Lebanese Cyber Security Strategy

by

Bassel HAJJAR

Beirut. Lebanon

Spring 2021

ABSTRACT

The Internet was conceived as a tool to be used in the interest of humankind, as a free open platform for the universal exchange of information and knowledge outside conventional geographical boundaries. If this target has been met, it must be acknowledged that the development of emerging technology has likewise expanded the dangers related to this space. Cyberspace is a virtual environment where power and influence are expressed, as well as cultural, political, military, and economic complexities. As such, it is constantly developing in the establishment of contemporary global affairs.

Today, the reliability, openness, and security of information and communication technology are critical to our everyday lives, social interactions, and economies. However, it appears that Lebanon, like all other countries, faces numerous cyber-threats (espionage, terrorism, or data fraud), thus weakening trust and security in cyberspace. In this context, the Lebanese state's primary duty is to provide Cyber Security resolutions to present and future challenges, as well as to establish an open and free Cyberspace that respects democracy while being secured, in order to provide security to people, and to all sectors. As a result of this observation, a National Committee to Establish a National Cyber Security System was established. The Strategy we propose here is the culmination of this intense collaborative work, and it is the cornerstone of our society's national security, which will definitely turn more digitalized, and thus must serve the common interest of all doers in Lebanon's society. This approach aims to control Lebanon's Cyberspace, to place the human element at the core of its obligations, to raise awareness about the importance of a national joint effort at home, and to achieve stronger international cooperation.

TABLE OF CONTENTS

LIST OF TABLES

N.B. *Use Word's Table of Figures feature to create this section (using caption style = "Table"). The List of Tables entries should adopt the Harvard Referencing format.*

LIST OF FIGURES

N.B. *Use Word’s Table of Figures feature to create this section (using caption style = “Figure”). The List of Tables entries should adopt the HARVARD format.*

PART I

THE THEORETICAL FRAMEWORK

CHAPTER 1: INTRODUCING THE PROJECT

1. INTRODUCTION

The Internet was conceived as a tool to be used in the interest of humankind, as a free open platform for the universal exchange of information and knowledge outside conventional geographical boundaries. If this target has been met, it must be acknowledged that the development of emerging technology has likewise expanded the dangers related to this space. Cyberspace is a virtual environment where power and influence are expressed, as well as cultural, political, military, and economic complexities. As such, it is constantly developing in the establishment of contemporary global affairs.

Today, the reliability, openness, and security of information and communication technology are critical to our everyday lives, social interactions, and economies. However, it appears that Lebanon, like all other countries, faces numerous cyber-threats (espionage, terrorism, or data fraud), thus weakening trust and security in cyberspace. In this context, the Lebanese state's primary duty is to provide Cyber Security resolutions to present and future challenges, as well as to establish an open and free Cyberspace that respects democracy while being secured, in order to provide security to people, and to all sectors. As a result of this observation, a National Committee to Establish a National Cyber Security System was established. The Strategy we propose here is the culmination of this intense collaborative work, and it is the cornerstone of our society's national security, which will definitely turn more digitalized, and thus must serve the common interest of all doers in Lebanon's society. This approach aims to control Lebanon's Cyberspace, to place the human element at the core of its obligations, to raise awareness about the importance of a national joint effort at home, and to achieve stronger international cooperation.

1.1. Research Problem

Content: *The problem statement is a brief discussion of a problem or observation succinctly identifying and documenting the need for and importance of the study.*

Start here…

1.2. Objectives of the Project

Content: *This part is a concise paragraph that describes the intent of the study. It specifically addresses the reason for conducting the study, and reflects the research questions and the building of the interview questionnaire.*

Start here…

CHAPTER 2: LITERATURE REVIEW

N.B. About the Theoretical Part: *Conduct a thorough literature search based on relevant key words. A literature review is discursive prose, not a list describing or summarizing one piece of literature after another. Organize the literature review into sections that present themes or identify trends, including relevant theory. Do not list all the material published, but rather synthesize and evaluate the relevant scholarly research according to the context of the Graduate Project. The literature review will contain a* ***main topic*** *and* ***related subtopics*** *that will be specific to the Project.*

1. MAIN TOPIC (State the main topic)

Content: *Present the theoretical or conceptual framework(s) related to the project. Present the literature related to the main topic of study. Include appropriate scholarly source citations for each assertion (See below for explanations about Quotations and Citations).*

N.B. *See below example of Outline Numbered Headings.*

ee below for explanations about Quotations and Citations, and relevant examples.

