LEBANON NATIONAL CYBER SECURITY STRATEGY

Towards year 2022

**"Lebanon wants to have a secure and stable cyberspace,
both within the national territory and in international exchanges."**

2019

الجمهورية اللبنانية
رئاسة مجلس الوزراء

Table of Contents

Message from the Prime Minister

In today's increasingly connected global world, we are witnessing exploding growth of the digital tool, a source of opportunities and prosperity, but also a potential threat to our security. Indeed, Cyber Attacks are increasingly frequent and sophisticated, which is a real challenge for our country: How to become resilient to the risks of Cyber Space while allowing users the freedom to use a safe and trustworthy space? But also, how to put that trust in place? Trust in the use of personal data and more particularly of sensitive data. Trust in the systems that produce, host, or distribute them. Ultimately, trust in all stakeholders, companies, partners, suppliers, public services, states, whose digital existence has a genuine impact on the lives of our fellow citizens.

There is no digital transformation without trust and there can be no trust without Cyber Security.

A Cyber Security strategy is therefore an obvious priority, especially that Lebanon is a signatory to the Paris Call[1] and remains committed of the need to secure its Cyber Space in the cooperation framework with all its international partners.

In the course of preparation of this Strategy, we placed special emphasis on implementing an open and interdepartmental process to involve stakeholders from many public sectors, namely the security services and the judicial branch. Thus, a National Committee was created by Resolution 173, under the direction of the General Secretariat of the High Council of Defense, and Resolution 172 allowing the appointment of a National Coordinator for Cyber Security, all under the authority of the Prime Minister. The Committee participated actively and intensively in workshops and conferences, in exploratory visits organized by the European Union delegation to Lebanon, to European expert missions. In addition, it implemented an academic collaboration with the Lebanese University and Saint-Joseph University, indicating that there is great interest in finding common solutions. I express my gratitude to all those who contributed to this process.

[1] On 12 November at the UNESCO Internet Governance Forum (IGF), President Emmanuel Macron launched the Paris Call for Trust and Security in Cyberspace. This high-level declaration in favour of the development of common principles for securing cyberspace has already received the backing of 552 official supporters: 66 States, 139 international and civil society organizations, and 347 entities of the private sector.

This work has provided certainty and showed us how it is done: The creation and institutionalization of an Agency at the national level, under the authority of the Presidency of the Council of Ministers and attached to the General Secretariat of the Higher Council of Defense, seems essential. The Agency will be the authority responsible for securing the information systems and fighting against Cyber Crime. It will also guarantee our protection against Cyber Attacks by implementing our strategy throughout the national territory and will contribute maintaining our digital sovereignty.

But this undertaking would be fruitless if we do not perform at the same time a significant effort to raise the awareness of our fellow citizens on the daily risks of the use of digital tools and if we do not encourage the professional training of the key actors. I think the sentence should stop here from a grammatical point of view. If you want to keep the same meaning then it has to be reformulated who will be in charge of protecting the nation in Cyber Space.

My project is ambitious: To guarantee a minimum of security for our fellow citizens and for the well-functioning of our democracy and to ensure that this strategy is collectively carried by all the stakeholders in Lebanon as part of an effort at the national and international levels.

Today it is necessary to develop a broad cooperation between public authorities, the private sector, and civil society. I therefore appeal to the whole nation for all the stakeholders to participate in this collective effort and for the implementation of this strategy to be effective and beneficial to the interests of our Country.

Saad Hariri

PRIME MINISTER

Preamble

At its creation, the Internet was intended as a tool to be put at the service of humanity within the framework of a freely accessible platform for the universal sharing of information and knowledge, outside the confines of traditional geographical boundaries. If this goal has been achieved, it must be recognized that the evolution in digital technologies has also increased the risks associated with this space. Cyber Space is indeed a virtual space for the expression of power and strength, for cultural, political, military, and economic tensions. As such, it is constantly evolving in the construction of current international relations.

Today, our daily lives, our social interactions, and our economies depend on the reliability, transparency, and security of information and communication technologies. However, it turns out that Lebanon, like all other States, faces many threats in Cyber Space (Cyber Crime, espionage, sabotage, blackmail or fraudulent or excessive use of personal data), which undermines trust and security in Cyber Space.

In this context, the primary responsibility of the Lebanese State is therefore to provide Cyber Security solutions to current and future challenges, and to create an open and free Cyber Space, respectful of democracy while it is protected, to bring security to the public sector, the private sector, and citizens. From this observation arose the necessity to create, in 2018, a National Committee with the objective to set up a National Cyber Security Strategy. The Strategy we present here is the result of this intensive collective work and is the cornerstone of the national security of our society, which will inevitably become ever more digitalized, and must therefore serve the common good of all actors in the Lebanese society.

It is a bold and ambitious approach that Lebanon has set for itself. The objectives of this approach are to regulate Lebanon's Cyber Space, to position the human element at the center of its responsibilities, to go through the awareness of building a national collective effort on home front, and to reach a stronger cooperation at the international level.

PART I.
LEBANON NATIONAL CYBER SECURITY STRATEGY

1. Lebanon strategic context

Lebanon stands in the midst of all the advancement in the technology that we are currently witnessing. By relying on modest and insecure digitization, Lebanon is exposed to disruption, which targets its security as well as the safety and privacy of its citizens.

The lack of a unified and clear Cyber Security strategy across different public sector bodies and private organizations makes it difficult to defend and prevent such attacks. **Considering the vulnerabilities, data breaches, and all the different attacks that some Lebanese entities suffered, especially during the year 2018, and for the ease with which attackers were able to gain access to different entities in the public and private sectors**, the need for Cyber Security in Lebanon is becoming an urgency along with the necessity to fight malicious cyber behavior and maintain a good standard of data security and system integrity.

Despite the timid attempts by some institutions and entities at securing their data and systems, the initiatives implemented in Lebanon were greatly insufficient to accomplish the desired goal. These efforts need to be integrated in a collaborative approach, following a well-defined strategy that better defends against attacks and counters Cyber Crime. The unorganized efforts of today, in the field of Cyber Security in Lebanon are not achieving the desired results. Below are some of the reasons that explain the current situation:

- **The absence of a unified National Cyber Security Strategy**: Every institution in both the private and public sectors has its own security vision and procedures, which might be efficient in their current situations but makes it more difficult to collaborate without well-defined criteria, KPIs, and, most importantly, information sharing and a common framework at the highest level.
- **The absence of laws and regulations that govern cybercrimes**: Lebanon lacks laws and regulations that protect government institutions, private companies, and cyber rights of individuals. It also has no clear definitions for criminal acts and the consequences and implications of these criminal acts lack clarity.
- **The absence of a National Cyber Security Agency**: Lebanon does not have a Cyber Security Agency that implements and enforces Cyber Laws; employs/utilizes people with the required level of expertise to assist organizations set up their security frameworks; offers trainings; supports research and development; and guarantees the continuity of Cyber Security awareness programs.

- **The struggle between corruption and the digital economy**: In 2018, Lebanon maintained its ranking within the upper range of corrupt nations, a situation held since the early 1990s and that can be attributed to the consequences of the sectarian war. An entire generation grew up living in a society that lacked structure and order. Instead of restoring the traditional, pre-war Lebanese culture built on integrity, respect, and competence, this generation came out of this war rationalizing its need to satiate its hunger in compensation for years of deprivation.

  Corruption and the digital economy are diametrically opposed since corruption is the major threat against the implementation of Cyber Security, while the digital economy can potentially destroy or at best disrupt corruption patterns.

  Corrupt agents could become implicated in active or passive, direct or indirect, and internal or external cyber-attacks intended to disable the services provided through the digital infrastructure of the national digital economy. Their aim could be to allege the inefficiency of the digital services provided in order to fall back on the previous manual operations, under which corruption schemes could not be tracked.

- **The multi-faceted socio-demographic context**: The Lebanese Constitution is based on a democracy that preserves the equity of rights amongst its multiple religious communities. Multiplicity is a unique and distinctive component of the nation which may be used to destabilize every single area of the public and civic life. As a consequence, cooperation, sharing of means, and the use of appropriate qualifications can be hampered if the multiple entities that make up the Lebanese society veer towards isolationism and individualism, which would in turn drain the nation from the necessary skills required for well-functioning institutions and affect the overall resilience built on collaboration across agencies.

  To avoid this end, individuals appointed to positions of responsibility should possess expertise or be required to obtain a certification in the related business area. This directive reflects mandatory Cyber Security requirements.

  Cyber-Attacks are similar to a virus infecting an organ of a living body. If left untreated or treated inadequately, it will endanger the entire body, and could spread to other individuals, to contaminate and potentially decimate an entire population.

  To eradicate the spread of such a potential threat to the entire nation, action should be coordinated through involving all relevant stakeholders, using a wide range of enforcement tools and reliable expertise.

  In summary, the state must ensure that people appointed for the implementation of the Cyber Security Strategy shall be competent, reliable, experienced,

responsible for upholding the common interest and promoting the common good, and motivated by a powerful sense of patriotism.

- **The lack of collaboration mandates between administrations at the national level**: Every institution is working on its security separately without a clear framework of collaboration with other institutions. Institutions would benefit from sharing and exchanging information and data. In addition, there is a lack of collaboration and cooperation across the different departments of the same institution, especially in the field of security. Each department and unit act and work independently rather than cooperating to secure the overall organization/institution.

- **The lack of active participation of the private sector in the advancement of the public sector**: The public sector lacks a regulatory role and awareness-building system and relies on the private sector to cover the shortage in experience and development capacity of its IT departments and positions, and to secure and provide IT-related and Cyber Security services. It is important for the public sector to outsource such services. However, the Lebanese public sector came out weaker from such collaboration with the private sector. Records show that the private sector did not successfully or adequately manage handing over these IT projects to the public sector and it did not benefit as it should have from the completion of such projects. This should be addressed in any future partnerships with the private sector and/or international cooperation in order to ensure constructive outcomes.

- **The absence of an initiative for a National Information System and Digital Transformation Strategy at the highest level**: Despite all the efforts exerted independently or through OMSAR in e-government and automation projects since 1995 in various ministries, Lebanon continues to fall short on developing a nation-wide vision with a cooperative inter-institutional approach. There is an evident and serious imbalance between institutions and ICT coordination is not institutionalized at the highest level, which makes detecting, identifying, and managing Cyber Security-related incidents very difficult. Within such an environment, the effective use of Cyber Security and Cyber Defense to protect citizens, and public or private organizations targeted by Cyber Attacks becomes seriously compromised.

- **The shortage of Cyber Security experts and the difficulty to adapt to rapid changes**: Administrative bodies, companies, and universities in Lebanon are in desperate need of developing awareness and creating a well-structured and balanced Cyber Security atmosphere by targeting educational and training programs at all levels (universities, jobs, conferences, etc.), to be ready to respond to the rapid development in the nature of Cyber Crimes and the methods used.

Unfortunately, Cyber Security trainings are limited to some areas in educational organizations, communities, or in some universities or other educational programs. Students tend to rely on self-education in this field rather than seek formal education and training programs that would provide them with the necessary tools to feed all the sectors that require such talent in Lebanon's exposed industries.

Lebanon and its institutions are exposed to threats and Cyber Crimes like any other country. Cyber Security in Lebanon is not properly structured at the nation-wide level and lacks the cooperation and coordination between organizations in the public and private sectors and at the international level to secure its citizens' basic needs for safety and privacy.

Today, many Lebanese institutions provide online services to various clients, who thus become dependent on the Internet. However, Internet use is not secure, and users will always be exposed to attempts of Cyber Attacks. Although this risk cannot be eliminated completely, it can be significantly reduced by restricting the attack surface and mitigating the spread of attacks to a level that would allow society to continue to prosper and benefit from the huge opportunities that the digital technology offers.

1.1 What has been achieved

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.

Other Security and Intelligence Services have worked extensively to strengthen their investigative capabilities in order to prevent threats to national security, including Cyber Attacks and Cyber Espionage.

In 2010, the Lebanese Prime Minister established a National Commission, comprising representatives of major governmental and security agencies. The main function of this National Committee was to develop a national strategy for Cyber Security and fight against Cyber Crimes. 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 the Lebanon's information system infrastructure at 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.

In 2018, the Lebanese Parliament ratified Law number 81, "Law of electronic transactions", which contains a chapter on the preservation of electronic evidence.

Some universities in Lebanon have restructured their curricula and opened Master's degree programs in Cyber Security and digital forensics.

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.

In 2018 and 2019, under the framework of the CyberSouth project which was organized by the Council of Europe, the Ministry of Justice trained around 20 judges on how to face Cyber Criminality. Though it is in the right direction, this effort is not sufficient and the Ministry of Justice needs to address the subject on the highest level.

The Ministry of Telecommunications is playing a major role in the deployment of a decently effective infrastructure in an intensive collaboration with private operators and OGERO, and regularly addresses Cyber Security issues with national stakeholders. It has established coordinating efforts with ITU (International Telecommunication Union) to improve the Cyber Security index in Lebanon.

