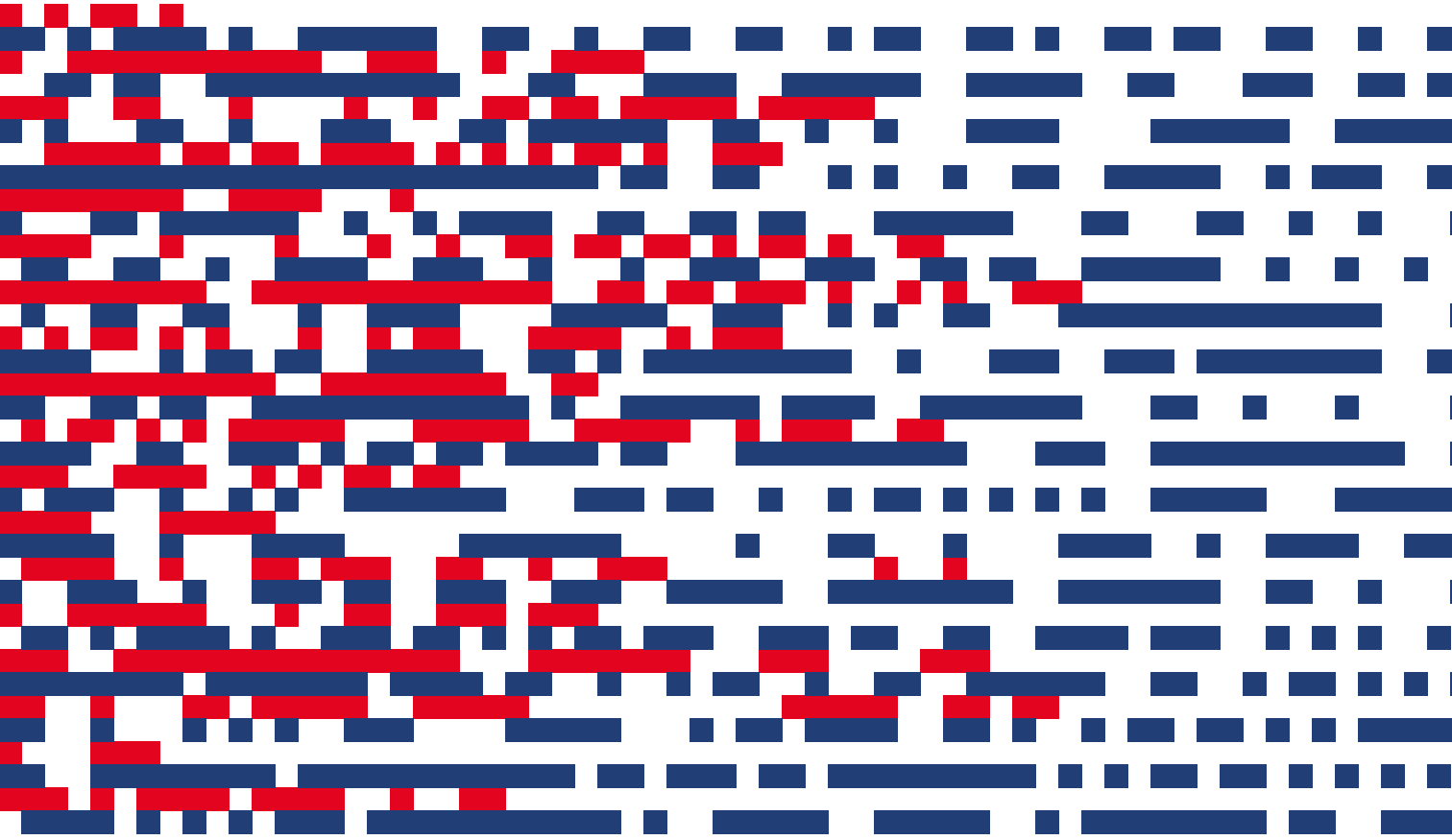
STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III



VERSION FRANÇAISE

Approuvée et rendue exécutoire par le Conseil de gouvernement le 26 janvier 2018.

· AVANT-PROPOS DU PREMIER MINISTRE, MINISTRE D'ÉTAT ·

J'ai le plaisir de vous présenter la nouvelle stratégie nationale en matière de cybersécurité pour la période 2018-2020. Elle illustre la réponse que le Gouvernement entend donner aux défis et transformations qui caractérisent un environnement numérique en constant changement.

La stratégie a été élaborée par un groupe de travail réunissant, sous la présidence du Haut-Commissariat à la Protection nationale, des représentants du Centre des technologies de l'information de l'État, du CERT gouvernemental, de l'ANSSI, du Service des médias et des communications, du Ministère de l'Économie, du Ministère des Affaires étrangères et européennes, de la Défense luxembourgeoise, du Service de renseignement de l'État et de la Police grand-ducale.

Elle traduit au niveau national les objectifs du paquet sur la cybersécurité que la Commission européenne vient de publier et s'inscrit dans la continuité d'une série de mesures récemment adoptées par le Gouvernement, que ce soit au niveau des procédures de gestion d'une cyberattaque, de la gouvernance en matière de cybersécurité ou encore de la promotion de la cybersécurité auprès des entreprises avec l'inauguration du « Cybersecurity Competence Center ». Permettez-moi de soulever, dans ce contexte, que le Forum économique mondial a classé le Luxembourg, dans son rapport 2017, en première position parmi 137 pays évalués en termes d'aptitudes technologiques, grâce à l'agenda de digitalisation ambitieux que le Gouvernement a poursuivi ces dernières années.

Prenant en considération l'expérience acquise dans le contexte de la mise en œuvre de la deuxième stratégie adoptée en mars 2015, et les conclusions tirées d'une analyse générale des cybermenaces, cette troisième stratégie trace le cadre pour profiter pleinement des nouvelles opportunités numériques, tout en donnant une réponse aux risques liés à une connectivité toujours plus importante.

A cette fin, la stratégie cherche d'abord à renforcer, dans l'esprit de l'initiative « Digital Lëtzebuerg » la confiance du public dans l'environnement numérique afin de permettre aux citoyens d'en profiter intégralement. Elle vise ensuite à renforcer la sécurité des systèmes d'information, à améliorer la capacité à identifier des cyberattaques, à protéger les infrastructures numériques critiques et à sensibiliser les acteurs au sujet de la résilience. Elle dépasse, enfin, le seul aspect de la sécurité et de la sensibilisation, pour tenir compte des enjeux stratégiques de l'infrastructure numérique pour notre économie et pour faire de la cybersécurité un facteur d'attractivité économique.