Start here …

2. SUBTOPIC 1 (State subtopic1)

Content: *Present the literature related to subtopics that are relevant to the main topic of study. Include appropriate scholarly source citations for each assertion.*

Start here …

3. SUBTOPIC 2 (State subtopic 2)

Start here …

Accomplishments

In 2006, the Cybercrime Bureau of the Judicial Police of the Internal Security Forces was established. It was assigned the dual role of investigating complaints, Cyber Security breaches, and technology-related crimes under the supervision of the Judicial Authorities, and of providing basic awareness to public and educational institutions on the latest Cyber Threats and Cyber Attacks.

Various security and intelligence agencies have performed extensively to enhance their investigative capabilities to block threats to national security, including cyber attacks and cyber espionage. The Lebanese prime minister established a national committee that includes representatives of the main government and security agencies. The main task of this national committee was to improve a national strategy for cybersecurity and striving cybercrime. Nine years following such a decision, the rapid growth and continuous evolution of the technology industry, Cyber Security approaches and best practices, and the proliferation of attack and defense techniques make this special and unique subject critical and more and more complicated to address.

It is necessary to give shape to the National Cyber Security Strategy in order to define the effective actions to be taken by the above-mentioned National Commission. From a practical and operational perspective, compared to the 2010 approach, the strategy now needs to focus on: making it a requirement that Cyber Security becomes a mandatory, legally binding, and enforceable target for Lebanon’s information system infrastructure ءat large; enhancing the Cyber Defense capabilities of our Country against the many different malicious Cyber Crimes and Cyber Attacks; and outlining the structure of a centralized body placed under the authority of the Presidency of the Council of Ministers, which will be responsible for implementing the components of this strategy.

The Lebanese Parliament approved Law No. 81 in 2018, “Electronic Bargains Law,” which includes a chapter on maintaining electronic evidence. Lebanon has also cooperated with other ICT-advanced countries and International Organizations in the field of Cyber Security. A digital transformation strategy on the State level is being developed under the supervision of OMSAR.

The Ministry of Telecommunications is playing a central role in the deployment of properly efficient infrastructure in a robust communion with private operators and OGERO and orderly handles Cyber Security matters with national stakeholders. It has established coordinating efforts with ITU (International Telecommunication Union) to improve the Cyber Security index in Lebanon.

Many Lebanese institutions, both public and private, have been subjected to and continue to be subjected to cyber-attacks that primarily target their websites and render them inoperable. Other attacks have resulted in the public disclosure and publication of some Lebanese residents' personal information.

Threats

Malicious cyber actions are intended to jeopardize the confidentiality, integrity, and availability of networks and systems. These actions share a few characteristics: they know no bounds, are difficult to trace and do not always necessitate large funds and/or highly technical expertise. Furthermore, different actors can knowingly or unknowingly install these risks, making a wide spectrum of hostile cyber actions even more difficult to detect, identify, and manage.

Based on who launches and how the attack is carried out, the primary threats can be classed. They could be “Cyber-dependent threat”, “Cyber-enabled threat”, “State-sponsored threat”, “Terrorist threats”, or “Insider threat”.

Cyber-dependent threat: Where Information Communication Technology devices can be used as both a tool for committing a crime and a primary target for the crime.