Banque du Liban (BDL) has developed and implemented, in a continuous improvement approach, a mature, standard-based, advanced and innovative Cyber Security Program that permits BDL to anticipate and defeat Cyber Attacks. This program is composed of two main pillars, and follows continuously the latest Worldwide IT Security Best Practices and Standards:

- The Security Governance & Compliance Part: the first pillar contains the Definition & Update of BDL IT Security Roadmap, elaboration and follow-up of IT Security Policies, proactive risk assessment & management, and the launching and evaluation of the Security Awareness program.
- The Defense-in-Depth Security Approach: is composed of multi-layered, multi-technology security solutions, covering the Network & Endpoint Security

Infrastructure, the Application Security Intelligence, and the Advanced & Intelligent Security Operations.

Many Lebanese organizations, both in the public and private sectors, have witnessed and still face, at an alarmingly growing rate, Cyber Attacks that mainly target their websites and putting them out of service. Other types of attacks have resulted in the public disclose and release of some personal records of Lebanese citizens.

1.2 Threats

Malicious cyber activities are designed to compromise the confidentiality, the integrity, and the availability of Networks, IT Systems, and Information.

Malicious cyber activities have some common characteristics: they have no boundaries; they cannot be easily attributed; and they do not necessarily require huge budgets and/or high technical skills. Moreover, different actors can put in place these threats, knowingly or unknowingly, making the range of malicious cyber activities even more difficult to detect, identify, and manage.

The main threats can be classified as follows, based on who launches and how the attack is carried out:

- **Cyber-dependent crimes**, where ICT devices can constitute both the main tool for committing the crime and the main target of the crime itself. The most relevant examples are developing and propagating malware for financial gain; hacking to steal sensitive data; DDoS; ransomware and blackmailing; or damaging, altering, or destroying data. Money is generally the main goal of such threats.

- **Cyber-enabled crimes**, where computers are used to commit traditional crimes. The main activities are Cyber-enabled fraud, data theft, espionage, robberies, extortion, propaganda, or destruction.

  These Cyber Crimes can emanate from other countries and regions but also from inside the country and generally seek to obtain money or data for use in other malicious actions.

- **States and State-sponsored threats**, where foreign States or entities sponsored by foreign States attempt to penetrate the Cyber Space, a public or a private network, or sensitive files on Cloud networks. The purpose is to gain political, diplomatic, military, technological, commercial, financial, and strategic advantage. In particular, these activities target critical national infrastructures of a country, such as defense, finance, energy, health, utilities, and telecommunications assets.

  Main activities include developing Cyber Espionage and destruction operations capabilities rather than using off-the-shelf techniques.

- **Terrorists threats**, 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.

  Terrorist groups continue to aspire to conduct damaging Cyber activities against Lebanon.

- **Hacktivist threats**, where activities mainly have a disruptive and criminal purpose to their victims. Such actors use the Internet with the same purposes as terrorist organizations.

- **Insider threats**, where these constitute a continuous risk. They are committed by malicious insiders, who are implicitly "trusted" employees of an organization and who may have access to critical systems and data. These threats can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive Cyber Threat if they use privileged knowledge or access to facilitate or launch an attack to disrupt critical services on the network of their organization or wipe out data from the network.

  Some insider threats can be victims of social engineering and thus cause unintentional damage.

- **Script kiddies**, where inexperienced actors use scripts or tools developed by others – and/or downloaded from the Internet – to conduct Cyber Attacks. They generally have access to hacking guides, resources and tools available on the internet and downloadable from public open sources.

- **Computer network attack**, where hostile actors can use malicious software (or malware) to disrupt and damage cyber infrastructure. This can range from taking a website offline to manipulating industrial process command and control systems.

1.3 Trend of threats

The continuous and rapid development of information and communication technologies, globalization, the tremendous increase in data volumes, and the growing number of

various devices and equipment connected to data networks have made a great impact on daily life, on the economy, and on the functioning of the State. In addition, the Internet is becoming increasingly accessible, the number of users continues to grow, and new technological services and solutions such as Internet of Things (IoT), Industrial Internet of Things (IIoT) and cloud services are on the rise. All the above result in a wider threat landscape and in a growth of attack vectors that have increased complexity, sophistication, and damages when successful.

The number of State Actors involved in Cyber Space and engaged in Cyber Espionage activities targeting computers connected to the Internet as well as closed networks continues to grow. This reality is due to the fact that collecting information on national security as well as economic assets represents an important resource in the regional and international arena. The number and activeness of Nations capable to perform State-sponsored Cyber Attacks are increasing, posing unknown and unexpected critical threats and risks to Lebanon.

In addition to the activeness of State actors, politically-motivated individuals and groups with limited financial means have a growing ability to organize their activities using social networks and carry out Denial of Service and other types of attacks.

Moreover, the recent but fast-growing diffusion and implementation of encryption standards by governmental institutions and private companies – such as the SSL or the SSH protocols, just to mention a couple – revealed an unexpected side effect: They rendered real-time detection, post-incident analysis, defense, and investigation much more complex. Under some specific circumstances and ICT architectures, such as very large and complex data centers, it is becoming nearly impossible to perform real-time detection successfully.

Nowadays, such scenarios are allowing different Threat Actors massively to exfiltrate sensitive and critical information using the very same encryption protocols that the victims use to enhance their Cyber Security.

Very often this causes previously used detection and data protection solutions, such as DLP (Data Leakage Prevention), to fail in their core scope, usually greatly broadening the so-called "attack window" and resulting in increased and long-lasting data breaches, instead of the previously totally undetected, shorter breaches. The rapid evolution in the profile and capabilities of attackers makes tracing and attributing the attack drastically more complex.

1.4 Challenges

The main Cyber Security risks arise from the extensive and growing dependence on ICT infrastructure and e-services by the Lebanese State, economy, and population.

Cyber Crime undermines the functioning of the economic space and reduces trust in digital services. Therefore, competent personnel and modern technical tools are needed in order to ensure prevention, detection, and prosecution of Cyber Crime. Operational information exchange among countries is becoming increasingly important in the fight against Cyber Crime.

In order to prevent and deter future security threats, it is necessary to constantly develop know-how related to Cyber Security and to invest in technological infrastructures and solutions.

One of the main challenges is to develop a **modern legal framework and to strengthen the means of the LEA** (Law Enforcement Agencies: Army, Internal Security Forces, General Security and State Security) in order to provide a brand new, complete, and mixed legal and technical approach, with the main goal of allowing to clearly target penal responsibilities throughout the investigation phases, while implementing actions and measures to counter Cyber Crimes efficiently.

This new legal framework shall include both high-level and low-level processes, the most important of which are the application of Digital Forensics science by default and the mandatory compliance with the "chain of custody" best practices and logical concept within all the possible types of digital evidence. The above shall then be used in all the different possible crime scenes and scenarios, such as Host Forensics, Mainframe Forensics, Network Forensics, GPS Forensics, Cloud Forensics, Mobile Forensics, Drone Forensics, Industrial Automation Forensics, Audio & Video Forensics, and IoT Forensics. The overall goal of the technical aspects of the new legal framework is always to preserve the digital evidence from regular and ICT based crime scenes.

At the national level, it is possible to use the capabilities and know-how of the Banking Sector in terms of Cyber Security and Cyber Defense measures. At the international level, it is mandatory to strengthen Lebanon's relations with trusted partners and develop new cooperative networks with other countries in order to improve the Lebanese economy and share security interests. Since threats are global, the defense must also be global, via strong cooperation with international professional bodies. No country is able to deal with Cyber Threats on its own. International cooperation is mandatory in accordance with Lebanese legal provisions.

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 in order to operate safely on the Internet.

From a technical perspective, Cyber Crime and Cyber Attacks exploit the evolution of technology and the lack of a proper Cyber Security strategy and its factual implementation. In particular, we can identify five main challenges that could represent a concrete threat if not properly managed:

- An expanding range of targeted devices

  The Internet of Things (IoT) and Industrial Internet of Things (IIoT) create new opportunities for exploitation and increase the potential impact of attacks, which can cause both ICT and physical damage, and even death. The rapid implementation of connectivity in Industrial Control Processes in critical systems across a wide range of industries, such as energy, mining, agriculture, and aviation, has created the Industrial Internet of Things. This process allows devices and industrial and non-industrial operations, which were never vulnerable to such interferences in the past, to be hacked and tampered with, leading to potentially disastrous consequences.

- Poor Cyber Hygiene and Compliance

  These two elements depend on and can be addressed through the adequate technical solutions and implementations. However, they also heavily rely on cultural awareness. In fact, without a proper understanding of the importance of the concept of Cyber Hygiene, neither defense solutions nor compliance with existing or upcoming Cyber Security standards would be sufficient.

  If not enough awareness is raised, maintained, and nourished at the widest national level, across all the public and private institutions of the country, and amongst individual citizens, the country and all its infrastructures will never be safe from threats. The below list of facts and scenarios gives an idea of possible risks and their consequences if the Government, across all its institutions, the public and private institutions, at large, do not take full awareness of the seriousness of the threats:

  - 99% of Exploit-Based Attacks will still not be based on 0-Day Vulnerabilities. This means that, for example, if citizens do not understand the importance of very simple, basic security actions, such as "Windows Update" and if they do not apply them properly and regularly, their computers will always be prone to mass-attacks that will exploit known and public vulnerabilities;
  - Home Networks in Work-From-Home scenarios will expose Enterprises to BYOD-like Security Risks. The employee working from home must understand the importance of simple best practices, such as changing the default password on his/her home router, rather than always using VPNs in order to remotely connect to his/her office;
  - Sextortion Cases will rise dramatically;
  - The skills gap will widen and fewer trained experts will be available to fill security roles. Such lack in human resources will result in improper/poor testing, auditing, and certifying Cyber Security compliances in different environments and under different scenarios.

- Insufficient training and skills

  The gap in Cyber skills is a national vulnerability that needs to be resolved. There is a lack in the following:

  - Skills and knowledge to meet Cyber Security across both the public and private sectors;
  - Awareness building and formal training in Cyber Security for all public employees, who deal, in any form, with IT systems;
  - Hands-on training and simulations on the actual implementation of Cyber Security defense measures and techniques.

- Legacy and unpatched systems

  - Using vulnerable legacy systems with no updated versions means having unpatched systems that make entire networks vulnerable to attacks leading to massive data breaches, allowing the attackers to steal thousands, if not millions, of personal and business data;
  - Using unsupported software for which updates and patching no longer exist leads to an increased level of vulnerability that might be used by attackers to succeed in their criminal operations.

- Availability of hacking resources

  - Widely available free hacking information and hacking tools on the Internet give hackers access to knowledge and know-how that can be used for criminal purposes. This is something that cannot be combated, since the Internet itself is intrinsically designed for sharing information of any kind, both legal and not.
  - The availability of such information and hacking resources cannot be considered a crime (thus not allowing the blacklisting of such data), because most of the time, such know-how, tools, and how-to guides are (or claim to be) meant to foster knowledge about Cyber Security and security testing, even though in some cases they may be used as attacking know-how.

The only solution to countering all the above Cyber Threats and Cyber Attacks is the creation of a nation-wide system that can orchestrate a coordinated response, within a unified legal and technical framework.

2. The State responsible for Cyber Security

Securing the national Cyber Space will require a collective and multidimensional (human and technical) effort, which means engaging all the actors of the Lebanese society. In Cyber Security, the most important involved actors are:

- Government;
- Businesses and Organizations;
- Individuals, as citizens, employees, and consumers.

In a fast-moving digital world, Lebanon must exert all its efforts in an attempt to reach a better position in terms of Cyber Security, which is a key condition to the safeguard and preservation of our digital sovereignty. The digital world is in constant change, evolution, growth, and mutation. It is therefore of paramount importance for Lebanon to position itself at the highest best-practice level. Lebanon must also be aware, and ready, to keep up – and hopefully at one point in the future – to stay ahead of the fast-evolving Cyber Threats. Lebanon cannot be vulnerable to Cyber Attacks. Cyber Security is thus a key perimeter in preserving the country's sovereignty.

2.1 Government

The Government's main duty is to defend the country from attacks by other States and non-state actors, to protect citizens and the economy from harm, and to define the national and international framework necessary to protect the national interests, fundamental rights, and bring criminals to court.

As an important data holder and service provider, the State is taking strict measures to protect its information assets. It also has a major responsibility to advise and inform citizens and organizations about what they need to do in order to protect themselves online and, where appropriate, set the standards expected from key businesses and organizations. The key sectors of the Lebanese economy fall within the realm of the private sector, the strongest among them being the banking sector. However, when it comes to Cyber Security and countering Cyber Crimes, the ultimate responsibility to ensure resilience and the maintenance of essential services and functions falls to the state, in a well-managed and well-balanced collaboration with LEA, the Ministry of Telecommunications, the regulatory bodies of the banking sector, and all other governmental institutions, each within its jurisdiction, as well as other national and international partners.

2.2 Businesses and organizations

Public and private sector organizations and other institutions own personal data, provide services, and operate systems in the digital domain. The connectivity of information systems containing data and services has revolutionized their operations. However, with this technological transformation, one of their key responsibilities is to protect the assets they hold, to maintain the services they provide, and to incorporate the appropriate level of security into the products they sell.

