Convention

Budapest Convention Key Requirements	**Estonia**	**Lebanon**
National Cybercrime Legislation	Estonian Penal Code	Unavailable
Criminal Procedural Legislation for Cybercrimes	Estonian Code of Criminal Procedure	Unavailable
Effective International Co-operation	NATO; European Union; Bilateral agreements with other states	Unavailable
Point of Contact (24/7 Network)	Computer Emergency Response Team (CERT-Estonia)	Cybercrime Bureau[99]

Lebanon is clearly left behind in terms of complying to the currently available international standard. In contrast, Estonia matches all the requirements. One could

[99] While the Cybercrime Bureau is not the same as a CERT, however, in Lebanon's case we will perceive it as the organization that manages cybersecurity incidents.

say that it is unfair to analyze both state in terms of the Budapest Convention's requirements, as Estonia is one of the founding parties of the agreement. Yet, the following table allows us to understand that it is not the case.

Table 2. Initiatives to Secure Cyberspace Environment by Both States

Other Initiatives To Secure Cyberspace Environment			
Estonia		Lebanon	
Initiative	Result	Initiative	Result
Principles of the Estonian Information Policy	Implemented	E-signature	Not enacted
Principles of the Estonian Information Policy 2004-2006	Implemented	E-commerce law	Not enacted
Estonian Information Strategy 2013	Implemented	Cybercrime and Intellectual Property Rights Bureau	Implemented
Estonian E-Government Services	Implemented	Lebanese E-Government Services	Partially implemented
Estonian Computer Emergency Response Team	Implemented	Lebanese National Cyber Security Policy Guidelines	Partially implemented
Cyber-Security Strategy 2008 and 2014-2017	Implemented	Lebanese Cyber-Security Strategy	Unavailable
NATO CCDCOE	Implemented		
Emergency Act 2009	Implemented		
Estonian Information System's Authority	Implemented		

This table reveals that Estonia has undertaken far more initiatives than Lebanon and succeeded in implementing them. It must be noted, that Estonia's strategies were far more complex. Lebanon has fully succeeded only in creating the Cybercrime Bureau, while it's other measures have either failed or were partly implemented.

Regrettably, Lebanese authorities have underestimated the treats of cyberspace to the state's national security. In today's world, states are developing all aspects of cyber-security, defensive and offensive, in order to conduct cyber-operations and retaliate in the events of cyber-attacks. Lebanon, from the available information and comparative analysis, has left its cyberspace unshielded from foreign cyber-activities. It has no internal resources that could deal or retaliate in the events of cyber-warfare, or even cyber-crimes. Lebanon's cyberspace can be utilized by state and non-state actors to pursue their own interests. Furthermore, the scandal of the Lebanese intelligence unit participating in international spying shows that the state is also an active player in conducting cyber-operations. It reveals that Lebanon has capabilities of conducting certain cyber-operations. Unfortunately, offensive capabilities are not sufficient to protect your own cyberspace. Kissinger (2015, p. 346), while discussing cyberspace and its threats impact on international order, formulated:

> "*The history of warfare shows that every technological offensive capability will eventually be matched and offset by defensive measures, although not every country will be equally able to afford them. Does this mean that technologically less advanced countries must shelter under the protection of high-tech societies? Is the outcome to be a plethora of tense power balances?"*

This formulation corresponds perfectly to Lebanon. While certain cyber-offensive capabilities are developed, its defensive abilities are ignored. In future cyber-conflict, such situation could force Lebanon to request help from a more developed cyber country, most probably from the Middle-East region. Such action could come with consequences in an already volatile environment of the Middle-East, where states are

aligned into alliances accordingly to either political or religious beliefs. In case of a powerful cyber-attack and the need of assistance, Lebanon would be forced to pick its allies and draw its enemies.

Lebanon's failure to catch-up to today's cyber-security standards is the lack of effort by the Lebanese authorities. It questions their ability in protecting their national security, at least within the field of cyberspace. Such disarray provides opportunity for foreign states, non-state actors and individuals to perform complex cyber-operations through Lebanon's cyberspace, without ramifications. In contrast, any illegal cyber-operation through Estonia could bear high risks, as the state has all the tools to unleash variety of counter-measures against the attackers.

5.2 Lessons for Lebanon

It is crystal clear that Lebanon's cyber-security is in dire need of development. At such rate, the state will not have the capabilities to deal with lesser degrees of cyber-attacks. As such, the analysis conducted on Estonia's cyber-security offers an established framework on the development of an up-to-date mechanism to protect cyberspace. Thus, the following sections will identify the lessons from the Estonia's successful cyber-security model for Lebanon to taken.

5.2.1 Organizational Reforms

Currently, the organizational structure of cybersecurity in Lebanon could be best described as anarchic. It is completely opposite from Estonia's structures that are well organized and coordinated. The Estonian cyber-security structure begins from the

Ministry of Economic Affairs and Communications, which is responsible for the overall cyber-security policy coordination. The Cyber Security Council of the Security Committee of the Government is responsible for facilitating inter-agency cooperation and overseeing the implementation of cybersecurity strategies in Estonia. In addition, the Committee is obliged to present to the Government annual progress reports that show the results of cybersecurity objectives realization in the country. To combat cyber-crimes and cyber-attacks, Estonia has established RIA. This agency is responsible for developing and administering the state's cyberspace, drafting policies and strategies, organizing cyber-security drills and reacting to cyber-incidents on Estonian networks. In addition, RIA constantly develops and overlooks the application of security measures on information systems and supervises the cybersecurity of critical infrastructures. Within the RIA, the CERT of Estonia monitors incidents related to cyber-attacks in the state's networks, raising security and cyber-threats awareness to the population and facilitates the cooperation between the government and the private sector in cases of major cyber-incidents. In Estonia's case, each institution has a defined role that it has to perform and accountability mechanisms are implemented to ensure the fulfillment of their duties.

In Lebanon, the National Cyber Security committee was tasked to create a national cybersecurity policy that would protect governmental websites. Eventually, it was the OMSAR that published the NCSPG. The TRA of Lebanon is responsible of implementing cyber-security strategies and policies. However, a few problems arise from these structures in Lebanon. The first one is that OMSAR published a NCSPG that does not include the private sector in its creation. Secondly, TRA is unable to perform as there are no national strategies or policies regarding cyber-security, thus

leaving the institution paralyzed with its assigned duties. In this case, the institutions are not performing their roles and no accountability mechanism exists to enhance their work performance. Furthermore, as highlighted in chapter three, the sole entity that is capable and equipped to combat cyber-crimes, the Cybercrime Bureau, has been entangled in spying scandals and in problems related to its legitimacy. When the interviewees were asked if the state's military could overtake the task of defending the nation's cyberspace, as it is done in the U.S. and Australia, they were cynical about such ideas. They believe that no institution alone can protect Lebanon's cyberspace. There must be a governmental body or a special agency that unites experts from all sectors and coordinates their actions for the benefit of an effective Lebanese cyber-security. Such entity would need to host a virtual team encompassing representatives from the private sectors (education, healthcare, finances and others) and Government agencies[100]. Eventually, a proper organization would ensure that initiatives related to cyber-security are processed and fulfilled.