Cyber-enabled threat: When traditional crimes are committed using technology Cyber-enabled fraud, data theft, espionage, robbery, extortion, propaganda, or destruction are the major activities. These cyber-crimes can come from other countries and regions, as well as from within the country, and they all aim to steal money or data to use in other destructive activities.

State-sponsored threat: when foreign states or entities backed by foreign states try to hack into cyberspace, a public or private network, or sensitive data on cloud networks. The goal is to acquire a strategic, political, diplomatic, military, technological, commercial, and financial advantage. These efforts specifically target a country's essential national infrastructure, such as defense, finance, energy, health, utilities, and telecommunications assets.

Terrorist threat: where terrorist organizations make use of the Internet in order to perform the following:

Publicity/advertising and propaganda;

Recruiting and mobilization;

Fundraising;

Secure networking; encrypted/anonymous sharing of information;

Remote training;

Planning and coordination;

Claiming responsibility for attacks, thus showcasing their capabilities as an intimidation technique;

Using the Internet with continuously improved skills, by flooding the targets.

The threat from within: These threats possess a constant threat. malignant insiders commit these crimes and are tacitly "trusted" employees of a company who may have access to critical systems and data. By stealing sensitive data and intellectual property, these risks can cause financial damage to reputation. They can also pose a malicious cyber threat if they use privileged knowledge or access to facilitate or initiate an attack that disrupts essential services on their organization's network or wipes out data. Some insider threats may fall prey to social engineering and cause unintended harm. The continuous and rapid development of information and communication technologies, globalization, the massive increase in data volumes, and the increasing number of various devices and equipment connected to data networks have had a major impact on daily life, the economy, and the functioning of the state.

Accessing the Internet is increasing, the number of users continues to multiply, and new technological services and solutions such as the Internet of Things (IoT), Industrial Internet of Things (IIoT), and cloud services are mounting. All of those lead to a vaster threat range and an expansion in attack vectors that increase complication and damage upon hit.

Obstacles

The biggest Cyber Security concerns stem from the Lebanese governments', economy, and population's large and rising reliance on ICT infrastructure and e-services.

Cybercrime jeopardizes the economy's functioning and erodes trust in digital services. To ensure the prevention, detection, and punishment of Cyber C, qualified individuals and contemporary technology are required.

To prevent and repel future security risks, it is vital to continually expand cyber security expertise and invest in technology infrastructures and solutions.

One of the most complex obstacles is to develop a modern legislative framework and to improve the capabilities of law enforcement agencies in order to provide a brand new, definitive, and mixed legal and technical methodology with the main goal of clearly defining penal responsibilities all across the investigation phases while enforcing proactive steps to effectively combat cybercrimes. The main purpose of the new constitutional mechanism's technical features is to preserve digital evidence from both traditional and ICT-based crime scenes.

To boost the Lebanese economy and share security interests, it is critical to strengthen Lebanon's contacts with reliable partners and build new cooperative networks with other countries at the international level. Since dangers are global, the defense must be global as well, requiring close collaboration with worldwide professional bodies. Cyber risks are a puzzle that no country can singly handle. In compliance with Lebanese legal provisions, international cooperation is required.

All parties should be able to adapt their behaviors to the required security patterns in order to operate safely on the Internet, and the government should be able to raise Cyber Security standards across the country and enforce proper security measures to ensure that individuals, organizations, and businesses adapt their behaviors to the required security patterns.

From a practical standpoint, Cyber Crime and Cyber Attacks take advantage of technological advancements as well as a lack of a solid Cyber Security plan and its implementation. In specific, we can identify several difficulties that, if not effectively addressed, might pose a serious threat:

Inadequate skills, training, and awareness.

Hacking resources are readily available.

Unpatched and cracked systems and applications.

An ever-increasing number of areas and gadgets that are specifically targeted, since the Industrial Internet of Things was born out of the rapid installation of connectivity in key systems across a wide range of industries.

Who is responsible?