Citizens, consumers, and society in general rely on businesses and organizations to take all reasonable measures to protect their personal data and strengthen the resilience of their systems and services. Businesses and organizations must understand that they operate in an environment that will hold them responsible for the consequences and indirect impacts of Cyber Attacks, to which they fall victim.

2.3 Individuals as citizens, employees and consumers

Today, the national and international contexts require that valuable assets are secure, not only in the physical world but also in the digital, virtual world. Since, in the virtual world, everything is connected and interdependent, it is crucial that everyone assumes his/her responsibility to take all reasonable steps to protect the hardware – smart phones, tablets, laptops – as well as the data, software, and systems that stand behind the freedom, flexibility, and convenience everyone enjoys in their private and business lives.

3. Pillars of the National Cyber Security Strategy

Considering the realities raised above, the current situation of Lebanon, and the upcoming challenges, the Government should engage all its institutions in the implementation of a comprehensive strategy capable of accomplishing the mission of providing a more secure Cyber Space and an increasing level of awareness among the main actors of the Lebanese society.

The Lebanese Government is aware of the extreme dependence of the new economy on the Internet, both from public and private perspectives. In this sense, security exposure creates consistent levels of risk and will always motivate and provoke Cyber Attack attempts.

The path Lebanon must take in order to accomplish each of the steps identified and analyzed above is quite challenging. It will require much effort, starting with mustering the political will to creating the legislation, technological, and Cyber Security assets, with the help of and reliance on dedicated and highly specialized human resources.

Once the shift to this totally new approach is put in motion, the strategy will require at least two to four full years to be implemented. **It is very important to state that, without claiming to be able to completely eliminate the threats that the National Cyber Security Strategy aims to counteract, it is of utmost importance to take all possible measures to reduce risks and to reach an acceptable level of security.** Lebanon must allow companies and citizens to continue to prosper and to take advantage of the enormous opportunities that digital technology offers.

A Cyber Security Strategy developed by a Government, thus representing a whole country, with nationwide impacts and enhancements, must foresee clear objectives and continuous, long-term actions.

As Lebanon readies itself to create and launch a National Cyber Security Strategy, it is crucial to identify and itemize the key pillars, upon which a prospective Strategy must rely on. It is only by clearly identifying and prioritizing these foundational pillars that the development of a Strategy and its operational implementation can consequently be envisioned and achieved.

Given the above, the National Cyber Strategy shall be based on the following strategic, key, founding axes, which shall be referred to as Pillars:

1. **Defend, deter, and reinforce against threats from inside and outside;**
2. **Develop international cooperation in the field of Cyber Security;**

3. **Continuously grow State capacities to support the development of information and communication technologies;**
4. **Promote educational capacity on the Lebanese territory;**
5. **Promote industrial and technical capacity;**
6. **Support the export and internationalization of Cyber Security companies;**
7. **Strengthen collaboration between the public and the private sectors;**
8. **Promote the role of security and intelligence services and strengthen the mutual cooperation and coordination with the support and supervision of the higher authorities.**

It is only once the above Pillars are recognized and addressed that we can begin to develop a Cyber Security Strategy with clear objectives.

3.1 Defend, deter, and reinforce against threats

The Lebanese State shall put in place a deterrence strategy in order to significantly reduce the number of Cyber Crimes. A deterrence strategy in Cyber Space refers to a set of actions designed to stop and identify attackers as they make their first malicious operations on the network, taking as a premise that after gaining access to a network, attackers always follow a predictable Cyber Kill Chain.

The Cyber Kill Chain is distributed across eight phases: reconnaissance, intrusion, exploitation, privilege escalation, lateral movement, obfuscation, denial of service, and exfiltration.

During the reconnaissance phase, the hacker will discover passively the Network in order to gather all the necessary information. It is absolutely vital to put in action proper deterrence technologies and tools in order to redirect the actions of the attackers in a controlled path, which will be easily handled by defenders.

The intrusion phase is then launched based on the information discovered in the reconnaissance phase. The objective is to enter the system and gain access to the data it contains.

The exploitation phase employs an active attack, where the hacker uses different types of vulnerabilities identified on the target victims in order to quickly exploit them, gaining remote or local access – as regular users or administrators.

Attackers then use privilege escalation technique to get increased access to resources.

The lateral movement phase aims to allow unauthorized access to internal servers and the data they store and manage. Sometimes such access can also enable attackers in

extending offensive actions towards external third parties, i.e. digital assets that are physically or logically located out of the victim's network perimeter.

Following this stage, obfuscation is being used to mask the activity and evade any forensic analysis.

The Denial of Service Phase then stops the attack from being tracked or blocked by disrupting the normal activity of the users and servers.

The last phase, exfiltration, represents the real and most important goal of the attackers, especially when dealing with the most experienced and skilled among them. It aims to remotely transfer different information and data through different exfiltration techniques, which could range from simple to very complex, and often using dedicated network infrastructures.

Once Lebanon has complied with basic Cyber Security standards and has applied this Strategy, the Government and the **National Cyber Security Information System Agency** (**NCISA)** shall be able to assess vulnerabilities; to alert with recommendations on preventative measures against the main consequences; to identify threats; to respond promptly and efficiently to attacks; and to maintain the Lebanese cyber environment secure. Several tools and technologies can be used in order to create a functional cyber deterrence framework. Before implementing them, however, it is mandatory to develop defense-specific technical and judicial capabilities.

A commonly agreed upon definition of deterrence in Cyber Space involves two elements: defense capabilities (deterrence by denial) and offensive capabilities (deterrence by punishment). Defensive capabilities are here understood to be Cyber Defense, i.e. the protection of a State's essential Information Systems (IS) and their ability to withstand constant and varied attacks. On the other hand, under an ongoing attack, deterrence is achieved by initiating the appropriate actions leading to stop the attack and to pursue the offenders.

Another component of deterrence is *Cyber Dissuasion* which involves the threat of retaliating with intolerable consequences in Cyber Space, designed to convince an opponent not to attack in the first place. It is about putting enough force on display for the purpose of eliminating the need of using it.

Developing defensive capabilities must follow the below course of actions:

- Create an active Lebanese Cyber Defense Model, which must include best practices and incorporate low-level and high-level technical actions, such as blocks, filters, white and black lists, etc., against phishing attacks, malicious domains and related command & control takedowns, malware-based attacks, 0-day based attacks and exploitation frameworks, email spoofing, IP reputation services, etc.

- Use proven and well-known security information feeds to compile the necessary information to build a reputation database of resources in Cyber Space, allowing for better control and filtering of malicious and dangerous content and threats. Using international Cyber Security standards and best practices will allow the Lebanese Cyber Security model not only to be complete, but also to benefit from the existing vast expertise of international standards bodies.
- Classify data and define critical infrastructures, thus setting the foundations to build a more secure National internet environment, from the perspective of proactive defense. This should go along with protecting Government institutions and other priority sectors, taking into consideration the latest Cyber Security standards and Cyber Security best practices, such as, but not limited to: upgrading to the latest software versions; applying patching to customers; and scanning for known vulnerabilities.
- Change public and business behavior, ensuring that individual organizations, regardless of their size, are taking the proper steps to protect themselves.
- Manage incidents and the understanding of threats from an operational, national security, geopolitical, and technical perspectives that will allow better control of security risks by combining reactivity and proactivity, in order to reduce the cyber risk exposure window. In parallel, design, build, and run innovative multi-layered security solutions, permitting to anticipate advanced attacks.
- Make Lebanese computer systems a harder target for Cyber Criminals, reducing benefits to hackers (deterrence by prohibition) and increasing costs (deterrence by reprisal). It is therefore necessary to be able to identify the interests and objectives of the potential aggressor but also to have sufficiently credible and persuasive capacities.
- Ensure that the State's national capabilities and intention to react are clearly understood in order to influence (discourage) the decision-making of potential attackers.
- Eliminate easy-to-use opportunities for attackers, who want to compromise Lebanese networks and IT systems. The Government shall have the necessary tools and capabilities to carry out the following: deny the attackers' easy opportunities to compromise the Lebanese networks and systems; understand the intentions and abilities of attackers; overcome large-scale basic malware threats; and respond and protect the nation in Cyber Space.
- Prevent people from being attracted to or get involved in Cyber Crime by reinforcing early intervention measures.

- Establish a systemized and inculcated action plan that can prepare advanced options for reacting to a Cyber Attack so that Authorities can respond to a crisis while it occurs. Response to Cyber Threats and Cyber Attacks must become an automatic action doctrine. This doctrine shall be based on Lebanon's interpretation of the application of existing international law in Cyber Space. In fact, Lebanon cannot decide to react autonomously to a Cyber Attack without considering and respecting existing international laws and regulations.
- Incorporate international legal standards to the national classification system of Cyber Attacks. Integrating national and international principles related to Cyber Security is an essential element of an action doctrine, that also represent an important support tool for the authorities in order to take more effective decisions and act as a relevant means of supporting international cooperation.
- Strengthen law enforcement capacity and expertise at the national, regional, and local levels to identify and deter Cyber Criminals in Lebanon and abroad.
- Improve the capabilities of digital sovereignty and using data centers physically on the national territory. The prospect of digital sovereignty over data must lead to the establishment of legal and technical solutions. Moreover, mastering key technologies is essential to the exercise of our digital sovereignty. Key technologies include, but are not limited to the encryption of communications and the detection of Cyber Attacks and professional mobile radios.
- Adopt a certification framework for high-level security products. The current certification framework is poorly suited to the evaluation of commonly used products, such as connected objects, for which costs and time are prohibitive. For this reason, it is recommended to introduce a basic Cyber Security certification on products, in addition to the existing certification framework. The latter could build on existing systems in contexts other than Cyber Security, such as the CE marking required for the marketing of certain goods and services within Europe. This basic Cyber Security certification shall involve compliance and analysis on Cyber Security best practices, based on predefined specifications. It shall be placed under the control of a private body, with public authorities' participation limited to indirect actions, such as NCISA-approved assessment entities of Cyber Security accreditation.
- Strengthen the fight against Cyber Crime through the advanced criminal tools detection; by increasing the skills and number of people working in the field and improving specification; training different stakeholders, such as judges, public prosecutors, as well as bank employees, etc.; legal assistance to victims of Cyber Crime; disincentives against abusers and offenders; regular Cyber Security training to law enforcement authorities; and finally, regular updating of laws and

procedures in line with the development of Information and Communication Technologies.

Under specific circumstances, while acting under an on-going attack, strategy might shift from a defense-only operational mindset to an offensive one. On such occasions, the following actions should be taken:

- Prosecute Cyber Crime offenders. The Government – through the legal authorities, LEAs, and the NCISA – must dissuade those who would harm the interests of the Nation. To achieve this, efforts must continually be made to make it clear that any cyber attempt on the Nation, whether to rob or harm, is neither easy nor cheap. Attackers must know that they cannot act with impunity. The Government – through the legal authorities, LEAs, and the activity of the NCISA – should be able to identify attackers and act against them, using the most appropriate action among a set of available tools. Law Enforcement Agencies shall focus on criminals who persist in attacking Lebanese citizens and businesses. National authorities should cooperate with international partners to target criminals wherever they are and to dismantle their infrastructure and facilitation networks. LEAs shall also continue to contribute to awareness building and standardization in Cyber Security issues, in close collaboration with the NCISA.
- Strengthen the effectiveness of the judicial action to improve the fight against Cyber Crime thus being able to identify, if and when needed, the actors behind a Cyber Attack. In order to be able to accomplish such a complex goal, it is mandatory to have the legal means, along with the technical capabilities, expertise, dedicated infrastructures, and ad-hoc tools.
- Strengthen the effectiveness of Law Enforcement Agencies correctly to perform "Attribution to a Cyber Attack." Authorizations to deploy such a set of actions should be prudently released to specific government institutions according to the nature of action.
- Develop an international network of collaboration between judges and investigators, as well as introduce dedicated trainings and educational programs at existing national and international entities located on the Lebanese territory.

3.2 Develop international cooperation in Cyber Security

To reinforce the positive effects of the implementation of the National Cyber Security Strategy, it is mandatory that Lebanon works closely with other regional and international actors. In particular, the following actions are highly recommended:

- Work with international partners, such as INTERPOL, UN organizations (ITU, UNODC, UNICRI, etc.), European Delegation in Lebanon and European institutions and agencies (Council of Europe, EUROPOL, CEPOL, ENISA, etc.),

as well as other international Standard Institutes for Framework (NIST, EBIOS, etc.), and international and regional CERTS.

- Use existing networks and relationships with the Government's key international partners and build new links with other international entities to share information about current and nascent threats, adding value to existing thought and expertise.
- Establish strategic bilateral relations and open dialogue channels with key stakeholders to share information about potential incidents.
- Build international partnerships to end the perceived impunity of Cyber Criminals acting against Lebanon by bringing criminals in overseas jurisdictions to justice.
- Cooperate with the international community on Cyber Space issues to harmonize and increase the efficiency of a shared body of laws and regulations. This shall allow the Government of Lebanon to optimize timing, procedures, and costs, thus establishing or adapting to common mechanisms for crisis management, communication, and de-escalation. Lebanon must continue to work for the universalization of certain standards applied in Cyber Space with a view to enhancing its security. This approach should be based on three principles:
  - *Prevention*: the inherent uncertainty of the attribution of an attack should encourage the States to concentrate their efforts on preventive measures;
  - *Cooperation*: improving cooperation within the international community on Cyber Space issues is an effective way to increase stability through better mutual understanding and even trust between stakeholders. This will also create common mechanisms of crisis management, communication, and de-escalation. Lebanon must work towards the conclusion of an international agreement on the obligations of a State, the infrastructure of which could be used for malicious purposes, such as "launch pads" in order to proxy-attack other countries ("triangulation" of a Cyber Attack), etc.
  - *Stability*: the country must continue to promote the principle of the existence of certain rights enabling States that are victims of computer attacks to take appropriate measures while maintaining international peace and security.