5.2.2 Legislative Reforms

Due to the rapid evolution of cyber-crimes, many countries in the world have modified or adjusted their criminal laws to correspond to the modern threats. Lebanon remains an exception till this day, as the Lebanese criminal law does not cover crimes related to cyberspace. Currently, various amendments to Lebanon's Penal Code in consideration of the Budapest Convention were proposed in order to integrate

[100]Barakat, Jihad. Personal interview. 5 Jul, 2018;
Chebat, Khaled. Personal interview. 1 Sep, 2018;
Karam, Marie-Line. Personal interview. 1 Jul, 2018;
Khalife, Joseph. Personal interview. 15 Jun, 2018.

cybercrimes into the state's criminal laws[101]. However, proposing amendments and actually passing them and implementing them are completely different matters, especially in Lebanon's case. In Estonia's case, the criminal law was harmonized with the Budapest Convention requirements. Furthermore, while Lebanon has only proposed some amendments, Estonia has seven laws specifically designated for cyberspace: Digital Signatures Act, Electronic Communications Act, Information Society Services Act Penal Code, Code of Criminal Procedures and the Data Protection Act[102]. In Lebanon, investigations related to cybercrimes are conducted under the Criminal Procedure Code, however, no special procedures for cyber-crimes exist[103]. Clearly, Lebanon must step up in the legislative field in order to empower its authorities to deal with cybercrimes. Obviously, the Lebanese government must concern itself with the activities of the Cybercrime Bureau. While its original objective was to combat cyber-crimes, it has involved itself with interrogation and arrests with issues unconnected to cyber-crimes. As mentioned in chapter three, in many cases the Bureau was involved in spying campaigns or arrests that targeted social media users that expressed their opinion. Such activities conflict with the Lebanese Constitution which guarantees public freedom, personal freedom and freedom of speech and press[104]. A state that contradicts its constitutional guarantees can lose its credibility in the international arena. As such, the Lebanese authorities must enact laws that would ensure that the Bureau's activities, or any other future institution related to cyberspace

[101] Lebanon's profile regarding cybercrime policies/strategies. The suggested amendments can be found at https://www.coe.int/da/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/lebanon/pop_up?_101_INSTANCE_hFPA5fbKjyCJ_viewMode=print&_101_INSTANCE_hFPA5fbKjyCJ_languageId=da_DK. Accessed 18 April, 2018.
[102] *Ibid.*
[103] *Ibid.*
[104] *Ibid.*

and security, would not undermine the guarantees laid in the constitution. Furthermore, it was highlighted that even if legal tools were upgraded to combat cyber-crimes, the judges and prosecutors would need to receive special training to understand the complicated nature of cyber-crimes[105]. Providing legal tools without adequate training to the related law enforcers would maintain the current state of affairs.

5.2.3 Public-Private Partnership in Cyber-Security

Another vital lesson that Lebanon should take into consideration is the public-private cooperation in cyber-security. As discussed before, while the Estonian government was working on strategies and other initiatives, they allowed the private sector to actively participate in strategy formations. Furthermore, when the Estonian private sector cooperated with the government this led to the formation of "Computer Protection 2009" initiative that popularized the digital ID-card usage in the state, and further investment to cyber-security and staff training (European Network and Information Security Agency 2014; Estonia Country Study Guide 2013, p.148). Furthermore, the cyber-attacks of 2007 in Estonia were countered through an active cooperation of experts from public and private sectors through the coordination of the CERT (Pernik and Tuohy n.d.). The NCSPG of Lebanon cannot be considered as complete as it did not include the private sector. This is a tremendous flaw, as even states like the U.S, where the defense of the cyberspace belongs solely to the government, admitted to the dire need of public-private cooperation[106]. This could be

[105] Karam, Marie-Line. Personal interview. 1 Jul, 2018;
Khalife, Joseph. Personal interview. 15 Jun, 2018;
Khayrallah, Jean. Personal interview. 29 Jun, 2018.

[106] Pellerin, Cheryl, " Cybercom Commander: Public-Private Partnerships Needed for Cybersecurity", Nov. 16, 2016. Accessed 5 April, 2018.
https://www.defense.gov/News/Article/Article/1006807/cybercom-commander-public-private-partnerships-needed-for-cybersecurity/

attributed to the lack of professional knowledge that is required for drafting such policy[107].

Currently, only one type of public-private cooperation in cyber-security exists in Lebanon. The Bureau is cooperating with the Banque Du Liban (BDL) Special Investigation Commission to combat cyber-crimes and their culprits[108]. However, this cooperation has limitations as it is active only in cases of cyber-attacks related to the banking sector. This means that other institutions, such as universities or hospitals, are left alone to deal with cyber-attacks that could steal private information of individuals.

Bank involvements with Estonia's government resulted in a successful partnership in the field of cyber-security. Lebanese banks also hold that potential. Since the government has been somehow in stagnation mode, the banks have been dealing with cyber-attacks all by themselves. Their experiences with cyber-attacks could be an advantage for the Lebanese government in creating a proper national strategy for cyber-security. The Central Bank of Lebanon (BDL) has actively taken the lead in the fight against cyber-crimes. In 2000, BDL released circular that defined electronic financial and banking operations[109]. In 2017, the BDL released Basic Decision No 12725 that aimed at providing guidelines for cybercrime procedures and minimum technical requirements[110]. In addition, the Lebanese banks have gathered sufficient

[107] A statement suggested by all five interviewees.
[108] El-Amine, Yehia, "Cyber security awareness growing in Lebanon", Nov. 29, 2016. Accessed 10 November, 2018. https://en.annahar.com/article/503624-cyber-security-awareness-growing-in-lebanon
[109] Halawi, Dana and Paul Fargues,"Salameh calls for ratification of anti-cybercrime laws", *The Daily Star*, Nov. 13, 2015. Accessed 10 April, 2018. http://www.bccl.gov.lb/salameh-calls-for-ratification-of-anti-cybercrime-laws/
[110] Banque Du Liban, Circular No 144, 2017. Accessed 10 April, 2018 http://www.bdl.gov.lb/files/circulars/144_en.pdf

technical experience in combating cyber-crimes as well. The incident of "Gauss" virus, that specifically targeted Lebanese banks, and other cyber-attacks that were thwarted has increased the technical capabilities of the financial institutions. Yet, this is not sufficient. The BDL has been actively urging the state authorities to finally ratify e-commerce laws that could protect individuals from cyber-threats[111]. Commercial banks have also urged the government to take an active role in cyber-security and modifying legislation to combat cyber-crimes[112]. Interestingly, Lebanese banks are actually utilizing older systems for their daily operations allowing them to be less vulnerable to powerful cyber-attacks. If banks utilized newer systems, they would be prone to more complex cyber-attacks that would inflict tremendous damages, but because they are using older systems for their daily operations, they are prone to lesser scale of cyber-attacks resulting into lower cost of damages[113].

It is important to mark that while Lebanese banks have gained tremendous experience in combating cyber-threats, they alone are not enough. To withstand cyber-threats, Lebanon must rely on an in-depth defense model that is not just an organization, industry or sector-specific: infrastructure service providers, telecom agencies and even utility services should be on-board in identifying, blocking and mitigating cyber-threats[114].

While discussing a potential Lebanese public-private partnership in the field of cyber-security, all five interviewees agreed on the need of such collaboration. By

[111] *Ibid*.
[112] Schellen, Thomas, "Fresh thinking needed to protect the banking system", *Executive Magazine,* Mar. 15, 2017. Accessed 10 April, 2018. http://www.executive-magazine.com/cybersecurity/cyberinsecurities
[113] Barakat, Jihad. Personal interview. 5 Jul, 2018;
Khayrallah, Jean. Personal interview. 29 Jun, 2018
[114] Chebat, Khaled. Personal interview. 1 Sep, 2018

having a similar platform like Estonia's Cyber Defense League where different organization, industries and sectors provide their expertise on cyber-security, it would be a huge leap for Lebanon. However, they noted that such collaboration must be constantly checked. In their opinion, it is a must to create governmental institution which overviews such collaboration, because if it is uncontrolled, it will create more risks for the state.

Therefore, a public-private cooperation, or a creation of a platform similar to the Cyber Defense League, for the Lebanese government should be an essential part of Lebanon's cybersecurity. By creating legislations for cyberspace and involving the private sector in cyber-security initiatives, Lebanon can develop more effective policies and be better equipped to handle future cyber-threats. As such, the retrieved information reveals that in order to carry out such sophisticated initiatives, Lebanon must develop a governmental institution solely dedicated for affairs related to cyber-security.

5.2.4 International Cooperation

Estonia's success in cyber-security can also be attributed to its active collaboration with international organizations. After the 2007 cyber-attacks, Estonia's cyber-security strategies highlighted the importance of international cooperation against cyber-threats. Estonia is one of the leading states in voicing the importance of cyber-security in EU, NATO, UN, CoC, OSCE, ITU and other international organizations (Pernik and Tuohy 2013, p.4). This serves as a good example to Lebanon, that in cyber-security the size of a state is not a major factor in gaining influence in international relations.