Government, Businesses and Organizations, and Individuals, as citizens, employees, and customers, are the most significant engaged parties in Cyber Security. In today's fast-paced digital world, Lebanon must make every effort to improve its position in terms of cyber security, which is a critical requirement for safeguarding and preserving our digital independence. The digital world is always evolving and growing. As a result, it is critical for Lebanon to be prepared to keep up with the rapidly expanding Cyber Attacks.

Stanchions of the National Cyber Security Strategy

In light of the aforementioned realities, Lebanon's current situation, and upcoming challenges, the government should involve all of its institutions in the development of a comprehensive strategy capable of achieving the task of implementing a more secure Cyber Space and increasing awareness among the main actors in Lebanese society.

From both a governmental and private perspective, the Lebanese government is cognizant of the new economy's heavy reliance on the Internet.

In this way, security exposure provides consistent levels of risk, which will always inspire and inspire efforts at cyber-attacks.

The road Lebanon must follow to complete each of the phases described and evaluated above is extremely difficult.

It will take a lot of work, from mustering the political will to drafting legislation, technological, and cyber security assets, all while relying on dedicated and highly specialized people resources.

The strategy will take at least two to four years to implement after the move to this completely new approach has been made. It's critical to emphasize that, while no one can claim to be able to entirely remove the risks that the National Cyber Security Strategy attempts to combat, it's critical to take all available precautions.

Lebanon must help businesses and citizens to grow while also taking advantage of the vast opportunities that digital technology provides.

A government-developed Cyber Security Strategy, which represents the entire country and has national implications and enhancements, must include clear targets and ongoing, long-term measures.

As Lebanon prepares to develop and implement a national cybersecurity strategy, it is critical to identify and list the major pillars on which such a strategy must be built.

The formulation of a Strategy and its operational implementation can only be envisioned and executed by explicitly identifying and prioritizing the foundational pillars.

Given the foregoing, the National Cyber Strategy will be founded on the following strategic, important, founding axes, referred to as Stanchions:

Protect against threats from both within and outside by defending, deterring, and reinforcing;

Strengthen international collaboration in the sphere of cyber security.

Continue to build State capacity to assist the growth of information and communication technologies;

Expand educational capacity on Lebanese soil;

Expand the industrial and technical capability

Promote the role of security and intelligence services and strengthen mutual cooperation and coordination with the support and supervision of higher authorities;

Promote cooperation between the public and private sectors;

Promote the role of security and intelligence services and strengthen cooperation and coordination with the support and supervision of higher authorities.

We can only begin to design a Cyber Security Strategy with defined objectives once the aforementioned Pillars have been identified and addressed.

Objectives

At the national level, a Cyber Security strategy must be established to implement a strategic defense plan against Cyber Threats for the public and private sectors, as well as individuals, while assuring its long-term viability by institutionalizing it through a clear structure and objectives. A Cyber Security Strategy must also include bold efforts to safeguard the Lebanese economy and residents' privacy. Overall, the National Strategy's major purpose is to lay out a series of decisions that must lead to operational activities that will make Lebanon confident, capable, and resilient in a fast-changing digital world.

The primary goals that must be met are:

Improve service availability and usability, increase transparency, stimulate citizen participation in governance, and reduce public and private sector cyber threats and cyber-attack costs by urging the government, organizations, corporations, and individuals to join this collaborative effort to secure the nation's cyberspace.

Adopt an acceptable and effective incident management notification and response strategy.

Observe security events and risks, allowing you to accurately assess current and future cyber threats.

To guarantee the integrity and resilience of networks, data, and systems, and to respond quickly and effectively to Cyber Threats in Cyber Space, utilizing the most appropriate capabilities.

Strengthen the country's defenses against the most frequent cyber-threats by putting in place appropriate measures and boosting cyber-attack response capabilities. To drastically improve ICT security standards on domestic networks, the government must actively support the development and implementation of active Cyber Defense measures, building on its own and the industry's capabilities.