3.3 Reinforcement of State capacities to support the development of ICT

The State must initiate an awareness and training programs that familiarize its civil servants working in the IT and ICT sectors as well as its citizens and professionals with good practices in digital uses. It is by being aware of cyber risks and by being trained to adopt the appropriate behavior that users will be able to face Cyber Threats. Whether in

the context of private use (young people exposed, in particular, to inappropriate content or harassment and malice on the web) or professional practices (administrations and companies), educated and sensitized citizens represent the first barrier in the protection of information. Cyber Security trainings need to be considered as part of the National Strategy to ensure that today's and tomorrow's decision-makers are aware of the risks and the know how to deal with threats. In this context, it seems essential for the State to promote research and its industrial capabilities, to improve the defense capabilities of the public sector, and to engage the public sector in a dialogue with the banking sector and the private sector involved in the digital economy.

3.4 Promote educational capacity on the Lebanese territory

To address the shortage in skilled Cyber Security specialists, the Government and the Lebanese University, along with private universities, schools, and organizations, must invest in Cyber Security awareness programs via a Cyber Academy platform. These same actors must set up university curricula to train qualified and talented high-level specialists to bridge the gap between supply and demand in the Cyber Security field.

Digital security awareness should be an essential part of non-specialized higher education to introducing future graduates to Cyber Security. Each institution shall therefore ensure that organizations providing initial or continuing training courses integrate Cyber Security awareness teaching into their various courses and that the material is adapted to each training offered.

It would be desirable to integrate Cyber Security in IT subjects in the National Education System (pre-university curriculum), including a Cyber Security component in school curricula as well as innovative and motivating activities in the classroom, challenges, and summer programs.

Under the aegis of a future national information systems security agency which will be set up (see Part II), the NCISA, the State shall have to assess the needs for initial and continuous training programs in the short, medium, and long term. This shall require a proactive collaboration with the Ministry of Education and all relevant actors in the administration and the private sector, including trade unions.

Key technologies for which in-depth knowledge is required in Cyber Security trades and in general for the development of a trusted digital environment, should also be identified.

As part of continuing education, the human resources of institutions and companies, specifically those in professional categories with social and state responsibilities, should be able to benefit from digital training that includes Cyber Security awareness.

ENA Civil Servant College, in partnership with professional syndicates, shall be called upon to develop and implement continuing education programs tailored to the needs of

public administration employees and managers to match the pace of growth and development in the private sector.

The State is aware of the need to promote scientific and technological research in the digital fields, so that Lebanese universities and research institutes attract the best minds in the field of Cyber Security. The Government therefore proposes to encourage an active partnership between training institutes and industry, which shall lead to a real collaborative, mutually beneficial dialogue between the State and the actors in Cyber Security. To achieve this goal, the following actions should be considered:

- Identify areas of science and technology that Government, industry, and academia consider important and identify potential gaps in Lebanon.
- Fund and Government-support academic centers of excellence, research institutes, and doctoral training centers to address important areas, such as large data analysis, trusted industrial control systems, science-based research, and more.
- Establish centers of excellence (or encourage existing centers) that attract the most competent and dynamic scientists and researchers, and deepen the active partnership between universities, government, and industry. In particular, the Government should support the development of leading cyber products and dynamic new businesses in Cyber Security.
- Fund research and develop high-level security equipments to improve the level of product security for businesses and the general public.
- Provide funding and governmental support to academic centers of excellence and research institutes that address important research in digital technologies, and sponsor PhD students and holders of PhD degrees to increase the number of Lebanese experts with cyber expertise.
- Strengthen the partnership between research and industry, through scholarships, bilateral funding, and State-funded research. This form of collaboration shall always respect the principles of equity and meritocracy, thus enhancing the technical skills in Cyber Security of the people involved.
- Create an expert panel for digital trust entrusted with the mission to:
  - Identify the key technologies for which in-depth knowledge is required for Cyber Security professions;
  - Evaluate initial and continuing education needs;
  - Monitor research and support its development;
  - Support young PhD holders;
  - Encourage financing and support research and industrial development in the field of digital technologies.

As main actors of public life, civil servants should be aware at their different post levels, of responsibilities for the protection of the data to which they have access. To improve the protection of all the components of the country and to prevent any threat, the State must:

- Strengthen the security of its information systems by developing and monitoring security policies for interdepartmental electronic communications network and by ensuring secure deployment of mobile devices.
- Evaluate on a yearly basis the application of the State Information Systems Security Policy and the effectiveness of the measures adopted. Parliament shall be informed by means of indicators, which shall also include the responsiveness to its official recommendations to address Cyber Security. More generally, senior quality regulation officials will ensure that issues related to strengthening the security of information systems are taken into account in the standard-setting process, which is carried out on a regular basis.
- Attract competent, effectively-trained cyber specialists to the Government to maintain our National Security, including an understanding of the impact of Cyber Space on security operations.
- Include Cyber Security elements in all public service training programs and in the recruitment exam for the Corps of Information and Communication Systems Engineers. Public servants process sensitive data, which they must know how to protect at the level of each ministry.
- Ensure that the experience of public servants in the field of Cyber Security is optimized throughout their career.
- Give Law Enforcement Agencies, public authorities, and the banking sector a high level of independence on matters related to Cyber Security, infrastructures, process approaches, and operational decisions, as they relate to their own, internal mandates. This general approach must always be aligned with the Cyber Security Strategy of the Government, which shall be ensured through a National Agency at the highest national defense level.
- The Prime Minister shall receive a semestrial confidential report with the result of the audits on Cyber Threats, Cyber Attacks, Cyber Vulnerabilities, and the coordinated response of all the concerned authorities.
- Preserve Lebanon's autonomy in decision-making, including the mobilization of human and budgetary resources.

3.5 Promote industrial and technical capacity

Lebanon must develop an ecosystem conducive to the development of the digital economy and the international promotion of its digital products and services. It must ensure that administrations, companies, and citizens have access to digital products and services at levels of trust and security adapted to uses and Cyber Threats. For this purpose, the country must:

- Develop and enhance the national offering of security products and services. In collaboration with the various ministries (Telecom, Industry, Economy, Interior, Defense, Foreign Affairs, OMSAR, etc....) and a National Agency for Cyber Security (NCISA), the State must promote an industrial policy to strengthen national companies developing computer security products and services. The State must also encourage dynamic new businesses in Cyber Security and the development and the production of advanced cyber-products.

- Collaborate with stakeholders – with Cyber Security companies in particular – and academic environments to provide training and advice to the public and private sectors. As the burgeoning and innovative Cyber Security sector is a necessity for the national modern, digital economy, the State shall seek to develop opportunities for collaboration with the private sector in training and education and to promote facilities for maintaining and exercising skills. For their part, Cyber Security companies shall provide governments and businesses with cutting-edge technologies, training, and advice.

- Produce or procure reliable equipment to detect and protect from Cyber Attacks, primarily for life-critical operators (OIV- *Opérateur d'Importance Vitale*), as well as secure mobile products for all businesses. Most of the equipment and digital products available on the market today do not have the level of computer security to keep them safe. For companies, the level of product security must therefore become a differentiator, a competitive advantage. An adequate security evaluation and certification process must be put in place to clear mission-critical equipment.

- Identify and list, through NCISA, all the country's critical infrastructures (OIVs) to implement *ad-hoc* security policies and best practices.

- Qualify and monitor Cyber Security products, hardware, and services to identify those which can endanger IT activities by enabling Cyber Espionage and government-sponsored attacks.

3.6 Support the export and internationalization of Cyber Security companies

It is essential for Lebanon to support the creation and development of an industrial sector of Cyber Security, for which it must:

- Support collaborative initiatives generated by the private sector. The State shall support the economic development of the industrial Cyber Security sector to encourage the local development of Cyber Security products and services that will ensure Lebanon's non-dependency on foreign and foreign-controlled security products.
- The State shall seek to enhance the visibility and competitiveness of the Lebanese products abroad and facilitate access for SMEs and start-ups to international markets. Interdepartmental coordination will be structured and strengthened. An organization in support of companies will be implemented beyond the one-off and often isolated actions currently carried out by the various ministries and state entities. Export control procedures for Cyber Security solutions will be clarified and optimized.
- Create specific support systems for Cyber Security actors, with clear conditions for access and implementation methods. In parallel, clarify and optimize the conditions of access to implementation methods of existing support systems.
- Establish clear procedures to control the export of Cyber Security solutions.
- Integrate security criteria into the selection of digital products and services in public procurement.

3.7 Strengthen collaboration between the public and private sectors

As a major player in the economy and the main service provider, the Government is the first potential user of high-level Cyber Security products. Greater permeability between the public and private sectors would allow Lebanon to enhance its efforts in the area of every-day digital security, by enabling each beneficiary better to detect and deal with Cyber Threats. For that, it would be necessary to:

- Encourage the creation, development and innovation of the Cyber Security sector, in collaboration with the Government, academia and the private sector.
- Strengthen collaboration between Government and industry to provide each with proactive information on threats. In order to obtain information, each has to contribute to upstream disruption efforts.
- Encourage Government-industry partnerships to help define and target interventions for growth and innovation.
- Support the establishment of accelerators and start-ups dedicated to Cyber Security.
- Collaborate with the financial sector to make Lebanon a more hostile environment for those seeking to monetize stolen credentials, including disrupting their networks.

- Transfer, through NCISA, the gained knowledge to the private sector in order to enhance its Cyber Security, while identifying competent and trustworthy service providers, which should enable the detection and treatment of the inevitable growth in the number of Cyber Attacks against businesses. The requirements for Cyber Security must be integrated in public contracting and draft legislation, while stimulating growth in the Cyber Security sector through:
  - Integrating security criteria in the selection of digital products and services in public contracting;
  - Offering a bonus factor if the bid is accompanied by a Cyber Security risk analysis;
  - Ensuring that laws include a section in their impact assessment dedicated to digital technology, including Cyber Security.

3.8 The role of Law Enforcement Agencies

To improve Cyber Security capabilities, Law Enforcement Agencies (Army, Internal Security Forces, General Security, State Security) must take the following actions:

- Increase the capacity of LEA, in coordination with international partner agencies, to identify, anticipate, and disrupt hostile cyber activities of foreign actors, Cyber Criminals, and terrorists. This will improve their intelligence gathering and exploitation, in order to obtain preventative information about the intentions and abilities of attackers.
- Strengthen law enforcement efforts to prosecute and target criminals, wherever they may be, in coordination with local and international partners. Law Enforcement Agencies shall target criminals, who persist in attacking Lebanese citizens and businesses, by dismantling their infrastructure and facilitation networks.
- Law Enforcement Agencies and the banking sector shall also continue to contribute to the awareness and standardization of Cyber Security.
- Improve the actions of LEA and judicial services in investigations under judicial authority. The most important enabler factor and approach for all issues related to Cyber Crimes is dedicated, high-level, professional technical training, which must include laboratory-based, hands-on modules, sessions, and exercises. Additional boosters of quality can speed and enhance this process – these include dedicated procedural, technical, and operational relationships with international Cyber Security bodies, organizations, and specialized teams, supported by regular information sharing.
- Strengthen coordination across Law Enforcement Agencies, including exchanging information on threat analysis.

- Treat anticipation and prevention as a priority for competent authorities dealing in information system security. This can be achieved by building a Cyber Threats Intelligence platform. This CTI platform should receive continuous input data both from domestic (National Agencies) and foreign sources. Data may even be obtained through the acquisition of commercial data sets ("feeds") from the few specialized, private companies, which provide 100% neutral information, i.e. not officially or unofficially backed by any foreign Government. The CTI platform shall act as the core of the Government's National CERT (CERT-LB), **which must be established within the NCISA**. The CERT-LB shall then provide data feeds, alerts, early warnings, etc. to domestic SOCs (Security Operation Centers).
- Enhance the Cyber Warfare capabilities of Intelligence Agencies and the Army, by, for instance, securing training sessions and support, exposing them to the activities and best practices of similar Cyber Security Agencies in most advanced countries.
- Facilitate coordination among National Agencies, by, for example, hosting periodic meetings to discuss Cyber Security matters, providing facilities to the agencies in order to meet and respond to national cyber incidents, and hosting domestic Cyber Security incident response drills.

4. Objectives

At the national level, Cyber Security strategy must be designed to implement, for the public and private sectors and for citizens, a strategic defense plan against Cyber Threats, ensuring its sustainability by institutionalizing it through a clear structure and objectives. A Cyber Security Strategy shall also incorporate decisive actions to protect the Lebanese economy and the privacy of Lebanese citizens. Overall, the main goal of this National Strategy is to outline a set of decisions, which must lead to operational actions that make Lebanon confident, capable, and resilient in a fast-moving digital world.