Xavier Bettel

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

SOMMAIRE

Stratégie nationale en matière de cybersécurité III (SNCS III) 10
Définition de la cybersécurité 10

1. Gouvernance en matière de cybersécurité 11

1.1. Principales entités étatiques intervenant au niveau national en matière de cybersécurité 11
1.2. Comité interministériel de coordination en matière de cyberprévention et de cybersécurité 13

2. Lignes directrices de la stratégie nationale en matière de cybersécurité 15

2.1. Ligne directrice n° 1 – renforcement de la confiance publique dans l'environnement numérique 15

2.1.1. **Objectif 1 :** Partage des connaissances entre tous les acteurs 16
2.1.2. **Objectif 2 :** Diffusion de l'information sur les risques 16
2.1.3. **Objectif 3 :** Sensibilisation de toutes les parties concernées 16
2.1.4. **Objectif 4 :** Divulgation responsable 17
2.1.5. **Objectif 5 :** Lutte contre la cybercriminalité 17

2.2. Ligne directrice n° 2 – protection des infrastructures numériques 19

2.2.1. **Objectif 1 :** Recensement de l'infrastructure numérique essentielle et critique 19
2.2.2. **Objectif 2 :** Politiques de sécurité 19
2.2.3. **Objectif 3 :** Gestion de crise 20
2.2.4. **Objectif 4 :** Normalisation 20
2.2.5. **Objectif 5 :** Renforcement de la coopération internationale 21
2.2.6. **Objectif 6 :** Cyberdéfense 21
2.2.7. **Objectif 7 :** Renforcement de la résilience de l'infrastructure numérique de l'État 21

2.3. Ligne directrice n° 3 – promotion de la place économique 23

2.3.1. **Objectif 1 :** Création de nouveaux produits et services 23
2.3.2. **Objectif 2 :** Mutualisation d'infrastructures de sécurité 24
2.3.3. **Objectif 3 :** Référentiels d'exigences et maître d'œuvre 24
2.3.4. **Objectif 4 :** Création du Centre de Compétences en Cybersécurité (C3) 25
2.3.5. **Objectif 5 :** Gestion du risque et gouvernance informée 26
2.3.6. **Objectif 6 :** Formation et aides à la formation 26
2.3.7. **Objectif 7 :** Collaboration entre responsables de la sécurité de l'information 26
2.3.8. **Objectif 8 :** Collaboration entre experts en matière de réponse aux incidents 27
2.3.9. **Objectif 9 :** Priorité à la recherche : les start-ups 27
2.3.10. **Objectif 10 :** Le désassemblage de code et l'identification de vulnérabilités 27

2.4. Mise en œuvre de la SNCS III 29

3. Annexes 31

3.1. Retour d'expérience sur la stratégie nationale en matière de cybersécurité II 31

3.1.1. **Objectif 1 :** Renforcer la coopération nationale 31
3.1.2. **Objectif 2 :** Renforcer la coopération internationale 32
3.1.3. **Objectif 3 :** Augmenter la résilience de l'infrastructure numérique 32
3.1.4. **Objectif 4 :** Combattre la cybercriminalité 33
3.1.5. **Objectif 5 :** Informer, former et sensibiliser sur les risques encourus 34
3.1.6. **Objectif 6 :** Mettre en place des normes, standards, certificats, labels et référentiels d'exigences pour l'État et les infrastructures critiques 35
3.1.7. **Objectif 7 :** Renforcer la coopération avec le monde académique et de la recherche 35

3.2. Analyse des menaces au niveau national en matière de cybersécurité 37

3.3. Glossaire 40

INTRODUCTION

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

· INTRODUCTION ·

Le caractère évolutif qui caractérise l'environnement numérique en général et les technologies de l'information et de la communication en particulier a des répercussions directes sur notre vie quotidienne. De nos jours, nous sommes habitués à l'émergence ainsi qu'au développement à grande échelle, et surtout très rapide, de nouvelles technologies d'une part et à l'apparition de nouveaux vecteurs de risque qui accompagnent cette évolution d'autre part. L'adaptation de notre société aux transformations massives qui sont le corollaire de cet environnement numérique en constant changement reste un processus complexe.

A l'approche de la fin de la période couverte par la deuxième stratégie nationale en matière de cybersécurité, le « Cybersecurity Board » (CSB) a chargé un groupe de travail, composé de représentants du Centre des technologies de l'information de l'État (CTIE), du Centre gouvernemental de traitement des urgences informatiques (GOVCERT), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), du Service des médias et des communications, du Ministère de l'Économie, du Ministère des Affaires étrangères et européennes, de la Défense luxembourgeoise, du Service de renseignement de l'État et de la Police grand-ducale, et opérant sous la responsabilité du Haut-Commissariat à la Protection nationale, d'élaborer une nouvelle stratégie nationale en matière de cybersécurité. Le but est de donner une réponse aux transformations profondes mentionnées ci-avant et de consolider la confiance du public dans les nouvelles technologies, cela nonobstant l'apparition de plus en plus fréquente de cyberattaques de nature très variée, souvent organisées sur un plan transnational. Une autre préoccupation inhérente à la stratégie consiste à créer un environnement qui permet d'accompagner activement, dans l'intérêt du développement de notre économie numérique, l'approfondissement de nouveaux sujets comme l'internet des objets, l'intelligence artificielle, la technologie des algorithmes avancés ou encore l'ubiquité des technologies à double usage potentiel.

La nouvelle stratégie nationale en matière de cybersécurité montre que le Gouvernement est conscient aussi bien des opportunités que des risques inhérents aux nouvelles technologies. C'est dans cette optique que la stratégie, qui couvre la période 2018-2020, s'articule autour des trois lignes directrices centrales suivantes :

- **le renforcement de la confiance publique dans l'environnement numérique**, afin de permettre la transition numérique du Luxembourg vers un modèle de « Smart nation », qui sera durable du point de vue économique, social, environnemental et politique, notamment en respect du programme pour un développement durable à l'horizon de 2030 des Nations Unies ;
- **la protection des infrastructures numériques**, afin de garantir la disponibilité des services essentiels ainsi que l'intégrité et la confidentialité de l'information, et enfin
- **la promotion de la place économique**, notamment par la création d'un environnement propice à l'établissement et à l'épanouissement d'entreprises actives dans le domaine numérique.

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

La nouvelle version de la stratégie nationale en matière de cybersécurité tient compte du retour d'expérience de la stratégie couvrant la période 2015-2017, dont le détail est repris en annexe à partir de la page 22, et des conclusions d'une analyse générale sur les cybermenaces qui se trouve en annexe à partir de la page 27.

Le sujet de la cybersécurité couvre toute une série de mesures susceptibles d'être prises pour améliorer la résilience et la défense des systèmes et réseaux informatiques, d'une part, et des technologies numériques au sens général, d'autre part, contre des cyberattaques de nature très variée.

Afin de pérenniser la gouvernance en matière de cybersécurité et de faciliter la mise en œuvre des objectifs de la SNCS III, un comité de coordination interministériel a été mis en place par le Gouvernement. Un certain nombre des objectifs inscrits dans la deuxième stratégie restent d'actualité et sont partant repris, tout en étant adaptés à l'environnement actuel.

DÉFINITION DE LA CYBERSÉCURITÉ[1]

« On entend par cybersécurité l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs. Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement. La cybersécurité cherche à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs soient assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement. Les objectifs généraux en matière de sécurité sont les suivants :

- Disponibilité ;
- Intégrité, qui peut englober l'authenticité et la non-répudiation ;
- Confidentialité. »

[1] *Recommandation UIT–T X.1205 suivant la résolution des Nations Unies numéro 181 (Guadalajara/2010)*

1. GOUVERNANCE EN MATIÈRE DE CYBERSÉCURITÉ

Les défis actuels et futurs relatifs à la cybersécurité ne peuvent être maitrisés que moyennant une gouvernance nationale cyber efficace et efficiente. Considérant les engagements du Luxembourg en faveur de la cyberdéfense au niveau de l'OTAN et de l'Union européenne, les accords de coopération et de partage d'informations européens et internationaux à différents niveaux, l'impact de l'implémentation de la directive de l'Union européenne relative à la sécurité des réseaux et des systèmes d'information, ainsi que le caractère horizontal des sujets qui relèvent de la cybersécurité, le modèle de gouvernance existant sera renforcé par la mise en place d'un comité interministériel de coordination en matière de cyberprévention et cybersécurité.