Help and support institutions in the aftermath of security mishaps. In particular, the state must ensure that the government communicates effectively with the private sector, whether as a pre-emptive measure or in response to an occurrence. National event management criteria must comprehensively address disasters, allowing partners to learn from each other and share strategies.

Ensure that events are reported to the National Cyber Security Authority, particularly the NCISA, in a mandated and timely manner, so that the threat's magnitude, scope, and severity may be assessed.

Determine the source of intrusions on a national level to decrease the probability of multiple and recurrent assaults of diverse targets and sectors.

Create a database of cyber logs to allow for a broad and thorough investigation of Cyber Threat trends to identify security solutions and/or product and service needs. This would also benefit the cyber-insurance industry, which assesses risk based on statistical and historical data on cyber events.

Inspire hardware and software companies to create and sell devices that have security features by default.

Incorporate human values into cyberspace, fostering respect for human rights to ensure that people are empowered, have complete digital self-determination, and privacy.

Ensure that government bodies, organizations, businesses, and individuals have the knowledge and abilities to defend themselves and respond appropriately to safeguard themselves and their clients from the harm caused by cyber-attacks.

Orient the Lebanese community to excellent practices and start a large-scale campaign to create awareness among all Lebanese.

Maintain a consistent set of communications on Cyber Security guidelines from both the government and its allies to ensure a radical change in public behavior.

Understanding cyber dangers and the stages of cyber hygiene can help Lebanese society develop a cyber security culture.

Enlighten people about the dangers of online manipulation and propaganda strategies utilized by malevolent actors. The relevant defense and security services are in charge of detecting propaganda or Cyber Terrorism incidents and making suggestions to the government for countermeasures to be implemented. The establishment of an information platform to respond to acts of propaganda or destabilization is critical.

Enhance the security of critical infrastructure's most sensitive information systems, in both public and private operators, by enacting suitable and periodically updated legislative measures. This procedure will be gradually extended to public and private entities that handle or manage sensitive data systems.

Ascertain that the LEA has the best safeguards in place to keep their networks and platforms safe and secure. These stakeholders must be able to operate and maintain their freedom of action in the face of cyber threats and offer assistance in the case of a large-scale national cyber-attack.

Create a central authority at the highest level of defense: the NCISA, to prepare the legal and operational phases for institutionalization.

The Role of NCISA in the Lebanese Strategy

Lebanon, along with many other nations, requires a strong and sustainable national computer defense mechanism. To accomplish this objective, the National Cyber Security Committee has determined that the establishment of a national agency for information system security is a vital and important step in facilitating a coherent and assertive approach to handling Cyber Security issues, as well as tracking the growth and diversity of Cyber Threats and powerfully responding to their rapid advancement.

The establishment of a Lebanese agency appointed to the Prime Minister and affiliated to the General Secretariat of the Higher Council of Defense is a critical step in the Lebanese government's response to serious present and future cyber security issues.

The NCISA will carry out its authorization in close collaboration with the relevant ministries and LEA, without interfering with their legal and mandated responsibilities.

The NCISA will allow Lebanon to consolidate and coordinate decisions in the sphere of cyber security at the level of various governmental services, enhancing the country's resistance to digital attacks.

The NCISA's main responsibilities include establishing policies and procedures, developing plans, assessing vulnerabilities, identifying threats, raising awareness, alerting with recommendations, and responding quickly and effectively to cyber-attacks in order to keep the Lebanese cyber environment stable and flexible.It is part of the Higher Council of Defense's General Secretariat, which is in charge of Lebanon's information system and cyber security regulations.

The NCISA's primary function is that of a coordinator and facilitator, coordinating with all government agencies, related ministries, and other publicinstitutions, as well as encouraging collaboration between the public and private sectors, industry, and academia. The NCISA's mandate is to help and support all public and commercial sector stakeholders who are concerned about cyber security.

In terms of Cyber Security, the NCISA also provides technical assistance and creates rules that represent public and corporate interests and best practices.