Although Lebanon does not belong to the EU or NATO, other international organizations exist with whom cooperation could be fostered in cyber-security. The following table provides some of the international organizations that could potentially enhance Lebanon's cyber-security capabilities at various levels:

Table 3. International Organizations for Improving Cybersecurity

Organization	**Expertise in Cyber-Security**
Council of Europe	The Budapest Convention – building state capacities to adhere to the international treaty.
International Telecommunication Union	Legal Measures; Technical and Procedural Measures; Organizational Structure; Capacity Building; International Cooperation.
Interpol	Operational and Investigative Support; Cyber Intelligence and Analysis; Digital forensics; Innovation and research; Capacity Building; National Cyber Reviews.
United Nations Office on Drugs and Crime	Cybercrime Repository – provides database of legislations, case laws and lessons against cybercrimes)

The cybercrime repository offered by the UNODC could prove beneficial for Lebanon in the legislative area. The cybercrime repository aims to facilitate States' performances against cybercrimes[115]. This could help Lebanon on a few matters: a) helping Lebanese courts in cases related to cybercrime and b) providing examples that could be utilized for drafting anti-cybercrime laws.

[115] More information regarding the UNODC cybercrime repository can be found at https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html . Accessed 15 April, 2018.

A deeper cooperation with the ITU would be beneficial to Lebanon's cyber-security. Firstly, at the legislative level, the ITU has developed the "Toolkit for Cybercrime Legislation" that aims to assist states in creating harmonized cybercrime laws and procedural rules (International Telecommunication Unit 2010). The ITU toolkit was developed after analyzing the national legislations of developed states and the Budapest Convention[116]. As such, it could serve Lebanese authorities, policy experts and legislators as an sample in developing Lebanon's national framework against cybercrime. ITU is already providing its theoretical and technical experiences to Lebanon. The ITU is cooperating with the TRA, the Lebanese University and the private sector in building Lebanon's first national CERT structure[117]. Such structure would coordinate various Lebanese institutions' actions against cyber-attacks, assist in recoveries from these attacks and provide evidences in case of lawsuits related to cybercrimes.

Yet, the two organizations that deserve the most attention are the Council of Europe and Interpol. Since the Council of Europe is the creator of the Budapest Convention, it can assist Lebanon in developing the needed frameworks related to cyber-security that would fulfill the requirements required by the international treaty. The Cybercrime Convention Committee (T-CY) is tasked by the Council of Europe to consult parties regarding the Budapest Convention[118]. Furthermore, the T-CY main objective is to

[116] The ITU toolkit contains many provisions that are similar to the Budapest Convention's, yet they are more advanced. See more at http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf . Accessed 15 April, 2018.
[117] Declared by the Telecommunication Regulatory Authority of Lebanon. See more at http://www.tra.gov.lb/SubPage.aspx?pageid=3161 . Accessed 15 April, 2018.
[118] Council of Europe, "*Cybercrime Convention Committee (T-CY)".* T-CY Workplan, September 2015. Accessed 15 April, 2018. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804924d2

support the accession of non-member states to the Budapest Convention. As a result, if a request to join the Convention is received, the T-CY members have the duty to actively consult with the requester and to encourage governments to actively participate in accession requests within the Council of Europe's institutions[119]. In addition, the Council of Europe and the members of the Convention have obligations to provide technical assistance if needed to help the non-member attain minimum requirements for the Convention[120]. This kind of assistance would be beneficial for Lebanon. Firstly, the Party members would share their experience and knowledge in adhering to the Convention. Secondly, it would help Lebanon in creating legislative frameworks of cyber-laws that would be in harmony with the Convention. Thirdly, the creation of the framework would be assessed by the Council of Europe and would be under regular review. For example, the accession of Sri Lanka to the Convention was hailed not only for creating legislative framework and procedures against cyber-crimes, but also for the fact that the country will be under constant review and obliged to continuously improve its practices[121]. The Council of Europe has already began its assistance to Lebanon by conducting desk reviews on draft laws on cybercrime[122]. Furthermore, Lebanon is included in a joint project by the CoE and EU, CyberSouth, which aims to strengthen legislative and institutional capacities, provide trainings and

[119] *Ibid.*
[120] *Ibid.*
[121] The impact of the Budapest Convention on Si Lankan legal system was made by Jayantha Fernando, the Director/Legal Advisor of ICT Agency of Sri Lanka. See more at http://www.apbsrilanka.org/articales/28_ann_2016/7_28th_conv_a_Jayantha_Fernando.pdf. Accessed 15 April, 2018.
[122] Council of Europe. Information Documents SG/Inf(2017)42. C-PROC activity report, November 2017. Accessed 15 April, 2018. https://rm.coe.int/n-sg-inf-2017-42-coe-office-on-cybercrime-bucharest-activity-report-24/168076bdc0

various cooperation against cybercrimes[123]. Hopefully, this initiative can bring results in the area of cybersecurity in Lebanon.

Interpol is another international organizational that could assist Lebanon in combating cyber-crimes. Being the world's largest international police organization, Interpol works with state's national police structures around the world[124]. Due to the rise of cyber-crimes, Interpol has gained valuable expertise in combating cyber-threats. Interpol's ability to facilitate the work between various police structures from different countries is an important component in assisting states that suffered from cyber-crimes. Three aspects of Interpol would benefit Lebanon. Firstly, Interpol could send its operational and investigative support team. This team is deployed under the request of a member country and is able to deal with all types of criminal investigations, including cyber-crimes[125]. Interpol's expertise could help the inefficient and ineffective Lebanese internal structures in investigating cyber-crimes, especially those being conducted from foreign states. Secondly, Interpol provides capacity building and trainings which aims to equip the law enforcement officers and others with the required knowledge to meet cybercrime challenges[126]. This partnership would allow the Lebanese law officers, policy makers and other individuals related to the field to accumulate the needed experience through various training programs. Lastly, Interpol conducts the National Cyber Review that observes, assesses and recommends

[123] *Ibid.;* The project is set for a duration of 36 months and has a budget allocated for 3.33 million euros. The project targets the Southern Neighborhood countries: Algeria, Jordan, Lebanon, Morocco and Tunisia.
[124] INTERPOL has 192 member countries. See more at https://www.interpol.int/About-INTERPOL/Overview. Accessed 15 April, 2018
[125] More information about operational and investigate support team can be found at https://www.interpol.int/Crime-areas/Cybercrime/Activities/Operations-investigations. Accessed 15 April, 2018.
[126] More can be found at https://www.interpol.int/Crime-areas/Cybercrime/Activities/Capacity-building . Accessed 15 April ,2018.

measurements to enhance states' cyber-security at all levels[127]. National Cyber Review is created through Interpol's cooperation with external experts, the private sector of the state and the academic institutions[128]. It must be highlighted that having a top-ranked Lebanese officer in the Interpol could also be considered as an advantage for Lebanon's cyber-security[129]

5.2.5 Education

One must be reminded that the beginning point of Estonia's road in achieving high regards in the area of cyberspace and its security was the "Tiger Leap" program. While part of the program focused on improving the ICT infrastructure, it also aimed at harmonizing ICT with Estonia's education system. Having an education system that introduces and focuses on ICT technologies can create an entire generation with specialization and knowledge in the field of cyberspace and its security. This is apparent with the latest initiative, "ProgeTiger", which introduced computer programming throughout all grades in Estonia's schools. These initiatives ensure that Estonia constantly keeps raising new specialists in the cyber-security field that could assist in battling cyber-threats.

From an analysis perspective, there are two reasons that Lebanon should examine Estonia's educational initiatives. Firstly, Lebanon is in dire need of a developed ICT infrastructure. Lebanese citizens are known to be suffering from one of the worst internet speeds in the world. Lebanon was ranked 131st out of 133 for its

[127] See more at https://www.interpol.int/Crime-areas/Cybercrime/Activities/National-Cyber-Review. Accessed 15 April, 2018.
[128] *Ibid.*
[129] Chebat, Khaled. Personal interview. 1 Sep, 2018.

fixed internet speed, making it one of the worse not only in the region, but globally[130]. While it must be mentioned that there is a promise of massively upgrading Lebanon's internet speed by the end of 2018[131], it will be interesting to see if such a promise can be kept, knowing the high level of corruption and monopoly in the ICT area[132].