PRINCIPALES ENTITÉS ÉTATIOUES INTERVENANT AU NIVEAU NATIONAL EN MATIÈRE DE CYBERSÉCURITÉ.

Le grand nombre de secteurs, de domaines et de politiques touchés par la cybersécurité fait que le sujet relève de la responsabilité et des attributions de plusieurs entités étatiques.

- Le Ministère de l'Économie est chargé, en application de l'arrêté grand-ducal du 28 janvier 2015 portant constitution des ministères, de la sécurité informatique, de la sensibilisation aux risques et des vulnérabilités du secteur privé. Dans ce contexte, le Groupement d'intérêt économique Security Made in Luxembourg (GIE Smile), plateforme de promotion de la cybersécurité, opère notamment les initiatives CASES (promotion de la sécurité de l'information dans les entreprises), C3 (centre national de compétences en cybersécurité) et le CIRCL (service de coordination et d'action post-incidents), ce dernier exerçant également la fonction de CERT pour les entités privées et non gouvernementales et les communes.

- La Défense luxembourgeoise (Ministère des Affaires étrangères et européennes (MAEE) - Direction de la Défense et l'Armée luxembourgeoise) est en charge des aspects de cybersécurité qui relèvent de ses attributions nationales et des obligations générées au sein de l'OTAN et de l'UE.

- Le Ministère d'État – Service des Médias et des Communications suit le Conseil Telecom qui discute au niveau européen, tant de la stratégie européenne en matière

de cybersécurité que du « paquet sur la cybersécurité ». Le Service des Médias et des Communications coordonne également les travaux du Cybersecurity Board qui relève, en vertu de l'arrêté grand-ducal du 28 janvier 2015 portant constitution des ministères, de la compétence du Ministère d'État.

- Le Ministère des Affaires étrangères et européennes coordonne les travaux au niveau du groupe de travail horizontal « Cyber » du Conseil de l'Union européenne, qui vient d'élaborer la « boîte à outils cyberdiplomatique » adoptée en juin 2017 et appelée à évoluer, alors que la dimension internationale des menaces, tout comme celle de la réponse aux menaces, s'amplifiera.

- Le Centre des technologies de l'information de l'État voit sa mission régie par sa loi organique modifiée du 20 avril 2009. Il a, entre autres, pour mission d'assurer, dans le cadre de ses attributions, la sécurité de l'informatique, la gestion des équipements électroniques et informatiques et de sécurité appropriée, l'administration du réseau informatique de l'État ainsi que la production de documents administratifs sécurisés.

- Le Service de Renseignement de l'État a, quant à lui, pour mission de rechercher, d'analyser et de traiter les renseignements relatifs à la cyber-menace, dans la mesure où celle-ci peut avoir un rapport avec l'espionnage, l'ingérence, le terrorisme, l'extrémisme à propension violente et la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes.

- Le Haut-Commissariat à la protection nationale intervient au niveau de la gestion d'une crise cyber. Son action est définie à travers le plan d'intervention d'urgence face aux attaques contre les systèmes d'information, à partir du moment où la crise est de nature à engendrer des conséquences graves pour une partie du territoire ou de la population du Grand-Duché. Il assure en outre la fonction d'Agence nationale de la sécurité des systèmes d'information, qui a pour mission d'élaborer les lignes directrices en matière de la sécurité de l'information (ANSSI). Le Centre gouvernemental de traitement des urgences informatiques (GOVCERT), qui fonctionne également sous la responsabilité du Haut-Commissariat à la Protection nationale, intervient au niveau de la gestion des incidents de sécurité d'envergure affectant les réseaux et les systèmes de communication.

- La mission des entités précitées est évidemment complétée par l'action des autorités judiciaires et des services de la Police grand-ducale, qui interviennent notamment au niveau de la lutte contre la cybercriminalité.

COMITÉ INTERMINISTÉRIEL DE COORDINATION EN MATIÈRE DE CYBERPRÉVENTION ET DE CYBERSÉCURITÉ

Étant donné que le sujet de la cybersécurité couvre toute une panoplie de domaines et relève des attributions de plusieurs entités étatiques, le Gouvernement a décidé, en date du 13 décembre 2017, de mettre en place un comité interministériel qui regroupe les acteurs concernés et qui est chargé d'assurer la coordination nationale en matière de cybersécurité. Le comité devra assurer, à côté du Cybersecurity Board à vocation plutôt stratégique, la coordination pragmatique des initiatives faisant partie de la cybersécurité.

A cette fin, le comité a pour mission :

- de veiller à la cohérence des actions et initiatives entreprises dans les domaines de la cyberprévention et de la cybersécurité ;

- de coordonner la mise en œuvre des initiatives lancées et des mesures décidées au niveau européen et international en matière de cyberprévention et de cybersécurité ;

- d'assurer le monitoring de la mise en œuvre au niveau national des politiques décidées au niveau européen et international ;

- de conseiller le Gouvernement en matière de cyberprévention et de cybersécurité en identifiant les sujets et priorités à approfondir dans ce domaine, ainsi que les acteurs chargés de leur mise en œuvre ;

- de discuter les positions à adopter par les représentants nationaux dans les enceintes européennes et internationales en matière de cyberprévention et de cybersécurité.

Le comité se compose de membres des principales entités étatiques qui interviennent au niveau national en matière de cybersécurité, et la présidence du comité est assurée par le Haut-Commissaire à la protection nationale. Le Haut-Commissariat en assure également le secrétariat.

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

2. LIGNES DIRECTRICES DE LA STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ

Les objectifs prioritaires sont inscrits dans les trois lignes directrices suivantes :

- **RENFORCEMENT DE LA CONFIANCE PUBLIQUE DANS L'ENVIRONNEMENT NUMÉRIQUE**
- **PROTECTION DES INFRASTRUCTURES NUMÉRIQUES**
- **PROMOTION DE LA PLACE ÉCONOMIQUE.**

LIGNE DIRECTRICE N° 1 – RENFORCEMENT DE LA CONFIANCE PUBLIQUE DANS L'ENVIRONNEMENT NUMÉRIQUE

Chaque citoyen doit pouvoir profiter pleinement des opportunités offertes par les technologies de l'information et de la communication (TIC). Dans ce contexte, il importe de maintenir la confiance des utilisateurs dans ces technologies à un niveau élevé, tout en sachant que cette confiance est influencée par des facteurs externes (p. ex. cyberattaques, fraude au niveau du commerce électronique, etc.).

Le renforcement de la confiance numérique passe par une bonne perception des risques liés à l'utilisation des TIC, tout en étant capable d'en estimer l'intérêt et les opportunités. La consolidation de la confiance du public passe par une bonne maîtrise de la chaîne de valeur numérique, qui ne peut être garantie qu'en assurant la qualité et la sécurité des TIC. Il importe, dans ce contexte, de réussir à combiner le respect de la vie privée et de la sécurité de l'information avec le développement de domaines stratégiques comme le « cloud computing », le « big data » et l'internet des objets. C'est également dans cette optique que le Luxembourg a intérêt de suivre, voire de contribuer, au développement de l'état de l'art dans le domaine clé de l'intelligence artificielle (IA).

