STRATÉGIE NATIONALE LIBANAISE DE CYBERSÉCURITÉ

Vers l'an 2022

"Le Liban veut créer un cyberespace plus sûr et stable, tant sur le territoire national que dans les échanges internationaux"

الجمهورية اللبنانية
رئاسة مجلس الوزراء

2019

Table des Matières

Préface du Premier Ministre 4
Avant-propos 6
PARTIE I. STRATÉGIE NATIONALE LIBANAISE DE CYBERSÉCURITÉ 7
1. Le contexte stratégique du Liban 8
1.1 Actions réalisées 11
1.2 Menaces 13
1.3 Tendance des menaces 15
1.4 Défis 16
2. L'État responsable de la cybersécurité 20
2.1 L'État 20
2.2 Les entreprises et les organisations 21
2.3 Les particuliers: citoyens, professionnels et consommateurs 21
3. Piliers de la Stratégie Nationale de Cybersécurité 22
3.1 Défendre, dissuader et renforcer contre les menaces 23
3.2 Développer la coopération internationale en Cybersécurité 28
3.3 Renforcement des capacités de l'État à soutenir le développement des TIC 29
3.4 Promotion de la capacité éducative sur tout le territoire libanais 29
3.5 Promotion des capacités industrielles et techniques 32
3.6 Soutenir les entreprises de cybersécurité à l'international 33
3.7 Renforcer la collaboration entre les secteurs public et privé 34
3.8 Rôle des organismes chargés de l'application de la loi 35
4. Objectifs 37
PARTIE II. INSTITUTIONNALISATION – L'AGENCE NATIONALE DE LA CYBERSÉCURITÉ ET DES SYSTÈMES D'INFORMATION (NCSIA) 41
5. L'Institutionnalisation d'une Agence Nationale pour la Cybersécurité 42
5.1 Le mandat de la NCISA au niveau national 43
5.2 La NCISA et le public: des particuliers aux entreprises 44
5.3 L'implication de la NCISA dans la qualification et le suivi des produits 45
5.4 La NCISA face aux cybermenaces 45
5.5 La NCISA et la protection des OIV 46

5.6 L'Agence dans le cadre normatif et son écosystème 47
6. Conclusion 49
ACRONYMES 51
GLOSSAIRE 52
ANNEXES 59

Préface du Premier Ministre

Dans un monde globalisé de plus en plus connecté, nous assistons de nos jours à une croissance fulgurante de l'outil numérique, générateur d'opportunités et de prospérité, mais également menace potentielle pour notre sécurité. En effet, les cyberattaques sont de plus en plus fréquentes et sophistiquées, ce qui constitue pour notre pays un vrai défi : comment devenir résilients face aux risques liés au cyberespace tout en laissant aux usagers la liberté d'utiliser un espace sûr et digne de confiance? Mais aussi, comment mettre en place cette confiance ? Confiance dans l'usage qui serait fait des données personnelles et plus particulièrement des données sensibles. Confiance dans les systèmes qui les produisent, les hébergent ou les diffusent. Ultimement, confiance dans tous les acteurs, entreprises, partenaires, fournisseurs, services publics, États dont l'existence numérique a un impact bien réel sur la vie de nos concitoyens.

Il n'y a pas de transformation numérique sans confiance et il ne pourrait y avoir de confiance sans cybersécurité.

Une stratégie en cybersécurité se présente donc comme une priorité évidente d'autant plus que le Liban est signataire de l'Appel de Paris[1] et qu'il reste déterminer à sécuriser son cyberespace dans le cadre d'une coopération avec tous ses partenaires internationaux.

Lors de la préparation de cette Stratégie, nous avons mis un accent particulier sur l'application d'un processus ouvert et interministériel de manière à impliquer les parties prenantes des différents secteurs publics, et notamment les services de sécurité et le pôle judiciaire. Ainsi, un Comité National a vu le jour grâce à la résolution 173, sous la direction du Secrétariat Général du Conseil Supérieur de la Défense et la résolution 172 a permis de nommer un Coordinateur National pour la Cybersécurité, tous relevant de l'autorité du Premier Ministre. Le Comité a participé activement et intensivement à des ateliers et conférences, à des visites d'exploration organisées par la délégation de l'Union

[1] Le 12 novembre 2018, à l'occasion de la réunion à l'UNESCO du Forum de gouvernance de l'Internet (FGI), le Président de la République, Emmanuel Macron, a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace. Cette déclaration de haut niveau en faveur de l'élaboration de principes communs de sécurisation du cyberespace a déjà reçu l'appui de 552 soutiens, parmi lesquels 66 États, 347 entités du secteur privé et 139 organisations internationales et de la société civile.

Européenne au Liban, à des missions d'experts européens : en outre, il a mis en œuvre une collaboration académique avec l'Université Libanaise et l'Université Saint-Joseph, démontrant qu'il existe un grand intérêt pour trouver des solutions communes. J'exprime ma gratitude à tous ceux qui ont contribué à ce processus.

Ces travaux ont mené à une certitude et nous ont montré la voie à suivre : la création et l'institutionnalisation d'une Agence au niveau national, placée sous l'autorité de la Présidence du Conseil des Ministres et rattachée au Secrétariat Général du Conseil Supérieur de la Défense, paraît indispensable. L'Agence sera l'autorité en matière de sécurité des systèmes d'information et dans la lutte contre la Cybercriminalité. Elle sera également garante de notre protection face aux cyberattaques en mettant en œuvre notre stratégie sur tout le territoire national et contribuera ainsi à maintenir notre souveraineté numérique.

Mais cette entreprise serait vaine si nous ne menions pas en même temps un effort conséquent pour éveiller la conscience de nos concitoyens sur les risques au quotidien de l'usage des outils numériques et si nous n'encourageons pas la formation professionnelle des acteurs qui seront en charge de protéger la nation dans le cyberespace.

Mon projet est ambitieux : garantir un minimum de sécurité pour nos compatriotes et pour le bon fonctionnement de notre démocratie et faire en sorte que cette stratégie soit portée collectivement par tous les acteurs du Liban dans le cadre d'un effort aux niveaux national et international.

Il est nécessaire aujourd'hui de développer une vaste coopération entre les pouvoirs publics, le secteur privé et la société civile. Je lance donc un appel à toute la nation pour que tous les acteurs participent à cet effort collectif et pour que la mise en application de cette stratégie soit efficace et bénéfique aux intérêts de notre Pays.

Saad Hariri

PREMIER MINISTRE

Avant-propos

L'ambition de la création d'Internet était à l'origine de disposer d'un outil au service de l'humanité dans le cadre d'une plateforme libre d'accès pour un partage universel des informations et des connaissances qui s'affranchisse des frontières géographiques traditionnelles. Si cet objectif a été atteint, il faut reconnaître que l'évolution des technologies numériques a provoqué également une augmentation des risques liés à cet espace. Le cyberespace constitue en effet un lieu virtuel d'expression du pouvoir et de la force, de tensions culturelles, politiques, militaires, économiques. En tant que tel, il est en perpétuelle évolution au niveau de la construction des relations internationales actuelles.

De nos jours, notre vie quotidienne, nos interactions sociales et nos économies dépendent de la fiabilité, de la transparence et de la sécurisation des technologies de l'information et de la communication. Or, il s'avère que le Liban, à l'instar de tous les autres États, est confronté à de nombreuses menaces dans le cyberespace (cybercriminalité, espionnage, sabotage, chantage ou encore utilisation frauduleuse ou à outrance de données personnelles), ce qui porte atteinte à la confiance et à la sécurité dans le cyberespace.

Dans ce contexte, la responsabilité première de l'État Libanais est donc d'apporter des solutions en matière de cybersécurité face aux défis actuels et futurs, et de créer un cyberespace ouvert et libre, respectueux de la démocratie, mais en même temps protégé, pour apporter confiance au secteur public, au secteur privé et aux citoyens. De ce constat est née l'exigence de créer, en 2018, un Comité National dont l'objectif a été de mettre en place une Stratégie Nationale de Cybersécurité. La Stratégie que nous présentons ici est le fruit de ce travail collectif intense et constitue la pierre angulaire de la sécurité nationale dans notre société appelée à devenir toujours plus numérisée et doit, par conséquent, être au service du bien commun de tous les acteurs de la société libanaise.

C'est une approche audacieuse et ambitieuse que le Liban s'est fixée pour réguler son cyberespace, ayant pour objectif de mettre l'humain au centre de ses responsabilités et devant passer par une prise de conscience et un effort collectif national dans l'esprit d'une plus forte coopération à l'international.

PARTIE I.
STRATÉGIE NATIONALE LIBANAISE DE CYBERSÉCURITÉ

1. Le contexte stratégique du Liban

Le Liban se trouve au cœur de tous les progrès technologiques auxquels nous assistons actuellement. En s'appuyant sur une numérisation modeste et peu sûre, le pays est exposé à des perturbations qui affectent sa sécurité et la vie privée de ses citoyens.

De plus, l'absence d'une stratégie unifiée et claire en matière de cybersécurité entre les différents organismes du secteur public et les organisations privées rend difficile la défense et la prévention de telles attaques. **Compte tenu des vulnérabilités, des violations de données et de toutes les différentes attaques subies par certaines entités libanaises, notamment en 2018, et de la facilité avec laquelle les agresseurs ont pu accéder à différentes entités des secteurs public et privé**, le besoin de cybersécurité au Liban est devenue une vraie urgence, tout comme l'exigence de lutter contre les comportements malveillants dans le cyberespace et de maintenir un niveau élevé de sécurité des données et d'intégrité du système.

Malgré les timides tentatives de certaines institutions et entités pour sécuriser leurs données et leurs systèmes, les initiatives mises en œuvre dans le pays étaient largement insuffisantes pour atteindre l'objectif souhaité. Ces efforts doivent donc être intégrés dans une approche collaborative, suivant une stratégie bien définie pour mieux se défendre contre les attaques et lutter contre la cybercriminalité. Les efforts actuels dans le domaine de la cybersécurité au Liban, sans une vraie coordination, ne donnent pas les résultats escomptés. Voici quelques-unes des raisons qui expliquent la situation actuelle:

- **L'absence d'une stratégie nationale unifiée en matière de cybersécurité**: chaque institution, tant du secteur privé que du secteur public, a sa propre vision et ses procédures en matière de sécurité, qui peuvent être efficaces dans leur situation courante, mais rendent plus difficile la collaboration sans critères bien définis et, plus important encore, le partage d'informations et un cadre commun au plus haut niveau.
- **L'absence de lois et de réglementations régissant la cybercriminalité**: le Liban n'a pas de lois et de réglementations protégeant les institutions gouvernementales, les entreprises privées et les droits des individus dans le domaine numérique, et ne définit pas clairement les actes criminels. De plus, les conséquences et les implications de ces actes criminels ne sont pas claires.
- **L'absence d'une Agence Nationale de Cybersécurité**: le Liban ne possède aucune agence de cybersécurité qui applique et fasse respecter les lois relatives à la cybersécurité, ou qui collabore avec des personnes possédant l'expertise nécessaire pour aider les organisations à configurer leurs cadres de sécurité. De plus, le pays souffre également d'un manque d'offre au niveau des formations, ainsi que d'un

soutien inexistant à la recherche et au développement. De même, aucun organisme n'assure la continuité des programmes de sensibilisation à la cybersécurité.

- **La lutte contre la corruption dans l'économie numérique**: en 2018, le Liban a maintenu son rang élevé parmi les pays corrompus, une situation qui sévit depuis le début des années 1990 et qui peut être attribuée aux conséquences de la guerre civile. En effet, une génération entière a grandi dans une société sans structure ni ordre. Au lieu de restaurer la culture libanaise traditionnelle d'avant-guerre fondée sur l'intégrité, le respect et la compétence, cette génération est sortie du conflit en affirmant son besoin de compensation après des années de privations.

  La corruption et l'économie numérique sont diamétralement opposées, la corruption étant la principale menace contre la mise en œuvre de la cybersécurité, alors que l'économie numérique peut potentiellement détruire ou au mieux perturber les schémas de corruption habituels.

  Les agents corrompus peuvent être impliqués dans des cyberattaques actives ou passives, directes ou indirectes, internes ou externes, destinées à désactiver les services fournis par l'infrastructure de l'économie numérique nationale. Leur objectif pourrait être d'alléguer l'inefficacité des services numériques fournis afin de se rabattre sur les opérations manuelles précédentes, sous lesquelles les schémas de corruption ne pouvaient pas être tracés.

- **Le contexte sociodémographique aux multiples facettes**: la Constitution libanaise repose sur une démocratie qui préserve l'équité des droits entre ses multiples communautés religieuses. Le pluralisme est un élément unique et distinctif de la nation et pourrait être utilisée pour déstabiliser tous les domaines de la vie publique et démocratique. En conséquence, la coopération, le partage des moyens et l'utilisation de qualifications appropriées peuvent être entravés si les multiples entités qui composent la société libanaise se tournent vers l'isolationnisme et l'individualisme, ce qui priverait la nation des compétences nécessaires au bon fonctionnement de la société et affecterait la résilience globale construite sur la collaboration entre les acteurs.

  Pour éviter cela, des directives obligatoires concernant la cybersécurité devraient être édictées, à savoir que les personnes nommées à des postes de responsabilité devraient posséder une expertise ou être tenues d'obtenir une certification dans le domaine d'activité correspondant.

  Les cyberattaques ressemblent à un virus infectant l'organe d'un corps vivant. S'il n'est pas soigné ou traité de manière adéquate, il mettra tout le corps en danger et pourra se propager à d'autres individus afin de contaminer et éventuellement décimer une population entière.

Pour arrêter la propagation d'une telle menace, qui pourrait s'étendre potentiellement à l'ensemble de la nation, il faudra prendre des mesures coordonnées et globales, en associant toutes les parties prenantes concernées, à l'aide d'une expertise fiable et d'un large éventail d'outils de lutte contre cette forme de criminalité.

En résumé, l'État doit veiller à ce que les personnes désignées pour la mise en œuvre de la stratégie de cybersécurité soient compétentes, fiables, expérimentées, responsables de la défense de l'intérêt commun et de la promotion du bien commun, et motivées par un sens aigu du patriotisme.

- **Le manque de collaboration entre les administrations au niveau national**: chaque institution travaille sur sa sécurité séparément, sans un cadre clair pour la collaboration avec d'autres institutions, alors que le partage d'informations et de données profiterait à chaque entité. En outre, il existe un manque de collaboration et de coopération entre les différents départements de la même institution, en particulier dans le domaine de la sécurité. Chaque département et chaque unité agissent et travaillent de manière indépendante au lieu de coopérer pour sécuriser l'ensemble de l'organisation ou de l'institution auxquelles ils appartiennent.
- **L'absence de participation active du secteur privé au développement du secteur public**: le secteur public n'a pas de rôle réglementaire ni d'outil de sensibilisation. Il compte donc sur le secteur privé pour pallier le manque d'expérience et de capacité de développement concernant ses départements et ses postes informatiques. C'est pourquoi, le secteur public a eu recours à des sociétés privées pour sécuriser et fournir des services informatiques et de cybersécurité. Il est important que le secteur public sous-traite de tels services. Cependant, le secteur public libanais est sorti affaibli de cette expérience : les rapports montrent que le secteur privé n'a pas réussi à gérer correctement ou adéquatement le transfert de ces projets informatiques au secteur public, et que ce dernier n'en a pas tiré les bénéfices escomptés. Ce point devrait être abordé à l'avenir dans tout partenariat étatique avec le secteur privé et/ou dans le cadre d'une coopération internationale afin de garantir des résultats constructifs.
- **L'absence d'initiative pour un système national d'information et une stratégie de transformation numérique au plus haut niveau**: malgré tous les efforts déployés de façon indépendante ou par l'intermédiaire d'OMSAR dans le cadre de projets d'e-gouvernement et de numérisation depuis 1995 dans les différents ministères, le Liban est toujours dépourvu d'une vision nationale avec une approche interinstitutionnelle coopérative. Il existe un déséquilibre évident et important entre les institutions ; en outre, la gestion coordonnée des technologies de l'information et de la communication (TIC) n'est pas institutionnalisée au plus haut niveau, ce qui rend très difficile la détection, l'identification et la gestion des cyberincidents. Dans un tel environnement, l'efficacité de la cybersécurité et de la

cyberdéfense pour protéger les citoyens et les organisations publiques ou privées ciblés par les cyberattaques est gravement compromise.

- **La pénurie d'experts en cybersécurité et leur difficulté d'adaptation aux changements rapides**: les organes administratifs, les entreprises et les universités du Liban ont un grand besoin de sensibilisation en termes de cybersécurité en s'appuyant sur leurs programmes éducatifs à tous les niveaux (universités, emplois, conférences, ...). En outre, ces acteurs doivent être prêts à réagir à l'évolution rapide de la nature des cybercrimes et des méthodes utilisées. Malheureusement, les formations en cybersécurité sont limitées à certains domaines dans les organisations éducatives, les communautés, et dans les universités avec leurs programmes respectifs. Par conséquent, les étudiants ont tendance à rechercher une approche auto-éducative dans ce domaine et ne bénéficient pas de cursus et de programmes de formation appropriés. Une mise en place de programmes ciblés fournirait donc les ressources humaines nécessaires pour irriguer tous les secteurs libanais exposés à la cybercriminalité ayant de plus en plus besoin de talents.