The following main objectives must be accomplished:

- Encourage the Government, organizations, businesses, and individuals to play their part in this collective effort to secure the national Cyber Space;
- Improve the availability and usability of services, enhance transparency, encourage citizen participation in governance, and cut public and private sector Cyber Threats and the costs of Cyber Attacks;
- Apply an appropriate and effective incident management notification and response mechanism;
- Manage security incidents and reduce risk, thus being able accurately to estimate current and upcoming Cyber Threats;
- Respond quickly and effectively to Cyber Threats, using the most appropriate capability, to major incidents in Cyber Space as they occur to maintain the security and resilience of networks, data, and systems.
- Develop the legal, procedural, and technical means to defend Lebanon against constantly evolving Cyber Threats, to provide an effective response to incidents, and to ensure the protection and resilience of the country's networks, data, and systems;
- Improve response capabilities to Cyber Attacks by adopting appropriate measures and increasing the country's resistance to the most common Cyber Threats. The Government needs to build on its capabilities and those of the industry, actively supporting the development and implementation of active Cyber Defense measures to significantly improve ICT security levels on domestic networks;
- Provide support and assistance to organizations in response to security incidents. In particular, the State must ensure that the Government, whether from a preventive perspective or in response to an incident, collaborates actively with the private sector. National incident management processes must take a

comprehensive incident approach, through which it is possible to learn from partners and share mitigation techniques;

- Ensure that incidents are **mandatorily and promptly reported to the Nation's Cyber Security Authority, namely the NCISA**, thus allowing an understanding of the magnitude, scope, and severity of the threat;
- Identify the root causes of attacks at the national level, reducing the incidence of multiple and repeated exploitation on several victims and sectors;
- Use relationships with other IT security incident response teams, both at the domestic and international level, as part of an incident management protocol;
- Measure Cyber Crime using reliable statistics and analysis of digital crimes to guide responsive action. In the absence of such statistics, public authorities cannot continuously reassess policies and implement adequate measures. In this case, the Ministry of the Interior must implement new instruments to monitor the evolution of Cyber Crime to guide public action;
- Establish a database of cyber incidents to enable both a broad view and detailed analysis of Cyber Threat trends to identify security solutions and/or product and service needs. This would also benefit the cyber-insurance industry, which relies on statistical and historical data about cyber incidents in its assessment of risk;
- Promote a *Secure Internet* environment for Vital Operators. Each OIV should develop and implement its security measures and security policies in line with this Strategy, in order to operate their security operation center for monitoring and reacting efficiently to security incidents, with the support of behavioral analytics techniques, intelligent correlation, and filtering of security alerts;
- Encourage hardware and software vendors to develop and sell products, for which security controls are enabled by default;
- Once the Lebanese cyber environment and Cyber Hygiene comply with basic standards of security at the level of the single technological product/item and the single user (Stakeholders), the NCISA shall produce new standards with the main objective to obtain a full *Security by Design* for every ICT device connected to Lebanon's assigned public IP address space;
- Ensure that service providers comply with laws and regulations. The challenge here is to make a drastic change in the security controls built into the software and hardware already enabled by the manufacturer before the product is launched on the market. The user must be able to benefit from maximum security on a commercially viable product or service, while remaining in the context of a freely accessible and open Internet;

- Emphasize human values in Cyber Space, promoting respect for human rights to ensure that individuals are empowered, that they have complete digital self-determination, and privacy;
- Change behavior by ensuring that Governmental entities, organizations, businesses, and individuals have the knowledge and skills to defend themselves and take appropriate measures to protect themselves and their clients from the harm caused by Cyber Attacks;
- Sensitize the Lebanese people to good practices and launch an ambitious program to raise awareness among all Lebanese, following the below line of actions:
  - Integrate Cyber Security awareness into all higher education and continuing education programs; integrate Cyber Security into the pre-university education system (in the form of classroom activities, challenges, and summer courses) and into programs in specific fields, such as computer science; implement Cyber Security awareness programs in partnership with universities, schools, and private organizations;
  - Launch a call for expression of interest to produce awareness-raising content addressed to the general public;
  - Launch national initiatives in partnership with LEA to raise awareness of the risks of the Internet and educate school students;
  - Create a digital education portal in collaboration with the academic community;
  - Develop projects for communication campaigns as part of a "great national cause" (to build confidence in digital products);
  - Promote Cyber Security best practices and launch awareness campaigns to engage the society, and highlight the risks of enemy manipulations of information in the Cyberspace;
- Ensure a radical change in public behavior, maintaining a consistent set of messages on Cyber Security guidance from both the Government and its partners;
- Improve the culture of Cyber Security in Lebanese society by understanding cyber risks and the stages of Cyber Hygiene;
- Inform about the risks of manipulation and propaganda techniques used by malicious actors on the Internet. The relevant defense and security services are responsible for detecting propaganda or Cyber Terrorism incidences and providing the government with recommendations for the implementation of counter measures. It is crucial to put in place an information platform to respond to acts of propaganda or destabilization;

- Strengthen the security of the most sensitive information systems of critical infrastructures, in both public and private operators, through adequate and regularly updated legislative measures. This process will gradually be extended to public and private operators involved in handling or managing sensitive information systems;
- Ensure that the LEA have the strongest defenses to keep their networks and platforms secure and resilient. These stakeholders must be able to continue to operate and maintain their freedom of action despite Cyber Threats, and to provide assistance in the event of a large-scale Cyber Attack at the national level.
- Prepare the legal and operational phases for the institutionalization by creating a central authority at the highest level of defense: the NCISA.

PART II. INSTITUTIONALIZATION – THE NATIONAL CYBER SECURITY AND INFORMATION SYSTEM AGENCY (NCSIA)

The security of information systems is of crucial importance to a wide variety of organizations and actors, both public and private, domestically and internationally.

Whether in the political, diplomatic, economic, or military field, Cyber Security is today a collective concern and a national priority. Indeed, Cyber Threats and Cyber Attacks are on the rise and they can inflict serious damage to the interests of the Nation. Faced with this risk, Lebanon, like many other countries around the world, must have a strong and reliable national computer defense system.

To achieve this goal, the National Cyber Security Committee has concluded that the creation of a national agency for the security of information systems is a necessary and essential step to facilitate a coordinated and proactive approach to managing Cyber Security problems and to track the growth and diversity of Cyber Threats and to robustly address their increasing sophistication.

The creation of a Lebanese agency reporting directly to the Prime Minister and attached to the General Secretariat of the Higher Council of Defense is a crucial step in the response of the Lebanese State to major current and future challenges in the field of Cyber Security.

The NCISA shall perform its mandate in close coordination with the concerned ministries and LEA, without conflicting with their respective legal and mandated roles.

The NCISA will enable Lebanon to centralize and coordinate decisions at the level of the various state services in the field of Cyber Security, and thereby increase the country's resilience to digital threats.

Part II of the Strategy gives a detailed description of the NCISA's role and functions and the different sectors in which it will operate.

5. The Institutionalization of a National Agency for Cyber Security

The National Cyber Security and Information System Agency (NCISA) is a governmental authority, operating under the General Secretariat of the Higher Council of Defense, responsible for Lebanon's information system Cyber Security policies, procedures, and their implementations in line with the Lebanese National Cyber Security Strategy. The NCISA performs its public duties within the framework of the legislation, rules, and regulations pertaining to Cyber Security.

The area of activities of this NCISA are, inter alia, to set policies and procedures, to develop plans, to assess vulnerabilities, to identify threats, to enhance awareness, to alert - with recommendations- to respond promptly and efficiently to Cyber Attacks in order to maintain the Lebanese cyber environment secure and resilient.

The NCISA also defines critical information infrastructure and critical operators, helps to classify data, and establishes a certification framework for high-level digital security products. Moreover, the NCISA aims to raise the level of knowledge in Cyber Security by initiating and spreading awareness through training programs as well as the diffusion of know-how exchanged through international cooperation.

The NCISA's essential role is as a coordinator and facilitator: it coordinates with all government agencies, concerned ministries, and other public institutions and fosters cooperation among the public and private sectors, industry, and academia.

The NCISA, within its mandate, assists and supports all stakeholders from the public and private sectors concerned by Cyber Security. The NCISA also provides technical advice and establishes guidelines reflecting public and corporate priorities and best practices in terms of Cyber Security.

NCISA shall work closely with concerned ministries and institutions, LEA, and with the industrial sector to assess and share information on the latest criminal threats, help industries defend against threats, mitigate the consequences of Cyber Attacks on Lebanese victims (administration, corporate, industry, individuals…), and create a national template for handling emergency situations in Cyber Space or Cyber Security.

5.1 The NCISA's mandate at the national level

The National Cyber Security Information Agency (NCISA) draws its legitimacy from a country-wide mandate that defines its role and determines its functions, in accordance with the national needs in Cyber Security as defined by the Government's Strategy.

NCISA shall thus be assigned the following tasks:

1. Facilitate and supervise the design, implementation, and coordination of secure inter-ministerial/inter-departmental means of electronic communications at the governmental level.
2. Elaborate the implementation of the country's Cyber Security Policy for Information Systems and secure the effectiveness of the measures adopted based on a yearly, confidential audit and evaluation report that shall be submitted to the Prime Minister.
3. Support in establishing, at the national level, the Cyber Security Incidents Response Team (CSIRT) that works daily with the ministries and law enforcement agencies. The CSIRT is the central repository of cyber incidents across the territory, where all stakeholders exchange their notification of Cyber Attacks. The CISRT supports all participants in the remediation, defense and prevention against the notified attacks. Also, it defines the Cyber Threat scale and issues a yearly National Threat Watch Report. It cooperates closely with the international CSIRT community (FIRST).
4. Build an event or incident detection system for threats that can affect the national information systems security and coordinate the intervention in response to these events.
5. Organize, as needed, Cyber Security training courses and awareness-raising campaigns for governmental institutions, government personnel, and interested private entities in the field of information systems Cyber Security and Cyber Defense.
6. Assist and advise public administrative entities and institutions as well as the private sector on the implementation of secured information systems that are resistant to Cyber Attacks and diffuse threat assessment and recommendations to the public and private sectors and to the citizens.
7. Apply appropriate Cyber Security standards and enforce their adoption in all government agencies.
8. Provide dynamic intelligence on criminal Cyber Threats in a common database, which the industry can interface with to better defend itself.
9. Identify standards and practices and safety tips related to observed Cyber Security incidents.
10. Cooperate with relevant operators, mainly operators of vital importance (OIV) and critical infrastructure, to identify and characterize Cyber Attacks affecting their operation.
11. Protect the Government's classified and highly sensitive information and assets from Cyber Attacks.

12. Perform Cyber Security crisis management drills. Such drills that will be conducted at the national level shall progressively cover the entire territory and the sectors of activity of vital importance.

13. Law Enforcement Agencies and concerned administrative entities/ministries and institutions, in conjunction with NCISA, shall continue to set up operational Cyber Defense capabilities to deal with major Cyber Security-related crises.

5.2 The NCISA and the public – from individuals to companies

The NCISA provides quality support and recommendations to businesses and citizens on Cyber Threats. By doing so, it sets up, for example, an easily accessible database of information and prevention systems and conducts publicity campaigns aimed at informing and raising awareness about Cyber Threats among the general public.

As part of its role with the general public, the NCISA shall:

- Implement measures to defend Lebanese citizens and computer information systems against known and emerging threats by establishing a platform that allows corporate entities/citizens to notify NCISA of the Cyber Threats they face.
- For prevention purposes, recommend technical solutions and training programs aimed at protecting/securing the digital domain. These solutions shall include national and international drills, accessible to all companies and the general public to improve preparedness in Cyber Space.
- Participate in the orientation of academic research, studies, and the development of software, hardware, devices, and technologies centered on information systems security.

5.3 The NCISA's involvement in the qualification and monitoring of products

In ensuring the quality of digital products and services, the NCISA shall carry out the following tasks:

- Help ensure an active surveillance of digital security technologies used by government institutions, businesses, and citizens.
- Assist in qualifying and monitoring Cyber Security products and services and support the development of new digital security assets that reflect the latest trends and changes in usage patterns.
- Contribute to the promotion of national technologies and know-how in information systems security by developing a framework for product qualification and certification in line with the Government's objectives and sovereignty.

5.4 The NCISA facing Cyber Threats

The NCISA analyses and manages the risks of Cyber Attacks when new technologies are deployed in the digital transformation process. It shall be responsible for the following:

- Setting up a National Cyber Security Incident Management, which maps out the most critical systems, and conducts Cyber Threat analysis, detection, and understanding.
- Monitoring technological evolution to anticipate changes and propose the necessary innovations in information systems security.
- Conducting audits of service information systems and collecting technical information for the sole purpose of managing Cyber Security incidents affecting these systems.
- Strengthening and supporting LEA in the fight against Cyber Terrorism and organized Cyber Crime by improving the means in the following initiatives:
  - Countering hostile foreign actors;
  - Preventing Cyber Terrorism;
  - Countering, on the domestic territory, radical thinking and behavior related to Cyber Space;

5.5 The NCISA and the protection of Operators of Vital Importance (OVI)

An Operator of Vital Importance (OVI) or a critical infrastructure is any public or private entity that manages and operates sensitive data and important sectoral services, such as, but not limited to, the telecommunication infrastructure, energy sector, health infrastructure, national personal data platforms, etc....