LA MISE EN ŒUVRE DE LA LIGNE DIRECTRICE N° 1 PASSE PAR LA RÉALISATION DE CINQ OBJECTIFS.

OBJECTIF 1 : PARTAGE DES CONNAISSANCES ENTRE TOUS LES ACTEURS

Trop nombreux sont les utilisateurs – personnes physiques et personnes morales – victimes des attaques informatiques les plus courantes. Malgré les multiples démarches de sensibilisation initiées au cours des dernières années, il sera nécessaire de développer davantage les connaissances des utilisateurs sur les conséquences potentielles d'une menace numérique.

Des guides de bonnes pratiques comprenant des mesures comportementales, organisationnelles et techniques seront élaborés et publiés en plusieurs langues.

OBJECTIF 2 : DIFFUSION DE L'INFORMATION SUR LES RISQUES

Toutes les parties intéressées seront informées de façon appropriée sur le niveau de risque applicable à l'environnement spécifique dans lequel elles interviennent. Le Gouvernement entend ainsi diffuser les informations sur des sites accessibles aux utilisateurs et adaptés aux différents publics cibles.

Le but en est d'informer les différentes catégories d'utilisateurs sur les dernières évolutions au niveau des menaces, des vulnérabilités et de l'efficacité des mesures de sécurité ; informations qui sont indispensables pour la réalisation d'analyses de risques objectives et comparables.

Une diffusion systématique des informations sur les menaces, les vulnérabilités et les mesures de sécurité les plus communes devrait permettre aux responsables de la sécurité de l'information d'en tirer des conclusions pour un domaine d'activité déterminé en vue d'identifier les mesures adaptées par rapport à une menace spécifique, tout en étant proportionnées par rapport au niveau de sécurité à atteindre. Ces informations pourraient en outre utilement être utilisées, par exemple, par le secteur des assurances pour créer de nouveaux produits répondant aux besoins des citoyens et du secteur des PME.

OBJECTIF 3 : SENSIBILISATION DE TOUTES LES PARTIES CONCERNÉES

Le travail de sensibilisation à la sécurité de l'information est un processus à tâches multiples. De nombreuses initiatives et efforts ont déjà été initiés dans ce contexte. Néanmoins, une bonne partie de la population n'est toujours pas suffisamment sensibilisée aux risques et aux faiblesses présentes dans le domaine du numérique.

Parallèlement au partage des connaissances et à la diffusion des informations, l'effort de sensibilisation sera ainsi intensifié, tant auprès des jeunes qu'auprès des adultes, tant du côté du secteur public que du côté du secteur privé, avec un accent particulier sur les entreprises qui seront désignées opérateurs d'infrastructures critiques, conformément à la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale.

Les efforts de vulgarisation des informations relatives à la sécurité de l'information seront poursuivis, afin de rendre la matière plus compréhensible pour les utilisateurs.

Des programmes de sensibilisation seront en outre mis à leur disposition en recourant aux supports les plus variés : sites internet, imprimés, présentations, animations, vidéos et supports interactifs.

OBJECTIF 4 : DIVULGATION RESPONSABLE

Un modèle de « divulgation responsable », permettant la divulgation d'une vulnérabilité informatique ayant été détectée tout en laissant aux parties intéressées un délai pour corriger cette vulnérabilité avant sa divulgation, sera mis en place au Luxembourg. Cette démarche pourrait intéresser notamment le domaine de la recherche académique et privée. L'élaboration d'un cadre de travail avec des règles précises permettra de renforcer la sécurité juridique au profit des chercheurs dans le domaine de la sécurité de l'information.

OBJECTIF 5 : LUTTE CONTRE LA CYBERCRIMINALITÉ

La confiance publique par rapport à l'environnement numérique est renforcée en présence d'une lutte performante contre les activités numériques illégales.

Face à la croissance continue de la cybercriminalité en Europe et dans le monde, le Luxembourg restera vigilant dans son combat contre les abus et l'usurpation des outils numériques, et continuera à mettre en place les mesures nécessaires pour protéger son infrastructure numérique.
Il est envisagé de renforcer la formation des policiers et de former des magistrats spécialisés dans la lutte contre la cybercriminalité.

La cybercriminalité profite de plus en plus des structures du crime organisé, en particulier de leurs réseaux et systèmes financiers. Pour freiner et mettre un terme au développement de la fraude en ligne, la collaboration sera intensifiée entre le monde des experts en sécurité informatique (CERTs, etc.) et le secteur financier (banques, CSSF, etc.). Les acteurs concernés examineront l'opportunité de mettre en place une cellule spécialisée ayant pour objectif de proposer des actions en vue du démantèlement des structures financières de la cybercriminalité.

Étant donné que les autorités judiciaires nationales sont compétentes en cas d'attaques réalisées par l'intermédiaire de serveurs localisés au Luxembourg, même si la victime, respectivement l'auteur de l'attaque, ne sont pas établis au Luxembourg, il est également envisagé de renforcer la coopération entre experts techniques et juridiques afin de développer l'expertise nécessaire en la matière. La mise en place d'une coopération renforcée entre les spécialistes techniques et les experts juridiques permettra de réaliser des analyses plus efficaces et de simplifier des dossiers d'une haute complexité. Ces échanges entre experts pourront finalement être mis à profit pour développer de nouveaux plans de formation.

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

LIGNE DIRECTRICE N° 2 – PROTECTION DES INFRASTRUCTURES NUMÉRIQUES

De plus en plus de processus métiers, tous secteurs confondus, reposent sur des infrastructures et services numériques prestés par des acteurs spécialisés. La transformation du Luxembourg en une nation numérique accélère ce développement et accroît le besoin de sécurité de ces infrastructures et services, tant au niveau de la confidentialité et de l'intégrité, que de la disponibilité. Les infrastructures numériques jouent ainsi un rôle extraordinairement important au niveau de la protection des intérêts vitaux du pays, car elles transportent les vulnérabilités informatiques dans le monde physique. Le Gouvernement accorde pour cette raison une attention particulière à la résilience des infrastructures numériques.

LA MISE EN ŒUVRE DE LA LIGNE DIRECTRICE N° 2 PASSE PAR LA RÉALISATION DE SEPT OBJECTIFS.

OBJECTIF 1 : RECENSEMENT DE L'INFRASTRUCTURE NUMÉRIQUE ESSENTIELLE ET CRITIQUE

Le Gouvernement se chargera de recenser les infrastructures informatiques critiques, afin de veiller à la mise en place d'un niveau de protection adéquat. Les besoins de protection spécifiques seront, le cas échéant, élaborés en étroite collaboration avec les opérateurs et les exploitants desdites infrastructures. Le recensement se fera en ligne avec la transposition de la directive relative à la sécurité des réseaux et des systèmes d'information de l'Union européenne (directive SRI), et suivant les dispositions de la loi du 23 juillet 2016 portant création d'un Haut-Commissariat à la protection nationale.

OBJECTIF 2 : POLITIQUES DE SÉCURITÉ

L'application des politiques de sécurité de l'information (PSI-LU), qui ont été élaborées sous la responsabilité de l'Agence nationale pour la sécurité des systèmes d'information (ANSSI), sera recommandée aux infrastructures informatiques critiques. Il leur sera en outre suggéré de réaliser les analyses de risques spécifiques sur base de la méthodologie ISO 2700x. La méthode optimisée d'analyse des risques CASES (méthodologie MONARC) sera proposée aux opérateurs qui n'ont pas encore mis en place un processus de gestion des risques.

