Vers une stratégie nationale de cybersécurité

PASCAL BOU NASSAR, BASSEM HAIDAR, MONA AL ACHKAR
Agence universitaire de la Francophonie
Université Libanaise
Beyrouth, Liban
pascal.bou-nassar@auf.org, bassem.haidar@ul.edu.lb, moacja@ul.edu.lb

Résumé: - La révolution numérique gagne du terrain dans toutes les sphères du monde moderne. Plus que jamais, notre société profite du cyberespace pour son développement technologique, économique, social, culturel, scientifique et politique. Dans le même temps, notre dépendance croissante au cyberespace a apporté de nouveaux risques. Les données et les systèmes clés sur lesquels nous nous appuyons peuvent être facilement compromis ou endommagés. Dans ce contexte, le Liban est devenu particulièrement vulnérable. Société de service avant tout, la rapidité de l'évolution technologique ainsi qu'un certain nombre de facteurs spécifiques - organisationnelles, techniques, politiques et militaires – rendent le pays plus sensible aux risques. Dans ce papier, nous présentons une stratégie nationale de sécurité pour le Liban dont les objectifs sont inspirés d'autres stratégies nationales. Des approches applicatives sont proposées pour répondre aux défis particuliers du pays. Enfin, nous terminons par une proposition de création d'un Centre National de Cybersécurité et Cyberdéfense regroupant quatre entités dont le but sera d'assurer la stratégie nationale de sécurité.

Mots clefs: - Stratégie nationale de sécurité – Cybersécurité – Cyberdéfense – CERT – CNIL

1 Introduction

Le numérique a non seulement révolutionné le monde mais aussi pris place dans tous les domaines de notre vie quotidienne, modifiant nos modes de communication et facilitant nos échanges. Cependant, la prolifération des services fournis et la diversité des accès aux systèmes informatiques a fait émerger de nouveaux risques menaçant la sécurité des données. Afin de protéger nos vies privées, de préserver le bien-être social et d'assurer la stabilité économique, il est indispensable d'aborder cette problématique par une approche de gouvernance de la sécurité des systèmes d'information.

La société libanaise ainsi que son économie dépendent aujourd'hui fortement des nouvelles technologies. A titre d'exemple, le secteur bancaire, pilier de l'économie libanaise, fait aujourd'hui un appel massif au numérique : e-banking, paiement par téléphones portables, et forte collaboration entre les banques. De même, le secteur clef du tourisme, ne peut se passer de l'outil technologique nécessaire à son développement et à son bon fonctionnement (communication, services de réservations, paiement en ligne...). De la même manière, le numérique pénètre aujourd'hui les autres secteurs de notre société : les services médicaux, le secteur de l'éducation, le domaine militaire, les opérateurs de télécommunications, etc. Toutefois, la disponibilité et l'assurance d'un fonctionnement intègre tout comme l'empêchement de toute interruption et abus de service font face à de nombreux défis liés à différentes dimensions :

- Une dimension organisationnelle:

- Les acteurs : la cybersécurité concerne de nombreux acteurs tant du secteur public que du secteur privé parmi lesquels les ministères, les établissements financiers, les établissements scolaires et universitaires, les opérateurs de télécom ou encore les fournisseurs d'accès internet. Ces différents acteurs ne partagent pas la même vision de la cybersécurité et traitent ses défis de façons différentes. A titre d'exemple, si le ministère de la défense nationale et les institutions financières accordent une grande attention à cette nouvelle

problématique, les autres acteurs s'impliquent beaucoup moins.

- La coopération dans ce domaine (échange de bonnes pratiques en matière de cybersécurité, capitalisation de l'expérience et de l'expertise), au niveau national entre les différents protagonistes reste faible. En effet, l'échange d'informations entre les acteurs des différents secteurs est confronté à de nombreuses contraintes juridiques, politiques voire économiques. La collaboration aux échelons régional et international est encore moindre.
- Les rôles de chaque acteur en termes de gestion de la sécurité au niveau national ne sont pas définis. A titre d'exemple, aucune entité ne s'avère responsable d'identifier et de gérer les événements de sécurité et de le notifier aux acteurs concernés.
- La classification des différents services, infrastructures critiques et données sensibles n'étant pas réalisée, d'où une protection inadéquate.
- La sensibilisation et la formation du personnel (technique et non technique) à la cybersécurité n'entre pas dans un cadre de gouvernance établi et contraignant, et reste ainsi à l'appréciation des différents acteurs.
- La sélection du personnel n'étant pas encadré, le risque d'infiltration par des agents extérieurs dans divers domaines pouvant compromettre la sécurité des systèmes est non négligeable.