The NCISA's role in protecting OVIs shall follow the actions below:

- Strengthen the protection of vital operators, particularly in the areas of electronic communications, electricity supply, and digital service companies by adopting strong requirements for Cyber Security safety regulations.
- Involve electronic communications operators and web hosting companies in the implementation of detection systems in their networks to detect Cyber Attacks targeting their subscribers (probes, sensors, behavioral detection, etc.).
- Provide risk analysis tools and independent systems to assess the level of security and Cyber Security reliability of digital products and services in critical industries.

When digital products and services store personal data, or are intended for industries of vital importance, NCISA shall provide assistance for conducting risk analysis and for elaborating best practices in terms of cyber protection.

The NCISA shall also contribute to the establishment of mechanisms to independently assess the level of security and reliability of these products and services, and to provide their potential users with appropriate safeguards through labeling. For this purpose, the NCISA shall accomplish the following:

- Define best practices and mechanisms to strengthen key/critical national infrastructure (sensitive sites or OVIs) and protect them from Cyber Attacks. The NCISA, in collaboration with regional administrations and other responsible authorities, shall assist national organizations and enterprises in taking the necessary measures to remain sufficiently secure and resilient against Cyber Attacks.
- Ensure that public and private critical national infrastructures are aware of the level of threat and implement appropriate Cyber Crime countermeasures. Public institutions and private companies and organizations must understand the real level of Cyber Threat to the infrastructure and put in place measures to improve the protection and preservation of national interest and sovereignty.
- Assist companies that own and/or operate sensitive data to manage their cyber risks and vulnerabilities.

5.6 The normative framework of the Agency and its ecosystem

Since constructing the legal framework requires highly experienced bodies, the NCISA's normative framework shall be built with the help of a strong and regular international collaboration and support that respects Lebanon's sovereignty and constitution. The NCISA's ecosystem includes major local partners, such as the Government, the Ministry of Telecommunications and its operators, OGERO, LEA, the beneficiary ministries, OMSAR, academic institutions, Internet Service providers in Lebanon, and professional associations. The ecosystem is supported by the international partners listed in the Strategy.

The NCISA shall carry out the following steps in ensuring an adequate legal framework for Cyber Security:

- Adapt and create a regulatory framework for new emerging technologies. To do so, NCISA shall regularly inform ministries, government institutions, local authorities, companies, and citizens about threats facing digital systems through the communication channels appropriate to each.
- Prepare the legal environment to accommodate new digital products and services.
- Develop Cyber Defense guidelines and implement Cyber Defense measures to significantly improve Cyber Security levels across computer networks.

- Issue rules for the authorization of security devices and mechanisms designed to protect, in information systems, information covered by national defense secrecy.
- Participate in international negotiations and liaise with foreign counterparts.
- Define and assess the security of the devices and services offered by providers, necessary for the protection of information systems and infrastructures.
- Define the Cyber Security framework for the implementation of legally qualified electronic signatures.
- Contribute to the preparation of the framework of accreditation and certification related to Cyber Security and legally binding electronic signatures and digital logs/traces/proofs.
- Decide on the accreditation of recognized laboratories that may conduct digital security evaluations and certifications of IT products and systems (these legal provisions are not yet implemented in Lebanon).
- Set a framework for accreditation, certification, and technical standardization related to Cyber Security systems in line with existing laws and regulations. The said framework shall be set in collaboration with concerned ministries, LEA and governmental institutions, each within its own jurisdiction.

6. Conclusion

There are final, operation-critical, and strategic assumptions which must be highlighted in the National Cyber Security Strategy of Lebanon:

- The present document urgently calls for compulsory, critical, operational action: The official creation of a National Cyber Security Information Agency. Without the **NCISA**, none of the following actions can be pursued or accomplished;
- NCISA needs a solid commitment from the Government, which will enable the launching of multiple actions, such as correct and detailed operational planning, scheduling, and budgeting;
- NCISA needs a firm, official commitment for an operational budgetary, without which, nothing can be accomplished. While it is impossible to define a precise budget at this very early stage, budget ranges can definitely be projected based on the action plan approval;
- After the endorsement of the Strategy, the National Cyber Team created by the Prime Minister shall have a new mandate to support the Government in the transition phase with a clearly defined new mandate and partners to assist in the implementation of the Strategy;
- If the steps stated in the Lebanon National Cyber Security Strategy above are not put in place, the country shall face the following dangers and risks:
  - Lebanon will continue to be listed as one of the most underdeveloped countries in the world, as per ITU global statistics and scoring and Cyber Security Index, that assess a country's ability to deal with 21st Century Cyber Security needs and with the global fight against Cyber Crime threats, Information Warfare, and Cyber Terrorism;
  - All of Lebanon's Governmental assets, markets and business sectors, and citizens shall be strongly and dangerously exposed to Cyber Threat. Economic losses, as well as fear, uncertainty, and doubts shall ensue in dealing with the on-going global digital transformation, in which Lebanon still lags very far behind;
  - Lebanon shall not be able to evolve, losing international competitiveness;
  - Poor protection from Cyber Threats, Cyber Attacks, and Cyber Crime attract Cyber Criminals. This in turn depletes trust in the country. Lebanon shall thus lose foreign investments, especially in the IT and ICT industries, despite the encouraging economic and business-enabling incentives, which the Lebanese Government has put in place during the past years;

- Lebanon is home to a large number of registered and non-registered refugees, legal and illegal foreign workers, etc. These communities are in contact, directly or indirectly, knowingly or unknowingly, with countless organizations and entities (among them a large number of NGOs) both on the national territory and in their respective home countries. These populations are either very poorly or not at all supervised by the Lebanese Government and could thus be vulnerable to potential Cyber Attacks and could easily become a platform for potential Cyber Threats and other Cyber-criminal acts, which could place Lebanon under increased potential risks from organized crime;
- All of the above shall contribute to feed the continued perception of Lebanon as an "under developed" country.

Only a strong, cohesive, inclusive, institutionalized, and collaborative National Cyber Security Strategy, based on and addressing the identified Cyber Security Pillars can protect Lebanon, its public institutions, its private sector, and its citizens from the above threat, thanks to a codified, systematic, nation-wide, all-encompassing action plan.

ACRONYMS

Acronym	Full Expression
APT	Advanced Persistent Threat
BYOD	Bring Your Own Device
CCB	Cyber Crime Bureau
CEPOL	European Union Agency for Law Enforcement Training
CERT	Computer Emergency Response Team
CTI	Cyber Threat Intelligence
DoS -- DDoS	Denial of Service – Distributed Denial of Service
EBIOS	*Expression des Besoins et Identification des Objectifs de Sécurité* / Expression of Needs and Identification of Security Objectives
ENA	Public Administration National School of Lebanon
EUROPOL	European Union Agency for Law Enforcement Cooperation
ICP	Industrial Control Process
ICT	Information and Communication Technology
IIOT	Industrial Internet of Things
INTERPOL	International Crime Police Organization
IOT	Internet of Things
ISF	Internal Security Forces
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LEA	Law Enforcement Agencies (Army, Internal Security Forces, General Security, State Security)
NCISA	National Cyber Security and Information System Agency (of Lebanon)
NIST	National Institute of Standards and Technology
OGERO	Lebanese telecommunications company
OIV	*Opérateur d'Importance Vitale* ; critical infrastructure
OMSAR	Office of the Minister of State for Administrative
SSH	Secure SHell
SSL	Secure Sockets Layer
SME	Small and Medium Enterprise
TETRA	Terrestrial Trunked Radio
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNODC	United Nations Office on Drugs and Crimes
VPN	Virtual Private Network

GLOSSARY

Expression	Definition
0-Day Vulnerability	A vulnerability that is not known neither to the vendor, nor to the Cybersecurity or the hacking community. A zero-day vulnerability is also a software security flaw that is known to the software vendor but doesn't have a patch in place to fix the flaw.
Advanced Persistent Threat	It is a stealthy computer network attack in which a person or group gains unauthorized access to a network and remains undetected for an extended period. The term's definition was traditionally associated with state sponsorship, but over the last few years there have been multiple examples of non-state sponsored groups conducting large-scale targeted intrusions for specific goals.
Botnet	A botnet is a number of Internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial-of-service attack (DDoS attack), steal data, send spam, and allows the attacker to access the device and its connection.
BYOD - Bring Your Own Device	An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes.
CSIRT – Computer Security Incident Response Team	A group of people integrated at the enterprise with clear lines of reporting and responsibilities for standby support in case of an information systems emergency This group will act as an efficient corrective control, and should also act as a single point of contact for all incidents and issues related to information systems.
Cloud Computing	Cloud computing is the use of data center servers and software networks to dynamically allocate resources and run applications for remote end users. or Cloud computing is defined as the computing or processing of resources over the internet. These include storing of data, running application instances. Convenient, on-demand network access to a shared pool of resources that can be rapidly provisioned and released with minimal management effort or service provider interaction.
Cloud Network	Cloud network is a computer network within a cloud infrastructure on which provides connectivity to cloud-based applications, servers etc. or Cloud networking (and Cloud based networking) is a term describing the access of networking resources from a centralized third-party provider using Wide Area Networking (WAN) or Internet-based access technologies.
Cloud Services	A cloud service is any service made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers.

Expression	Definition
Critical Systems	Systems whose incapacity or destruction would have a debilitating effect on the economic security of an enterprise, community or nation.
Cyber (Security) Incidents	A malicious act or suspicious event that disrupts, or was an attempt to disrupt, the operation of those programmable electronic devices and communications networks including hardware, software and data that are essential to the Reliable Operation of the Bulk-Power System.
Cyber Attack(s), Cyberattack(s), Cyber-Attack(s)	An attempt by hackers to damage or destroy a computer network or system. The 10 most common cyber-attack types: - Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. - Man-in-the-middle (MitM) attack. - Phishing and spear phishing attacks. - Drive-by attack. - Password attack. - SQL injection attack. - Cross-site scripting (XSS) attack. - Eavesdropping attack.
Cyber crime(s), Cybercrime(s)	Crimes that use computer networks or devices to advance other ends include: Fraud and identity theft (although this increasingly uses malware, hacking or phishing, making it an example of both "computer as target" and "computer as tool" crime) Information warfare.
Cyber Dissuasion	The action of discouraging an action or event through instilling doubt or fear of the consequences.
Cyber Espionage	Activities conducted in the name of security, business, politics or technology to find information that ought to remain secret. It is not inherently military.
Cyber Hygiene, Cyber-hygiene	Refers to steps that computer users can take to improve their cybersecurity and better protect themselves online.
Cyber Security, Cybersecurity	Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. There is no universally accepted nor straightforward definition of cyber security. When comparing it to 'information security' some people regard it as overlapping, being the same thing. Or they may view information security as focused on protecting specific individual systems and the information within organizations, while cyber security is seen as being focused on protecting the infrastructure and networks of Computer Information Infrastructures.
CyberSouth	CyberSouth is a joint project of the European Union (European

Expression	Definition
	Neighborhood Instrument) and the Council of Europe. CyberSouth aims to strengthen legislation and institutional capacities on cybercrime and electronic evidence in the region of the Southern Neighborhood in line with human rights and rule of law requirements. Project area: Southern Neighborhood region. Initial priority areas: Algeria, Jordan, Lebanon, Morocco and Tunisia.
Cyber Space, Cyberspace	The notional environment in which communication over computer networks occurs. Cyberspace refers to the virtual computer world, and more specifically, is an electronic medium used to form a global computer network to facilitate online communication. It is a large computer network made up of many worldwide computer networks to aid in communication and data exchange activities. Cyberspace's core feature is an interactive and virtual environment for a broad range of participants.
Cyber Threat(s)	The possibility of a malicious attempt to damage or disrupt a computer network or system.
Cyber Warfare	The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of information systems for strategic or military purposes.
Cyber-Insurance	A cyber insurance policy, also referred to as cyber risk insurance or cyber liability insurance coverage (CLIC), is designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event.
Cybernetics	The science of communications and automatic control systems in both machines and living things.
Cyberpunk	A programmer who breaks into computer systems in order to steal or change or destroy information as a form of cyber-terrorism.
Data Theft	Data theft is the act of stealing computer-based information from an unknowing victim with the intent of compromising privacy or obtaining confidential information.
Denial of Service, DoS	A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses.
Distibuted Denial of Service, DDoS	A distributed denial-of-service (DDoS) is a DoS attack from multiple sources.
Digital Transformation	It is the novel use of digital technology to solve traditional problems. These digital solutions enable inherently new types of innovation and creativity, rather than simply enhance and support traditional methods. In a narrower sense, "digital transformation" may refer to the