OBJECTIF 3 : GESTION DE CRISE

Le plan d'intervention d'urgence face aux attaques contre les systèmes d'information ou en cas de failles techniques des systèmes d'information (PIU Cyber) a fait ses preuves au niveau de la gestion des incidents numériques récents. Le PIU Cyber continuera d'être adapté en fonction des évolutions de l'environnement numérique.

Les nouvelles procédures et mesures techniques inscrites dans le plan d'intervention d'urgence seront mises en œuvre prioritairement. A cette fin, le Haut-Commissariat à la protection nationale et la Cellule d'évaluation du risque cyber contacteront les opérateurs du secteur public et du secteur privé qui sont considérés comme essentiels pour la gestion d'un certain type de crise, afin d'élaborer des plans opérationnels par mesure (POMs). Le POM comporte d'abord une liste de contact des personnes qui interviennent au niveau de la gestion d'une crise. Il énumère ensuite une série de mesures prédéfinies qui devront être activées en cas de survenance d'une crise. Il inclut enfin une description de l'impact éventuel du déclenchement d'une mesure prédéfinie sur d'autres systèmes. Les POMs permettent ainsi aux opérateurs de mettre en œuvre les mesures prédéfinies de façon effective et rapide en cas de crise les concernant.

OBJECTIF 4 : NORMALISATION

La normalisation détermine le langage commun technique, tant sur le plan européen qu'au niveau international. Appliquée au domaine de la cybersécurité, cette capacité fédératrice permet de fixer les définitions et les besoins nécessaires, l'état de l'art en la matière ainsi que les architectures de référence, tout en établissant de manière consensuelle les exigences et les spécifications requises pour assurer un niveau de sécurité adapté. Cet ensemble, en évolution constante, facilite l'appropriation digitale, notamment pour ce qui est des évolutions « Smart ICT » (« Cloud Computing », « Big Data », « Internet of Things », « Blockchain », etc.).

Le suivi et l'investissement national dans le processus de développement des normes en lien avec le domaine de la cybersécurité seront renforcés, spécifiquement afin d'en faire un outil stratégique au niveau du développement de la confiance numérique nationale.

Cette démarche sera réalisée au niveau de la normalisation technique formelle (ISO, IEC, ETSI, CEN-CENELEC, ITU-T), tout en tenant compte des travaux développés par les fora et les consortia pertinents identifiés dans le contexte de la cybersécurité.

L'ILNAS (Organisme luxembourgeois de la normalisation) fédérera et développera ce suivi stratégique, afin d'en rendre compte au plan national, dans l'intérêt de la mise en place d'une « smart nation ».

OBJECTIF 5 : RENFORCEMENT DE LA COOPÉRATION INTERNATIONALE

La collaboration étroite sera poursuivie et renforcée au niveau international, d'une part pour échanger les informations sur les menaces, les vulnérabilités et l'efficacité des traitements et, d'autre part, pour mettre en place une prévention efficace, une détection fiable et une mitigation efficiente. Au niveau européen, la transposition de la directive SRI dans tous les États membres mènera à une harmonisation dans le domaine de la cybersécurité.

Cette dernière devra également être recherchée au niveau des méthodes de gestion de risques, des standards et normes, des systèmes d'accréditation et de certification, ainsi que dans le domaine de la gestion de la conformité. Une harmonisation minimale entre les systèmes européens sera soutenue pour faciliter le libre-échange des services et des produits.

OBJECTIF 6 : CYBERDÉFENSE

En juillet 2017, le Gouvernement a approuvé les lignes directrices de la défense luxembourgeoise à l'horizon de 2025 et au-delà. Parmi les objectifs y retenus figure celui de poursuivre le développement des compétences et capacités dans le domaine de la cyberdéfense. La Défense luxembourgeoise continuera ainsi ses travaux sur la définition et la mise œuvre des aspects relevant de ses attributions au niveau des stratégies nationales et internationales en matière de cybersécurité.

OBJECTIF 7 : RENFORCEMENT DE LA RÉSILIENCE DE L'INFRASTRUCTURE NUMÉRIQUE DE L'ÉTAT

Depuis un certain temps, les attaques ciblées contre les infrastructures numériques étatiques sont en forte augmentation en Europe. Le Gouvernement veillera à assurer un haut standard de protection des infrastructures numériques étatiques.

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

LIGNE DIRECTRICE N° 3
– PROMOTION DE LA PLACE ÉCONOMIQUE

Aujourd'hui, la cybersécurité est devenue un facteur d'attractivité économique. Elle représente un avantage compétitif. Face au professionnalisme des cybercriminels et à l'évolution rapide de la technologie et des menaces corollaires, une collaboration aussi intense qu'efficace entre tous les acteurs publics et privés constitue un gage de sécurité.

Le Gouvernement entend mettre en œuvre les mesures nécessaires pour continuer à démocratiser l'accès à la sécurité de l'information, notamment en mutualisant certains services et en capitalisant sur les synergies existantes. Cette approche devrait permettre de réduire la complexité ainsi que les coûts liés à la cybersécurité et d'augmenter par voie de conséquence l'attractivité d'un investissement. Cette nouvelle ligne directrice s'inscrit parfaitement dans l'ambition « Digital Luxembourg » du Gouvernement, également confirmée dans le cadre de la stratégie « TIRLUX »[2], à savoir, faire du Luxembourg une « Smart nation » en transformant les défis liés au numérique en opportunités pour le pays. La cybersécurité s'y intègre via le centre de compétence en cybersécurité, qui est mis en place et géré par SECURITYMADEIN.LU.

LA MISE EN ŒUVRE DE LA LIGNE DIRECTRICE N° 3 PASSE PAR LA RÉALISATION DE DIX OBJECTIFS.

OBJECTIF 1 : CRÉATION DE NOUVEAUX PRODUITS ET SERVICES

Le Luxembourg continuera à investir fortement dans les infrastructures de technologie de l'information, le cloud, la fintech, le biotech, le spacetech et la conduite autonome. L'implication du Luxembourg en tant que chef de file dans le projet IPCEI (« Important Project of Common European Interest »), « High Performance Computing » et le « Big Data »[3] ne fait que souligner l'ambition du Luxembourg de diversifier davantage son économie vers le numérique.

Les partenariats public-privé seront renforcés. Ces partenariats permettent d'associer les compétences et le savoir-faire des acteurs, en vue de créer des produits et services de très haute valeur ajoutée. Ils facilitent la création de services de sécurité qui respectent les principes de proportionnalité et de nécessité, et qui sont adaptés en termes de complexité et des coûts engendrés.

Dans ce même ordre d'idées, le Gouvernement proposera de nouveaux services innovateurs. Ainsi, des offres composées de services numériques étatiques de très haute qualité et de garanties basées sur des conventions internationales comme la Convention de Vienne sur les relations diplomatiques seront créées. Le développement de produits et services basés sur la technologie de la cryptographie, indispensables aux tiers de confiance dans le domaine de la gestion des données à caractère personnel, aux systèmes d'authentification forte, à la signature électronique et à la technologie du « blockchain », sera promu.

[2] *Cf. « Rifkin study »*

[3] *https://portail-qualite.public.lu/fr/publications/normes-normalisation/etudes/white-paper-big-data-1-2.html*

Pour mutualiser les risques et encourager la victime d'un incident numérique cyber à recourir à l'aide d'un expert pour gérer cet incident et pour rétablir le système affecté par un acte malicieux, les compagnies d'assurance seront encouragées à créer des produits spécifiques dans le domaine de l'assurance cyber.