  Le Liban et ses institutions sont exposés aux menaces et aux cybercrimes, comme tout autre pays. La cybersécurité au Liban n'est pas bien structurée au niveau national et manque de coopération et de coordination entre les organisations des secteurs public et privé et au niveau international pour répondre aux besoins fondamentaux de ses citoyens en matière de sécurité et de confidentialité.

  Aujourd'hui, de nombreuses institutions libanaises fournissent des services en ligne à divers clients, qui deviennent ainsi dépendants d'Internet. Cependant, l'utilisation d'Internet n'est pas sécurisée et les utilisateurs seront toujours exposés aux tentatives d'attaques cybernétiques. Bien que ce risque ne puisse pas être complètement éliminé, il peut être considérablement réduit en limitant la surface des attaques et leur propagation à un niveau acceptable pour permettre à la société de continuer à prospérer et de tirer parti des énormes possibilités offertes par la technologie numérique.

1.1 Actions réalisées

L'année 2006 a vu la création du Bureau de la Police Judiciaire des Forces de Sécurité Intérieure (FSI) chargé de la cybercriminalité. Sous le contrôle des autorités judiciaires, il avait pour mission d'enquêter sur les plaintes, les infractions à la cybersécurité et celles liées à la technologie. Il devait également sensibiliser le public et les établissements d'enseignement sur les dernières cybermenaces et cyberattaques.

D'autres services de sécurité et de renseignement ont beaucoup travaillé pour renforcer leurs capacités d'enquête afin de prévenir les menaces à la sécurité nationale, notamment les cyberattaques et le cyberespionnage.

En 2010, le Premier ministre libanais a mis en place un Comité national composé de représentants des principales agences gouvernementales et de sécurité. Ce comité avait essentiellement pour fonction d'élaborer une stratégie nationale de cybersécurité et de lutte contre la cybercriminalité. Neuf ans après cette décision, la croissance rapide et l'évolution constante de l'industrie des technologies, les approches et les bonnes pratiques en matière de cybersécurité ainsi que la prolifération des techniques d'attaque et de défense rendent ce sujet particulièrement critique et de plus en plus compliqué à traiter.

Il est nécessaire de donner forme à la stratégie nationale de cybersécurité afin de définir les mesures efficaces à prendre par le Comité national mentionné ci-dessus.

D'un point de vue pratique et opérationnel, par rapport à l'approche de 2010, la stratégie doit désormais se concentrer sur l'exigence que la cybersécurité devienne une priorité obligatoire, juridiquement contraignante et exécutoire pour l'ensemble des infrastructures du système d'information libanais. De même, la stratégie doit renforcer les capacités de notre pays en matière de cyberdéfense contre les nombreux comportements malveillants et répréhensibles, les cybercrimes et les cyberattaques. Elle doit également faire ressortir la structure d'un organe centralisé placé sous l'autorité de la présidence du Conseil des ministres, qui sera responsable de la mise en œuvre des éléments de cette stratégie.

En 2018, le Parlement libanais a ratifié la loi n° 81, intitulée « Loi sur les transactions électroniques », qui contient un chapitre sur la conservation des preuves électroniques.

Certaines universités libanaises ont restructuré leurs programmes et ouvert des programmes de master en cybersécurité et en sciences criminalistiques numériques.

Le Liban a également coopéré avec d'autres pays avancés en TIC et avec des organisations internationales dans le domaine de la cybersécurité.

Une stratégie de transformation numérique au niveau de l'État est en cours d'élaboration sous la supervision d'OMSAR.

En 2018 et 2019, le ministère de la Justice a formé une vingtaine de juges sur la manière de faire face à la cybercriminalité dans le cadre du projet « CyberSud », organisé par le Conseil de l'Europe. Cela ne suffit pas et le ministère de la Justice doit aborder la question au plus haut niveau.

Le ministère des Télécommunications joue un rôle majeur dans le déploiement d'une bonne infrastructure grâce à une collaboration intensive avec des opérateurs privés et OGERO, et il aborde régulièrement les problèmes de cybersécurité avec tous les acteurs du pays. Il a mis en place des efforts de coordination avec l'Union Internationale des Télécommunications (UIT) pour améliorer l'indice de cybersécurité au Liban.

La Banque du Liban (BDL) a développé et mis en œuvre, dans une approche d'amélioration continue, un programme de cybersécurité avancé, innovant et basé sur des

standards qui lui permet d'anticiper et de contrer les cyberattaques. Ce programme suit en permanence les dernières pratiques et normes mondiales en matière de sécurité informatique et est composé de deux piliers principaux:

- La partie Gouvernance de la sécurité et conformité: ce pilier contient la définition et la mise à jour de la feuille de route de sécurité informatique de la BDL, l'élaboration et le suivi des politiques de sécurité informatique, l'évaluation et la gestion proactives des risques, ainsi que le lancement et l'évaluation du programme « Sensibilisation à la Sécurité ».
- L'approche de sécurité Defense-in-Depth: cette partie est composée de solutions de sécurité multi-couches et multi-technologiques, couvrant l'infrastructure de sécurité du réseau et des terminaux, le renseignement de sécurité des applications et les opérations de sécurité avancées et intelligentes.

De nombreuses organisations libanaises dans les secteurs public et privé ont été témoins et font toujours face à un taux élevé et alarmant de cyberattaques qui ciblent principalement leurs sites Web et les mettent hors service. D'autres types d'attaques ont abouti à la divulgation et à la publication de certains dossiers personnels de citoyens libanais.

1.2 Menaces

Les cyberactivités malveillantes sont conçues pour compromettre la confidentialité, l'intégrité et la disponibilité des réseaux, des systèmes informatiques et des informations.

Les cyberactivités malveillantes présentent certaines caractéristiques communes: elles n'ont pas de frontières; elles ne peuvent pas être facilement attribuées; pour finir, elles ne nécessitent pas forcément d'énormes budgets et/ou de hautes compétences techniques. En outre, différents acteurs peuvent être à l'origine de ces menaces, consciemment ou inconsciemment, ce qui rend encore plus difficile leur détection, leur identification et leur gestion.

Les principales menaces peuvent être classées comme suit, en fonction des lanceurs et des auteurs de l'attaque:

- **Les crimes liés à la cyberdépendance**, lorsque les dispositifs informatiques peuvent constituer à la fois l'outil principal pour commettre le crime et la principale cible du crime lui-même. Les exemples les plus pertinents sont le développement et la propagation de logiciels malveillants à des fins financières ; le piratage informatique pour voler des données sensibles; DDoS; rançongiciel et chantage; l'endommagement, l'altération et la destruction de données. L'argent est généralement le principal objectif de ces menaces.
- ***Cyber-enabled crimes*** **(crimes cyberactivés)**, lorsque les ordinateurs sont utilisés pour commettre des crimes traditionnels. Les principales activités sont la

fraude, le vol de données, l'espionnage, les vols, l'extorsion, la propagande ou la destruction via le cyberespace.

Ces cybercrimes peuvent émaner d'autres pays et régions, mais également de l'intérieur du pays, et cherchent généralement à obtenir de l'argent ou des données pour les utiliser à d'autres fins malhonnêtes.

- **Menaces d'État ou lancées par des États** : lorsque des États étrangers ou des entités parrainées par ces derniers tentent de pénétrer dans le cyberespace, de percer un réseau public ou privé ou des fichiers sensibles sur le Cloud. Le but est d'obtenir un avantage politique, diplomatique, militaire, technologique, commercial, financier et stratégique. En particulier, ces activités ciblent les infrastructures sensibles d'un pays, telles que la défense, les finances, l'énergie, la santé, les services publics et les télécommunications.

  Les activités principales incluent le développement de capacités d'opérations de cyberespionnage et de destruction plutôt que l'utilisation de techniques standard.

- **Menaces terroristes** : lorsque des organisations terroristes utilisent Internet pour effectuer les tâches suivantes:

  - publicité et propagande;
  - recrutement et mobilisation;
  - collecte de fonds;
  - mise en réseau sécurisée; partage d'informations crypté ou anonyme;
  - formation à distance;
  - planification et coordination;
  - revendication de la responsabilité des attaques, démontrant ainsi leurs capacités en technique d'intimidation;
  - utilisation d'Internet avec des compétences constamment améliorées, en saturant les cibles.

  Les groupes terroristes aspirent constamment à la conduite d'activités cybernétiques dommageables contre le Liban.

- **Menaces hacktivistes**, où les activités ont principalement un but perturbateur et criminel pour les victimes. Ces acteurs utilisent Internet avec les mêmes objectifs que les organisations terroristes.

- **Menaces internes** : elles constituent un risque permanent. Elles sont commises par des utilisateurs malveillants, qui sont généralement des employés « de confiance » d'une organisation, pouvant avoir accès à des systèmes et à des données sensibles. Ces menaces peuvent causer des dommages financiers et nuire à la réputation à travers le vol de données sensibles et de propriété intellectuelle. Elles peuvent également constituer une menace cybernétique destructive si elles

utilisent des connaissances ou des accès privilégiés pour faciliter ou lancer une attaque. Cela perturbe par exemple les services essentiels sur le réseau des organisations où ces personnes travaillent, pouvant même aboutir à l'effacement des données du réseau.

Certaines menaces internes peuvent être victimes d'ingénierie sociale et causer ainsi des dommages non intentionnels.

- ***Script kiddies*** : il s'agit d'acteurs inexpérimentés utilisant des scripts ou des outils développés par d'autres personnes - et/ou téléchargés à partir d'Internet - pour mener des cyberattaques. Ils ont généralement accès à des tutoriels, des ressources et des outils de piratage disponibles sur Internet et téléchargeables à partir de sources ouvertes et publiques.
- **Attaque de réseau informatique** : des acteurs hostiles peuvent utiliser un logiciel malveillant (ou malware) pour perturber et endommager la cyber-infrastructure. Cela peut aller de la mise hors ligne d'un site Web à la manipulation de systèmes de commande et de contrôle de processus industriels.

1.3 Tendance des menaces

Le développement continu et rapide des technologies de l'information et de la communication, la mondialisation, l'augmentation considérable des volumes de données et le nombre croissant de divers appareils et équipements connectés aux réseaux de données ont eu un impact considérable sur la vie quotidienne, l'économie et le fonctionnement de l'État. En outre, Internet devient de plus en plus accessible, le nombre d'utilisateurs ne cesse de croître et de nouveaux services et solutions technologiques, tels que l'Internet des objets (IoT), l'Internet des objets industriels (IIoT) et le Cloud se multiplient. Tout cela aboutit à un spectre de menaces plus large et à une multiplication des vecteurs d'attaque, qui sont de plus en plus complexes, sophistiqués et qui causent d'avantage de dégâts en cas de succès.

Le nombre d'acteurs étatiques impliqués dans le cyberespace et engagés dans des activités de cyberespionnage ciblant des ordinateurs connectés à Internet ainsi que des réseaux fermés continue de croître. Cette réalité est due au fait que la collecte d'informations sur la sécurité nationale ainsi que sur les atouts économiques représente une ressource importante sur la scène régionale et internationale. Le nombre et le dynamisme des nations capables de mener des cyberattaques parrainées par les États augmentent, créant des menaces et des risques critiques inconnus et inattendus au Liban.

Au-delà du dynamisme des acteurs étatiques, il existe des individus et des groupes à motivation politique disposant de moyens financiers limités mais ayant une capacité croissante d'organiser leurs activités en utilisant les réseaux sociaux et pouvant mener des attaques par déni de service ou autres.

En outre, la diffusion et la mise en œuvre récente de normes de chiffrement par des institutions gouvernementales et des entreprises privées - telles que les protocoles SSL ou SSH, pour ne citer que quelques exemples - ont révélé un effet secondaire inattendu: elles ont provoqué une détection en temps réel, une analyse post incidents, une défense et des enquêtes fort complexes. Dans certaines circonstances et architectures TIC spécifiques, telles que les centres de données très importants et complexes, il devient presque impossible de réussir avec succès une détection en temps réel.

De nos jours, de tels scénarios permettent à différents auteurs de menaces d'exfiltrer massivement des informations sensibles et critiques en utilisant les mêmes protocoles de cryptage que les victimes utilisent pour améliorer leur cybersécurité. Très souvent, les solutions de détection et de protection des données précédemment utilisées, telles que la prévention des fuites de données (DLP), échouent : cela élargit généralement la «fenêtre d'attaque» de façon considérable et aboutit à des violations de données de plus en plus longues et durables, alors que jusque là les violations étaient plus courtes et non détectées. L'évolution rapide du profil et des capacités des criminels rend le traçage et l'attribution de l'attaque considérablement plus complexes.

1.4 Défis

Les principaux risques en matière de cybersécurité découlent de la dépendance croissante de l'État, de l'économie et de la population libanaises à l'égard des infrastructures TIC et des services électroniques.

La cybercriminalité compromet le fonctionnement de l'espace économique et réduit la confiance dans les services numériques. Par conséquent, un personnel compétent et des outils techniques modernes sont nécessaires pour assurer la prévention, la détection et la poursuite des cybercrimes. L'échange d'informations opérationnelles entre les pays devient de plus en plus important dans la lutte contre la cybercriminalité.

Afin de prévenir et de dissuader les futures menaces pour la sécurité, il est nécessaire de développer en permanence le savoir-faire lié à la cybersécurité et d'investir dans des infrastructures et des solutions technologiques.

L'un des principaux défis consiste à mettre en place un cadre juridique moderne et à renforcer les moyens des organismes chargés de l'application de la loi2 afin de fournir une nouvelle approche mixte à la fois juridique et technique, la plus complète possible. Le but principal est de cibler clairement les responsabilités pénales tout au long des phases de

[2] Par "organismes chargés de l'application de la loi" on entend dans le présent document: l'Armée, les forces de Sécurité Intérieure, la Sûreté Générale, la Sécurité de l'État.

l'enquête, tout en mettant en œuvre des actions et des mesures pour lutter efficacement contre la cybercriminalité.

Ce nouveau cadre juridique devra inclure des processus hiérarchisés; la partie la plus importante sera l'application par défaut de la science d'investigation numérique, le respect obligatoire des bonnes pratiques et le concept logique de la «chaîne de traçabilité» au sein de toutes les preuves numériques possibles. Les éléments cités doivent ensuite être utilisés dans la gestion des scènes de crime et en fonction de divers ca de figure possibles, tels que: la médecine légale, l'analyse judiciaire et ses sous-domaines l'analyse de réseau, l'analyse GPS, l'analyse de cloud computing, l'analyse de criminalistique mobile, l'analyse des drones, l'analyse liée à l'automatisation industrielle, l'analyse de l'audiovisuel et l'analyse de l'infraction. L'objectif général de ces aspects techniques du nouveau cadre juridique est de toujours préserver les preuves numériques des scènes de crime, qu'elles soient classiques ou basées sur les TIC.

Au niveau national, il est possible d'utiliser les capacités et le savoir-faire du secteur bancaire en matière de mesures de cybersécurité et de cyberdéfense. Au niveau international, il est impératif de renforcer les relations du Liban avec des partenaires de confiance et de développer de nouveaux réseaux de coopération avec d'autres pays afin d'améliorer l'économie libanaise et de partager ses intérêts sécuritaires. Les menaces étant globales, la défense doit l'être aussi, via une coopération étroite avec les organisations professionnelles internationales. Aucun pays n'est capable de gérer seul les cybermenaces. La coopération internationale est obligatoire conformément aux dispositions légales libanaises.

Le gouvernement devrait être en mesure de relever le niveau de cybersécurité dans tout le pays et d'appliquer des mesures de sécurité appropriées pour que les particuliers, les organisations et les entreprises adaptent leurs comportements aux structures de sécurité requises afin de fonctionner en toute sécurité sur Internet.

D'un point de vue technique, la cybercriminalité et les cyberattaques en général se nourrissent de l'évolution de la technologie et de l'absence d'une stratégie de cybersécurité appropriée et de sa mise en œuvre factuelle. En particulier, nous pouvons identifier cinq défis principaux qui pourraient représenter une menace concrète s'ils ne sont pas gérés correctement:

- Une gamme croissante de périphériques ciblés

  L'Internet des objets (IoT) et l'internet des objets industriels (IIoT) créent de nouvelles possibilités d'exploitation et accroissent l'impact potentiel d'attaques susceptibles de causer des dommages à la fois physiques ou virtuels, voire létaux. L'implantation rapide de la connectivité dans les processus de contrôle industriels et dans les systèmes sensibles d'un large éventail d'industries telles que l'énergie, les mines, l'agriculture et l'aviation, a créé l'Internet des objets industriels. Ce processus ouvre les possibilités de créer des appareils et des opérations

industrielles et non industrielles, autrefois non vulnérables à de telles interférences, qui peuvent être piratés et altérés avec des conséquences potentiellement désastreuses.

- Mauvaise cyberhygiène et faible conformité

  Ces deux éléments dépendent à la fois des solutions techniques et des mises en œuvre adéquates et peuvent être traités. Cependant, ils comptent aussi beaucoup sur la sensibilisation culturelle. En fait, sans une compréhension adéquate de l'importance du concept de cyberhygiène, aucune solution de défense ni le respect des normes existantes ou à venir en matière de cybersécurité ne seraient suffisants.