Secondly, supposing Lebanon began developing its outdated ICT infrastructure, the issue of educating its population about cyber-threats and raising cyber-security experts would likely become a serious concern. Up till 2007, Estonia concentrated its resources on developing general knowledge and awareness of its citizens. After the 2007, the policies switched into raising experts in the field of cyberspace. In Lebanon's case, educative initiatives regarding cyberspace and its threats could be described as non-existent. In 2012, an exploratory research including 635 students revealed that the educational community is ignorant of cyber-threats (Hejase et al. 2012). In addition, the study revealed that participants were mostly aware only of spams and junk mails as cyber-threats, while cyber-attacks were regarded as disruption of banking, financial and internet services (Hejase et al. 2012). Today the general awareness of cyber-threats is growing, however, the pace is too slow[133]. This comes as a result of a missing state institution with the power to formulate a clear strategy that would include educating the population on cyber-threats. Interestingly, it must be noted that while the state's overall cyber-security is in bad shape, Lebanese

[130] Speedtest Global Index ranks mobile and fixed broadband speeds from around the world. Rankings are being conducted on a monthly basis. More can be seen at http://www.speedtest.net/global-index/lebanon#fixed

[131] Redd, Benjami, "Ogero head stakes reputation on 50 Mbps internet by 2018", *The Daily Star*, Nov. 27, 2017. Accessed 29 May, 2018. http://www.dailystar.com.lb/News/Lebanon-News/2017/Nov-27/427928-ogero-head-stakes-reputation-on-50-mbps-internet-by-2018.ashx

[132] As reported by Freedom House, Lebanon's strategy and initiative regarding its ICT development has raised many concern for its lack of transparency. More can be found at https://freedomhouse.org/sites/default/files/FOTN%202016%20Lebanon.pdf

[133] Khalife, Joseph. Personal interview. 15 Jun, 2018

people specializing in cyber-security are heavily recruited by top IT companies abroad[134]. This shows that if the state managed to develop and systemize its cyber-security, it could actually utilize its internal human resources to protect cyberspace.

Another aspect from Estonia's model that must be noted is that its educational initiatives targeted the entire population. While the initiatives at first started with training teachers with IT technology to improve Estonia's education system and encouraging the population to utilize e-services, the 2007 cyber-attacks have radically changed the focus. Estonia decided to make its population knowledgeable in the domain of cyber-security starting with the development of experts of the field since school days. Lebanon should also design a curriculum where cyber-security is being taught in all educational institutions, whether school or universities[135]. In addition to the educational curriculum, Lebanon should invest in establishing research and development laboratories that would assist in protecting the state's data from being mishandled[136]. A cyber-security major would analyze the field from a technical, policy and legal level which would raise a generation of experts that would ensure the public and private sector's cyber-performances[137]. While some Lebanese universities do provide majors, such as computer science or computer engineering, only the Lebanese University has a major titled "Cyber-security". More Universities should provide such major that encompasses both technical and policy aspects of cyber-security[138].

---

[134] *Ibid,*
Barakat, Jihad. Personal interview. 5 Jul, 2018
Khayrallah, Jean. Personal interview. 29 Jun, 2018
[135] This was stated by all five interviewees.
[136] *Ibid.*
[137] Karam, Marie-Line. Personal interview. 1 Jul, 2018.
[138] Karam, Marie-Line. Personal interview. 1 Jul, 2018;
Khalife, Joseph. Personal interview. 15 Jun, 2018.

5.2.6 Cyber-Security Strategy

Conclusively, the above-mentioned elements must be cemented in order to benefit a state. As such, the final lesson that Lebanon should embrace is a national cyber-security strategy (NCSS). Only a national cyber-security strategy can help Lebanon achieve the developments it needs in the field of cyber-security. As showed in chapter two, Estonia's cyber-security policies took a different path after the 2007 cyber-attacks. If until the cyber-attack incident Estonia's policies and strategies concentrated on enhancing ICT structures and developing the nation's skills in the field of cyberspace, the post-2007 strategies took a radical switch and concentrated on combating cyber-threats.

As such Lebanon has to develop an NCSS that includes actions that are designed to improve the ICT infrastructure, enhance the state's cybersecurity by educating its population and raise local experts and make the national infrastructures and services resilient. This NCSS would include the state's objectives and priorities that should be achieved in a specific timeframe. Taking the Estonian NCSS as an example, the strategy begins with an overall analysis of the current state's cyber-security situation. Continuing on, Estonia's NCSS states the overall goal of the document which is to "*increase cybersecurity capabilities and raise the population's awareness of cyber threats, thereby ensuring continued confidence in cyberspace*"[139]. Secondly, it follows up to state the sub-goals that will lead to its overall objective:

[139] Estonia's Cyber Security Strategy 2014-2017, p.8.

- ensuring the protection of information systems underlying vital services by defined practices and the protection of critical information against cyber-threats;
- through improved detection methods of cyber-crime and international cooperation, as well as further advocating education and awareness;
- to continuously develop the state's cyber defense capabilities through a broad-based collective defense that includes civil and military competencies as well as international cooperation;
- to combat cyber-threats through various cyber-security solutions that includes trained professionals and training opportunities, research and development and entrepreneurship; and,
- to continuously develop the national legal framework and cyber foreign policies to protect critical services and combat cyber-crimes[140].

As it can be seen, the Estonian NCSS has a clearly defined objective with sub-goals with the timeframe being settled for the period of 2014-2017. In addition, Estonia's NCSS clearly states that parties from public and private sectors will be involved in the strategy's implementation, while agencies responsible for the realization of strategy will be annually evaluated[141].

Clearly, this thesis does not suggest to entirely copy the Estonian NCSS and apply it in Lebanon. Each state has a different perspective of threats to its security and has its own measures to combat them. However, the Estonian cyber-strategy could clearly be modified and utilized by Lebanon. The Estonian NCSS encompasses all the important elements of cyber-security that were mentioned throughout this paper: a) organizational structure; b) legislative frameworks; c) public-private partnership; d) international cooperation and e) education and awareness. If these elements were to be

[140] *Ibid,* p.8-12.
[141] *Ibid,* p.13.

adopted into a Lebanese NCSS, it would definitely improve Lebanon's cyber-security, as it would set up the required actions that would be needed to achieve them, the parties involved and responsible for the strategy's implementation and the evaluation of activities and achieved objectives.

5.3 Challenges in Developing Lebanon's Cybersecurity

Obviously, implementing cyber-security lessons of Estonia in Lebanon would face great challenges. The first reason that comes to mind in halting the development of Lebanon's cyber-security is sectarianism. Since the creation of the state of Lebanon, sectarianism has played a major role in the country's life. The Taif agreement that aimed to end the civil war in Lebanon and to bring back political stability in the country eventually ended up with the sectarian leaders consolidating their power and dominance in the state, rather than enhancing governance (Makdesi and Khalil 2013). Sectarianism eventually affected even the state's institutions. Lebanon's political power was distributed throughout various sects, state's institutions were allocated accordingly leading to obstruction of any reform or change (Salamey 2013). Furthermore, even the private sector, with the exception of the banking sector, became tainted with sectarian influences (Makdesi and Khalil 2013). As such, sectarianism could affect any major developments in the area of cyber-security. In fact, all interviewees have agreed that sectarianism is one of the main internal causes that hinder Lebanon's cyber-security. The interviewees stated that not only do sectarian leaders lack in the field knowledge of cyber-security, they are engaged in issues related to politics and finance leaving cyber-security overshadowed. However, at times, the

sectarian powers manage to reach a consensus on certain decisions. An agreement between the sectarian leaders is achieved only if it benefits their personal interests or if there is a threat to their dominance in the state (Majed 2017). A proper institutional reform for cyber-security would definitely attract attention from the sectarian leaders in Lebanon. The reason behind it is the fact that cyber-security encompasses information, transactions and even control of critical infrastructures in the physical world (Bruijn and Janssen 2007). This means that the institution that would be responsible for cyber-security in Lebanon would let a certain sect have access and control over the entire information data circulating in the country. Could sectarian powers in Lebanon reach a consensus on such a matter? Could cyber-security be given to a specific sectarian power that would have access to the state's entire information data? Or would sectarian leaders obstruct any possible cyber-security changes through state institutions? While this paper does not aim to analyze how sectarianism affects the development of cyber-security frameworks, this would require a deeper examination. It is important to note that the Lebanese Forces and Free Patriotic Movement have agreed on delegating experts from each side to examine the cyber-security situation in Lebanon[142]. This shows that cyber-security has started to attract the interest of the Lebanese political parties. It has yet to be seen if proper cyber-security foundation could be built in Lebanon, knowing the complicated governmental system due to the need of consensus of all parties.