Des produits et services de sondes (système de détection d'intrusion) seront élaborés pour pouvoir dresser des rapports situationnels sur le trafic dans les réseaux, en vue de repérer des activités anormales ou suspectes. Ces produits et services seront développés dans un esprit de « privacy by default » et « security by design ».

L'écosystème de la cybersécurité sera fédéré activement et s'adressera aussi bien aux entreprises, aux start-ups, aux incubateurs qu'aux acteurs financiers et aux régulateurs, l'objectif étant de pouvoir répondre de façon agile et coordonnée à l'évolution rapide des menaces, par le biais de services et produits qualitatifs, abordables et innovants.

OBJECTIF 2 : MUTUALISATION D'INFRASTRUCTURES DE SÉCURITÉ

Certaines attaques comme le déni de service distribué (DDOS) ont atteint un niveau de perturbation tellement élevé que des mesures nationales s'imposent. Ces attaques nécessitent des actions coordonnées au niveau des fournisseurs de service. Une coordination au niveau des outils de détection et une certaine mutualisation des infrastructures sont recommandées.

Pour pouvoir mitiger une attaque de type « déni de service », un opérateur doit être capable, en temps d'attaque, d'instruire avec l'aide du « Border Gate Protocol » les opérateurs en amont d'adapter leurs règles de routage. En même temps, il doit filtrer les communications illicites appartenant à l'attaque ayant atteint son réseau. L'État examine, dans ce contexte, la possibilité d'investir dans un « scrubbing center » (infrastructure de filtrage de communications illicites) national qui sera utilisé lorsque les moyens de filtrage des opérateurs locaux ne suffisent plus.

OBJECTIF 3 : RÉFÉRENTIELS D'EXIGENCES ET MAÎTRE D'ŒUVRE

Les fautes récurrentes faites lors de la conception ou de la configuration des systèmes informatiques sont la source de nombreux problèmes liés à la sécurité de l'information. Le Gouvernement publiera des référentiels d'exigences standards pour les systèmes les plus exploités. Le maître d'œuvre, à défaut l'acquéreur, sera encouragé de veiller à faire respecter le référentiel d'exigences par les différents intervenants.

OBJECTIF 4 : CRÉATION DU CENTRE DE COMPÉTENCES EN CYBERSÉCURITÉ (C3)

Le ministère de l'Économie et le G.I.E. SECURITYMADEIN.LU disposent d'un grand réservoir d'expériences, d'informations opérationnelles et de connaissances sur les menaces, les vulnérabilités et l'efficacité des mesures de protection qui sont mises au profit de toute l'économie par le biais de partenariats avec le privé, et qui devraient permettre le développement de produits et services innovants dans le domaine de la sécurité de l'information.

Le centre de compétences en cybersécurité mettra en œuvre les mesures nécessaires pour soutenir le développement de trois types de services : « Observatoire », « Formation » et « Testing », et ce en étroite collaboration avec des partenaires privés et publics :

- Les services liés à « l'observatoire » se concentreront sur les aspects de l'économie de la connaissance dans le domaine de la cybersécurité, en rassemblant les efforts publics et privés permettant de fournir des informations et tendances en la matière. La création de ce type de service réduira considérablement l'effort individuel et les coûts de la cybersécurité, tout en augmentant l'efficacité des mesures de protection. Ainsi, le centre fournit, en collaboration avec ses partenaires, non seulement des renseignements techniques, mais aussi un aperçu de menaces contextualisées et spécifiques aux différents métiers demandeurs, des mécanismes de protection ainsi que des métriques et des chiffres clés, nécessaires à une bonne gouvernance. L'interprétation des menaces dans un contexte spécifique (ISAC – « information sharing and analysis center ») est considérée comme un nouveau modèle économique à développer avec des partenaires spécialisés dans les différents domaines comme les finances, l'internet des objets, le secteur de la santé ou encore l'espace.

- Les services de type « formation » permettront d'aller au-delà de ce qui est disponible aujourd'hui au niveau des centres de formation au Luxembourg. Les entreprises et autres acteurs auront la possibilité de former leur personnel dans un environnement immersif, simulant des incidents informatiques. Les participants seront ainsi plongés dans un contexte concret pour apprendre à travailler en équipes multidisciplinaires pour acquérir les compétences techniques, organisationnelles, comportementales et juridiques nécessaires afin d'identifier et d'endiguer les risques numériques et « business » y associés. Ils apprendront aussi à formuler des notifications à l'adresse des régulateurs respectifs.

- Les services de type « testing » ouvriront aux partenaires et clients de nouvelles possibilités de tests d'applications numériques. Ainsi, les réseaux de « honeypots » de SECURITYMADEIN.LU seront mis à disposition pour tester des logiciels. Les entreprises et partenaires pourront tester des systèmes de gestion de la sécurité lors d'exercices basés sur divers scénarios. Les start-ups bénéficieront d'un accès à l'infrastructure de « testing » du centre à des prix avantageux pour faire valider leur nouvelle technologie ou service via un environnement de test simulant l'environnement réel dans lequel leur produit devra survivre, une fois en production.

OBJECTIF 5 : GESTION DU RISQUE ET GOUVERNANCE INFORMÉE

La gestion du risque, telle qu'introduite depuis la deuxième stratégie nationale en matière de cybersécurité, est reconnue comme étant l'outil approprié pour une bonne gouvernance de la cybersécurité. En effet, elle respecte d'un côté les principes de proportionnalité et de nécessité et offre d'un autre côté une analyse du risque et de la sécurité en fonction de différents points de vue (entreprise, personne physique, client). Elle permet ainsi de comprendre et de prendre en compte les besoins propres des divers acteurs qui participent à l'épanouissement de la société numérique.

C'est pourquoi le Gouvernement se chargera de publier des métriques indispensables à la réalisation d'analyses de risques objectives. Cette conscience situationnelle facilitera aussi la mise en place d'une gouvernance de gestion interne basée sur des métriques adaptées aux circonstances.

Doté d'une gouvernance informée, grâce à des décisions basées sur des rapports situationnels objectifs et réalistes, le Luxembourg pourra se positionner en tant que nation numérique (« digital nation ») à la fois moderne, ouverte, résiliente et digne de confiance.

OBJECTIF 6 : FORMATION ET AIDES À LA FORMATION

Le Gouvernement entend mettre en place une formation universitaire dans le domaine de la sécurité de l'information pour pallier le risque d'un manque d'experts de la sécurité de l'information, ce qui constituerait un frein au développement de l'écosystème de la sécurité.

Il est envisagé de proposer des aides à la formation spécifique pour le domaine de la sécurité de l'information. Ces aides seront liées à la formation continue d'experts, afin de les inciter à assister, par exemple, à des conférences et autres événements pertinents.

Pour pallier la pénurie d'experts dans le domaine de la sécurité, et vu l'interconnectivité des outils, il sera envisagé de développer des formations spécialisées qui s'adressent à des équipes multidisciplinaires.

OBJECTIF 7 : COLLABORATION ENTRE RESPONSABLES DE LA SÉCURITÉ DE L'INFORMATIONNUMÉRIQUE DE L'ÉTAT

L'opportunité de désigner une personne en charge de la sécurité de l'information au sein de chaque entité étatique sera examinée. Un plan de formation pour ces personnes sera, le cas échéant, mis en place et des plateformes d'échanges pour ces experts seront créées.