  Si la prise de conscience n'est pas suffisamment construite, maintenue et nourrie au niveau le plus large possible, à travers toutes les institutions publiques et privées du pays et avec les particuliers, le Liban et toutes ses infrastructures ne seront jamais à l'abri des menaces. La liste des faits et des scénarios ci-dessous donne une idée des risques possibles et de leurs conséquences si le gouvernement, au niveau de ses institutions publiques et privées, ne prend pas pleinement conscience de la gravité des ces menaces:

  - 99% des attaques basées sur l'exploit ne seront toujours pas basées sur des vulnérabilités 0-Day. Cela signifie par exemple que si les citoyens ne comprennent pas l'importance d'actions de sécurité très simples telles que «Windows Update» et s'ils ne les appliquent pas correctement et régulièrement, leurs ordinateurs seront toujours exposés à des attaques de masse qui exploiteront les vulnérabilités connues et publiques;
  - Les réseaux domestiques utilisés pour le télétravail exposeront les entreprises à des risques de sécurité de type BYOD/PAP: l'employé travaillant à domicile doit comprendre l'importance des bonnes pratiques de base, telles que la modification du mot de passe par défaut sur son routeur domestique, plutôt que toujours utiliser des VPN pour se connecter à distance à son bureau;
  - Les cas de sextorsion vont augmenter considérablement;
  - Le déficit grandissant de compétences et le nombre réduit d'experts formés pour assumer des rôles en matière de sécurité. Ce manque de ressources humaines se traduira par des tests incorrects, des audits et une certification non conformes en matière de cybersécurité dans différents environnements et scénarios.

- Formation et compétences insuffisantes

  Le manque de cybercompétences est une vulnérabilité nationale qui doit être résolue. Il y a des lacunes dans les éléments suivants:

- Compétences et connaissances nécessaires en matière de cybersécurité dans les secteurs public et privé;
- Campagnes de sensibilisation et formations agrées par l'État en cybersécurité pour tous les employés du secteur public, qui traitent, sous quelque forme que ce soit, avec les systèmes informatiques;
- Formations pratiques et simulations sur la mise en œuvre effective des mesures et techniques de défense en matière de cybersécurité.

- Systèmes hérités et non corrigés

  - Utiliser des systèmes hérités vulnérables sans versions mises à jour signifie avoir des systèmes non corrigés qui rendent des réseaux entiers vulnérables aux attaques menant à des violations massives de données, permettant aux attaquants de voler des milliers, voire des millions de données personnelles et professionnelles;
  - L'utilisation de logiciels non pris en charge pour lesquels il n'existe plus de mises à jour et de correctifs augmente le niveau de vulnérabilité que les attaquants pourraient utiliser pour réussir leurs opérations criminelles.

- Disponibilité de ressources de piratage

  - Les informations et les outils de piratage largement disponibles sur Internet permettent aux hackeurs d'accéder à des connaissances et à un savoir-faire pouvant être utilisés à des fins criminelles. C'est quelque chose qui ne peut être combattu, car Internet est intrinsèquement conçu pour le partage d'informations de toute nature, légales ou non.
  - La disponibilité de telles informations et des ressources de piratage ne peut pas être considérée comme un crime (ce qui explique que ces données ne peuvent pas être mises sur liste noire), car la plupart du temps, ces savoir-faire, outils et guides de procédures sont (ou prétendent être) destinés à favoriser la connaissance des tests de sécurité et de cybersécurité, même si, dans certains cas, ils peuvent être utilisés comme savoir-faire offensif.

La seule solution pour contrer toutes les menaces et les cyberattaques susmentionnées consiste à créer un système national capable d'orchestrer une réponse coordonnée, dans un cadre juridique et technique unifié.

2. L'État responsable de la cybersécurité

La sécurisation du cyberespace national nécessitera un effort collectif et multidimensionnel (humain et technique), qui implique l'engagement de tous les acteurs de la société libanaise. En cybersécurité, les principaux acteurs impliqués sont:

- L'État;
- Les entreprises et les organisations;
- Les individus, en tant que citoyens, scolaires, actifs, retraités et consommateurs.

Dans un monde numérique en rapide évolution, le Liban doit déployer tous ses efforts pour tenter d'adopter les bonnes pratiques en matière de cybersécurité, condition essentielle de la sauvegarde et de la préservation de notre souveraineté numérique.

Le monde numérique est en constante évolution, croissance et mutation. Il est donc primordial que le Liban se positionne au plus haut niveau des meilleures pratiques. Le pays doit être à la pointe de ces évolutions pour ne pas subir les cybermenaces. Comme tout État, le Liban est vulnérable aux attaques dans le cyberspace et doit donc renforcer sa sécurité pour préserver l'exercice de sa souveraineté dans le domaine numérique.

2.1 L'État

Le principal devoir du gouvernement est de défendre le pays des attaques d'autres États et d'acteurs non étatiques, de protéger ses citoyens et son économie et de définir le cadre national et international nécessaires pour protéger les intérêts nationaux, les droits fondamentaux et traduire les criminels en justice.

En tant qu'important détenteur de données et fournisseur de services, l'État prend des mesures strictes pour protéger ses informations. Il a également la responsabilité essentielle de conseiller et d'informer les citoyens et les organisations sur ce qu'ils doivent faire pour se protéger en ligne et, le cas échéant, définir les normes attendues des entreprises et organisations clés. Les secteurs essentiels de l'économie libanaise relèvent du secteur privé, le plus important étant le secteur bancaire. Toutefois, s'agissant de la cybersécurité et de la lutte contre la cybercriminalité, la responsabilité ultime de la résilience et du maintien des services et fonctions essentiels incombe à l'État, dans le cadre d'une collaboration bien gérée et équilibrée avec les organismes chargés de l'application des lois, le ministère des Télécommunications, les organismes de réglementation du secteur bancaire et toutes les autres institutions gouvernementales, chacune dans sa juridiction, ainsi que d'autres partenaires nationaux et internationaux.

2.2 Les entreprises et les organisations

Les organisations des secteurs public et privé et d'autres institutions possèdent des données personnelles, fournissent des services et exploitent des systèmes dans le domaine numérique. La connectivité des systèmes d'information contenant des données et des services a révolutionné leurs opérations. Cependant, avec cette transformation technologique, l'une de leurs principales responsabilités consiste à protéger les informations qu'ils détiennent, à maintenir les services qu'ils fournissent et à intégrer le niveau de sécurité approprié aux produits qu'ils vendent.

Les citoyens, les consommateurs et la société en général comptent sur les entreprises et les organisations pour prendre toutes les mesures nécessaires afin de protéger leurs données personnelles. Les entreprises et les organisations doivent comprendre qu'elles opèrent dans un environnement qui les tiendra responsables des conséquences et des impacts indirects des cyberattaques dont elles pourraient éventuellement être victimes.

2.3 Les particuliers: citoyens, professionnels et consommateurs

Aujourd'hui, les contextes national et international exigent que des biens de valeur soient sécurisés, non seulement dans le monde réel, mais également dans le monde numérique et virtuel. Puisque dans ce dernier tout est connecté et interdépendant, il est essentiel que chaque individu assume sa responsabilité et que chacun prenne toutes les mesures nécessaires pour protéger son matériel numérique - téléphones intelligents, tablettes, ordinateurs portables - ainsi que les données, les logiciels et les systèmes garantissant la liberté, la flexibilité et la commodité dont tout le monde devrait jouir dans sa vie privée et professionnelle.

3. Piliers de la Stratégie Nationale de Cybersécurité

Compte tenu des réalités évoquées ci-dessus, de la situation actuelle du Liban et des défis à venir, le gouvernement devrait engager toutes ses institutions dans la mise en œuvre d'une stratégie globale qui se fixe pour objectif de fournir un cyberespace plus sûr et de sensibiliser davantage les principaux acteurs de la société libanaise.

Le gouvernement libanais est conscient de l'extrême dépendance de la nouvelle économie à l'égard d'Internet, tant du point de vue public que privé. En ce sens, l'exposition à la sécurité crée des niveaux de risque importants et provoquera toujours des tentatives de cyberattaques.

Le chemin que doit suivre le Liban pour accomplir chacune des étapes identifiées et analysées ci-dessus est assez difficile. Il faudra déployer beaucoup d'efforts, à commencer par mobiliser la volonté politique nécessaire pour créer les conditions législatives et techniques au profit de la cybersécurité, en s'appuyant sur des ressources humaines dédiées et hautement spécialisées.

Une fois que cette approche totalement nouvelle sera lancée, la stratégie nécessitera au moins deux à quatre années complètes pour être mise en œuvre. Sans prétendre pouvoir éliminer complètement les menaces que la stratégie nationale de cybersécurité vise à contrecarrer, **il est très important de préciser qu'il faut prendre toutes les mesures possibles pour réduire les risques et atteindre un niveau de sécurité acceptable**. Le Liban doit permettre aux entreprises et aux citoyens de continuer à prospérer et de tirer parti des énormes possibilités offertes par le numérique.

Une stratégie de cybersécurité élaborée par un gouvernement et représentant ainsi tout un pays, avec des impacts et des améliorations à l'échelle nationale, doit prévoir des objectifs clairs et des actions continues et à long terme.

Alors que le Liban se prépare à élaborer et à lancer une stratégie nationale de cybersécurité, il est essentiel d'identifier et de détailler les principaux piliers sur lesquels doit reposer la stratégie à venir. Ce n'est qu'en identifiant clairement et en hiérarchisant ces piliers fondamentaux que l'élaboration d'une stratégie et sa mise en œuvre opérationnelle peuvent par conséquent être envisagées et réalisées.

Compte tenu de ce qui précède, la cyberstratégie nationale reposera sur les axes stratégiques fondamentaux suivants, qu'on appellera « piliers »:

1. **Défendre, dissuader et se renforcer contre les menaces internes et externes.**

2. **Développer la coopération internationale dans le domaine de la cybersécurité.**
3. **Accroître continuellement la capacité de l'État à soutenir le développement des technologies de l'information et de la communication.**
4. **Promouvoir la capacité éducative sur le territoire libanais.**
5. **Promouvoir les capacités industrielle et technique.**
6. **Soutenir les entreprises de cybersécurité à l'international.**
7. **Renforcer la collaboration entre les secteurs public et privé.**
8. **Promouvoir le rôle des services de sécurité et de renseignement et renforcer la coopération et la coordination mutuelles avec l'appui et la supervision des autorités supérieures.**

Ce n'est que lorsque les piliers ci-dessus seront reconnus et pris en compte que nous pourrons commencer à développer une stratégie de cybersécurité avec des objectifs clairs.

3.1 Défendre, dissuader et renforcer contre les menaces

L'État libanais doit mettre en place une stratégie de dissuasion afin de réduire considérablement le nombre de cybercrimes. Une stratégie de dissuasion dans le cyberespace fait référence à un ensemble d'actions conçues pour intercepter les attaquants lors de leurs premières opérations malveillantes sur le réseau, en partant du principe qu'après avoir obtenu l'accès à un réseau, les attaquants suivent toujours une chaîne de frappe prévisible.

La chaîne de frappe (Cyber Kill Chain) est répartie en huit phases: reconnaissance, intrusion, exploitation, élévation des privilèges, mouvement latéral, camouflage, déni de service et exfiltration.

Au cours de la phase de reconnaissance, le hackeur va découvrir passivement le réseau afin de rassembler toutes les informations nécessaires. Il est absolument vital de mettre en œuvre les technologies et les outils de dissuasion appropriés afin de rediriger les actions des attaquants de manière contrôlée, de manière à ce que les défenseurs puissent les gérer facilement.

La phase d'intrusion est ensuite lancée en fonction des informations découvertes lors de la phase de reconnaissance. L'objectif est d'entrer dans le système et d'accéder aux données qu'il contient.

La phase d'exploitation utilise une attaque active, dans laquelle le pirate informatique utilise différents types de vulnérabilités identifiées sur les victimes ciblées afin de les exploiter rapidement, en obtenant un accès distant ou local, en tant qu'utilisateur ou administrateur ordinaire.

Les attaquants utilisent ensuite la technique d'élévation des privilèges pour obtenir un accès accru aux ressources.

La phase de mouvement latéral vise à permettre un accès non autorisé aux serveurs internes et aux données stockées. Parfois, cet accès peut également permettre aux hackeurs d'étendre leurs actions offensives à des tiers externes, par exemple des ressources numériques physiquement ou logiquement situées en dehors du périmètre du réseau de la victime.

Après cette étape, le camouflage est utilisé pour masquer l'activité et éviter toute analyse légale.

La phase de déni de service empêche ensuite le suivi ou le blocage de l'attaque en perturbant l'activité normale des utilisateurs et des serveurs.

La dernière phase, l'exfiltration, représente l'objectif réel et le plus important des attaquants, en particulier lorsqu'il s'agit des plus expérimentés et des plus compétents d'entre eux. Son objectif est de transférer à distance différentes informations et données à l'aide de différentes techniques d'exfiltration, allant du simple au très complexe, et utilisant souvent des infrastructures de réseau dédiées.

Une fois que le Liban se sera conformé aux normes de base de la cybersécurité et qu'il aura appliqué cette stratégie, le gouvernement et l'Agence Nationale de Cybersécurité et des Systèmes d'Information (NCSIA) seront en mesure d'évaluer les vulnérabilités et d'alerter avec des recommandations sur les mesures préventives contre les principales conséquences. Ils pourront également identifier les menaces, réagir promptement et efficacement aux attaques et maintenir le cyberenvironnement libanais en sécurité. Un certain nombre d'outils et de technologies peuvent être utilisés pour créer un cadre fonctionnel de cyberdissuasion. Avant de les mettre en œuvre, toutefois, il est impératif de développer des capacités techniques et judiciaires spécifiques à la défense.

La dissuasion dans le cyberespace implique deux éléments: les capacités de défense et les capacités de réaction offensive. Les premières constituent ici la cyberdéfense, c'est-à-dire la protection des systèmes d'information essentiels d'un État et leur aptitude à résister à des attaques constantes et variées.

L'action contre-offensive représente alors la *cyberdissuasion*. Cette composante de la dissuasion est basée sur la menace de représailles aux conséquences intolérables dans le cyberespace, destinée à convaincre un adversaire de ne pas attaquer dès le départ.

Le développement des capacités défensives doit suivre le plan d'action ci-dessous:

- Créer un modèle de cyberdéfense libanais actif, qui doit inclure les bonnes pratiques et incorporer des actions techniques de haut niveau. Parmi les actions à mettre en œuvre : des blocs, des filtres, des listes noires et blanches, contrôler les mises au point, les attaques basées sur des programmes malveillants, les

infrastructures d'exploitation et d'attaques 0-Day, l'usurpation de courrier électronique, les services de réputation IP.

- Utiliser des sources d'informations de sécurité fiables et bien connues pour remplir les informations nécessaires à la création d'une base de données de e-réputation des ressources dans le cyberespace, permettant ainsi un meilleur contrôle et un meilleur filtrage du contenu et des menaces potentiellement malveillants et dangereux. L'utilisation des normes et des bonnes pratiques internationales en matière de cybersécurité permettra au modèle de cybersécurité libanais non seulement d'être complet mais également de bénéficier de la vaste expertise des organismes de normalisation internationaux.
- Classer les données et définir les infrastructures sensibles, jetant ainsi les bases d'un environnement national numérique plus sécurisé, dans une perspective de défense proactive. Cela devrait aller de pair avec la protection des institutions gouvernementales et des autres secteurs prioritaires, en tenant compte des dernières normes en matière de cybersécurité et des bonnes pratiques en matière de cybersécurité, telles que la mise à niveau des dernières versions des logiciels, l'application de correctifs aux clients, ou encore la recherche des vulnérabilités connues (la liste n'est pas exhaustive).
- Changer le comportement du public et des entreprises, en s'assurant que les organisations individuelles, quelle que soit leur taille, prennent les mesures appropriées pour se protéger.
- Gérer les incidents et comprendre les menaces d'un point de vue opérationnel, national, géopolitique et technique, en matière de sécurité nationale, permettant de mieux contrôler les risques de sécurité en combinant réactivité et proactivité, afin de réduire le risque d'exposition au cyber-risque. En parallèle, concevoir, construire et exécuter des solutions de sécurité multicouches innovantes, permettant d'anticiper les attaques avancées.
- Faire des systèmes informatiques libanais une cible plus dure pour les cybercriminels, en réduisant les avantages pour les pirates (dissuasion par interdiction) et en augmentant les coûts (dissuasion par représailles). Il est donc nécessaire de pouvoir identifier les intérêts et les objectifs de l'agresseur potentiel, mais également de disposer de capacités suffisamment crédibles et persuasives.
- Veiller à ce que les capacités nationales et l'intention de réagir de l'État soient clairement comprises afin d'influencer et de décourager la prise de décision d'agresseurs potentiels.
- Éliminer les opportunités faciles d'utilisation pour les attaquants qui veulent compromettre les réseaux et les systèmes informatiques libanais. Le gouvernement disposera des outils et des capacités nécessaires pour mener à bien les tâches

suivantes: refuser aux attaquants la possibilité de compromettre les réseaux et les systèmes libanais; comprendre les intentions et les capacités des attaquants; surmonter les menaces de logiciels malveillants de base à grande échelle; réagir et protéger la nation dans le cyberespace.