Expression	Definition
	concept of "going paperless" or reaching a "digital business maturity" affecting both individual businesses and whole segments of society, such as government, mass communications, art, medicine, and science.
EBIOS	Expression of Needs and Identification of Security Objectives) is a method for analysis, evaluation and action on risks relating to information systems. It generates a security policy adapted to the needs of an organization. The method was created in 1995 and is now maintained by the ANSSI, a department of the French Prime Minister.
e-services	Services which use of information and communication technologies (ICTs). The three main components of e-services are- service provider, service receiver and the channels of service delivery.
Exploit	Software code taking advantage of a vulnerability to cause unintended or malicious behavior to occur on computer software and systems. rr
Hack	Unauthorized, non-documented use, break-in.
Hacker	Someone who knows "how to hack" – generally speaking, or an individual who attempts to gain unauthorized access to a computer system.
Hacking	The action of a Hacker while he/she hacks something / on something.
Hacktivism	Hacking summed up with activism. More precisely, it is the use of computer technology to promote a political agenda or a social change.
Hacktivist	Someone who carries out the act of Hacktivism.
Insider Threats	An insider threat is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
Legacy Systems	It is an old method, technology, computer system, or application program, of, relating to, or being a previous or outdated computer system," yet still in use. Often referencing a system as "legacy" means that it paved the way for the standards that would follow it.
Malicious Cyber Activitie(s)	It is an activity, other than one authorized by or in accordance with the law, that seeks to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or the information resident thereon.
Ransomware	Ransomware is malicious software that, in many cases, restricts access to a computer or a device and its data by encrypting its

Expression	Definition
	content and demanding that a ransom be paid, usually via a cryptocurrency such as bitcoin, in order for the victim to regain access to systems and information. Ransomware can also lock systems in various ways without the use of encryption, disrupting device performance. Actors may threaten to expose sensitive, personal, or embarrassing information unless a ransom is paid. Ransomware is typically installed using a trojan or a worm deployed via phishing or by visiting a compromised website. Ransomware is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website.
Resilience	The ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state, and to rapidly recover operational capabilities for essential functions after a successful attack.
Emergency Response Drills	Exercises used to rehearse anticipated emergency scenarios. They are designed to provide training, reduce confusion, and verify the adequacy of emergency response activities and equipment." they are coordinated, supervised activities that are normally used to test a single specific operation or function; their role is to practice or perfect one small part of the response plan.
Script Kiddies	A person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own. or in programming and hacking culture, a script kiddie, skiddie, or skid is an unskilled individual who uses scripts or programs developed by others to attack computer systems and networks and deface websites.
Sextortion	Sextortion is a form of sexual exploitation that employs non-physical forms of coercion to extort sexual favors from the victim. Sextortion refers to the broad category of sexual exploitation in which abuse of power is the means of coercion, as well as to the category of sexual exploitation in which threatened release of sexual images or information is the means of coercion.
Social Engineering	Social engineering refers to all techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons.
State Sponsored Threats	The calculated use of violence (or the threat of violence) against civilians in order to attain goals that are political or religious or ideological in nature; this is done through intimidation or coercion or instilling fear.
Threat	Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure,

Expression	Definition
	modification of data, and/or denial of service.
Unpatched Systems	Unpatched software refers to computer code with known security weaknesses. Once the vulnerabilities come to light, software vendors write additions to the code known as "patches" to cover up the security "holes." Running unpatched software is a risky activity because by the time a patch emerges, the criminal underground is typically well-aware of the vulnerabilities.
Virtual World	A computer-based simulated environment which may be populated by many users who can simultaneously and independently explore it and participate in its activities and communicate with others.
Vulnerability(ies)	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.
Work-From-Home	It is a concept where the employee can do his or her job from home.

ANNEXES

Resolution no. 172/2018

Appointing Dr. Lina Oueidat the Advisor to the Prime Minister for Informatics as the National Coordinator for ICT

The Prime minister**,**

In accordance to the Decree number 2 dated 18/12/2016 (nominating Mr. Saad Hariri as Prime Minister),

In accordance with the agreement no 28/A dated 25/2/2017 between the Lebanese State represented by the Prime Minister and Dr. Lina OUEIDAT to undertake the duties of Advisor to the Prime Minister for Information & Communications Technology.

Decides the following

Article 1: Appointing Dr. Lina Oueidat the Advisor to the Prime Minister for Informatics Affairs to carry out the duties of the National Coordinator for Information & Communications Technology (ICT).

Article 2: This decision shall be notified where necessary

Beirut, dated 26/9/2018

The Prime Minister

Saad Hariri

Resolution no. 173/2018

Establishment of a national team to develop a plan to confront the dangers of cybercrime and prepare a national strategy for institutionalizing the work of cyber security

The prime Minister**,**

In accordance to the Decree number 2 dated 18/12/2016 (nominating Mr. Saad Hariri as Prime Minister),

In accordance with the Public interest necessities.

The following is Decided

Article 1: A National Team is established to develop a plan to confront the dangers of cybercrime and prepare a national strategy for institutionalizing the work of cyber security, composed of the following:

- Secretary General of the High Council of Defense	President
- Representative of the Presiden of the Republic	Member
- Representative of the Parliament	Member
- Representative of the Ministry of Justice	Member
- Representative of the Ministry of Finance	Member
- Representative of the Army Command – Ministry of Defense	Member
- Representative of the General Directorate of Internal Security Forces	Member
- Representative of the General Directorate of General Security	Member
- Representative of the General Directorate of State Security	Member
- Representative of the General Directorate of Civil Status – Ministry of Interior and Municipalities	Member
- Representative of the Ministry of Telecommunications	Member
- Representative of the Office of the Minister of State for Administrative Reform	Member
- Representative of the Banque du Liban	Member
- Representative of the High Council for Privatization	Member
- Dr. Lina Oueidat National Coordinator for Information and Communications Technology	Rapporteur

The members shall be named by the Specialized Minister and the Heads of the departments concerned.

Article 2: the mission of the Team will be as follows:

- Develop a plan to confront the dangers of cyber-crime and prepare a National Strategy for institutionalizing the work of cybersecurity
- Conduct an assessment of the risks related to the preparation of the National Strategy for cybersecurity, combating Information crime and proposing the necessary priorities, plans and projects
- Prepare the strategy for the work of cybersecurity in accordance with the road map prepared by the General Secretariat of the Supreme Council of Defense in coordination with the Commission of the European Union in Lebanon
- Propose the institutionalization mechanism for the implementation of this strategy

Article 3: The Team can seek the assistance of the persons deemed appropriate for the performance of its tasks.

Article 4: The said team shall submit to the Prime Minister a periodic report every month and submit its final report within a period of six months from the date of the issuance of this resolution.

Article 5: This decision shall be notified where necessary.

Beirut, dated 26/9/2018

The Prime Minister

Saad Hariri

Official National Cyber Security Team Members

Administration	Name	Title
The General Secretariat of the Higher Council of Defense	Mahmoud AL ASMAR	Major General – Secretary General of the Higher Council of Defense
	Brigadier General Wajdi CHAMSEDDINE	Engineer – Permanent Representative in the Committee
Presidency of the Council of Ministers	Dr. Lina OUEIDAT	Committee Rapporteur ICT Advisor to the Prime Minister
Parliament	Dr. Ali HAMIEH	Advisor to the Chairman Media and Communications Commission
Ministry of Justice	Hania AL HELWE	Judge
Ministry of Finance	George SAOUD	Head of Informatics
Army Command – Ministry of National Defense	Antoine KAHWAGI	Head of the Intelligence Technical Branch
General Directorate of Internal Security Forces	Khaled YOUSSEF	Colonel – Engineer -Information Branch Engineer
General Directorate of Public Security	Jamal KASHMAR	Colonel – Engineer – Head of Communications Department
OGERO	Dr. Toufic CHEBARO	Senior Engineer
General Directorate of State Security	Hamza DAMAJ	Captain Eng. Head of IT Department
Ministry of Telecommunications	Bassel AL AYOUBI	General Manager of Investment and Maintenance
OMSAR	Ihab CHAABAN	ICT Security Officer
Banque du Liban	Ali NAHLE	Director of IT
Special Investigation Commission	Nasser LEBBOS	Director of IT at the Banque du Liban
High Council for Privatization	Maya CHAMLI	Project Manager
Telecommunications Regulatory Authority	Said HAIDAR	Approval ,Quality and Standards Manager
Ministry of Economy and Trade	Dr. Linda KASSEM	Legal expert

Support of the European delegation in Beirut

Administration	Name	Title
European Commission	Jérôme Ribault Gaillard	Counter-Terrorism Expert

List of additional members and voluntary participants

Administration	Name	Title
Presidency of the Council of Ministers	Ahmad AL KHATIB	Head of Informatics Department
Army Command Ministry of National Defense	Ahmad AL HAJJ CHEHADE	Lieutenant Engineer, Intelligence Directorate
	President Carl IRANI	Advisor to the Minister of Defense
General Directorate of Internal Security	Brigadier General Ahmad AL HAJJAR	Commander of the Institute of Internal Security Forces
General Directorate of Public Security	Dr. Jihad FAHS	Major –Engineer
General Directorate of Personal Status	George BECHARA	National ID Platform
Ministry of Telecommunications	Nabil SHEIKH	Engineer
OMSAR	Joe HAGE	Advisor to the Minister
Banque du Liban	Zeina AOUN	Information Systems and Cyber Security Expert
	Hubert BAZ	Administrative
Lebanese University-Faculty of Engineering	Dr. Lina OUEIDAT	Academic Collaboration Master's degree Cyber Security-Habib El Amin Coordination
	Habib AL AMIN	
Saint Joseph University-ESIB	Dr. Maroun CHAMOUN	
	Tony FEGHALI Potech - Berytech	
Lebanese University Faculty of Law	Pr. Mona AL ACHKAR JABBOUR	Volunteer experts
	Dr. Bilal ABDALLAH	
ECS sarl	Darwiche CHEHADE	
	Mounif OUEIDAT	

Official Correspondence

LEBANESE REPUBLIC
President of the Council of Ministers

4/10/2018

No: 1637

H. E. Christina Lassen
Head of Delegation the European Commission
Charles Malek Avenue
Aschrafieh

Subject: **National Cyber Security Strategy for Lebanon**
Appointment of a National Focal point
Establishment of a National Commission
Project: **Cyber Crime initiative funded by the EU**

Dear Ambassador Lassen,

Reference is made to the initiatives conducted by the European Delegation and to the joint effort conducted by the Prime Minister the General Secretary of the High Council of Defense, and the EU delegation representative, and to our meeting of the 21st of Sept,

We believe, however that much work remains to be done, and that we must continue to collaborate with the various levels,

And due to the urgency of the matter, I would like to propose Dr. Lina OUEIDAT (National ICT Coordinator) to assume the responsibilities of the National Focal Point of the Commission.

Dr. Lina OUEIDAT supported the General Secretary of the High Council of Defense to issue the Roadmap for the Preparation of the **"National Cyber Security Strategy and the Fight against Cybercrime"**, and she will be the **Rapporteur Member** of the National team composed of representatives of Ministries and concerned public and private agencies.

You will find joined to this letter:
- The Road Map for the establishment of a national Security Strategy
- The nomination of Dr. Lina Oueidat as an advisor and National ICT Coordinator
- The resolution of the National Cyber Security Strategy Team

Saad Hariri

REPUBLIQUE LIBANAISE
Président du Conseil des Ministres

No: 1638 4/10/2018

S.E. Christina Lassen
Chef de la Délégation Européenne au Liban
Avenue Charles Malek
Aschrafieh

Sujet :: **préparation de la stratégie nationale de cyber sécurité et pour la lutte contre la cybercriminalité**
Mission d'experts niveau décideurs
Project: **EU Cyber Crime initiative**

Chère Ambassadeur Lassen

En référence aux visites engagées par la Délégation Européenne et particulièrement aux dialogues engagés depuis Octobre 2017 avec le Secrétariat General de la Défense, et à la visite du Secrétaire General Hamad avec des hauts fonctionnaires en France en Avril 2018,

Nous avons le plaisir de vous informer que cette collaboration a conduit à l'élaboration par Dr.Lina OUEIDAT de la Feuille de route et à l'établissement de la Commission Nationale qui doit établir la Stratégie Nationale pour la Cyber Sécurité, et pour la lutte contre la cybercriminalité pour le Liban

Et en vue de l'élaboration du cadre stratégique de la future politique publique en matière de cyber sécurité, et continuation des efforts entrepris, nous soutenons la sollicitation du Haut Conseil de Défense auprès de la Commission Européenne pour organiser à Beyrouth dans une prochaine étape une mission d'expertise (niveau décideurs) d'un Etat membre de l'UE de préférence la France pour cette mission afin de permettre un échange avec les services du Premier Ministre et les parties prenantes des administrations concernées ,sur les enjeux d'un modèle organisationnel et d'une doctrine pouvant inspirer le Liban.

La préférence de la France plus particulièrement pour cette mission a pour objectif de poursuivre le dialogue déjà entrepris sur l'aspect organisationnel au sein de la Présidence du Conseil des ministres vu la similitude des lois cadres relatives aux institutions administratives des deux pays.

Il serait opportun de joindre cette mission d'expertise à la mission en cours de préparation avec Cyber South le 16 novembre 2018, sur la convention de Budapest au Grand Sérail

Nous souhaitons également le support des services de l'ambassade de France pour aider à l'organisation de cette mission spécifique et nous vous serions gré de les informer par vos propres soins.