Another internal challenge, due to geopolitical reasons, with Lebanon's cyber-security development could be Hezbollah. While the group declared that it is in

[142] Barakat, Jihad. Personal interview. 5 July, 2018;
Khalife, Joseph. Personal interview. 15 June, 2018.

Lebanon only to resist Israel in the South of Lebanon, Hezbollah eventually developed into a "state within a state" (Abdul-Hussain 2009). Hezbollah has grown into something more powerful than simply a group, as it has engaged in the 2006 war against Israel, fought ISIS in Lebanon's territory and has been actively participating in Syria's conflict. Since 2008, Hezbollah has also succeeded in gaining political power in Lebanon[143]. Even in the area of cyberspace, Hezbollah is way ahead than the Lebanese state itself. Firstly, Hezbollah already participated in a cyber-war against Israel as discussed earlier, where it managed to gain support from the Arab world for its resistance campaign in Lebanon (Al-Rizzo 2010; Azan et al. n.d.). Secondly, while the state of Lebanon has only the Cybercrime Bureau that is technology equipped to combat cyber-crimes, Hezbollah has integrated cyber-units into its personnel since the beginning of this century (Jean-Loup 2015: 297). Not only it indicates that Hezbollah has gained tremendous experience in cyber-activities, it also leads one to the following question: – if Lebanon will continue to develop its ICT and cyber-security capabilities, will it clash with Hezbollah's? In 2008 Hezbollah engaged into a military confrontation against the Lebanese government, partly due to the latter's order to shut down the group's communication network (Ismael et al. 2016, p.345; Sloan & Anderson 2009, p.249). Could Hezbollah regard Lebanon's advancement in cyber-capabilities as a threat to its own cyberspace abilities? Could it lead to another violent conflict between the two sides? Or is there a possibility where each sides continues to develop its own digital capabilities within Lebanon's territory? These are questions that are beyond this research, yet, they offer new research paradigms. Yet one matter

[143] "Profile: Lebanon's Hezbollah movement", *BBC News*, Mar. 15, 2016. Accessed 20 April, 2018. http://www.bbc.com/news/world-middle-east-10814698

is certain that at some point in the future Lebanon's cyber-security will have to deal with Hezbollah's cyberspace activities. Time will show if Hezbollah will utilize its military and political power to affect Lebanon's cyber-security development.

Finally, Israel could be considered as one of the greatest challenge for the Lebanese state to develop a cyber-security through compliance with the Budapest Convention. Firstly, since the creation of Israel, Lebanon has had a long and hostile relation with its neighbor which it has refused to recognize till this date. In 1982, Israel invaded Lebanon with the goal of removing the Palestinian Liberation Organization (PLO) from the country[144]. During the1990's, Israel continued to occupy some of Lebanon's Southern territories up till 2000[145]. Furthermore, since Hezbollah cemented its position in the Southern Lebanon, Israel has seen it as a threat to its own security. The tension between Israel and Hezbollah eventually exploded culminating in the 2006 Summer War, which witnessed Israeli's massive air and artillery strikes and the destruction of Lebanese infrastructure[146]. Up till today, both states perceive each other as enemies. Recently, the tension between Lebanon and Israel augmented after disputes broke up over gas and oil resources in the Mediterranean Sea[147].

---

[144] The invasion of Lebanon began in 1982, when the Israel forces began its military intervention "Operation Peace for Galilee" that was aimed against the PLO.
Macintyre, Donald, "Israel set to invade Lebanon despite lessons of 1982 war", *The Independent*, Aug. 9, 2006. Accessed 12 May, 2018. https://www.independent.co.uk/news/world/middle-east/israel-set-to-invade-lebanon-despite-lessons-of-1982-war-411248.html

[145] "Lebanon profile – Timeline", *BBC NEWS*, Apr. 25, 2018. Accessed 12 May, 2018. http://www.bbc.com/news/world-middle-east-14649284

[146] "FACTBOX: Costs of war and recovery in Lebanon and Israel", *Reuters*, Jul. 9, 2007. Accessed 12 May, 2018. https://www.reuters.com/article/us-lebanon-war-cost/factbox-costs-of-war-and-recovery-in-lebanon-and-israel-idUSL0822571220070709

[147] Barrington, Lisa and Dan Williams, "Israel, Lebanon clash over offshore energy, raising tensions", Jan. 31, 2018. Accessed May 12, 2018. https://www.reuters.com/article/us-natgas-lebanon-israel/israel-lebanon-clash-over-offshore-energy-raising-tensions-idUSKBN1FK1J0

Due to the historical confrontations, the potential application to join the Budapest Convention could be challenging for Lebanon, as Israel is a member to the treaty. This is also reinforced by three interviewees which believe that Israel is the main reason as to why Lebanon's officials have not shown interests in the treaty. In addition, the problem also lays in Article 37 of the Convention which states:

"*After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers*"[148].

Since a unanimous consent is required to invite a non-party state to join the Convention, Israel could possibly veto an invitation to Lebanon. Any diplomatic attempts to fix the situation would hit a wall, as both states are in a legal state of war since 1948 and have no diplomatic relations[149]. Conflicts related to both countries were regulated through resolutions of the UN. However, it is doubtful that the UN would actually involve itself in such case. As such, it would be interesting to observe whether the issue of Lebanon applying for the Budapest Convention could open minimum channels of discussion or negotiation with Israel. Another possible solution is other

[148] Article 37 (1) of the Budapest Convention.
[149] Baroudi, Roudi, " Lebanon-Israel maritime dispute: Rules of (diplomatic) engagement", Mar. 16, 2018. Accessed 12 May, 2018. https://en.annahar.com/article/776079-lebanonisrael-maritime-disputes-rules-of-diplomatic-engagement

members acting as mediators between the two states, as it has been the case in many past conflicts[150]. Surprisingly, it is also possible that Israel's participation in the Convention would not be a road-block for Lebanon in the following scenarios: a) if the Convention did not require a state to respond to the inquiries from another state; and b) if another party would conduct the inquiries on behalf of the interested state[151]. For instance, Lebanon and Israel are both member countries of the Interpol[152]. In the case of Budapest Convention, the second scenario would seem as the most feasible in the current circumstances.

[150] Barakat, Jihad. Personal interview. 5 July, 2018; Khayrallah, Jean. Personal interview. 29 Jun, 2018.
[151] Chebat, Khaled. Personal interview. 1 Sep, 2018.
[152] *Ibid.*

Chapter Six

Conclusion and Recommendation

6.1 Conclusion

This research has presented a new issue that has not been adequately presented before in relation to Lebanon's security problems. This paper can be considered as an analysis on Lebanon's cyber-capabilities and its ability to protect itself from cyber-threats. While attempting to examine whether Lebanon is able to defend itself from cyber-attacks, this study and the conducted interviews have led to various findings and revealed some of the limitations in addressing this topic.