- Empêcher la population d'être attirée par la cybercriminalité ou de s'y impliquer en renforçant les mesures d'intervention précoce.
- Établir un plan d'action systématisé et assimilé qui puisse préparer des options avancées pour réagir à une cyberattaque, afin que les autorités puissent réagir à une crise lorsqu'elle se produit. La réaction aux cybermenaces et aux cyberattaques doit devenir une doctrine d'action automatique. Cette doctrine sera fondée sur l'interprétation par le Liban de l'application du droit international en vigueur dans le cyberespace. En fait, le pays ne peut pas décider de réagir de manière autonome à une cyberattaque ou de considérer une cyberattaque en réponse naturelle à une cybercrise, sans tenir compte des lois et réglementations internationales en vigueur.
- Intégrer les normes juridiques internationales dans le système de classification national des cyberattaques. L'intégration des principes nationaux et internationaux relatifs à la cybersécurité est l'élément essentiel d'une doctrine d'action, et constitue également un outil de soutien important pour les autorités afin de prendre des décisions plus efficaces et de constituer un moyen pertinent de soutenir la coopération internationale.
- Renforcer les capacités et l'expertise du pays en matière d'application de la loi aux niveaux national, régional et local afin d'identifier et de dissuader les cybercriminels au Liban et à l'étranger.
- Améliorer les capacités de souveraineté numérique du Liban en utilisant des centres de données physiquement présents sur le territoire national. La perspective de la souveraineté numérique sur les données doit conduire à la mise en place de solutions juridiques et techniques. De plus, la maîtrise des technologies clés est essentielle à l'exercice de notre souveraineté numérique. Les technologies clés incluent, entre autres, le cryptage des communications et la détection des cyberattaques et des radios mobiles professionnelles.
- Adopter un cadre de certification pour les produits de sécurité de haut niveau. Le cadre de certification actuel est mal adapté à l'évaluation de produits couramment utilisés, tels que les objets connectés, pour lesquels les coûts et les délais sont prohibitifs. Pour cette raison, il est recommandé d'introduire une certification de base en cyber sécurité sur les produits, en plus du cadre de certification existant. Ce dernier pourrait s'appuyer sur des systèmes existants dans des contextes autres que la cybersécurité, tels que le marquage CE requis pour la commercialisation de certains biens et services en Europe. Cette certification de base en cybersécurité

doit impliquer une analyse de la conformité et des bonnes pratiques en matière de cybersécurité, sur la base de critères prédéfinis. Il sera placé sous le contrôle d'un organisme privé, avec la collaboration des autorités publiques (limitée aux actions indirectes), telles que les entités d'évaluation de l'accréditation en cybersécurité agréées par l'Agence Nationale de Cybersécurité et des Systèmes d'Information.

- Renforcer la lutte contre la cybercriminalité grâce à la détection avancée des outils criminels. Cela pourra se faire en augmentant les compétences et le nombre de personnes travaillant sur le terrain et en améliorant les spécifications des produits. Il faudra notamment former les différentes parties prenantes, telles que les juges, les procureurs ou les employés de banque ; fournir également une assistance juridique aux victimes de la cybercriminalité; mettre en place des moyens de dissuasion contre les agresseurs et les délinquants; organiser des formations en cybersécurité à l'intention des forces de l'ordre; et enfin, mettre à jour régulièrement les lois et les procédures en fonction de l'évolution des technologies de l'information et de la communication.

Dans des circonstances spécifiques, comme dans le cadre d'une attaque en cours, la stratégie pourrait passer d'un état d'esprit opérationnel axé uniquement sur la défense à un état offensif. Dans ce cas, les actions suivantes doivent être entreprises:

- Poursuivre les auteurs d'infractions cybercriminelles. Le gouvernement - à travers la NCISA - doit dissuader ceux qui voudraient nuire aux intérêts de la nation. Pour y parvenir, des efforts doivent constamment être faits pour préciser que toute tentative de cyberattaque contre la Nation, que ce soit pour voler ou pour nuire, n'est ni facile ni rentable. Le gouvernement - à travers l'activité de la NCISA - devrait être en mesure d'identifier les attaquants et d'agir contre eux, en utilisant la réponse la plus appropriée parmi un ensemble d'outils disponibles. Les services répressifs doivent se concentrer sur les criminels qui persistent à attaquer les citoyens et les entreprises libanais : les hackeurs doivent savoir qu'ils ne peuvent pas agir en toute impunité. Les autorités nationales devraient coopérer avec les partenaires internationaux pour cibler les criminels où qu'ils se trouvent et pour démanteler leurs infrastructures et leurs réseaux. Les services répressifs continueront également à contribuer à la sensibilisation et à la normalisation en matière de cybersécurité, en étroite collaboration avec la NCISA.

- Renforcer l'efficacité de la réponse judiciaire pour améliorer la lutte contre la cybercriminalité, afin de pouvoir identifier, si nécessaire, les acteurs à l'origine d'une cyberattaque. Pour pouvoir atteindre un objectif aussi complexe, il est indispensable de disposer des moyens légaux, ainsi que des capacités techniques, de l'expertise, des infrastructures dédiées et des outils ad-hoc.

- Renforcer l'efficacité des organismes chargés de l'application de la loi pour exécuter correctement le protocole d'attribution d'une cyberattaque. Les

autorisations pour déployer un tel ensemble d'actions devront être divulguées avec prudence à des institutions gouvernementales spécifiques, en fonction de la nature de l'action. En fait, les contre-attaques et les opérations invasives faisant appel à des données personnelles pourraient créer de graves problèmes de confidentialité qui devront être gérés correctement au plus haut niveau de l'État.

- Développer un réseau international de collaboration entre juges et enquêteurs, et mettre en place également des formations et des programmes éducatifs dédiés dans les entités nationales et internationales existantes situées sur le territoire libanais.

3.2 Développer la coopération internationale en Cybersécurité

Pour renforcer les effets positifs de la mise en œuvre de la stratégie nationale de cybersécurité, il est impératif que le Liban travaille en étroite collaboration avec d'autres acteurs régionaux et internationaux. Les actions suivantes sont particulièrement recommandées:

- Travailler de façon structurée et continue avec des partenaires internationaux, tels qu'INTERPOL, les organisations des Nations Unies (UIT, UNODC, UNICRI, …), la Délégation Européenne au Liban et les autres institutions et agences européennes (Conseil de l'Europe, EUROPOL, CEPOL, ENISA, …), ainsi que les instituts internationaux de normalisation (NIST, EBIOS, …) et les équipes d'intervention au niveau régional et international.

- Utiliser les réseaux existants et les relations avec les principaux partenaires internationaux du gouvernement et créer de nouveaux liens avec d'autres entités internationales afin de partager des informations sur les menaces actuelles et naissantes, en ajoutant de la valeur aux idées et aux compétences existantes.

- Établir des relations bilatérales stratégiques et des canaux de dialogue ouverts avec les principales parties prenantes afin de partager des informations sur des incidents potentiels.

- Construire des partenariats internationaux pour mettre fin à l'impunité perçue des cybercriminels agissant contre le Liban en traduisant en justice les criminels des pays d'outre-mer.

- Coopérer avec la communauté internationale sur les questions relatives au cyberespace afin d'harmoniser et d'accroître l'efficacité d'un ensemble de lois et de réglementations. Cela permettra au gouvernement libanais d'optimiser le calendrier, les procédures et les coûts, établissant ou adaptant ainsi des mécanismes communs de gestion de crise, de communication et de désescalade. Le Liban doit continuer à œuvrer pour l'universalisation de certaines normes appliquées dans le cyberespace en vue de renforcer sa sécurité. Cette approche devrait reposer sur trois principes:

- La *prévention*: l'incertitude inhérente à l'attribution d'une attaque devrait inciter les États à concentrer leurs efforts sur les mesures préventives;
- La *coopération*: le renforcement de la coopération au sein de la communauté internationale sur les questions relatives au cyberespace constitue un moyen efficace d'accroître la stabilité grâce à une meilleure compréhension mutuelle et aussi à la confiance entre les parties prenantes. Cela créera également des mécanismes communs de gestion de crise, de communication et de désescalade. Le Liban doit œuvrer en faveur de la conclusion d'un accord international sur les obligations des États dont les infrastructures pourraient être utilisées à des fins malveillantes, telles que des "tremplins" pour attaquer par procuration d'autres pays ("triangulation" d'une cyberattaque).
- La *stabilité*: le pays doit continuer à promouvoir le principe de l'existence de certains droits permettant aux États victimes d'attaques informatiques de prendre les mesures appropriées tout en maintenant la paix et la sécurité internationales.

3.3 Renforcement des capacités de l'État à soutenir le développement des TIC

L'État doit mettre en place un programme de sensibilisation et de formation qui prépare ses fonctionnaires des secteurs de l'informatique et des TIC, ainsi que ses citoyens et professionnels, aux bonnes pratiques en matière d'utilisation numérique. C'est en prenant conscience des cyber-risques et en étant formés à adopter le comportement approprié que les utilisateurs seront en mesure de faire face aux cybermenaces. Que ce soit dans le cadre d'une utilisation privée (jeunes exposés, en particulier, à un contenu inapproprié ou au harcèlement et à la malveillance sur le Web) ou de pratiques professionnelles (administrations et entreprises), les citoyens éduqués et sensibilisés constituent la première barrière de protection de l'information. Les formations à la cybersécurité doivent donc être envisagées dans le cadre de la stratégie nationale pour faire en sorte que les décideurs d'aujourd'hui et de demain soient conscients des risques et sachent faire face aux menaces. Dans ce contexte, il semble essentiel que l'État promeuve la recherche et ses capacités industrielles, améliore les capacités de défense du secteur public et engage le secteur public dans un dialogue avec le secteur privé impliqué dans l'économie numérique et les banques.

3.4 Promotion de la capacité éducative sur tout le territoire libanais

Pour remédier à la pénurie de spécialistes qualifiés en cybersécurité, le gouvernement et l'Université Libanaise, ainsi que les universités, écoles et organisations privées, doivent investir dans des programmes de sensibilisation à la cybersécurité via une plate-forme

Cyber Academy. Ces mêmes acteurs doivent mettre en place des programmes universitaires pour former des spécialistes de haut niveau qualifiés et talentueux afin de combler le fossé entre l'offre et la demande dans le domaine de la cybersécurité.

La sensibilisation à la sécurité numérique devra être un élément essentiel de l'enseignement supérieur non spécialisé pour initier les futurs diplômés à la cybersécurité. Chaque institution veillera donc à ce que les organisations offrant des cours de formation initiale ou continue intègrent l'enseignement de sensibilisation à la cybersécurité dans leurs cursus et à ce que le matériel soit adapté à chaque formation proposée.

Il serait souhaitable d'intégrer la cybersécurité dans les matières informatiques du système éducatif national (programme pré-universitaire), y compris une composante de cybersécurité dans les programmes scolaires, ainsi que des activités novatrices et motivantes en classe, comme des défis et des programmes d'été centrés sur les problématiques de cybersécurité.

Sous l'égide d'une future Agence Nationale de Cybersécurité et des Systèmes d'Information qui sera mise sur pied (voir Partie II), l'État doit évaluer ses besoins en programmes de formation initiale et continue à court, moyen et long terme. Cela nécessitera une collaboration proactive avec le Ministère de l'Éducation et avec tous les acteurs concernés de l'administration et du secteur privé, y compris les syndicats.

Les technologies clés pour lesquelles une connaissance approfondie est requise dans les métiers de la cybersécurité et en général pour le développement d'un environnement numérique de confiance doivent également être identifiées.

Dans le cadre de la formation continue, les ressources humaines des institutions et des entreprises, en particulier celles appartenant à des catégories professionnelles ayant des responsabilités sociales et étatiques, devraient pouvoir bénéficier d'une formation numérique incluant une sensibilisation à la cybersécurité.

L'École Nationale d'Administration Libanaise, en partenariat avec les syndicats professionnels, sera appelée à élaborer et à mettre en œuvre des programmes de formation continue adaptés aux besoins des employés et des gestionnaires de l'administration publique, afin de correspondre au rythme de croissance et de développement du secteur privé.

L'État est conscient de la nécessité de promouvoir la recherche scientifique et technologique dans le domaine numérique, afin que les universités et les instituts de recherche libanais attirent les meilleurs cerveaux dans le domaine de la cybersécurité. Le gouvernement propose donc d'encourager un partenariat actif entre les instituts de formation et l'industrie, ce qui devrait déboucher sur un véritable dialogue de coopération mutuellement bénéfique entre l'État et les acteurs de la cybersécurité. Pour atteindre cet objectif, les actions suivantes doivent être envisagées:

- Identifier les domaines de la science et de la technologie que le gouvernement, l'industrie et les universités considèrent comme importants et identifier les lacunes potentielles au Liban.
- Financer et apporter le soutien de l'État aux centres d'excellence académiques, aux instituts de recherche et aux centres de formation doctorale pour traiter des domaines importants, tels que l'analyse de données volumineuses, les systèmes de contrôle industriels de confiance, ou la recherche scientifique.
- Établir des centres d'excellence (ou encourager les centres existants) qui attirent les scientifiques et les chercheurs les plus compétents et les plus dynamiques, et approfondir le partenariat actif entre les universités, le gouvernement et l'industrie. En particulier, soutenir le développement de cyberproduits de premier plan et de nouvelles entreprises dynamiques en cybersécurité.
- Financer des recherches et développer des équipements de sécurité de haut niveau afin d'améliorer le niveau de sécurité des produits pour les entreprises et le grand public.
- Fournir un financement et un soutien gouvernemental aux centres d'excellence universitaires et aux instituts de recherche qui traitent d'importantes recherches dans le domaine des technologies numériques. Parrainer également des doctorants et des titulaires de doctorat afin d'augmenter le nombre d'experts libanais possédant une cyberexpertise.
- Renforcer le partenariat entre la recherche et l'industrie, par le biais de bourses, de financements bilatéraux et de recherches financées par l'État. Cette forme de collaboration doit toujours respecter les principes d'équité et de méritocratie, et renforcer ainsi les compétences techniques en matière de cybersécurité des personnes impliquées.
- Créer un panel d'experts pour la confiance numérique chargé de:
  - Identifier les technologies clés pour lesquelles des connaissances approfondies sont requises pour les professions de la cybersécurité;
  - Évaluer les besoins en formation initiale et continue;
  - Suivre la recherche et soutenir son développement;
  - Soutenir les jeunes titulaires d'un doctorat;
  - Encourager le financement et soutenir la recherche et le développement industriel dans le domaine des technologies numériques.

En tant que principaux acteurs de la vie publique, les fonctionnaires doivent être conscients, à leurs différents niveaux de poste, de la responsabilité de la protection des données auxquelles ils ont accès. Pour améliorer la protection de toutes les composantes du pays et prévenir toute menace, l'État doit:

- Renforcer la sécurité de ses systèmes d'information en élaborant une politique de sécurité des systèmes d'information et un réseau de communication électronique interministériel et en assurant un déploiement sécurisé des périphériques mobiles.
- Évaluer annuellement l'application de la politique de sécurité des systèmes d'information de l'État et l'efficacité des mesures adoptées. Le Parlement devra être informé au moyen d'indicateurs, qui incluent également la réponse à ses recommandations concernant la cybersécurité. Plus généralement, les hauts responsables de la réglementation de la qualité veilleront à ce que les questions liées au renforcement de la sécurité des systèmes d'information soient prises en compte dans le processus d'établissement des normes, qui sera effectué régulièrement.
- Attirer auprès du gouvernement des cyberspécialistes compétents et bien formés pour maintenir notre sécurité nationale, et pour comprendre l'impact du cyberespace sur les opérations de sécurité.
- Inclure des éléments de cybersécurité dans tous les programmes de formation de la fonction publique et dans l'examen de recrutement du corps des ingénieurs en systèmes d'information et de communication. Les fonctionnaires traitent des données sensibles qu'ils doivent savoir protéger au niveau de chaque ministère.
- Veiller à ce que l'expérience des fonctionnaires dans le domaine de la cybersécurité soit optimisée tout au long de leur carrière.
- Donner aux organismes chargés de l'application de la loi, aux autorités publiques et au secteur bancaire un haut niveau d'indépendance en ce qui concerne la cybersécurité, les infrastructures, les processus et les décisions opérationnelles, dans la mesure où ils se rapportent à leurs propres mandats internes. Cette approche générale doit toujours être alignée sur la stratégie du gouvernement en matière de cybersécurité, qui doit être assurée par le biais d'une Agence nationale au plus haut niveau de la défense nationale.
- Le Premier ministre recevra un rapport semestriel confidentiel contenant le résultat des audits sur les cybermenaces, les cyberattaques, les cybervulnérabilités et la réponse coordonnée de toutes les autorités concernées.
- Préserver l'autonomie du Liban dans la prise de décision, y compris la mobilisation de ressources humaines et budgétaires.