- Une dimension légale:

Les défis soulevés au niveau législatif sont liés à plusieurs éléments dont : la nature du cyberespace ; qui est ouverte et qui ne connaît pas de frontières, autres que celles de la technologie, l'infrastructure qui traverse plusieurs souverainetés et qui est contrôlée et managée non seulement par les États mais aussi par le secteur privé (comme c'est le cas aux États-Unis), l'interconnexion des dimensions sociales, économiques, technologiques et politiques quant à la gouvernance et la gestion des ressources de l'internet. Tout cela, sans oublier la nature technologique du cyberespace, en évolution continue et rapide, face à la lenteur du droit, qui peut rendre les législations désuètes. Ces défis touchent aux points suivants :

- La protection de l'ordre publique : L'utilisation illicite des systèmes et des technologies numériques en général, dite cybercriminalité, ruine la confiance dans le cyberespace, et entrave le développement de l'économie numérique. Effectivement, les cas d'abus du cyberespace à des fins criminelles, se font de plus en plus nombreux. Les crimes cybernétiques visent les biens et les personnes (le vol et la falsification de cartes de crédit, et l'utilisation non autorisée d'ordinateur, le vol d'identité et la fraude à l'identité, la cyber intimidation, contenu illégal etc…) ainsi que l'État dans les attaques terroristes, ou celles visant l'infrastructure telles que les systèmes d'alimentation électrique ou de télécommunication et qui peuvent déstabiliser un pays.
- Les poursuites et les investigations en dehors du terrain national, ainsi que l'échange d'informations sur les incidents, et sur les personnes créent des conflits et engendrent des difficultés dû au principe de la souveraineté des États, qui empêche les autorités judiciaires et policière d'un pays, d'intervenir sur le terrain national d'un autre, sauf autorisation de l'État concerné.
- La coopération dans la lutte contre la cybercriminalité, entre les différentes administrations gouvernementales exige un échange de données personnelles et d'informations, qui peut être entravée par l'absence de cadre législatif l'autorisant.
- La protection des personnes physiques et morales qui doit être assumée par l'État, face à la collecte massive d'informations utilisée à des fins commerciales, comme la publicité, ou bien, dans le cadre des opérations d'espionnage industrielle .
- L'établissement d'un équilibre entre les exigences de la protection de la sécurité nationale et celles de la protection des libertés civiles. Dans l'exercice de son rôle d'autorité publique, responsable de l'ordre et de la sécurité, les données personnelles

(nom, communication, téléphone, déplacements, domicile etc…), sont des ressources précieuses pour les forces de l'ordre. Pourtant, en l'absence de cadre législatif, d'autorité compétente, et de mécanisme de protection, la collecte de ces données peut servir à abuser des libertés et droits, telle que la liberté d'expression, la vie privée, et le droit de l'accès à l'information. Sur un autre plan, le filtrage, la surveillance, et l'interception des communications exercées hors la loi, représentent un danger supplémentaire.

- L'adaptation des systèmes et des principes juridiques, aux exigences de nouvelles formes de contrats et de service (externalisation, cloud computing, etc…). Les obligations et les droits a un contrat sont décidés en fonction de la nature des contrats traditionnels faits sur papier ou oralement, alors que, la nature des contrats électroniques, et les services émergeants, imposent d'autres moyens de preuve et probablement, d'autres principes de responsabilité. Il est important, par exemple, de préciser qui sera responsable de la perte des données sauvegardées, dans le cloud, ou de la divulgation des secrets industrielles, ou personnelles, dans les contrats d'externalisation, et quelle loi sera appliquée aux conflits les concernant.