NCISA will collaborate closely with involved authorities and organizations, the LEA, and the industrial sector to evaluate and exchange intelligence on the most recent threats, assist industries in defending against threats, minimize the effects of cyber attacks on Lebanese parties, and develop a national layout for dealing with emergency circumstances in Cyber security.

The NCISA provides comprehensive cyber threat assistance and suggestions to businesses and citizens:

Conduct steps to secure Lebanese citizens and computer information systems against recognized and developing risks by building a platform that enables various parties to alert NCISA of Cyber Threats they experience as part of its responsibilities with the general public.

Propose technical solutions and educational opportunities focused at defending and preserving the digital domain as preventative measure.These solutions will include national and international simulations that are open to all parties in order to strengthen Cyber Space readiness.

When new technologies are introduced in the digital transformation process, the NCISA analyzes and manages the risks of cyber attacks by tracking technical advancements in order to predict changes and suggest appropriate information system security enhancements.

Boosting and assisting the LEA in the battle against cyber terrorism and planned cyber-crime by enhancing the tools available through the following practices:

Tackling potentially hostile entities;

Hindering Cyber Terrorism;

Neutralizing extremist ideas and behavior related to Cyber Space on home territory.

PART II

THE PRACTICAL FRAMEWORK

CHAPTER 3: RESEARCH METHODOLOGY

1. DATA COLLECTION METHOD

Content:

1. Indicate the adopted research method (qualitative, quantitative, mixed),

2. Provide a description of the data collection tools used (interviews, surveys, observation, focus groups, or other),

3. Provide an overview of questions used, (number of question, open-ended, closed-ended) and how the questions relate to the main topic and subtopic reviewed in the literature Chapter 2,

P.S. Include the Questions / Questionnaire in Appendix A.

4. Provide a description of the participants, their names, background, and position and function in the organization.

P.S. Include completed and signed Interview Forms in Appendix B, either by attached the form, or pasting a scanned copy of it.

Start here …

2. STUDY LIMITATIONS

Content: *Describe the main limitations faced when collecting the data, including (but not limited to) lack of information about the company, confidentiality and secrecy issues, and cooperation of interviewees.*

Start here …

CHAPTER 4: FINDINGS AND RESULTS

1. DATA ANALYSIS METHOD

Content: *Describe the approach used to analyze the collected information* Start here

2. FACT FINDING RESULTS

Content: *Present the results in a logical fashion, answering the questions as stated in the interview questionnaire, and appropriate to the type of data and information collected.*

Start here …

PART III

PROJECT CONCLUSIONS AND RECOMMENDATIONS

CHAPTER 5: CONCLUSIONS & RECOMMENDATION

1. CONCLUSIONS

In Lebanon's National Cyber Security Strategy, there are a few fundamental, mission-critical, and strategic assumptions that must be highlighted:

- If the steps outlined in the Lebanon National Cyber Security Strategy are not implemented, the country will face the following dangers and risks:
    - Lebanon will remain one of the world's least developed countries, according to ITU global statistics and standings, as well as the Cyber Security Ranking, which evaluates a country's power to handle 21st-century threats.
- Entire Lebanon's state assets, markets, and commercial sectors, as well as its inhabitants, will be highly vulnerable to the cyber threat.
- Dealing with the ongoing global digital transition, in which Lebanon currently lags far behind, will result in economic losses, as well as dread, ambiguity, and worries.
- Lebanon will be unable to progress, resulting in a loss of global competitiveness.
- Everything mentioned above will sustain Lebanon's status as a "poorly developed" country.

2. RECOMMENDATIONS

Content: *Present all recommendations relevant to the conclusions.*

Start here …

REFERENCES

{There should be a Minimum 10 scholarly articles “references”, to a Maximum 25 scholarly articles “references”}

REFERENCE LIST

Students are to refer to the Harvard referencing manuals provided by their advisers.

{There should be a Minimum 30 scholarly articles “references”, to a Maximum 150 scholarly articles “references”}

APPENDIXES