3.5 Promotion des capacités industrielles et techniques

Le Liban doit développer un écosystème propice au développement de l'économie numérique et à la promotion internationale de ses produits et services numériques. Il doit veiller à ce que les administrations, les entreprises et les citoyens aient accès à des

produits et services numériques à des niveaux de confiance et de sécurité adaptés aux utilisations et aux cybermenaces. À cette fin, le pays doit:

- Développer et améliorer l'offre nationale de produits et services de sécurité. En collaboration avec les différents ministères (Télécommunications, Industrie, Économie, Intérieur, Défense, Affaires étrangères, OMSAR, etc.) et avec la NCISA, l'État doit promouvoir une politique industrielle visant à renforcer les entreprises nationales qui développent des produits et des services de sécurité informatique. L'État doit également encourager les nouvelles entreprises dynamiques en matière de cybersécurité, ainsi que le développement et la production de cyberproduits avancés.

- Collaborer avec les parties prenantes - avec les sociétés de cybersécurité en particulier - et les milieux universitaires pour fournir une formation et des conseils aux secteurs public et privé. Le secteur en plein essor et innovant de la cybersécurité étant une nécessité pour l'économie numérique moderne et nationale, l'État s'efforce de créer des possibilités de collaboration avec les entreprises privées dans le domaine de la formation et de l'éducation et de promouvoir les moyens de maintenir et d'exercer ses compétences. Pour leur part, les sociétés de cybersécurité doivent fournir au gouvernement et aux entreprises des technologies des formations et des conseils de pointe.

- Produire ou acquérir des équipements fiables pour détecter les cyberattaques et s'en protéger, principalement pour les opérateurs d'importance vitale, ainsi que des produits mobiles sécurisés pour toutes les entreprises. La plupart des équipements et produits numériques disponibles sur le marché ne disposent pas d'un niveau de sécurité informatique satisfaisant. Pour les entreprises, le niveau de sécurité des produits doit donc devenir un facteur de différenciation, voire un avantage concurrentiel. Un processus adéquat d'évaluation et de certification de sécurité doit par conséquent être mis en place.

- Identifier et répertorier, par le biais de la NCISA, toutes les infrastructures d'importance vitale (OIV) du pays afin de mettre en œuvre des politiques de sécurité et des bonnes pratiques ad hoc.

- Qualifier et surveiller les produits, le matériel et les services de cybersécurité afin d'identifier ceux qui peuvent mettre en danger les activités informatiques en activant le cyberespionnage et les attaques parrainées par les États.

3.6 Soutenir les entreprises de cybersécurité à l'international

Il est essentiel que le Liban soutienne la création et le développement du secteur industriel de cybersécurité. Pour atteindre cet objectif, le pays doit:

- Soutenir les initiatives de collaboration générées par le secteur privé. L'État doit appuyer le développement économique du secteur de la cybersécurité industrielle afin d'encourager le développement local de produits et services de cybersécurité qui garantiront l'indépendance du Liban à l'égard des produits sous contrôle étranger.
- Chercher à renforcer la visibilité et la compétitivité de l'offre libanaise à l'étranger et facilitera l'accès des PME et des jeunes entreprises sur les marchés internationaux. La coordination interministérielle sera structurée et renforcée. Une organisation d'appui aux entreprises sera mise en œuvre au-delà des actions ponctuelles et souvent isolées actuellement menées par les différents ministères et entités de l'État. Les procédures de contrôle des exportations pour les solutions de cybersécurité seront clarifiées et optimisées.
- Créer des systèmes de support spécifiques pour les acteurs de la cybersécurité, avec des conditions claires pour les méthodes d'accès et de mise en œuvre. En parallèle, clarifier et optimiser les conditions d'accès aux méthodes de mise en œuvre des systèmes de support existants.
- Établir des procédures claires pour contrôler l'importation et l'exportation de solutions de cybersécurité.
- Intégrer les critères de sécurité dans la sélection des produits et services numériques au niveau des marchés publics.

3.7 Renforcer la collaboration entre les secteurs public et privé

Acteur majeur de l'économie et principal fournisseur de services, l'État est le premier utilisateur potentiel de produits de haute sécurité. Une plus grande perméabilité entre les secteurs public et privé permettrait au Liban de renforcer ses efforts dans le domaine de la sécurité numérique au quotidien, en faisant en sorte que chaque bénéficiaire détecte et gère mieux les cybermenaces. Pour cela, il faudrait:

- Encourager la création, le développement et l'innovation du secteur de la cybersécurité, en collaboration avec le gouvernement, les universités et le secteur privé.
- Renforcer la collaboration entre le gouvernement et l'industrie afin de fournir à chacun des informations proactives sur les menaces, pour obtenir des renseignements auxquels chacun doit contribuer et qui permettront de perturber les efforts criminels en amont.
- Encourager les partenariats gouvernement-industrie pour aider à définir et à cibler les interventions en faveur de la croissance et de l'innovation.
- Soutenir la mise en place d'accélérateurs et de start-up dédiés à la cybersécurité.

- Collaborer avec le secteur financier pour faire du Liban un environnement plus hostile pour ceux qui cherchent à monétiser les informations d'identification volées, notamment en perturbant leurs réseaux.

- L'Agence Nationale de Cybersécurité et des Systèmes d'Information (NCISA) devra transférer les connaissances acquises au secteur privé, afin de contribuer à la gestion de la cybersécurité, tout en identifiant des fournisseurs de services compétents et dignes de confiance. Cela devrait permettre de détecter et de traiter la croissance inévitable du nombre de cyberattaques contre les entreprises. De même, il faudra intégrer les exigences de cybersécurité dans les contrats publics et les projets de législation, tout en stimulant la croissance du secteur de la cybersécurité:

  - En insérant les critères de sécurité dans la sélection de produits et services numériques qui remportent les marchés publics;
  - En accordant un bonus aux entreprises si la réponse à l'appel d'offre est accompagnée d'une analyse de risque de cybersécurité;
  - En s'assurant que les lois incluent une section dans leur évaluation d'impact dédiée à la technologie numérique, y compris la cybersécurité.

3.8 Rôle des organismes chargés de l'application de la loi

Pour améliorer les capacités de cybersécurité, les organismes chargés de l'application de la loi (Armée, Forces de Sécurité Intérieure, Sûreté Générale, Sécurité de l'État) devront prendre les mesures suivantes:

- Accroître la capacité des organismes chargés de l'application de la loi, en coordination avec les partenaires internationaux, pour identifier, anticiper et perturber les activités cybernétiques hostiles d'acteurs étrangers, de cybercriminels et de terroristes. Cela améliorera la collecte et l'exploitation de leurs renseignements afin d'obtenir des informations préventives sur les intentions et les capacités des attaquants.

- Renforcer les efforts des forces de l'ordre pour poursuivre et cibler les criminels, où qu'ils se trouvent, en coordination avec leurs partenaires locaux et internationaux. Les services répressifs doivent cibler les criminels qui persistent à attaquer les citoyens et les entreprises libanais en démantelant leurs infrastructures et leurs réseaux de facilitation.

- Les forces de l'ordre et le secteur bancaire contribueront également à la sensibilisation et à la normalisation de la cybersécurité.

- Améliorer les actions des organismes chargés de l'application de la loi et des services judiciaires dans les enquêtes sous l'autorité judiciaire. L'enjeu le plus important pour toutes les questions liées à la cybercriminalité est une formation

technique professionnelle spécialisée de haut niveau, qui doit inclure des modules, des sessions et des exercices pratiques. Des améliorations supplémentaires de la qualité peuvent accélérer et améliorer ce processus : il s'agit notamment de relations procédurales, techniques et opérationnelles dédiées avec des organismes, des institutions et des équipes spécialisées au niveau international en matière de cybersécurité, soutenues par un échange régulier d'informations.

- Renforcer la coordination entre les organismes chargés de l'application de la loi, notamment en leur permettant d'échanger des informations sur l'analyse des menaces.

- Faire en sorte que l'anticipation et la prévention soient une priorité pour les autorités compétentes en matière de sécurité des systèmes d'information. Cela peut être réalisé en construisant une plate-forme *Cyber Threats Intelligence* (CTI). Cette plate-forme devrait recevoir une transmission continue de données d'entrée provenant de sources nationales (agences nationales) et étrangères. Les données peuvent même être obtenues par l'acquisition d'ensembles de données commerciales («sources») auprès des sociétés privées spécialisées, qui fournissent des informations neutres à 100%, car elles ne sont pas officiellement ou officieusement protégées par un gouvernement étranger. La plate-forme CTI doit constituer le noyau du CSIRT national du gouvernement (CERT-LB), **qui doit être établi au sein de la NCISA**. Le CERT -LB fournira ensuite des sources de données, des alertes, et des alertes précoces aux SOCs (centres d'opération de sécurité) nationaux.

- Améliorer les capacités de l'armée ainsi que des agences renseignement en matière de cyberguerre, par exemple en organisant des sessions de formation et de soutien, en informant ces acteurs sur les activités et les bonnes pratiques d'agences de cybersécurité similaires dans la plupart des pays avancés.

- Faciliter la coordination entre les agences nationales, par exemple en organisant des réunions périodiques pour discuter de questions de cybersécurité, en leur fournissant des installations qui leur permettent de se rencontrer et de réagir aux cyberincidents, et en organisant des exercices de réponse aux incidents nationaux en cybersécurité.

4. Objectifs

Au niveau national, la stratégie en matière de cybersécurité doit être conçue pour mettre en œuvre, pour les secteurs public et privé et pour les citoyens, un plan de défense stratégique contre les menaces cybernétiques : cela doit tendre à assurer la durabilité de son application en l'institutionnalisant à travers une structure et des objectifs clairs. Une stratégie de cybersécurité doit également comporter des actions décisives visant à protéger l'économie libanaise et la vie privée des citoyens libanais. Dans l'ensemble, l'objectif principal de cette stratégie nationale est de définir un ensemble de décisions qui doivent aboutir à des actions opérationnelles rendant le Liban confiant, capable et résilient dans un monde numérique en rapide évolution.

Les principaux objectifs qui doivent être atteints sont les suivants:

- Encourager le gouvernement, les organisations, les entreprises et les particuliers à jouer leur rôle dans cet effort collectif visant à sécuriser le cyberespace national;
- Améliorer la disponibilité et l'ergonomie des services, ainsi que la transparence, et encourager la participation des citoyens à la cybergouvernance pour réduire les menaces et les cyberattaques dans les secteurs public et privé;
- Appliquer un mécanisme de notification et d'intervention dans la gestion des incidents qui soit approprié et efficace;
- Gérer les incidents de sécurité et réduire les risques, afin de pouvoir estimer avec précision les cybermenaces actuelles et à venir ;
- En cas d'incidents majeurs dans le cyberespace, réagir rapidement et efficacement, en utilisant la capacité la plus appropriée, afin de maintenir la sécurité et la résilience des réseaux, des données et des systèmes.
- Développer les moyens juridiques, procéduraux et techniques pour défendre le Liban contre les cybermenaces en constante évolution, pour apporter une réponse efficace aux incidents et pour assurer la protection et la résilience des réseaux, des données et des systèmes du pays.
- Améliorer les capacités de réaction aux cyberattaques en adoptant les mesures appropriées et en augmentant la résistance du pays aux menaces cybernétiques les plus courantes. L'État doit s'appuyer sur ses capacités et sur celles de l'industrie, en soutenant activement l'élaboration et la mise en œuvre de mesures actives de cyberdéfense visant à améliorer de manière significative les niveaux de sécurité des TIC sur les réseaux nationaux.

- Fournir un soutien et une assistance aux organisations en réponse aux incidents de sécurité. En particulier, l'État doit veiller à ce que les pouvoirs publics collaborent activement avec le secteur privé, que ce soit du point de vue préventif ou en réaction à un incident. Les processus nationaux de gestion des incidents doivent adopter une approche globale, grâce à laquelle il sera possible d'apprendre des partenaires et de partager des techniques de désescalade ;
- S'assurer que les incidents soient signalés de manière **obligatoire et rapide à l'autorité nationale de la cybersécurité du pays, à savoir la NCISA**, permettant ainsi de comprendre l'ampleur, la portée et la gravité des menaces;
- Identifier les causes profondes des attaques au niveau national, en réduisant l'incidence de l'exploitation multiple et répétée sur plusieurs victimes et secteurs ;
- Utiliser les relations avec les autres équipes de réponse aux incidents de sécurité informatique, aux niveaux national et international, dans le cadre d'un protocole de gestion des incidents ;
- Mesurer la cybercriminalité à l'aide de statistiques fiables et d'analyses de la criminalité numérique pour orienter les actions appropriées. En l'absence de telles statistiques, les autorités publiques ne peuvent continuellement réévaluer les politiques de réponses aux attaques ni mettre en œuvre des mesures adéquates. Dans ce cas, le Ministère de l'Intérieur doit adopter de nouveaux outils pour suivre l'évolution de la cybercriminalité afin d'orienter l'action publique ;
- Établir une base de données sur les cyberincidents pour permettre à la fois une vue globale et une analyse détaillée des tendances en matière de cybermenaces afin d'identifier les solutions de sécurité et/ou les besoins en produits et services. Cela profiterait également au secteur de la cyberassurance, qui s'appuie sur des données statistiques et historiques sur les cyberincidents pour en évaluer les risques.
- Promouvoir un environnement *Internet sécurisé* pour les opérateurs vitaux. Chaque OIV devrait élaborer et mettre en œuvre ses mesures et ses politiques de sécurité conformément à cette stratégie, afin de faire fonctionner son centre opérationnel de sécurité pour surveiller et réagir efficacement aux incidents, en s'appuyant sur des techniques d'analyse, de corrélation intelligente et de filtrage des alertes de sécurité.
- Encourager les fournisseurs de matériel et de logiciels à développer et à vendre des produits pour lesquels les contrôles de sécurité sont activés par défaut ;
- Une fois que le cyberenvironnement et la cyberhygiène libanais seront conformes aux normes de base en matière de sécurité au niveau des produit technologiques et des utilisateurs (parties prenantes), la NCISA devra établir de nouvelles normes ayant pour objectif principal d'obtenir une sécurité intégrale dès la conception de chaque dispositif TIC connecté à l'espace adresse IP public attribué au Liban;

- S’assurer que les fournisseurs de services respectent les lois et les règlements. Le défi consiste à modifier radicalement les contrôles de sécurité intégrés aux logiciels et au matériel déjà activés par le fabricant avant le lancement du produit sur le marché. L'utilisateur doit pouvoir bénéficier d'un maximum de sécurité sur un produit ou service commercialement viables, tout en restant dans le contexte d'un Internet libre, accessible et ouvert à tous ;

- Insister sur les valeurs humaines dans le cyberespace, en promouvant le respect des droits de l'homme afin de garantir aux individus les moyens nécessaires pour l'autodétermination informationnelle complète, le respect de la vie privée et la protection des données personnelles;

- Changer les comportements en veillant à ce que les entités gouvernementales, les organisations, les entreprises et les particuliers disposent des connaissances et des compétences pour se défendre et prendre les mesures appropriées pour se protéger des dommages causés par les cyberattaques;

- Sensibiliser le peuple libanais aux bonnes pratiques en lançant un programme ambitieux qui suive les lignes d’action suivantes:

  - Intégrer la sensibilisation à la cybersécurité dans tous les programmes d'enseignement supérieur et de formation continue; intégrer la cybersécurité dans le système d'éducation pré-universitaire (sous forme d'activités en classe, de concours et de stages d'été) et dans des programmes concernant les domaines spécifiques de l'informatique; mettre en œuvre des programmes de sensibilisation à la cybersécurité en partenariat avec des universités, des écoles et des organisations privées;
  - Lancer un appel à manifestation d'intérêt pour la production de contenu de sensibilisation destiné au grand public ;
  - Lancer des initiatives nationales en partenariat avec les organismes chargés de l’application de la loi pour sensibiliser le public aux risques d'Internet et éduquer les élèves du cycle primaire ;
  - Créer un portail d’éducation numérique en collaboration avec la communauté universitaire ;
  - Développer des projets de campagnes de communication dans le cadre d'une "grande cause nationale" (renforcer la confiance dans les produits numériques).
  - Promouvoir la cybersécurité et lancer des campagnes de sensibilisation pour engager la société et diminuer les risques de manipulation d'informations dans le cyberespace.

- Assurer un changement radical du comportement du public, en maintenant un ensemble cohérent de consignes de cybersécurité émanant du Gouvernement et de ses partenaires.

- Améliorer la culture de la cybersécurité dans la société libanaise en faisant comprendre quels sont les cyber-risques et les étapes de la cyberhygiène.
- Informer sur les risques liés aux techniques de manipulation et de propagande utilisées par les acteurs malveillants sur Internet. Les services de défense et de sécurité concernés sont chargés de détecter les incidents de propagande ou de cyberterrorisme et d'adresser au Gouvernement des recommandations pour la mise en œuvre de contre-mesures. Il est essentiel de mettre en place une plate-forme d'information pour réagir aux actes de propagande ou de déstabilisation.
- Renforcer la sécurité des systèmes d'information les plus sensibles des infrastructures critiques, tant des opérateurs publics que privés, par le biais de mesures législatives adéquates et régulièrement mises à jour. Ce processus sera progressivement étendu aux opérateurs publics et privés impliqués dans la manutention ou la gestion de systèmes d'informations sensibles.
- Veiller à ce que les organismes chargés de l'application de la loi disposent des moyens de défense les plus efficaces pour protéger leurs réseaux et leurs plates-formes et les rendre résilients. Ces acteurs doivent pouvoir continuer à fonctionner et à conserver leur liberté d'action malgré les cybermenaces et être capables de fournir une assistance en cas de cyberattaque à grande échelle au niveau national.
- Préparer les phases juridique et opérationnelle de l'institutionnalisation en créant une autorité centrale au plus haut niveau de défense: la NCISA.