This study concludes that with current capabilities, Lebanon is unable to defend itself from cyber-attacks. The combination of several internal factors have hindered Lebanon's cyber-security development. Firstly, cyber-security in Lebanon has not received the required attention leaving the state vulnerable to cyber-threats. This comes as a result of missing a governmental body that would be solely tasked with cyber-security initiatives and developing the currently absent national cyber-security strategy. It has to be understood that a cyber-security strategy is a political act, as it creates expectations and raises awareness among the population. The absence of cyber-security foundational elements, a specifically responsible governmental body and a cyber-security strategy, leave Lebanon's public and private sectors vulnerable to cyber-attacks. As such, it should not be surprising that Lebanon has no laws related to cyber-security or cyberspace in general. Secondly, the analysis of OMSAR's National

Cyber Security Policy Guidelines and the actions undertaken by the Cybercrime Bureau lead us to conclude that the measures adopted are controversial. The entire development of NCSPG could be deemed as faulty. This initiative simply covered the governmental institutions, leaving aside the entire private sector. The latter's expertise, opinions and fears were neglected. The Cybercrime Bureau has ignored its original task of combating cyber-crimes and has become an instrument in protecting the Lebanese political elite. It has detained and imprisoned citizens that voiced their opinions about the state's political system and politicians. In addition, this study has found that the Cybercrime Bureau is involved in spying on the Lebanese citizens and is connected to a worldwide spying campaign.

Thirdly, the compliance or attempt to meet the requirements of the Budapest Convention on Cybercrime would greatly improve the cyber-security capabilities of Lebanon. In order to adhere to the Convention's requirements, Lebanon would be required to adjust its national legislation to cover the area of cyber-crimes. In addition, it would have to establish its own CERT that would be tasked of monitoring and reporting intrusions into the state's cyberspace and providing assistance to various sectors in emergency situations. Such developments would greatly improve Lebanon's cyber-security. Unfortunately, at the current moment, Lebanon is ineligible to join the only legally binding Convention against cyber-crimes.

Finally, despite its lack of initiatives in building defensive capabilities, Lebanon's intelligence units succeeded in conducting cyber-operations not only within the state, but in the world. This has two implications in terms of international relations. Firstly, it means that Lebanon is an active actor in the international arena when it

comes to cyber-operations, despite being unnoticed by the global community. Secondly, while its offensive capabilities seem functional its defensive measures, according to the available information, are below the standard of developed countries. This will eventually force Lebanon to request assistance from a more cyber-technology developed state. Such assistance would force Lebanon to pick its allies and categorization of unfriendly states, at least in the field of cyberspace, in a conflict torn Middle-East region.

6.2 Recommendation

Cyber-security should become a matter of concern for Lebanon's national security. This thesis has shown that Lebanon has suffered, and still is suffering, from a number of cyber-attacks. In order to counter the sophisticated cyber-threats and protect its public and private sectors, the state must step forward and take action. First of all, a governmental institution must be established that would be solely responsible for strategy implementation regarding cyber-security. If modeled according to the Estonian example, a Lebanese Information System Authority should become the main cyber-security body in the state with government agency status. Most importantly, in order to perform its duties effectively, this institution should be allowed to operate disregarding the sectarian conflicts that have entangled other governmental bodies. Only then, by creating such an institution, could the state move on to create a multidimensional and comprehensive strategic approach - Lebanese national cyber-security strategy. Such a strategy would set the objectives and aims of the state in the field of cyber-security and the means in obtaining them. Furthermore, such a policy

would strengthen the cooperation and ensure the participation of all stakeholders of the public and private sectors in protecting the state's cyberspace. It would also ensure that specific regulations would be developed and incorporated within the state's legislations which would broaden Lebanon's capabilities in combating cyber-criminals. Finally, such strategy would highlight the need of international cooperation which would allow Lebanon to coordinate action and conclude agreements with other states regarding cyber-crimes. International cooperation would greatly benefit Lebanon as it could obtain best practices and lessons learnt from other states in preventing and countering cyber-threats. Eventually it would strengthen Lebanon's capabilities of protecting its national security in the field of cyberspace.

6.3 Limitation of the Study

This study encountered obstacles in obtaining information pertaining to Lebanon and cyber-security. Firstly, the literature regarding the matter is absent. This is because Lebanon in general is mostly reviewed and examined in the context of sectarianism, its turbulent history, relation with its neighbors and its role in the conflict ridden Middle East region. However, terms such as cyberspace, cyber-threats and cyber-security are relatively new for Lebanon. In addition, retrieving governmental documents, initiatives and policies in relation to cyberspace was a challenge.

Another limitation was the difficulty of finding experts that are knowledgeable in both, the technical and the strategic sphere. While technical cyber-security experts in Lebanon are available, most are not versed in international agreements or governmental policies related to cyber-security. Fortunately, the required interviewees

for this study were identified and interviews were conducted. Some interviewees were found locally and some were located working abroad in relation to their field.

Additionally, knowing the nature of the Lebanese institutions and their secrecies, it was challenging to retrieve official information about reported cyber-attacks and their damages. Although newspapers provided some reports and statements regarding cyber-incidents, it was difficult to find disclosures provided by the institutions themselves. As such, it must be noted that some of the information related to cyber-attacks are undisclosed and kept as a secret by the relevant Lebanese institutions. Therefore, managing to get interviews with officials within the government, especially in the intelligence institutions, would be of great value for any future research.

Finally, Hezbollah's cyber-activities within Lebanon's territory and abroad have yet to be fully examined. It has demonstrated its capabilities during the Summer War of 2006, proving that it is constantly developing its offensive and defensive cyber-power. Retrieving information on Hezbollah's cyber-activities could be of a great value for future research, concretely in topics related to non-state actors' impact on states relations.

6.4 Future Prospects

Despite the research limitations that were reported above, a topic such as cyber-security in Lebanon cannot be adequately covered in a single research thesis. As such, attempting to answer the question of this thesis, it uncovered related areas of

investigation in different fields. This thesis could provide the direction for Lebanese policy and law makers in formulating cyber-security frameworks based on the Budapest Convention and Estonia's example. Furthermore, it can serve as a starting point for future research pertaining to cyber-security and cyber-threats related to Lebanon, as this topic has been overshadowed by the traditional security issues. Research regarding the formation of a functional governmental body responsible for cyber-security in the Lebanese political environment could be of great value. It would be particularly interesting to see if it is viable to create a body that would not be hindered by sectarian elites. Secondly, the cyber-activities conducted by Lebanese intelligence agencies also deserve to be researched. This should attract attention as such activities contravene the essence of the constitution and international agreements that safeguard the privacy and freedom of an individual. Furthermore, a research of the private sector, especially the banks, deserves important attention. It would be interesting to analyze how the private sector is able to cope with the sophisticated cyber-threats threatening its daily operations in a state that has no legal, organizational or strategic framework for cyber-security. Such a study would unveil the cost that the private sector is sustaining from cyber-attack damages due to the impossibility of receiving state assistance in combating cyber-threats. Additionally, cyber-security in the Lebanese education curriculum could also be an interesting subject to study. It would be intriguing to discover how a curriculum pertaining to cyber-security could be integrated in the Lebanese educational system and what could be its potential benefits. Finally, Lebanon could serve as an interesting case study in regards to the state's cyber-opportunities in the Middle East region and the challenges related to a

powerful non-state actor, Hezbollah, and its cyber-operations within the borders of the country.

Bibliography

Abdo, Geneive. "Salafists and Sectarianism: Twitter and Communal Conflict in the Middle East." Brookings. 2016. Accessed May 24, 2018. https://www.brookings.edu/research/salafists-and-sectarianism-twitter-and-communal-conflict-in-the-middle-east/

Abdul-Hussain, Hussain. "Hezbollah: A State Within a State." *Current Trends in Islamist Ideology*, May 21, 2009. 2009. Accessed April 20, 2018. https://www.hudson.org/research/9801-hezbollah-a-state-within-a-state.

Alaaraj, Hassan, and Fatima Ibrahim. "The Influence of E-government Practices on Good Governance from the Perspective of Public in Lebanon." *Journal of Public Administration and Governance* 4, no. 3 (2014). Accessed March 25, 2018. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.671.627&rep=rep1&type=pdf

Areng, Liina. "LILLIPUTIAN STATES IN DIGITAL AFFAIRS AND CYBER SECURITY." *The Tallinn Papers*, 2014. Accessed May 26, 2018. https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf

Bruijn, Hans De, and Marijn Janssen. "Building Cybersecurity Awareness: The Need for Evidence-based Framing Strategies." *Government Information Quarterly*34, no. 1 (2017): 1-7. Accessed April 19, 2018. doi:10.1016/j.giq.2017.02.007.