S'agissant de la dimension technique, plusieurs problèmes sont à souligner, parmi lesquels :

- L'utilisation des logiciels piratés (applications ou systèmes d'exploitation) dans les secteurs public et privé conduit à des intrusions dans les systèmes et les réseaux à cause des portes dérobées (backdoors). Ces intrusions créent des vulnérabilités au niveau des systèmes les exposant ainsi à toute sorte d'attaque. En outre, les logiciels piratés ne permettant pas les mises à jour périodiques nécessaires, les failles de sécurité s'accroissent avec le temps.
- L'accès internet non contrôlé accroît également les risques. A titre d'exemple, les routeurs sans fils résidentiels sont installés avec une sécurité minimale permettant des accès non autorisé aux réseaux. Par ailleurs, la distribution de l'accès Internet dans certaines régions n'étant pas encadrée, certains fournisseurs ne gardent pas traces des activités permettant de garantir un anonymat aux attaques.
- La distribution des cartes SIM sans enregistrement et le trafic illégal des téléphones portables permet de masquer l'identité des intrus sur les réseaux mobiles.

Il faut également ajouter à cela, des éléments de protection matérielle comme la sécurité des locaux techniques et la limitation de leur accès mais aussi les problèmes d'électricité qui posent autant de risques pour la confidentialité, la disponibilité et l'intégrité des services.

- Une dimension militaire :

Les travaux sur la cyberdéfense n'ont pas atteint une maturité jusqu'à ce jour et se limitent à des initiatives séparés au niveau de différents services et des acteurs dans le domaine. Nous ajoutons à cette dimension le conflit israélo-arabe, et le déséquilibre des niveaux technologiques.

Afin de prendre en compte ces différentes dimensions et d'assurer une sécurité globale, l'élaboration d'une stratégie nationale de sécurité est primordiale. Dans ce qui suit, nous présentons brièvement les éléments communs des stratégies nationales existantes dans divers pays afin de proposer un modèle pour l'élaboration de la stratégie nationale de sécurité au Liban.

2 Les stratégies nationales de sécurité

La stratégie de sécurité a pour but de renforcer la sécurité et la résilience des infrastructures et contribuera à assurer, dans l'environnement numérique, la protection des citoyens, des professionnels et des acteurs de la vie publique. Jusqu'à ce jour différents pays ont élaboré leur propre stratégie nationale de sécurité à partir desquels nous avons identifié les objectifs stratégiques communs suivants :

1. Classer, établir et mettre en œuvre les exigences de sécurité minimales pour protéger les infrastructures critiques. [SGDN], [BMI], [MCSI], [MoICT], [MoED].
2. Sécuriser et protéger les systèmes gouvernementaux. [AG], [BMI], [MoED].
3. Promouvoir et développer la coopération nationale et internationale. [GGDL], [BMI], [KSK], [MSCI], [DSS].
4. Développer une culture de sensibilisation à la cybersécurité au niveau national et renforcer les capacités des ressources humaines, développer l'expertise nationale et la sensibilisation de la sécurité de l'information. [BMI], [KSK], [GGDL], [MoICT], [MoED], [DSS].
5. Moderniser le cadre juridique, adopter un cadre réglementaire approprié pour appuyer l'utilisation sûre des systèmes d'information [KSK], [GGDL], [MSCI].

En se basant sur ces objectifs communs, nous élaborons dans ce qui suit l'approche et le domaine d'action pour une éventuelle stratégie nationale de sécurité au Liban.

3 Stratégie Nationale de Sécurité

La mise en œuvre d'une feuille de route élaborant la stratégie nationale de sécurité au Liban doit adopter les objectifs communs au contexte du pays. Pour cela, nous élaborons des priorités selon les quatre dimensions mises en avant : organisationnelle, légale, technique et enfin militaire.

Au niveau de la dimension organisationnelle, nous priorisons :

- la classification des infrastructures techniques en identifiant dans une première phase les organisations à prendre en compte et en classant comme critiques celles assurant des services essentiels à la société.
- la coopération au niveau national : la communauté universitaire du Liban, les organisations non gouvernementales et le secteur privé doivent se joindre au gouvernement dans la sécurisation des systèmes d'information. Chacun de ces acteurs a des capacités technologiques et analytiques uniques à offrir, et un intérêt fort à sécuriser leurs propres systèmes. Leur collaboration est donc essentielle pour assurer une sécurité globale.
- Une politique à court et moyen terme doit être mise en place pour supporter la création de ressources humaines qualifiées dans le domaine de la cybersécurité. Une prise de conscience de la part des utilisateurs des risques et dangers du cyberespace est une nécessité. A cette fin, nous proposons de sensibiliser les élèves et les étudiants dans les établissements scolaires et universitaires à travers l'organisation de colloques et de conférences. Le but sera de construire à terme une culture de compréhension des risques et de permettre aux gens d'utiliser le numérique en développant leurs compétences à tous les niveaux.
- Les savoir-faire techniques et la capacité de réagir face aux incidents doivent être renforcés par une collaboration entre le secteur public et privé, l'encouragement à des projets de recherche et par la création de formations professionnelles.