PARTIE II. INSTITUTIONNALISATION – L'AGENCE NATIONALE DE LA CYBERSÉCURITÉ ET DES SYSTÈMES D'INFORMATION (NCSIA)

La sécurité des systèmes d'information revêt une importance cruciale pour un large éventail d'organisations et d'acteurs, publics et privés, aux niveaux national et international.

Que ce soit dans les domaines politique, diplomatique, économique ou militaire, la cybersécurité est aujourd'hui une préoccupation collective et une priorité nationale. En effet, les cybermenaces et les cyberattaques sont en augmentation et peuvent infliger de graves dommages aux intérêts de la nation. Face à ce risque, le Liban, comme de nombreux autres pays dans le monde, doit disposer d'un système national de défense informatique robuste et fiable.

Pour atteindre cet objectif, le Comité national de cybersécurité a conclu que la création d'une Agence Nationale de Cybersécurité et des Systèmes d'Information est une étape nécessaire et essentielle pour faciliter une approche coordonnée et proactive de la gestion des problèmes de cybersécurité, pour suivre la croissance et la diversité des cybermenaces ainsi que pour répondre de manière efficace à leur sophistication croissante.

La création d'une agence libanaise, chargée d'assister directement le Premier ministre et rattachée au Secrétariat Général du Conseil Supérieur de la Défense, constitue une étape cruciale dans la réponse de l'État libanais aux grands défis actuels et futurs en matière de cybersécurité.

La NCISA s'acquitte de son mandat en étroite coordination avec les ministères concernés et les organismes chargés de l'application de la loi, sans entrer en conflit avec leur rôle légal et leurs mandats.

La NCISA permettra aussi au Liban de centraliser et de coordonner les décisions prises au niveau des différents services de l'État dans le domaine de la cybersécurité, et de renforcer ainsi la résilience du pays face aux menaces numériques.

La deuxième partie de la stratégie décrit en détail le rôle et les fonctions de cette Agence, ainsi que les différents secteurs dans lesquels elle exercera ses activités.

5. L'Institutionnalisation d'une Agence Nationale pour la Cybersécurité

L'Agence Nationale de Cybersécurité et des Systèmes d'Information (NCISA) est une autorité gouvernementale qui relève du Secrétariat Général du Conseil Supérieur de la Défense et qui est responsable des politiques et procédures du système d'information libanais et de leur mise en œuvre, conformément à la stratégie nationale libanaise. La NCISA exerce ses fonctions publiques dans le cadre de la législation, des règles et des règlements relatifs à la cybersécurité.

Les domaines d'activité de cette agence consistent notamment à définir des politiques et des procédures, à élaborer des plans, à évaluer les vulnérabilités, à identifier les menaces, à sensibiliser davantage, à alerter – en diffusant ses recommandations - afin de réagir rapidement et efficacement aux cyberattaques et maintenir le cyberenvironnement libanais en sécurité et en résilience.

La NCISA définit également quels sont les infrastructures essentielles de l'information et les opérateurs sensibles, aide à la classification des données et établit un cadre de certification pour les produits de sécurité numérique de haut niveau. En outre, elle vise à élever le niveau de connaissances en matière de cybersécurité en initiant et en diffusant des activités de sensibilisation au moyen de programmes de formation, ainsi qu'en partageant des savoir-faire dans le cadre de la coopération internationale.

La NCISA joue un rôle essentiel en tant que coordonnateur et facilitateur: elle coordonne toutes les agences gouvernementales, les ministères concernés et d'autres institutions publiques et favorise la coopération entre les secteurs public et privé, l'industrie et le monde universitaire.

Dans le cadre de son mandat, la NCISA assiste et soutient toutes les parties prenantes des secteurs public et privé concernés par la cybersécurité. Elle fournit également des conseils techniques et établit des lignes directrices reflétant les priorités du public et des entreprises, ainsi que les bonnes pratiques en matière de cybersécurité.

La NCISA travaillera en étroite collaboration avec les ministères et les institutions concernés, les forces de l'ordre et le secteur industriel pour évaluer et partager les informations sur les dernières menaces criminelles, aider les industries à se défendre contre ces menaces, atténuer les conséquences des cyberattaques sur les victimes libanaises (administration, secteur privé, particuliers…) et créer un modèle national pour la gestion des situations d'urgence dans le cyberespace.

5.1 Le mandat de la NCISA au niveau national

La NCISA tire sa légitimité d'un mandat national qui définit son rôle et détermine ses fonctions, conformément aux besoins nationaux en matière de cybersécurité, définis dans la stratégie du Gouvernement.

Elle se verra ainsi confier les tâches suivantes:

1. Faciliter et superviser la conception, la mise en œuvre et la coordination de moyens de communication électroniques interministériels/interdépartementaux sécurisés au niveau gouvernemental.

2. Élaborer la mise en œuvre de la politique de cybersécurité du pays pour les systèmes d'information et garantir l'efficacité des mesures adoptées sur la base d'un rapport d'audit et d'évaluation confidentiel qui sera soumis annuellement au Premier ministre.

3. Mettre en place et faire fonctionner, au niveau national, l'équipe d'intervention en cas d'incidents de cybersécurité (CSIRT), qui collabore quotidiennement avec les ministères et les organismes chargés de l'application de la loi. Le CSIRT est le référent principal pour les cyberincidents sur l'ensemble du territoire, où toutes les parties prenantes échangent leur notification des cyberattaques. Le CISRT soutient tous les participants à la réhabilitation, à la défense et à la prévention contre les attaques notifiées. En outre, il définit l'échelle de gravité des cybermenaces et en publie un rapport de surveillance annuel. Il coopère étroitement avec la communauté internationale CSIRT (FIRST).

4. Construire un système de détection d'événements ou d'incidents pour les menaces pouvant affecter la sécurité des systèmes d'information nationaux et coordonner l'intervention en réponse à ces événements.

5. Organiser, en fonction des besoins, des cours de formation et des campagnes de sensibilisation à la cybersécurité à l'intention des institutions gouvernementales, du personnel gouvernemental et des entités privées intéressées dans le domaine des systèmes d'information, de la cybersécurité et de la cyberdéfense.

6. Assister et conseiller les entités et institutions administratives publiques ainsi que le secteur privé sur la mise en place des systèmes d'information sécurisés résistants aux cyberattaques et diffuser l'évaluation des menaces et les recommandations aux secteurs public et privé et aux particuliers.

7. Appliquer les normes appropriées en matière de cybersécurité et imposer leur adoption par toutes les agences gouvernementales.

8. Fournir des informations dynamiques sur les cybermenaces criminelles dans une base de données commune, sur laquelle l'industrie peut éventuellement se connecter pour mieux se défendre.

9. Identifier les normes et pratiques ainsi que les conseils de sécurité relatifs aux incidents de cybersécurité observés.

10. Coopérer avec les opérateurs concernés, principalement les OIV et les infrastructures critiques, pour identifier et caractériser les cyberattaques affectant leur fonctionnement.

11. Protéger les informations confidentielles et hautement sensibles du Gouvernement contre les cyberattaques.

12. Effectuer des exercices de gestion de crise en cybersécurité. Ces exercices, menés au niveau national, couvriront progressivement l'ensemble du territoire et des secteurs d'activité d'importance vitale.

13. Les services répressifs, les entités administratives et ministérielles et les institutions concernés, en liaison avec la NCISA, continueront de mettre en place des capacités opérationnelles de cyberdéfense pour faire face aux crises majeures liées à la cybersécurité.

5.2 La NCISA et le public: des particuliers aux entreprises

La NCISA fournit un soutien et des recommandations de qualité aux entreprises et aux citoyens sur les cybermenaces. Pour ce faire, elle crée, par exemple, une base de données facilement accessible sur les systèmes d'information et de prévention et organise des campagnes de publicité visant à informer et à sensibiliser le grand public aux menaces cybernétiques.

Dans le cadre de son rôle auprès du grand public, la NCISA devra:

- Mettre en œuvre des mesures pour défendre les citoyens libanais et les systèmes informatiques contre les menaces connues et émergentes en établissant une plate-forme permettant aux entreprises et aux particuliers de notifier à la NCISA les cybermenaces auxquelles ils sont confrontés.

- À des fins de prévention, recommander des solutions techniques et des programmes de formation visant à protéger et sécuriser le domaine numérique. Ces solutions doivent inclure des exercices nationaux et internationaux, accessibles à toutes les entreprises et au grand public afin d'améliorer l'état d'alerte préventive dans le cyberespace.

- Participer à l'orientation des recherches académiques, des études et du développement de logiciels, matériels, périphériques et technologies centrés sur la sécurité des systèmes d'information.

5.3 L'implication de la NCISA dans la qualification et le suivi des produits

En assurant la qualité des produits et services numériques, la NCISA s'acquitte des tâches suivantes:

- Contribue à assurer une surveillance active des technologies de sécurité numérique utilisées par les institutions gouvernementales, les entreprises et les particuliers.
- Assiste dans la qualification et la surveillance des produits et services de cybersécurité et soutient le développement de nouveaux biens de sécurité numérique suivant les dernières tendances et modifications.
- Contribue à la promotion des technologies et du savoir-faire nationaux en matière de sécurité des systèmes d'information en élaborant un cadre de qualification et de certification des produits conforme aux objectifs et à la souveraineté du gouvernement.

5.4 La NCISA face aux cybermenaces

La NCISA analyse et gère les risques de cyberattaques lorsque de nouvelles technologies sont déployées dans le processus de transformation numérique. Elle sera responsable de ce qui suit:

- Mise en place d'une gestion nationale des incidents de cybersécurité, qui répertorie les systèmes les plus critiques et effectue l'analyse, la détection et la compréhension des cybermenaces.
- Suivi de l'évolution technologique pour anticiper les changements et proposer les innovations nécessaires en matière de sécurité des systèmes d'information.
- Réalisation des audits des systèmes d'information des services et collecte des informations techniques dans le but de gérer les incidents de cybersécurité affectant ces systèmes.
- Renforcement et soutien des organismes chargés de l'application de la loi dans la lutte contre le cyberterrorisme et la cybercriminalité organisée en adoptant les initiatives suivantes:
  - lutter contre les acteurs étrangers hostiles;
  - prévenir le cyberterrorisme;
  - contrer, sur le territoire national, la pensée et les comportements radicaux liés au cyberespace.

5.5 La NCISA et la protection des OIV

Un opérateur d'importance vitale ou une infrastructure critique est toute entité publique ou privée qui gère et exploite des données sensibles et des services sectoriels importants, tels que les télécommunications, les transports, le secteur de l'énergie, la santé ou les plates-formes nationales de données personnelles nationales.

Le rôle de l'agence dans la protection des OIV doit suivre les actions suivantes:

- Renforcer la protection des opérateurs essentiels, en particulier dans les domaines des communications électroniques, de la fourniture d'électricité et des entreprises de services numériques, en adoptant des réglementations strictes en matière de cybersécurité.
- Impliquer les opérateurs de communications électroniques et les hébergeurs Web dans la mise en œuvre de systèmes de détection dans leurs réseaux afin de déceler les cyberattaques ciblant leurs abonnés (sondes, capteurs, détection comportementale, …).
- Fournir des outils d'analyse des risques et des systèmes indépendants pour évaluer le niveau de sécurité et la fiabilité de la cybersécurité des produits et des services dans les industries critiques.

Lorsque des produits et services numériques stockent des données à caractère personnel ou sont destinés à des industries d'importance vitale, la NCISA doit fournir une assistance pour la réalisation d'analyses de risques et l'élaboration de bonnes pratiques en matière de cyber-protection.

La NCISA contribue également à la mise en place de mécanismes permettant d'évaluer de manière indépendante le niveau de sécurité et de fiabilité de ces produits et services, et de fournir à leurs utilisateurs potentiels des garanties appropriées, par le biais d'une labellisation. À cette fin, la NCISA accomplit les tâches suivantes:

- Elle définit les meilleures pratiques et mécanismes pour renforcer les infrastructures nationales clés (sites sensibles ou OIV) et les protéger des cyberattaques. La NCISA, en collaboration avec les administrations régionales et les autres autorités responsables, aidera les organisations et les entreprises nationales à prendre les mesures nécessaires pour rester suffisamment sécurisées et résilientes contre les cyberattaques.
- Elle veille à ce que les infrastructures nationales critiques publiques et privées soient conscientes du niveau de menace et mettent en œuvre des mesures appropriées de prévention de la cybercriminalité. Les institutions publiques et les entreprises et organisations privées doivent comprendre le niveau réel de la cybermenace sur leur infrastructure et mettre en place des mesures pour améliorer la protection et la préservation de l'intérêt et de la souveraineté nationaux.

- Elle vient en aide aux entreprises qui possèdent et/ou exploitent des données sensibles à gérer leurs cyber-risques et leurs vulnérabilités.

5.6 L'Agence dans le cadre normatif et son écosystème

Puisque la construction du cadre juridique nécessite des organes hautement expérimentés, le cadre normatif de la NCISA doit être construit à l'aide d'une collaboration internationale forte et régulière respectant la souveraineté et la constitution du Liban. L'écosystème de la NCISA regroupe d'importants partenaires locaux, tels que le Gouvernement, le Ministère des télécommunications et ses opérateurs, OGERO, les forces de l'ordre, les ministères bénéficiaires, OMSAR, des établissements universitaires, des fournisseurs de services Internet au Liban et des associations professionnelles, tous soutenus par les partenaires internationaux énumérés dans la stratégie.

Afin de mettre en place un cadre juridique adéquat pour la cybersécurité, la NCISA prend les mesures suivantes:

- Elle adapte et crée un cadre réglementaire pour les nouvelles technologies émergentes. Pour ce faire, la NCISA informera régulièrement les ministères, les institutions gouvernementales, les autorités locales, les entreprises et les citoyens des menaces qui pèsent sur les systèmes numériques par le biais des canaux de communication appropriés pour chacun.
- Elle prépare l'environnement juridique pour accueillir les nouveaux produits et services numériques.
- Elle élabore des directives en matière de cyberdéfense et met en œuvre des mesures de cyberdéfense pour améliorer considérablement les niveaux de cybersécurité sur les réseaux informatiques.
- Elle impose des règles pour l'autorisation des dispositifs de sécurité et des mécanismes conçus pour protéger, dans les systèmes d'information, les informations couvertes par le secret défense.
- Elle participe aux négociations internationales et assurer la liaison avec les homologues étrangers.
- Elle définit et évalue la sécurité des dispositifs et services offerts par les fournisseurs nécessaires à la protection des systèmes et des infrastructures d'information.
- Elle définit le cadre de cybersécurité pour la mise en œuvre de signatures électroniques qualifiées.
- Elle contribue à la préparation du cadre d'accréditation et de certification relatifs à la cybersécurité et aux signatures électroniques qualifiées, ainsi qu'aux identifications, aux traces et aux preuves numériques.

- Elle décide de l'accréditation des laboratoires reconnus pouvant effectuer des évaluations de sécurité numérique et des certifications de produits et systèmes informatiques (ces dispositions légales ne sont pas encore mises en œuvre au Liban).
- Elle définit un cadre pour l'accréditation, la certification et la normalisation technique relatives aux systèmes de cybersécurité, conformément aux lois et réglementations en vigueur. Ce cadre sera établi en collaboration avec les ministères concernés, les organismes chargés de l'application de la loi et les institutions gouvernementales, chacun dans sa propre juridiction.

6. Conclusion

Finalement, il existe des constats critiques et stratégiques pour le bon fonctionnement de la Stratégie Nationale Libanaise de Cybersécurité, qui méritent d'être soulignés:

- Le présent document appelle de toute urgence une action obligatoire, critique et opérationnelle fondamentale: la création officielle d'une Agence Nationale de Cybersécurité et des Systèmes d'Information. Sans la NCISA, aucune des actions suivantes ne peut être poursuivie ou accomplie.
- La NCISA a besoin d'un engagement ferme de la part du gouvernement, ce qui lui permettra de lancer plusieurs actions, telles qu'une planification opérationnelle, un calendrier et une budgétisation corrects et détaillés.
- La NCISA a besoin d'un engagement ferme et officiel en faveur d'un budget opérationnel sans lequel rien ne peut être accompli. Bien qu'il soit impossible de définir un budget précis à ce stade précoce, des fourchettes de budget peuvent certainement être projetées, sur la base de l'approbation d'un plan d'action.
- Après l'approbation de la stratégie, le comité national pour la cybersécurité créé par le Premier ministre aura un nouveau mandat clairement défini pour soutenir le Gouvernement dans la phase de transition et des partenaires pour aider à la mise en œuvre de la stratégie.
- Si les étapes énoncées dans la stratégie de cybersécurité nationale du Liban ci-dessus ne sont pas mises en place, le pays sera confronté aux dangers et aux risques suivants:
  - Le Liban continuera à figurer parmi les pays les plus sous-développés du monde. Cet état de fait est prouvé par les statistiques et les scores globaux de l'UIT et par l'indice de cybersécurité, qui évaluent la capacité d'un pays à faire face aux besoins en matière de cybersécurité du vingt et unième siècle et à la lutte mondiale contre le cyberespace, aux menaces criminelles, à la guerre de l'information et au cyberterrorisme.
  - Tous les atouts, les marchés et les secteurs d'activité du Gouvernement libanais, ainsi que les citoyens, pourront être exposés à la cybermenace de manière forte et dangereuse. Des pertes économiques, ainsi que des craintes, des incertitudes et des doutes s'ensuivront dans le traitement de la transformation numérique en cours dans laquelle le Liban est encore très en retard.
  - Le Liban ne pourra pas évoluer, perdant sa compétitivité internationale.