Bucaj, Enver. "The Need for Regulation of Cyber Terrorism Phenomena in Line With Principles of International Criminal Law." *Academic Journal of Business, Administration, Law and Social Sciences*, 1st ser., 3 (2017): 141-60. 2017. Accessed April 8, 2018. journals.univ-danubius.ro/index.php/juridica/article/view/388

Chelala, Chantal, and Lina Koleilat Ghalayini. "THE IMPACT OF THE LACK OF DATA PROTECTION REGULATIONS ON THE DEVELOPMENT OF E - COMMERCE IN LEBANON." 2015. Accessed March 25, 2018. http://webscience-digitaleconomy-workshop.blogs.usj.edu.lb/files/2015/03/WebSci15-WORKSHOP_submission_2-CHELALA.pdf

Chernenko, Elena, Oleg Demidov, and Fyodor Lukyanov. "Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms." Council on Foreign Relations. 2018. Accessed April 5, 2018. https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

Choueiri, Elias, Bernard Choueiri, and Georges Choueiri. "An Overview of E-Government Strategy in Lebanon." *International Arab Journal of E-Technology* 3, no. 1 (2013): 54-55. Accessed March 26, 2018. http://www.iajet.org/iajet_files/vol.3/no.1/An Overview of e-Government.pdf

Council of Europe. Committee of Ministers. "*Explanatory Report to the Convention on Cybercrime*". Budapest, 2001. Accessed April 8, 2018. https://rm.coe.int/16800cce5b

Csonka, Peter. "The Council of Europes Convention on Cyber-crime and Other European Initiatives." *Revue Internationale De Droit Pénal* 77, no. 3 (2006): 473-501. Accessed April 8, 2018. doi:10.3917/ridp.773.0473

Estonia. Ministry of Economic Affairs and Communication. "*Cyber Security Strategy 2014-2017."* 2014. Accessed March 20, 2018. https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

Fayad, Mira, and Habib Kazzi. "ELECTRONIC ARBITRATION IN LEBANON – OVERVIEW AND TRENDS." *European Scientific Journal* 11, no. 7 (2015): 40-41. Accessed March 25, 2018. https://eujournal.org/index.php/esj/article/view/5304

Frangieh, Ghida. "Lebanon's Cybercrime Bureau: A License to Censor". *The Legal Agenda*, Feb. 27, 2014. Accessed April 1, 2018 at http://legal-agenda.com/en/article.php?id=590&lang=en

Freedom House. "*Lebanon Country Profile*." Report. 2017. Accessed March 25, 2018. https://freedomhouse.org/report/freedom-net/2017/lebanon.

Goldman, David. " Cyberweapon targets Middle East bank accounts". *CNN Tech*, Aug. 9, 2012. Accessed April 1, 2018. http://money.cnn.com/2012/08/09/technology/gauss-cyberweapon-bank-accounts/index.html

International Telecommunication Union. "*Global Cybersecurity Index 2017."* Publication. 2017. Accessed March 24, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

International Telecommunication Union. "*ITU Toolkit For Cybercrime Legislation."*Draft. 2010. Accessed April 15, 2018. http://www.cyberdialogue.ca/wp-content/uploads/2011/03/ITU-Toolkit-for-Cybercrime-Legislation.pdf

Isnarti, Rika. "A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War." *Andalas Journal of International Studies* (AJIS) 5, no. 2 (2016). Accessed October 9, 2018. http://ajis.fisip.unand.ac.id/index.php/ajis/article/view/53.

Holdorf, Polly M. "Prospects For An International Cybersecurity Regime." *US Air Force Institute for National Security Studies*, INSS strategic paper (2015). Accessed 17 November, 2018. http://www.usafa.edu/app/uploads/Holdorf_Prospects_for_an_International_Cybersecurity_Regime9July2015.pdf

Karam, Jeffrey G. "Beyond Sectarianism: Understanding Lebanese Politics through a Cross- Sectarian Lens." *Middle East Brief*, no. 107 (2017): 2. Accessed March 25, 2018. https://www.brandeis.edu/crown/publications/meb/MEB107.pdf

Kissinger, Henry. *World Order*. NY, NY: Penguin Books, 2015.

Kshetri, Nir. "Cybersecurity in National Security and International Relations." *The Quest to Cyber Superiority*, 2016, 53-74. Accessed October 8, 2018. doi:10.1007/978-3-319-40554-4_3

Freedom House. *"Lebanon Country Profile."* Report. 2017. Accessed April 1, 2018. https://freedomhouse.org/report/freedom-net/2017/lebanon

Lebanon. Office of the Minister of State for Administrative Reform. *E - Government Strategy for Lebanon.* 2002. Accessed March 20, 2018. http://www.omsar.gov.lb/Cultures/en-US/Publications/Strategies/Documents/0c1a2448c3f2450a94ccc000ed7234d2eGov_Strategy_Executive_Summary_En.pdf.

Lebanon. Office of the Minister of State for Administrative Reform. "*Lebanese National Cyber Security Policy Guidelines".* 2015. Accessed March 25, 2018. http://www.omsar.gov.lb/Cultures/en-US/ResourcesSupport/SupportAdministration/Documents/Lebanese National Cyber Security Policy Guidelines v1.7.pdf

Lewis, Andrew James. *State Practice and Precedent in Cybersecurity Negotiations.* Center for Strategic and International Studies, 2018. Accessed October 5, 2018. https://csis-prod.s3.amazonaws.com/s3fs-

public/publication/180801_Lewis_StatesPSI_.pdf?b_08nboCus3pMi1PDWwkPh5FflJB5Brm

Liang, Christina Schori. "Christina Schori Liang: Cyber Jihad: Understanding and Countering Islamic State Propaganda. 2015." Geneve Centre for Security Policy, policy paper 1, no. 1 (2017). February 2015. Accessed May 24, 2018. https://www.gcsp.ch/News-Knowledge/Publications/Cyber-Jihad-Understanding-and-Countering-Islamic-State-Propaganda

Lookout and Electronic Frontier Foundation. " *Dark Caracal Cyber-espionage at a Global Scale,"* Security Research Report, (2018). Accessed April 1, 2018. https://info.lookout.com/rs/051-ESQ-475/images/Lookout_Dark-Caracal_srr_20180118_us_v.1.0.pdf

Maghaireh, Alaeldin. "Shariah Law and Cyber-Sectarian Conflict: How Can Islamic Criminal Law Respond to Cyber Crime?" *International Journal of Cyber Criminology* 2, no. 2 (2008): 337-45. Accessed May 24, 2018. https://pdfs.semanticscholar.org/60ec/44469cc3190ec95936c3ba94df11d8f4891c.pdf.

Makdisi, Samir, and Youssef El-Khalil. 2013. "Lebanon: The Legacy of Sectarian Consociationalism and the Transition to a Fully-fledged Democracy." Working Paper Series No. 14, Issam Fares Institute for Public Policy and International Affairs American University of Beirut. Accessed 20 March, 2018. https://website.aub.edu.lb/ifi/public_policy/rapp/Documents/working_paper_series/20130301samir_makdesi_youssef_khalil_rapp_wp.pdf

Majed, Rima. "The Political (or Social) Economy of Sectarianism in Lebanon". *Middle East Journal,* (2017). Accessed 26 March, 2018. http://www.mei.edu/content/map/political-or-social-economy-sectarianism-lebanon

Marion, Nancy E. "The Council of Europe's Cyber Crime Treaty: An Exercise in Symbolic Legislation." *International Journal of Cyber Criminilogy* 4, no. 1&2 (2010): 699-712. 2010. Accessed April 8, 2018. http://www.cybercrimejournal.com/marion2010ijcc.pdf

Nye, Joseph S. "The Regime Complex for Managing Global Cyber Activities." Global Commission on Internet Governance Paper Series, 1. 2014. Accessed 5 April, 2018. https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Petallides, Constantine J. 2012. Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat. *Inquiries Journal/Student Pulse* 4 (03), http://www.inquiriesjournal.com/a?id=627

Pernik, Piret, and Emmet Tuohy. “Interagency Cooperation on Cyber Security: The Estonian Model.” *International Centre for Defence Studies*, pp. 9–6. Accessed 5 April, 2018. www.sto.nato.int/publications/.../STO-MP-HFM-236/MP-HFM-236-09.pdf

Raiyn, Jamal. "A Survey of Cyber Attack Detection Strategies." *International Journal of Security and Its Applications* 8, no. 1 (2014): 247-56. Accessed March 25, 2018. https://pdfs.semanticscholar.org/942a/4ce3f6ddadc5bbdd55497861dc8c85703cdd.pdf

Salem, Paul. "Lebanon's Government Should Lay the Groundwork for Fairer Representation and Accountability." *Middle East Institute*. 2017. Accessed April 1, 2018. https://www.mei.edu/content/article/lebanon-s-government-should-lay-groundwork-fairer-representation-and-accountability-0

Sorby, Karol R. "LEBANON: THE CRISIS OF 1958." *Asian and African Studies 9* (2000): 76-109. Accessed March 24, 2018. https://www.sav.sk/journals/uploads/082713259_Sorby.pdf.