REPUBLIQUE LIBANAISE
Président du Conseil des Ministres

Vous trouvez ci-joint également la résolution de l'établissement du comite (no. 173/2018) et la nomination de Dr. Lina OUEIDAT Conseiller du Premier Ministre (no. 172/2018) qui est à votre disposition pour la coordination de tous ces efforts

Saad Hariri

cc : Mr. Bruno Foucher Ambassadeur de France à Beyrouth

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

DIRECTORATE GENERAL
HUMAN RIGHTS AND RULE OF LAW

INFORMATION SOCIETY - ACTION AGAINST CRIME
DIRECTORATE

THE DIRECTOR

Ref ► DGI/JK/AS/VS/MAW/le195

Prime Minister of Lebanon
His Excellency Saad HARIRI
Grand Sérail
Rue des Capuchins
Beirut

Strasbourg, 26 October 2018

Dear Prime Minister,

The Council of Europe welcomes the intention of the Government of Lebanon to develop a National Cyber Security Strategy.

We are prepared to support this effort and suggest holding meetings on 15 and 16 November in Beirut.

The meeting on 15 November would permit the sharing of good practices between the National Commission of Lebanon responsible for the establishment of the cybersecurity strategy and international experts.

The meeting on 16 November would be aimed at discussing the benefits of the Budapest Convention on Cybercrime for Lebanon with members of the National Commission and representatives of other relevant Ministries.

Both events would be supported under the joint project CyberSouth of the Council of Europe and the European Union.

Should this proposal find your approval, I would suggest that your authorities contact Ms Marie AGHA-WEVELSIEP, project manager of CyberSouth (marie.agha-wevelsiep@coe.int, +40 21 201 78 09; + 40 744 673 826) for further information and practical arrangements.

Yours sincerely,

Jan Kleijssen

COUNCIL OF EUROPE
F-67075 Strasbourg Cedex
Tel ► +33 (0)3 88 41 21 16
Fax ► +33 (0)3 88 41 37 39
Mail ► jan.kleijssen@coe.int
Site ► www.coe.int/justice
www.coe.int

الجمهورية اللبنانية
رئاسة مجلس الوزراء

قرار رقم ١٧٢ / ٢٠١٨ ق

تشكيل فريق وطني لوضع خطة لمواجهة مخاطر جرائم المعلوماتية واعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني

ان رئيس مجلس الوزراء،

بناء على المرسوم رقم ٢ تاريخ ٢٠١٦/١٢/١٨ (تسمية السيد سعد الحريري رئيساً لمجلس الوزراء)،

بناء لضرورات المصلحة العامة،

يقرر ما يأتي :

المادة الاولى : يشكل فريق وطني لوضع خطة لمواجهة مخاطر جرائم المعلوماتية واعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني قوامها السادة :

– أمين عام المجلس الأعلى للدفاع	رئيساً
– ممثل عن رئاسة الجمهورية	عضواً
– ممثل عن مجلس النواب	عضواً
– ممثل عن وزارة العدل	عضواً
– ممثل عن وزارة المالية	عضواً
– ممثل عن قيادة الجيش – وزارة الدفاع الوطني	عضواً
– ممثل عن المديرية العامة لقوى الامن الداخلي	عضواً
– ممثل عن المديرية العامة للامن العام	عضواً
– ممثل عن المديرية العامة لامن الدولة	عضواً
– ممثل عن المديرية العامة للاحوال الشخصية – وزارة الداخلية والبلديات	عضواً
– ممثل عن وزارة الاتصالات	عضواً
– ممثل عن مكتب وزير الدولة لشؤون التنمية الادارية	عضواً
– ممثل عن مصرف لبنان	عضواً
– ممثل عن المجلس الاعلى للخصخصة	عضواً
– الدكتورة لينا عويدات المنسق الوطني لتكنولوجيا المعلومات والاتصالات	عضواً مقرراً

تتم تسمية الاعضاء من قبل الوزير المختص ورؤساء الادارات المعنية

المادة الثانية : تكون مهمة الفريق:

- وضع خطة لمواجهة مخاطر جرائم المعلوماتية واعداد استراتيجية وطنية لمأسسة عمل الامن السيبراني.
- اجراء تقييم للمخاطر والتهديدات فيما يخص الاعداد للاستراتيجية الوطنية للامن السيبراني ومكافحة جرائم المعلوماتية واقتراح الاولويات والخطط والمشاريع اللازمة.
- اعداد استراتيجية عمل الامن السيبراني وفقاً لخارطة الطريق المعدة من قبل الامانة العامة للمجلس الاعلى للدفاع بالتنسيق مع مفوضية الاتحاد الاوروبي في لبنان.
- اقتراح آلية المأسسة لتنفيذ هذه الاستراتيجية.

المادة الثالثة : يمكن للفريق الاستعانة بمن يراه مناسباً لتأدية مهامه.

المادة الرابعة : على الفريق المذكور ان يرفع الى رئيس مجلس الوزراء تقريراً دورياً كل شهر على ان يرفع تقريره النهائي خلال مهلة ستة أشهر اعتباراً من تاريخ صدور هذا القرار.

المادة الخامسة : يبلغ هذا القرار حيث تدعو الحاجة.

بيروت ، في : ٢٠١٨/ ٩/٢٦

رئيس مجلس الوزراء

سعد الحريري

الجمهورية اللبنانية
رئاسة مجلس الوزراء

قرار رقم ١٧٢ / ٢٠١٨

تكليف الدكتورة لينا عويدات مستشار رئيس مجلس الوزراء لشؤون المعلوماتية القيام بمهام منسق وطني لتكنولوجيا المعلومات والاتصالات

ان رئيس مجلس الوزراء،

بناء على المرسوم رقم ٢ تاريخ ٢٠١٦/١٢/١٨ (تسمية السيد سعد الحريري رئيساً لمجلس الوزراء)،

بناء على عقد اتفاق رقم ٢٨/أ تاريخ ٢٠١٧/٢/٢٥ فيما بين الدولة اللبنانية ممثلة بدولة رئيس مجلس الوزراء والدكتورة لينا عويدات للقيام بمهام مستشار رئيس مجلس الوزراء لشؤون المعلوماتية،

يقرر ما يأتي :

المادة الاولى : تكلف الدكتورة لينا عويدات مستشار رئيس مجلس الوزراء لشؤون المعلوماتية القيام بمهام منسق وطني لتكنولوجيا المعلومات والاتصالات.

المادة الثانية : يبلغ هذا القرار حيث تدعو الحاجة.

بيروت ، في : ٢٠١٨/٩/٢٦

رئيس مجلس الوزراء

سعد الحريري

Roadmap for the Preparation of the National Cybersecurity Strategy and the Fight Against Cybercrime

Document presented on September 13, 2018 to the European delegation in Beirut.

Objectives

Nations are faced with the obligation to go digital due to the rapid development of information and communication technologies (ICTs). The development of computer services, internet communications services and digital applications presents security challenges that require the State and its institutions to develop a national strategy to combat the different types of cyber threats and attacks whether internal or external.

The standardization and multiplication of administrative electronic services and the development of technologies connecting directly State institutions and citizens present the risk of allowing unauthorized and potentially malicious entities to gain access to State information systems. To alleviate these problems, which are bound to increase in number and complexity, particularly with the rapid development of technology, it is incumbent on the State to implement, for its civilian and security organs, a strategic defense plan against these threats while reflecting on the institutionalization of this work to ensure its sustainability in accordance with a clear vision and structure. The most important axes of this strategy are:

1. **Defense, deterrence and reinforcement** against threats from inside and outside.
2. **The continuous development** of State capacities to support the development of information and communication technologies. Indeed, the State has an obligation to protect itself against various electronic threats, to be able to withstand and mitigate the effects of attacks, and to be resilient in the rapid recovery of its functions. It must ensure the quality, integrity, and reliability of its data especially when embarking on a rapid transformation to digital. Lebanon is lagging in these areas and has not put in place the legal, administrative and technical measures related to e-government. Transformation to digital is a difficult and risky task in the absence of a national strategy for data security and cybersecurity.
3. **Increase the level of computerization in public administrations** through validated and systematized automation processes and methodologies carried out in parallel between and within administrations, in accordance with the evolution of the needs of the public sector and the expectations of the public authorities and citizens.

4. **Promotion of the role of the security and intelligence services** and strengthening the mutual cooperation and coordination with the support and supervision of the higher authorities (Presidency of the Council of Ministers and its associated bodies), in particular the General Secretariat of the Higher Defense Council under the authority of the Prime Minister ...

5. **Development of human resources, tools, technological components and their use**, in partnership with the IT sector in public and private institutions, universities and associations concerned by this field, selected after a reliability survey.

6. **The institutionalization of the centralization of data security activities within the Presidency of the Council of Ministers**. Indeed, ensuring electronic security at the national level requires the centralization of means of surveillance, exchanges of experience and information, technical support, the capitalization of skills, technological monitoring of developments in this field, and the fight against such challenges and terrorism, as well as organized crime and its ramifications.

Note: The majority of countries have institutionalized their strategies at the national level and as part of government action. The condition for success is a high level of coordination among the different state agencies.

In the absence of an administrative development strategy and what follows from it, Lebanon finds itself relegated to the rank of the countries most lagging in terms of cybersecurity according to the International Telecommunication Union (ITU) of which Lebanon is a member and holding the rank 119 among 165 countries surveyed.

Considering that the General Secretariat of the Higher Defense Council, which reports directly to the Prime Minister, has worked tirelessly to raise the level of awareness in the field of cybersecurity,

Considering that the European Commission has presented a methodology for developing the cybersecurity plan and has expressed its willingness to assist the Lebanese State in this area, provided that the relationship between the Commission and the State is a centralized relationship in order to avoid fragmentation of efforts, and that the state is ready to express accurately its needs, and that to this end, the state proposes a unified road map, built on a clear strategy, as well as an executive device to implement this strategy accompanied by a well-defined financing plan and guaranteed results,

Considering that the European Commission has already drawn up guidelines to support this vision of development for the benefit of military, security and judicial institutions, and is ready to mobilize the necessary expertise of the Member States in favor of an initiative centrally presented by the Lebanese State in this regard,

Considering that the Prime Minister and the General Secretariat of the Council of Ministers are in the process of drafting a plan for the modernization of the General Directorate of the Presidency of the Council of Ministers with the aim of transforming it into a state-of-the-art institution at the national level through the implementation of a gradual plan of automation of its functions. This plan also provides for a modernization of the management structure, particularly through the implementation of advanced computer technologies that necessarily take into account the security dimension through the centralization and securing of data,

As a result of multiple working meetings, we agreed on the definition of a preliminary roadmap that includes the establishment of the National Commission against Cybercrime and for the Strengthening of Cybersecurity, that will be tasked with the preparation of a National Strategy for Cybersecurity and the fight against cybercrime and whose missions shall be:

1. Development of a national strategy for the defense, deterrence and reinforcement against cyber-attacks and cybercrime.
2. Participation in the preparation of the administrative structure of the national institution to be placed under the authority of the Presidency of the Council of Ministers and which will take charge of the implementation of the National Cybersecurity Strategy in its various components, and in a way that is not incompatible with the ongoing project of modernization of the Presidency of the Council of Ministers, especially in relation to information and communication technologies.
3. Invitation of the various administrations and public sector organizations, military and civilian, who are involved in this endeavor to each appoint a representative to the National Commission to ensure the broadest participation of all stakeholders as well as the adherence to the Commission's guidelines on this subject which has become a full-fledged business sector given the multiplicity and complexity of tasks, techniques and procedures as well as the rapid development it is witnessing. The required expertise of that person and the type of administrative activity that (s)he is called upon to carry out will be determined in the general plan.

The participants in the commission:

- Presidency of the Republic
- Presidency of the Chamber of Deputies
- Presidency of the Council of Minister – National Coordinator of Information and Communications Technology
- General Secretariat of the High Defense Council
- Ministry of Finance
- Ministry of Defense – Army Command – Intelligence Directorate
- Ministry of Interior and Municipalities – General Directorate of General Security – Internal Security Forces
- General Directorate of State Security
- Ministry of Telecommunications (General directorates - Ogero)
- Bank of Lebanon - banking sector – Special Investigation Commission
- Higher Council for Privatization

The commission will be assisted by representatives of the following administrations:

- Ministry of Foreign Affairs and Immigrants
- Ministry of Economy and Trade
- Ministry of Industry
- Economic and Social Council
- Telecommunications Regulatory Authority
- Office of the Minister of State for Administrative Reform
- Ministry of Education and Higher Education
- Lebanese University
- Other institutions and bodies

Work group

For the Lebanese State

Major General Saadallah Al Hamad	Secretary General of the Higher Defense Council
Brigadier General engineer Wajdi Chamseddine	General Secretariat of the Higher Defense Council
Brigadier General Tony Kahwaji	Head of the Intelligence -Technical Branch
Judge Hania Al Helweh	Ministry of Justice
Dr. Lina Oueidat	Advisor to the Prime Minister for Information and Communication Technologies - National ICT Coordinator

For the European Union

Mr. Jérôme Ribault-Gaillard	Counter -Terrorism Expert