Au niveau juridique, il est impérativement nécessaire d'élaborer un cadre législatif adapté, qui permettra de répondre aux exigences de la sécurité des systèmes informatiques, de la protection de la vie privée, et de l'économie numérique. Pour cela, ce cadre devra prendre en considération les points suivants :

- définir les cybercriminalités en tenant compte des tendances mondiales et des conventions internationales. Le but à terme étant de permettre une coopération régionale et internationale efficace dans la lutte contre la cybercriminalité.
- reconnaître aux documents électroniques, ainsi qu'aux correspondances et signature électroniques la force probatoire.
- créer les entités administratives et institutionnelles pouvant prévoir, détecter, définir et répondre aux risques cybernétiques. Autrement dit, agir au lieu de réagir.

- mettre en place des autorités de protection des libertés civiles, et des citoyens contre l'abus dans la collecte des informations, ainsi que dans la surveillance.
- reconnaître les responsabilités des différents acteurs dans la société de l'information et du savoir, tels que : les fournisseurs de services et de contenu, les services de publicité, les moteurs de recherche, les fabricants des softwares, etc…
- protéger les citoyens en général, et plus spécialement certaines tranches d'âge ou classes sociales contre le contenu illégal en ligne.
- prévoir un renforcement des formations continues et des capacités d'action des instances de justice et de police dans le domaine des nouvelles technologies, pour qu'ils soient capables de coopérer avec leurs homologues, au niveau régional et international.

Au niveau de la dimension technique, nous priorisons la création d'un CERT (Computer Emergency Response Team) au niveau national et de CERT privés afin de gérer les incidents de sécurité. Ces équipes d'experts techniques mettront en place des systèmes de détection et de prévention d'intrusions au niveau des infrastructures et systèmes critiques et des plans d'urgence en cas d'incidents majeurs. En outre, les savoir-faire techniques et la capacité de réagir face aux incidents devront être renforcés par une collaboration entre ces différentes équipes d'experts.

Au niveau de la dimension militaire, nous priorisons la collaboration entre les différents acteurs du domaine, voire les forces de sécurité intérieure, l'établissement de la Sûreté Générale et l'Armée Libanaise.

Vu les défis que soulève la cybersécurité au Liban et dans l'objectif de faciliter le développement, la mise en œuvre et la mise à jour d'une stratégie nationale de sécurité, nous proposons dans la partie suivante la création du Centre National de Cybersécurité et Cyberdéfense (CNCC) dont le rôle sera de centraliser le travail sur les quatre dimensions mentionnées dans ce papier.

4 Centre National de Cybersécurité et Cyberdéfense (CNCC).

Comme le montre la Figure1, le Centre National de Cybersécurité et Cyberdéfense sera composé de quatre entités :

1- Le Centre de Recherche, de développement et d'innovation (CRDI) qui aura pour mission de favoriser et de promouvoir le développement des projets en cybersécurité et cyberdéfense en créant et consolidant des partenariats entre les différents acteurs des secteurs privé et public. En rassemblant des équipes académiques, industrielles, et militaires, le CRDI offrira plusieurs services parmi lesquels :

- L'analyse et la recherche stratégique
- Le développement des capacités humaines et militaires en matière de cybersécurité et cyberdéfense.
- Le développement d'événements scientifiques, d'actions d'éducation et de formation et de sensibilisation.