- Une protection médiocre contre les cybermenaces, les cyberattaques et la cybercriminalité attirera les cybercriminels. Cela minera ultérieurement la confiance collective. Le Liban perdra donc des investissements étrangers, en particulier dans les secteurs des TIC, malgré les incitations économiques et commerciales encourageantes instaurées par le Gouvernement libanais au cours des dernières années.
- Le Liban abrite un grand nombre de réfugiés recensés et non recensés, de travailleurs étrangers légaux ou illégaux. Ces communautés sont en contact, directement ou indirectement, sciemment ou non, avec d'innombrables organisations et entités (parmi lesquelles un grand nombre d'ONG) sur le territoire national et dans leurs pays respectifs. Le gouvernement libanais supervise très mal ces populations ou ne les surveille pas du tout. Elles pourraient donc être vulnérables aux cyberattaques potentielles et pourraient facilement devenir une plate-forme pour des menaces cybernétiques potentielles et d'autres actes cybernétiques, ce qui pourrait exposer le Liban à un risque accru de crime organisé.
- Tout ce qui précède contribuera à nourrir la perception persistante du Liban en tant que pays « sous-développé ».

Seule une stratégie nationale de cybersécurité solide, cohérente, inclusive, institutionnalisée et collaborative, fondée sur les piliers identifiés en matière de cybersécurité, peut protéger le Liban, ses institutions publiques, son secteur privé et ses citoyens, de la menace susmentionnée, grâce à un plan d'action national, codifié, systématique et global.

ACRONYMES

Acronyme	Expression Complète
APT	Menace persistante avancée
CCB	Cyber Crime Bureau
CEPOL	Collège européen de police
CERT	Computer Emergency Response Team
CTI	Renseignements pour contrer les cybermenaces
DOS	Déni de service
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
ENA Liban	École Nationale d'Administration Libanaise
EUROPOL	Agence européenne de police criminelle
FSI/IFS	Forces de sécurité intérieure
ICP	Supervision des procédés
IIOT	L'internet des objets industriels
INTERPOL	Organisation internationale de police criminelle
IOT	Internet des objets
KPI/ICP	Indicateur clé de performance
NCISA	Agence nationale de cybersécurité et des systèmes d'information
NIST	National Institute of Standards and Technology (Institut national des normes et de la technologie)
OGERO	Entreprise libanaise des télécommunications
OMSAR	Cabinet du Ministre d'État chargé de la réforme administrative
ONU	Organisation des Nations Unies
PAP	« Prenez vos appareils personnels »
SSH	Secure Shell (Session à distance sécurisée)
SSL	Secure Sockets Layer. Rebaptisé par L'IETF Transport Layer Security (TLS) ou Sécurité de la couche de transport
TIC	Technologies de l'information et de la communication
UIT	Union Internationale des Télécommunications
UNICRI	Institut interrégional de recherche des Nations Unies sur la criminalité et la justice
UNODC	Office des Nations Unies contre la drogue et le crime
VPN	Réseau privé virtuel

GLOSSAIRE

Expression	Définition
Menace persistante avancée (APT)	Une menace persistante avancée, ou APT (*Advanced Persistent Threat*), est une cyberattaque prolongée et ciblée par laquelle une personne non autorisée accède au réseau et passe inaperçue pendant une longue période. Une attaque APT vise généralement à surveiller l'activité réseau et à voler des données plutôt qu'à porter atteinte au réseau ou à l'organisation.
Botnet	Un *botnet* (ou réseau de machines zombies) est un ensemble d'ordinateurs connectés à Internet qui, à l'insu de leurs propriétaires respectifs, ont été configurés de manière à transmettre des informations (notamment des spams ou des virus) à d'autres ordinateurs reliés à Internet. Ces ordinateurs ou appareils connectés, appelés « zombies » ou « bots », servent les intérêts de l'auteur du spam ou du virus.
BYOD/PAP – prenez vos appareils personnels	BYOD, abréviation de l'anglais « *bring your own device* », en français, PAP pour « prenez vos appareils personnels » ou AVEC pour « apportez votre équipement personnel de communication », est une pratique qui consiste à utiliser ses équipements personnels (smartphone, ordinateur portable, tablette électronique) dans un contexte professionnel.
CERT ou CSIRT - Computer Emergency Response Team	Un *computer emergency response team* (CERT) ou *computer security incident response team* (CSIRT) est un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations, mais dont les informations sont généralement accessibles à tous.
Cloud Computing	Le *cloud computing*, en français informatique en nuage ou nuagique, consiste à exploiter la puissance de calcul ou de stockage de serveurs informatiques distants par l'intermédiaire d'un réseau, généralement Internet. Les serveurs sont loués à la demande, le plus souvent par tranche d'utilisation, selon des critères techniques (puissance, bande passante, etc.), mais, également, au forfait. Le *cloud computing* se caractérise par sa grande souplesse : selon le niveau de compétence de l'utilisateur client, il est possible de gérer soi-même son serveur ou de se contenter d'utiliser des applicatifs distants en mode SaaS.
Cloud Network	Un *cloud network*, ou "réseau en nuage" est un réseau informatique au sein d'une infrastructure en nuage sur lequel est fournie la connectivité aux applications et serveurs basés sur le *cloud*.
Cloud Services	Un service *cloud* est un service mis à la disposition des utilisateurs à la demande via Internet à partir des serveurs d'un fournisseur informatique Cloud (en nuage) et non à partir des serveurs locaux

Expression	Définition
	de l'entreprise.
Cyberincident	Tentative non autorisée, réussie ou non, visant à accéder à un réseau ou à un système informatique ou visant à le modifier, à le détruire, à le supprimer ou à le rendre non disponible.
Cyberactivité malveillante	C'est une activité autre que celle autorisée ou conforme à la loi, qui cherche à compromettre la confidentialité, l'intégrité ou la disponibilité des ordinateurs, des systèmes d'information ou de communication, des réseaux, des infrastructures virtuelles contrôlées par des ordinateurs ou des systèmes d'information, ou les informations résident sur celui-ci.
Cyberattaque	Une cyberattaque est un acte malveillant envers un dispositif informatique via un réseau cybernétique.
Cybercrime	Un cybercrime est une « infraction pénale susceptible de se commettre sur ou au moyen d'un système informatique généralement connecté à un réseau». Il s'agit donc d'une nouvelle forme de criminalité et de délinquance qui se distingue des formes traditionnelles en ce qu'elle se situe dans un espace virtuel, le « cyberespace ». Depuis quelques années la démocratisation de l'accès à l'informatique et la globalisation des réseaux ont été des facteurs de développement du cybercrime.
Cyberdissuasion	Le fait de décourager une action ou un événement en instillant le doute ou la crainte des conséquences.
Cyberespionnage	Espionnage par internet.
Cyberhygiène	La cyberhygiène est un moyen de garantir une protection et une maintenance adéquates des terminaux et systèmes informatiques, et de mettre en œuvre les meilleures pratiques en matière de cybersécurité.
Cyberassurance	Une cyberassurance, également appelée assurance contre les risques informatiques permet d'assurer une entreprise, financièrement et juridiquement contre les attaques provenant du cyberespace.
Cybersécurité	Le mot cybersécurité est un néologisme désignant le rôle de l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations.
CyberSud	CyberSud est un projet conjoint de l'Union européenne (l'instrument européen de voisinage) et du Conseil de l'Europe. CyberSud a pour objet d'aider au renforcement de la législation et des capacités institutionnelles en matière de cybercriminalité et de preuve numérique dans la région du Voisinage Sud dans le

Expression	Définition
	respect des droits de l'homme et de l'état de droit. Les zones prioritaires: Algérie, Jordanie, Liban, Maroc et Tunisie.
Cyberespace	Un « ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs ».
Cybermenace	Toute circonstance ou tout événement potentiels susceptibles de porter atteinte aux réseaux et systèmes d'information, à leurs utilisateurs et aux personnes exposées.
Cyberguerre ou guerre cybernétique	La cyberguerre, ou guerre cybernétique (en anglais : cyberwarfare) ou guerre de la toile consiste en l'utilisation d'ordinateurs et d'Internet pour mener une guerre dans le cyberespace.
Cybernétique	La cybernétique est une science du contrôle des systèmes, vivants ou non-vivants, fondée en 1948 par le mathématicien américain Norbert Wiener.
Cyberpunk	Un programmeur qui s'introduit dans les systèmes informatiques dans le but de voler, de modifier ou de détruire des informations en tant que forme de cyberterrorisme.
DoS : Attaque par déni de service	Une attaque par déni de service (abr. DoS attack pour *Denial of Service attack* en anglais) est une attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. À l'heure actuelle la grande majorité de ces attaques se font à partir de plusieurs sources, on parle alors d'attaque par déni de service distribuée (abr. DDoS attack pour *Distributed Denial of Service attack*). Il peut s'agir de : - L'inondation d'un réseau afin d'empêcher son fonctionnement ; - La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ; - L'obstruction d'accès à un service pour une personne en particulier ; - - Également le fait d'envoyer des milliards d'octets à une box internet.
EBIOS	La méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) est une méthode d'évaluation des risques en informatique, développée en 1995 par la Direction centrale de la sécurité des systèmes d'information (DCSSI) et maintenue par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) qui lui a succédé en 2009.
e-Services	Services utilisant les technologies de l'information. Les trois composantes principales des services électroniques sont: le fournisseur de service, le récepteur de service et les canaux de distribution de service.
Exploit	Un exploit est, dans le domaine de la sécurité informatique, un élément de programme permettant à un individu ou à un logiciel

Expression	Définition
	malveillant d'exploiter une faille de sécurité informatique dans un système informatique. Que ce soit à distance (*remote exploit*) ou sur la machine sur laquelle cet exploit est exécuté (*local exploit*), le but de cette manœuvre est de s'emparer des ressources d'un ordinateur ou d'un réseau, d'accroître le privilège d'un logiciel ou d'un utilisateur sur la machine-cible, ou encore d'effectuer une attaque par déni de service.
Hack	Le terme de *hack* est l'action visant à pénétrer sans autorisation dans un réseau, câblé ou non. C'est surtout grâce à la démocratisation des réseaux sans fil que le terme de hack resurgit dans toute sa splendeur. Le principe est le même que pour une attaque d'un site Internet : accéder à un domaine privé sans autorisation, et être capable ou non de modifier tout contenu derrière cette barrière.
Hacker ou Hackeur	Spécialiste en informatique qui utilise ses connaissances de la sécurité informatique pour en rechercher et en exploiter les faiblesses.
Hacking	Le *hacking* peut s'apparenter au piratage informatique. Dans ce cas, c'est une pratique visant à un échange « discret » d'informations illégales ou personnelles. Cette pratique, établie par les *hackers*, apparaît avec les premiers ordinateurs domestiques. Le *hacking* peut se définir également comme un ensemble de techniques permettant d'exploiter les failles et vulnérabilités d'un élément ou d'un groupe d'éléments matériels ou humains.
Hacktivisme	Contraction de hacker et activisme, aussi appelé cyberactivisme au Québec, le hacktivisme est une forme de militantisme utilisant des compétences du piratage informatique dans le but de favoriser des changements politiques ou sociétaux.
Hacktivist	*Hackeur* qui fait de l'activisme par le moyen d'action ou d'attaques informatiques.
Ingénierie sociale	L'ingénierie sociale (*social engineering* en anglais) est, dans le contexte de la sécurité de l'information, une pratique de manipulation psychologique à des fins d'escroquerie. Les pratiques d'ingénierie sociale exploitent les faiblesses psychologiques, sociales et plus largement organisationnelles des individus ou organisations pour obtenir quelque chose frauduleusement (un bien, un service, un virement bancaire, un accès physique ou informatique, la divulgation d'informations confidentielles, etc.). En utilisant ses connaissances, son charisme, son sens de l'imposture ou son culot, l'attaquant cherche à abuser de la confiance, de l'ignorance et de la crédulité de sa cible pour obtenir ce qu'il souhaite.

Expression	Définition
Menace	Une menace est une cause potentielle d'incident, qui peut résulter en un dommage au système ou à l'organisation.
Menaces internes	Une menace interne est une menace malveillante adressée à une entreprise et émanant de membres de celle-ci, comme des employés, anciens employés, sous-traitants ou partenaires commerciaux, qui disposent d'informations privilégiées sur les pratiques de sécurité, les données et les systèmes informatiques de l'entreprise.
Monde virtuel	Un monde virtuel est un monde créé artificiellement par un logiciel informatique et pouvant héberger une communauté d'utilisateurs présents sous forme d'avatars ayant la capacité de s'y déplacer et d'y interagir1. La représentation de ce monde et de ses habitants est en deux ou en trois dimensions. Ce monde peut simuler le monde réel, avec ses lois physiques telles que la gravité, le temps, le climat, la géographie ou tout au contraire être régie par d'autres. Les lois humaines peuvent également être reproduites. La communication entre les utilisateurs se fait le plus souvent sous forme de texte (ou audio).
Ransomware ou rançongiciel	Un *ransomware*, ou rançongiciel en français, est un logiciel informatique malveillant, prenant en otage les données. Le *ransomware* chiffre et bloque les fichiers contenus sur votre ordinateur et demande une rançon en échange d'une clé permettant de les déchiffrer.
Résilience	La résilience est la capacité d'un système ou d'une architecture réseau à continuer de fonctionner en cas de panne.
Système critique	Un système critique est un système dont la panne peut avoir des conséquences dramatiques, comme des morts ou des blessés graves, des dégâts matériels importants, ou des conséquences graves pour l'environnement. L'analyse des systèmes critiques ne se limite pas à celle que permet, aujourd'hui de plus en plus, l'informatique de contrôle des processus, fussent-ils mécaniques ou humains.
Système hérité	Un système hérité, système patrimonial ou *legacy system* en anglais est un matériel et/ou logiciel continuant d'être utilisé dans une organisation (entreprise ou administration), alors qu'il est supplanté par des systèmes plus modernes. L'obsolescence de ces systèmes et leur criticité les rendent difficilement remplaçables sans engendrer des projets coûteux et risqués.
Script Kiddies	*Script kiddie* ou encore *lamer* est un terme péjoratif d'origine anglaise désignant les néophytes qui, dépourvus des principales compétences en matière de gestion de la sécurité informatique, passent l'essentiel de leur temps à essayer d'infiltrer des systèmes, en utilisant des scripts ou programmes mis au point par d'autres. L'expression signifie « gamin à script », mais le terme n'est pas

Expression	Définition
	traduit par les informaticiens francophones. Malgré leur niveau de qualifications faible voire nul, les *script kiddies* sont parfois une menace réelle pour la sécurité des systèmes. En effet, outre le fait qu'ils peuvent par incompétence altérer quelque chose sans le vouloir ou le savoir, d'une part les *script kiddies* sont très nombreux, et d'autre part ils sont souvent obstinés au point de passer parfois plusieurs jours à essayer toutes les combinaisons possibles d'un mot de passe, avec le risque d'y parvenir bien que souvent, ce soit le *script kiddie* lui-même qui se fasse infecter.
Secure SHell (SSH)	Le *Secure SHell* (SSH) est à la fois un programme informatique et un protocole de communication sécurisé. Le protocole de connexion impose un échange de clés de chiffrement en début de connexion. Par la suite, tous les segments TCP sont authentifiés et chiffrés.
Secure Sockets Layer (SSL)	Les *Secure Sockets Layer* (SSL), sont des protocoles de sécurisation des échanges sur Internet. Le protocole SSL a été développé à l'origine par Netscape. L'IETF en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.
Sextorsion	Délit qui consiste en l'extorsion via internet de faveurs sexuelles ou monétaires. Il se double le plus souvent de celui de chantage à la webcam.
Télétravail	Le télétravail désigne une organisation du travail particulière, c'est-à-dire l'exercice d'une activité professionnelle, en tout ou en partie à distance (c.-à-d. en dehors du lieu où le résultat du travail est attendu, généralement les locaux de son employeur) grâce aux technologies de l'information et de la communication (Internet, téléphonie mobile, fax, etc.). Le télétravail peut s'effectuer depuis le domicile, un télécentre, un bureau satellite ou de manière nomade (lieux de travail différents selon l'activité à réaliser), dans le cadre du travail salarié, mais aussi depuis des espaces partagés (*coworking*), dans le cadre du télétravail indépendant. Le « télétravail nomade » a été encouragé par la mondialisation économique.
Unpatched Systems ou Systèmes non corrigés	Les systèmes non corrigés sont des programmes pour lesquels un correctif logiciel qui modifie un système, une application ou un autre programme est indisponible ou n'a pas été appliqué.
Vulnérabilité	Une vulnérabilité ou faille est une faiblesse dans un système informatique permettant à un attaquant de porter atteinte à l'intégrité de ce système, c'est-à-dire à son fonctionnement normal, à la confidentialité ou à l'intégrité des données qu'il contient. Ces vulnérabilités sont la conséquence de faiblesses dans la

Expression	Définition
	conception, la mise en œuvre ou l'utilisation d'un composant matériel ou logiciel du système, mais il s'agit souvent d'anomalies logicielles liées à des erreurs de programmation ou à de mauvaises pratiques. Ces dysfonctionnements logiciels sont en général corrigés à mesure de leurs découvertes, mais l'utilisateur reste exposé à une éventuelle exploitation tant que le correctif (temporaire ou définitif) n'est pas publié et installé. C'est pourquoi il est important de maintenir les logiciels à jour avec les correctifs fournis par les éditeurs de logiciels. La procédure d'exploitation d'une vulnérabilité logicielle est appelée exploit.