Vaishnav, Chintan, Nazli Choucri, and David D. Clark. "Cyber International Relations as an Integrated System." *Environment Systems and Decisions* 33 (2013): 561-76. Accessed October 6, 2018. doi:10.1007/s10669-013-9480-3.

Vassil, Kristjan. “*Estonian e-Government Ecosystem: Foundation, Applications, Outcomes”.* WorldBank, 2016. Accessed June 15, 2018. http://pubdocs.worldbank.org/en/165711456838073531/WDR16-BP-Estonian-eGov-ecosystem-Vassil.pdf

Appendix

Consent to participate in a Questionnaire
Master Thesis "Cybersecurity in Lebanon: Learning from Estonia's model"

I would like to invite you to participate in a research project by completing the following questionnaire. (I am a student at the Lebanese American University and I am completing this research project as part of my Master Thesis). The purpose of this questionnaire aims to gather primary data on Lebanon and its cybersecurity.

There are no known risks, harms or discomforts associated with this study beyond those encountered in normal daily life. The information you provide will be used to enrich the existing literature regarding Lebanon in the field of cybersecurity. You will not benefit from participation in this study. Completing the interview questionnaire will take 25-35 minutes of your time. Your name and answers will be revealed and utilized as a reference in the study. Do you agree? ☐ YES / ☐ NO

By continuing with the questionnaire, you agree with the following statements:

1. *I have been given sufficient information about this research project.*
2. *I understand that my answers will be released in my research paper and my identity will be known.* ***My name and answers will be utilized as a reference in the study of "Cybersecurity in Lebanon".***
3. ***I understand that if I wish to remain anonymous, my name will not be written on the questionnaire not kept in any other records. I will not be identified by name or any other information that could infer to my identity.*** *Only researchers will have access to view any data collected during this research however data cannot be linked to me.*
4. *I understand that I may withdraw from this research any time I wish and that I have the right to skip any question I don't want to answer.*
5. *I understand that my refusal to participate will not result in any penalty or loss of benefits to which I otherwise am entitled to.*
6. *I have been informed that the research abides by all commonly acknowledged ethical codes and that the research project has been reviewed and approved by the Institutional Review Board at the Lebanese American University*
7. *I understand that if I have any additional questions, I can ask the research team listed below.*
8. *I have read and understood all statements on this form.*
9. *I voluntarily agree to take part in this research project by completing the following questionnaire.*

If you have any questions, you may contact:

Name (PI)	*Phone number*	*Email address*
Kristofas Barakat	*76108588*	*Chris.barakat92@gmail.com*
Dr. Makram Ouaiss	*LAU extension: 2401*	*makram.ouaiss@lau.edu.lb*

If you have any questions about your rights as a participant in this study, or you want to talk to someone outside the research, please contact the:

Institutional Review Board Office, Lebanese American University, 3rd Floor, Dorm A, Byblos Campus
Tel: 00 961 1 786456 ext. (2546), irb@lau.edu.lb
This study has been reviewed and approved by the LAU IRB:

Participant's name:_____ **Participant's signature:**_____

Questions for interviews for thesis "Cybersecurity in Lebanon: Learning from Estonia's model"

General questions

- In your opinion where does cyber-threat rank in Lebanon's security agenda? Has it become a top priority, or is it still behind other issues?
- When visiting the Telecommunication Authority website, it is clear that Lebanon has no policy, strategy or vision in cyber-security. What is stopping the state of from adopting a cyber-strategy?
- While the issues relating to cyber-security and cyber-threats are gaining prominence in Lebanon, it is still far away from the level of awareness found globally and even regionally. In your opinion, what should be done in Lebanon to have higher awareness regarding these issues?

Cyberspace in Lebanon's politics

- It is known that sectarianism plays a major role in Lebanon's daily life. Is sectarianism one of the main reasons as to why Lebanon has not created a cyber-strategy?
- In your opinion, what are the main threats to Lebanon's cyberspace security? (Foreign states, non-state actors or others)
- In your opinion, why has Lebanon not passed laws against cyber-crimes? Are the complimenting reasons external or internal (lack of political will, lack of experts, funds or others)
- Currently, the Middle-East region is engaged in various conflicts. Regional powers have been heavily using cyberspace to portray the conflicts in their own colors while dashing their opposing sides. Do you believe the leaders of the Lebanese state are doing something in order to resist the battles that are occurring on cyberspace?
- Lebanon's Parliamentary elections will take place soon. Is there any potential in cyber-security becoming an important focus of the future Parliament, or will it still be overshadowed by the traditional issues, such as sectarianism, terrorism or regional power conflicts?

Lebanon's Cybercrime Bureau

- In 2015, the Internal Security Forces (ISF) established the Cybercrime Bureau in order to combat the misuse of cyberspace. In your own words, what is the Cybercrime Bureau's job?
- What is your view on the alleged reports that Cybercrime Bureau has so far been detaining citizens that expressed their opinions against Lebanon's politicians on the internet? Could we say that the political parties are interested in having such an institution only to control the public opinion, rather than to combat cyber-threats?
- In addition to having matters of cybersecurity addressed by the ISF, should universities and the private sectors, such as the banks play a role in this field? One providing experts on a technical and policy level, the other providing expertise and experience in combating cyber-attacks.
- In general, do you believe that the protection of cyberspace should be solely given to the military? In countries such as the US or Australia such approach was criticized.

International cooperation in cyber-security

- In 2001, the Budapest convention was created to combat cyber-crimes. Currently, it has 56 signatories and Lebanon is not a signatory to it. Has there been any attempts by Lebanon to fulfill the requirements of the convention? What has been the level of interest from Lebanon's leaders towards the cyber-crime convention?
- The convention allows the states to share their expertise and cooperate in case of major cyber-crimes. Would it be beneficial for Lebanon to be part of such convention where it could seek support in case of major cyber-attacks?
- One of the signatories of Budapest convention is Israel. Can it be one of the factor as to why Lebanon has not become a signatory, nor it has shown interest in the convention?
- Could Lebanon attract international cooperation to strengthen its cyberspace? International organizations such as the UN, the EU delegation in Lebanon or USAID are funding various

projects in Lebanon. Is there a possibility to negotiate with these organizations that part of their funds in Lebanon be utilized for projects on building cyber-security in the state?

- Can INTERPOL be one of the organizations that could provide support for Lebanon in matters related to cyber-security, especially when the current head-chief is Elias Murr, a Lebanese citizen?

Public-private cooperation in cyber-security

- Is there any potential for creating a platform where private and public sectors could cooperate against cyber-threats? For example, Estonia has created the cyber defense league that involves government experts, businesses and even individual volunteers that combine their knowledge in combating cyber-threats? Could Lebanon create a similar platform?

- To my knowledge, there is only one academic institution, the Lebanese University that provides a major related to cyber-security. In your opinion, is one academic institution enough to supply cyber-experts for the state?

- In recent years, the banking sector witnessed major cyber-attacks. In 2012, the "Grauss" virus was created which was specifically designed to cyber-espionage the Lebanese banks. While it was reported that the banks were able to take counter-measures, there were no mentions of the state helping the banking sector. Do you believe the private sector, especially the banking sector which is considered as one of the main pillars of Lebanese economy, should be the one to combat cyber-threats alone?