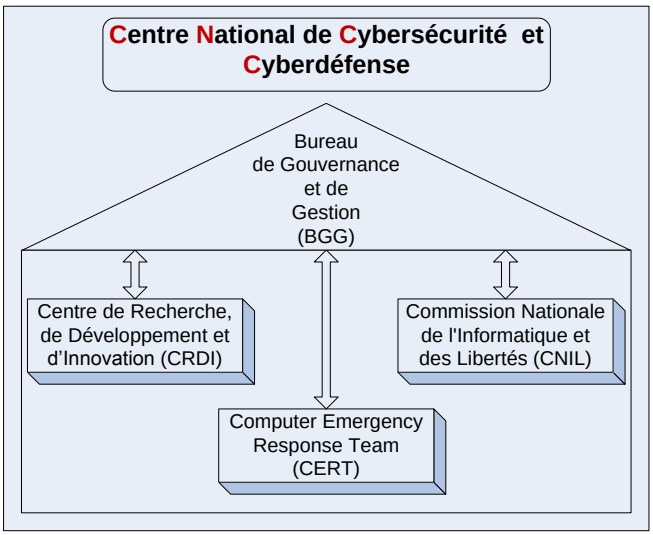

Figure 1 : Centre National de Cybersécurité et Cyberdéfense

2- La Commission Nationale de l'Informatique et des Libertés (CNIL) a pour mission de veiller à la protection des données personnelles, de l'identité humaine, des droits de l'homme, de la

vie privée et des libertés individuelles ou publiques. Parmi ses fonctions :

- Informer les personnes sur leurs droits et obligations.
- Vérifier si les personnes respectent les lois, sinon émettre des sanctions.
- Réguler et recenser les données et autoriser les traitements les plus sensibles avant leurs mises en place [CNIL]

3- Le 'Computer Emergency Response Team' CERT dont le rôle se focalise sur la dimension technique, se charge principalement des fonctions suivantes :

- Identification en temps réel des intrusions sur les infrastructures et services critiques.
- Mettre en place des plans d'urgences et de continuité des services et infrastructures critiques.
- Coordonner avec les différents acteurs sur des incidents de grande ampleur affectant la sécurité des réseaux.

Enfin, le Bureau de Gouvernance et de Gestion (BGG) dont l'objectif principal est d'améliorer la sécurité des systèmes d'information aura le rôle suivant :

- Elaborer et mettre en œuvre la stratégie nationale de sécurité en concertation avec les différents acteurs.
- Centraliser la décision au sujet de la sécurité des systèmes d'information, partager l'expérience et l'expertise dans le domaine entre les différents acteurs.
- Gérer les activités et le bon fonctionnement du CNCC (les différentes entités : CRDI, CERT, CNIL).

Le CNCC devra être créé par l'Etat et subventionné par le secteur privé.

5 Conclusion

La révolution technologique a créé de nouveaux risques qui menacent la vie privée des utilisateurs portant atteinte au bien-être social et empêchant le développement économique. Cette étude met en valeur l'urgence et la nécessité de l'application d'une stratégie nationale de sécurité. Nous avons identifié et catégorisé les principaux défis auxquels doit faire face cette stratégie, pour ensuite mettre en avant les principaux objectifs à atteindre, et enfin proposer la formation d'un centre National de Cybersécurité et Cyberdéfense regroupant des entités capables de protéger et défendre les données des dangers du numérique.

References:

[AG] (2009) *Cyber Security Strategy*, Office of the Attorney General, Australia, disponible sur http://www.ag.gov.au

[BMI] (2011) *Cyber Security Strategy for Germany*, Federal Ministry of the Interior, Berlin, Germany, disponible sur http://www.cio.bund.de

[CNIL] - Commission nationale de l'informatique et des libertés.", disponible sur : http://www.cnil.fr/

DSS (2012) *Statement on the Approval by Cabinet of the Cyber Security Policy Framework for South Africa*, Department of State Security, Pretoria, South Africa, disponible sur : http://www.info.gov.za

[GGDL] (2011) *Stratégie Nationale en Matiére de cyber Sécurité*, Le Gouvernement du Grand-Duché de Luxembourg, Luxembourg, Luxembourg, disponible sur : http://www.gouvernement.lu

[KSK] (2008) *Cyber Security Strategy*, Cyber Security Strategy Committee, Ministry of Defence, Tallinn, Estonia, disponible sur: http://www.mod.gov.ee

[MoED] (2011) *New Zealand's Cyber Security Strategy*, Ministry of Economic Development, New Zealand, disponible sur: http://www.med.govt.nz

[MoICT] (2011) *National Information Security Strategy*, Ministry of Information and Communication Technology, Republic of Uganda, disponible sur : http://www.ict.go.ug

[MSCI] (2011) *Strategia de Securitate Cibernetică a României*, Bratislava, Romania, disponible sur http://www.mcsi.ro

[SGDN] (2011) Défense et Sécurité des Systèmes D'information: Stratégie de la France, Paris, France, disponible sur : http://www.ssi.gouv.fr/

[TWH] (2003) *The National Strategy to Secure Cyberspace*, The White House, USA, disponible sur http://www.uscert.gov