ANNEXES

Résolution no. 172/2018

Nomination de Dr Lina Oueidat conseiller auprès du Premier ministre pour l'informatique en tant que coordinateur national pour les TIC

Le Permier ministre**,**

Conformément au décret n° 2 du 18/12/2016 (désignant M. Saad Hariri comme Premier ministre),

Conformément à l'accord n° 28/A du 25/02/2017 entre l'État libanais représenté par le Premier ministre et Dr. Lina Oueidat pour assumer les fonctions de conseiller auprès du Premier ministre pour les technologies de l'information et de la communication.

Décide ce qui suit

Article 1: Dr Lina Oueidat, conseiller auprès du Premier ministre pour Les affaires informatiques, sera chargée de remplir les fonctions de Coordonnateur National des Technologies de l'Information et de la Communication (TIC).

Article 2: Cette décision sera notifiée où c'est nécessaire.

Beyrouth, en date du 26/9/2018

Le Premier ministre

Saad Hariri

Résolution no. 173/2018

Former une équipe nationale pour élaborer un plan de lutte contre les dangers de la cybercriminalité et préparer une stratégie nationale pour institutionnaliser le travail de cybersécurité

Le Premier ministre**,**

Conformément au décret n° 2 du 18/12/2016 (désignant M. Saad Hariri comme Premier ministre),

Conformément aux nécessités de l'intérêt public.

Décide ce qui suit

Article 1: Une équipe nationale est créée pour élaborer un plan de lutte contre les dangers de la cybercriminalité et préparer une stratégie nationale pour institutionnaliser le travail en matière de cybersécurité, composée des personnes suivants::

- Secrétaire général du Conseil Supérieur de la Défense	Président
- Représentant de la Présidence de la République	Membre
- Représentant du Parlement	Membre
- Représentant du Ministère de la Justice	Membre
- Représentant du Ministère des Finances	Membre
- Représentant du Commandement de l'Armée – Ministère de la Défense	Membre
- Représentant de la Direction Générale des Forces de Sécurité Intérieure	Membre
- Représentant de la Direction Générale de la Sûreté Générale	Membre
- Représentant de la Direction Générale de la Sécurité de l'État	Membre
- Représentant de la Direction Générale de l'État Civil - Ministère de l'Intérieur et des Municipalités	Membre
- Représentant du Ministère des Télécommunications	Membre
- Représentant du cabinet du Ministre d'État chargé de la Réforme Administrative	Membre
- Représentant de la Banque du Liban	Membre
- Représentant du Conseil Supérieur de la Privatisation	Membre
- Dr. Lina Oueidat Coordonnateur National des Technologies de	Rapporteur

l'Information et des Communications

Les membres seront nommés par le ministre spécialisé et les chefs des départements concernés.

Article 2: La mission de l'équipe sera la suivante:

- Elaborer un plan pour faire face aux dangers de la cybercriminalité et préparer une stratégie nationale pour institutionnaliser le travail de cybersécurité
- Mener une évaluation des risques liés à la préparation de la stratégie nationale pour la cybersécurité, lutter contre la criminalité informatique et proposer les priorités, plans et projets nécessaires.
- Préparer la stratégie pour les travaux sur la cybersécurité conformément à la feuille de route préparée par le Secrétariat général du Conseil supérieur de la défense en coordination avec la Commission de l'Union européenne au Liban.
- Proposer le mécanisme d'institutionnalisation pour la mise en œuvre de cette stratégie

Article 3: L'équipe peut employer les personnes qu'elle juge appropriées pour exercer ses fonctions.

Article 4: Ladite équipe soumettra au Premier ministre un rapport périodique tous les mois et soumettra son rapport final dans un délai de six mois à compter de la date à laquelle cette résolution a été publiée.

Article 5: Cette décision est notifiée où c'est nécessaire.

Beyrouth, en date du 26/9/2018

Le Premier ministre

Saad Hariri

Membres officiels de l'équipe nationale de cybersécurité

Administration	Nom	Titre
Secrétariat Général du Haut Conseil de Défense	Mahmoud AL ASMAR	Major General – Secretary General of the High Council of Defense
	Brigadier General Wajdi CHAMSEDDINE	Engineer – Permanent Representative in the Committee
Présidence du Conseil des Ministres	Dr. Lina OUEIDAT	Committee Rapporteur ICT Advisor to the Prime Minister
Parlement	Dr. Ali HAMIEH	Advisor to the Chairman Media and Communications Commission
Ministère de la Justice	Hania AL HELWE	Judge
Ministère des Finances	George SAOUD	Head of Informatics
Commandement de l'Armée – Ministère de la Défense Nationale	Antoine KAHWAGI	Head of the Intelligence Technical Branch
Direction Générale des Forces de Sécurité Intérieure	Khaled YOUSSEF	Colonel – Engineer -Information Branch Engineer
Direction Générale de la Sûreté Générale	Jamal KASHMAR	Colonel – Engineer – Head of Communications Department
OGERO	Dr. Toufic CHEBARO	Senior Engineer
Direction Générale de la Sécurité de l'État	Hamza DAMAJ	Captain Eng. Head of IT Department
Ministère des Télécommunications	Bassel AL AYOUBI	General Manager of Investment and Maintenance
OMSAR	Ihab CHAABAN	ICT Security Officer
Banque du Liban	Ali NAHLE	Director of IT
Commission Spéciale d'Investigation	Nasser LEBBOS	Director of IT at the Banque du Liban
Conseil Supérieur de la Privatisation	Maya CHAMLI	Project Manager
Autorité de Régulation des Télécom	Said HAIDAR	Approval ,Quality and Standards Manager
Ministère de l'Économie et du Commerce	Dr. Linda KASSEM	Legal expert

Support de la délégation européenne à Beyrouth

Administration	Nom	Titre
Commission européenne	Jérôme Ribault Gaillard	Expert Contre-terrorisme

Liste des membres supplémentaires et des participants volontaires

Administration	Nom	Titre
Présidence du Conseil des Ministres	Ahmad AL KHATIB	Chef du Département Informatique
Commandement de l'Armée – Ministère de la Défense Nationale	Ahmed AL HAJJ CHEHADE	Lieutenant – Ingénieur, Direction du Renseignement
	Président Carl IRANI	Conseiller du Ministre de la Défense
Direction Générale des Forces de Sécurité Intérieure	Brigadier General Ahmad AL HAJJAR	Commandant de l'Institut des Forces de Sécurité Intérieure
Direction Générale de la Sûreté Générale	Dr. Jihad FAHS	Major – Ingénieur
Direction Générale de l'État Civil – MoIM	George BECHARA	Plateforme Carte ID Nationale
Ministère des Télécommunications	Nabil SHEIKH	Ingénieur
OMSAR	Joe HAGE	Conseiller du Ministre
Banque du Liban	Zeina AOUN	Expert systèmes d'information et cybersécurité
	Hubert BAZ	Administratif
Université Libanaise – Faculté de Génie	Dr. Lina OUEIDAT	Collaboration Académique Master de Cybersécurité – Habib Al Amin Coordination
	Habib EL AMIN	
Université Saint Joseph – ESIB	Dr. Maroun CHAMOUN	
	Tony FEGHALI Potech - Berytech	
Université Libanaise – Faculté de Droit	Pr. Mona AL ACHKAR JABBOUR	Experts bénévoles
	Dr. Bilal ABDALLAH	
ECS sarl	Darwiche CHEHADE	
	Mounif OUEIDAT	

Correspondance Officielle

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 l6 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/MA/Wle195

Prime Minister of Lebanon
His Excellency Saad HARIRI
Grand Séraï
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 10
Fax ► +33 (0)3 88 41 27 99
Mail ► jan.kleijssen@coe.int
Site ► www.coe.int/cybercrime
www.coe.int

الجمهورية اللبنانية
رئاسة مجلس الوزراء

قرار رقم ١٧٢ / ٢٠١٨

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

Feuille de route pour la préparation de la stratégie nationale de cybersécurité et pour la lutte contre la cybercriminalité.

Document présenté le 13 Septembre 2018 à la délégation européenne à Beyrouth.

Objectifs

Les nations se trouvent confrontées à l'obligation de passer au numérique en raison du développement rapide des technologies de l'information et de la communication (TIC). La diffusion des services informatiques, les services de communications internet et applications numériques présente des défis au niveau sécuritaire qui imposent à l'État et à ses institutions d'élaborer une stratégie nationale pour lutter contre les différentes sortes de menaces et attaques électroniques qu'elles soient internes ou externes.

La standardisation et la multiplication des services électroniques administratifs et le développement des technologies mettant en liaison directe les institutions étatiques et les citoyens présentent le risque de permettre à des entités non autorisées et potentiellement malveillantes d'avoir accès aux systèmes d'information de l'État. Pour pallier à ces problèmes qui sont appelés à croître en nombre et en complexité, en particulier avec le développement rapide de la technologie, il incombe à l'État de mettre en place pour ses organes civils et de sécurité un plan stratégique de défense contre ces menaces tout en menant une réflexion sur l'institutionnalisation de ce travail pour assurer sa pérennité conformément à une structure claire. Les axes les plus importants de cette stratégie sont:

1. **La défense, la dissuasion et le renforcement** contre les menaces provenant de l'intérieur et de l'extérieur.
2. **Le développement continu** des capacités de l'État pour accompagner le développement des technologies de l'information et de la communication. En effet, l'État a l'obligation de se protéger contre les menaces électroniques diverses, d'être en mesure de résister et d'atténuer les effets des attaques, et d'être résiliant dans la récupération rapide de ses fonctions. Il doit assurer la qualité, l'intégrité, et la fiabilité de ses données particulièrement lorsqu'il embarque dans une transformation rapide vers le numérique. Or, le Liban est en retard dans ces domaines et n'a pas mis en place les mesures juridiques, administratives et techniques liées au gouvernement électronique. La transformation vers le numérique est une tâche difficile et risquée en l'absence d'une stratégie nationale pour la sécurité des données et la cybersécurité.
3. **L'élévation du niveau d'informatisation dans les administrations publiques** à travers des processus et méthodologies d'automatisation validés et systématisés

menés en parallèle inter et intra-administrations, en accord avec l'évolution des besoins du secteur public et des attentes des citoyens.

4. **La promotion du rôle des services de sécurité et de renseignement** et le renforcement de la coordination entre eux avec le soutien et la supervision des autorités supérieures (Présidence du conseil des ministres et ses organismes associés), en particulier le Secrétariat Général du Conseil Supérieur de Défense, placé sous l'autorité du Premier ministre ...

5. **Le développement des ressources humaines, des outils, des composants technologiques et leur utilisation**, en partenariat avec le secteur informatique dans les établissements publics et privés, les universités et les associations concernées par ce domaine, sélectionnés après enquête de fiabilité.

6. **L'institutionnalisation de la centralisation des activités de sécurisation des données** au sein de la Présidence du Conseil des Ministres. En effet, assurer la sécurité électronique au niveau national exige la centralisation des moyens de surveillance, des échanges d'expériences et d'informations, du soutien technique, de la capitalisation des compétences, de la veille technologique des développements dans ce domaine, et de la lutte contre ce type de défis et le terrorisme, ainsi que le crime organisé et ses ramifications.

Note: La majorité des pays ont institutionnalisé leurs stratégies au niveau national et dans le cadre de l'action gouvernementale. La condition du succès est un haut niveau de coordination entre les différentes agences de l'État.

En l'absence de stratégie de développement administratif et de ce qui en découle, le Liban se trouve relégué dans le rang des pays les plus en retard en matière de cybersécurité selon l'Union internationale des télécommunications (UIT) dont le Liban est membre et où il a été classé à la 118ème position comparé au Sultanat d'Oman qui est classé en quatrième position.

Vu que le secrétariat général du Conseil supérieur de défense, qui est rattaché directement au premier ministre, a œuvré sans relâche pour élever le niveau de sensibilisation dans le domaine de cybersécurité,

Vu que la Commission Européenne a présenté une méthodologie de développement du plan de cybersécurité et a exprimé sa volonté d'apporter son aide à l'État libanais dans ce domaine, sous condition que la relation entre la Commission et l'État soit une relation centralisée afin d'éviter la fragmentation des efforts, et que l'État soit prêt à exprimer de manière correcte et précise ses besoins, et que dans ce but, l'État propose une feuille de route unifiée, bâtie sur une stratégie claire, ainsi qu'un dispositif exécutif pour mettre en œuvre cette stratégie accompagné d'un plan de financement bien défini et des résultats garantis,

Vu que la commission européenne a déjà élaboré des orientations pour accompagner cette vision de développement au profit des institutions militaires, de sécurité et des organes judiciaires, et qu'elle est prête à mobiliser l'expertise nécessaire des états membres en faveur d'une initiative centralisée présentée par l'État libanais à cet égard,

Considérant que le premier ministre et le secrétariat général du conseil des ministres sont en cours d'élaboration d'un plan de modernisation de la direction général de la présidence du conseil des ministres visant à la transformer en une institution à la pointe au niveau national en matière d'automatisation à travers l'implémentation d'un plan graduel d'automatisation des ses fonctions. Ce plan prévoit également un chantier de modernisation de la structure de la direction, particulièrement à travers la mise en œuvre de technologies informatiques avancées qui prend nécessairement en compte la dimension sécuritaire à travers la centralisation et la sécurisation des données,

En conséquence de quoi, et à la suite de multiples réunions de travail, nous sommes arrivés à établir une feuille de route préliminaire qui comporte la mise en place de la commission nationale de la lutte contre la cybercriminalité et le renforcement de la cybersécurité, chargée de la préparation d'une stratégie nationale pour la cybersécurité et la lutte contre la cybercriminalité et dont les missions sont:

1. Développement d'une stratégie nationale pour la défense, la dissuasion et le renforcement contre les cyberattaques et la cybercriminalité.

2. Participation à la préparation de la structure administrative de l'institution nationale placée sous l'autorité de la Présidence du conseil des ministres et qui prendra en charge la mise en œuvre continue de la stratégie nationale de cybersécurité dans ses différentes composantes, et qui ne soit pas incompatible avec la projet de modernisation de la structure de la Présidence du conseil des ministres en cours, en particulier dans tout ce qui concerne les techniques de l'information et de la communication.

3. Invitation des diverses administrations et organismes du secteur public, militaires et civils, impliqués dans cet effort à désigner chacun une personne les représentant au sein de la commission nationale afin d'assurer la plus large participation de toutes les parties prenantes ainsi que l'adhésion aux directives de la commission sur ce sujet qui est devenu un secteur d'activité à part entière compte tenu de la multiplicité et la complexité des tâches, des techniques et des procédures ainsi que le développement rapide dont il témoigne. L'expertise requise de cette personne et le type d'activité administrative qu'elle est appelée à exécuter seront déterminés dans le plan général.

Les participants à la commission:

- Présidence de la République
- Présidence de la Chambre des Députés
- Présidence du Conseil des Ministres – Coordinateur National des Technologies de l'Information et de la Communication
- Secrétariat général du Conseil Supérieur de Défense
- Ministère des Finances
- Ministère de la Défense – Commandement de l'Armée – Direction du Renseignement
- Ministère de l'Intérieur et des Municipalités – Direction Générale de la Sûreté Générale – Forces de Sécurité Intérieure
- Sécurité de l'État
- Ministère des Télécommunications (les directions générales – Ogero)
- Banque du Liban – secteur bancaire – SIC
- Conseil Supérieur pour la Privatisation

La commission sera assistée par des représentants des administrations suivantes:

- Ministère des Affaires Étrangères et des Immigrés
- Ministère de l'Économie et du Commerce
- Ministère de l'Industrie
- Conseil Économique
- Autorité de Régulation du Secteur des Télécommunications
- Bureau du Ministre d'État pour la Réforme Administrative
- Ministère de l'Éducation et de l'Enseignement Supérieur
- Université Libanaise
- Autres institutions et organismes

Groupe de travail

Pour l'État Libanais

Général de division Saadallah Al Hamad	Secrétaire général du Conseil Supérieur de Défense
Général de brigade l'ingénieur Wajdi Chamseddine	Secrétariat Général du Conseil Supérieur de Défense
Général de brigade Tony Kahwaji	Commandement de l'Armée – Direction du Renseignement – Chef du Service Technique
Juge Hania Al Helweh	Déléguée du Ministère de la Justice pour la cybersécurité
Dr. Lina Oueidat	Conseillère du Premier ministre pour les Technologies de l'Information et de la Communication – Coordinateur National TIC

Pour l'Union Européenne

Mr. Jérôme Ribault-Gaillard	Expert anti-terrorisme