Dans le secteur privé, les dirigeants seront encouragés à conférer aux responsables de la sécurité de l'information les moyens nécessaires pour mettre en place des mesures de protection efficaces. Des efforts devront être réalisés pour améliorer la communication et la collaboration entre les équipes chargées de différentes missions : sécurité de l'information, conformité, management, gestion clients, etc.

Le Gouvernement encouragera la coopération entre experts de sécurité technique et experts de processus métier, pour créer et échanger ainsi des rapports de risques contextualisés selon des domaines clés.

OBJECTIF 8 : COLLABORATION ENTRE EXPERTS EN MATIÈRE DE RÉPONSE AUX INCIDENTS

L'existence de nombreuses entités privées et publiques spécialisées dans le domaine de la gestion d'incidents représente d'ores et déjà un atout pour le Luxembourg. Le Gouvernement soutiendra le renforcement de la coopération entre ces entités spécialisées, ce qui permettra de faciliter la gestion d'incidents de nature trans-sectorielle ou de grande envergure.

En exécution des exigences inscrites dans les nouveaux règlements et directives (RGPD, Télécom, SRI), les régulateurs seront, à l'avenir, amenés à s'impliquer davantage dans la gestion d'incidents, ce qui engendrera une coopération plus étroite entre régulateurs et équipes spécialisées. Cette coopération devrait augmenter la confiance des utilisateurs dans les structures existantes et améliorer ainsi la qualité au niveau de la gestion des incidents numériques.

Le Gouvernement continuera en outre à promouvoir l'échange d'informations entre CERTs. Les quatre CERTs publics (GOVCERT.LU, circl.lu, HealthNet CSIRT et RESTENA-CSIRT) sont connus et sollicités par leur public respectif. Ils disposent d'un grand réservoir d'informations, aussi bien sur les menaces et vulnérabilités existantes, que sur l'efficacité réelle des mesures de sécurité. La renommée des CERTs contribue à accroître l'attractivité de la place économique luxembourgeoise.

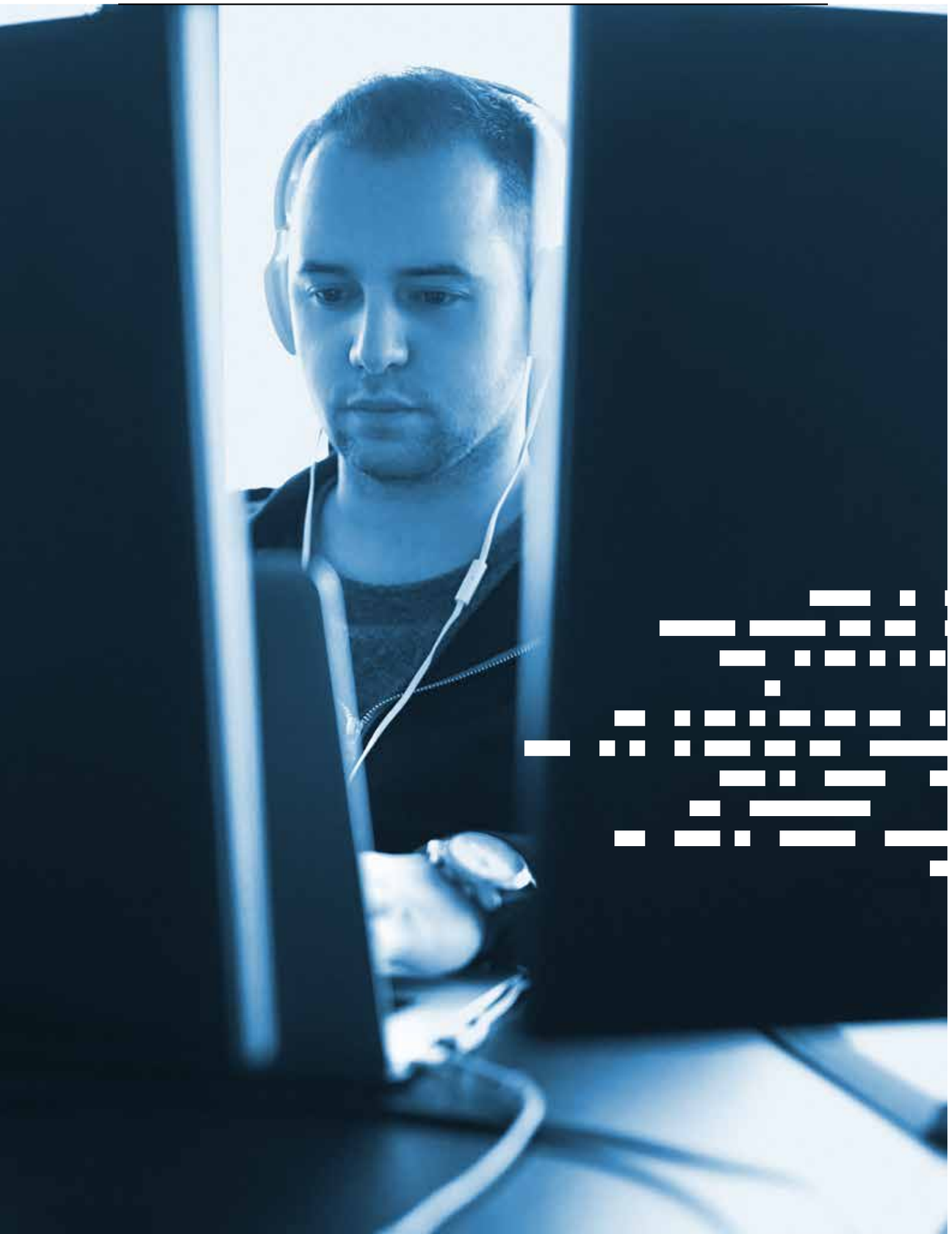
OBJECTIF 9 : PRIORITÉ À LA RECHERCHE : LES START-UPS

Parmi les besoins identifiés au sein de l'écosystème de la sécurité numérique luxembourgeoise, figure aussi celui de start-ups proposant des solutions innovantes. Il en sera tenu compte au niveau des priorités dans le domaine de la recherche, en promouvant la création de jeunes entreprises.

OBJECTIF 10 : LE DÉSASSEMBLAGE DE CODE ET L'IDENTIFICATION DE VULNÉRABILITÉS

Il est envisagé de créer un cadre visant à autoriser au Luxembourg le désassemblage de code (« reverse engineering ») et les tests de pénétration à des fins d'identifier des vulnérabilités. Ces compétences seront utiles pour améliorer l'interopérabilité des systèmes et aident à assurer un niveau de sécurité informatique plus élevé par l'identification de logiciels malicieux, de logiciels de type spyware, etc.

En cas de publication de vulnérabilités graves, les CERTs publics sont autorisés, sur le plan national, à identifier les dispositifs connectés à l'internet présentant ces vulnérabilités et à en avertir les responsables (p. ex. vulnérabilité Heartbleed dans OpenSSL).



STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

MISE EN ŒUVRE DE LA SNCS III

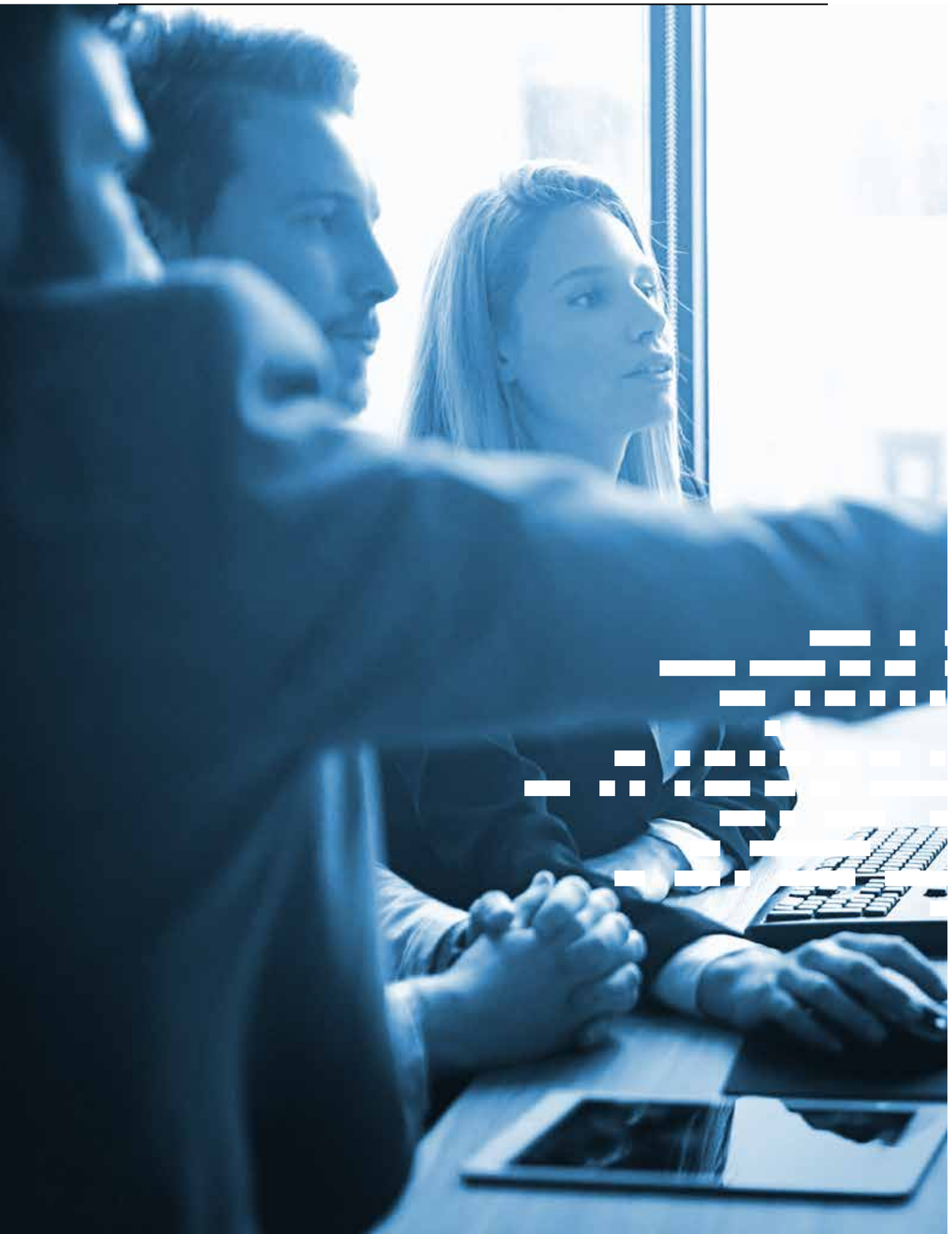
La présente stratégie définit les objectifs qu'il importe d'atteindre dans les trois années à venir.

Ces objectifs sont complétés par un plan d'action qui décrit les mesures techniques à mettre en œuvre suivant un calendrier déterminé, ainsi que les acteurs appelés à contribuer à leur mise en œuvre.

Le plan d'action est disponible sur demande au Haut-Commissariat à la protection nationale (courriel : info@hcpn.État.lu ; Sujet : #SNCS Plan d'action).

Le Cybersecurity Board et le comité interministériel de coordination en matière de cybersécurité accompagnent l'exécution du plan d'action.

La stratégie nationale en matière de cybersécurité a vocation à évoluer dans le temps. Le plan d'action sera ainsi périodiquement révisé au sein du comité interministériel de coordination, afin de rester adapté à un environnement numérique en constant changement.



STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

3. ANNEXES

RETOUR D'EXPÉRIENCE SUR LA STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ II

La SNCS II avait mis l'accent sur la sécurité de l'information comme un défi à relever par la société dans son ensemble. Que ce soit au niveau d'une entreprise, du service public ou du citoyen ; chaque partie porte une responsabilité dans la construction d'une société numérique sûre.

Cette annexe fait le point sur l'avancement et la mise en œuvre des points d'action de la SNCS II, tout en sachant qu'une partie des actions sont récurrentes, étant donné que la cybersécurité représente un processus continu et dynamique à caractère évolutif.

OBJECTIF 1 : RENFORCER LA COOPÉRATION NATIONALE

Sur le plan national, de nombreuses initiatives ont été prises pour intensifier la collaboration – aussi bien sur le plan organisationnel que sur le plan opérationnel – entre les acteurs étatiques. Des échanges réguliers ont eu lieu entre l'ANSSI, les régulateurs et les ministères concernés pour établir une politique de sécurité de l'information au niveau du secteur public et des opérateurs d'infrastructures critiques.

Des échanges fréquents ont été organisés au sujet de la protection des données à caractère personnel dans le domaine de la cybersécurité, deux sujets intimement liés et qui méritent d'être traités partiellement ensemble.

Sur le plan opérationnel, des échanges continus ont eu lieu entre les CERTs, grâce à des outils de collaboration modernes et efficaces. Les incidents déclarés au CERT national sont gérés en commun effort par le GOVCERT et le CIRCL. Par ailleurs, les efforts communs de sensibilisation qui ont été organisés à l'adresse des décideurs du secteur public et privé au sujet de l'importance de la sécurité de l'information portent déjà leurs premiers fruits. Les collaborations étroites dans le domaine de la sensibilisation des enfants, des adolescents, des adultes et des personnes âgées, ainsi que des personnes encadrantes ont également connu beaucoup de succès.

Depuis sa mise en place en 2015, l'ANSSI a élaboré une politique de sécurité de l'information générale pour l'État (PSI-LU). Elle a également conclu des accords de coopération avec différents acteurs au niveau national.

Le Centre des technologies de l'information de l'État (CTIE) et le Centre de Communications du gouvernement (CCG) ont fusionné afin d'améliorer l'offre de services au niveau de la gestion des communications sécurisées étatiques.

Le portail de la sécurité de l'information www.cybersecurity.lu est en ligne depuis juillet 2017. Il présente les différents acteurs du secteur et leurs sites respectifs. Sa vocation principale est d'être le « guichet unique » en matière de sécurité de l'information.

Les outils tels que « Malware Information Sharing Platform (MISP) » et « Analysis of Information Leaks (AIL) » créés par le CIRCL, ou encore le Diagnostic CASES et l'analyse de risque MONARC élaborés par CASES, contribuent à une collaboration, respectivement à un échange plus intense sur les menaces et vulnérabilités numériques entre parties concernées. Ils permettent également de rassembler des informations sur les différents degrés de maturité présents sur le terrain dans les secteurs privé et public en vue d'une gouvernance informée en matière de cybersécurité.

L'utilisation de l'analyse de risques comme méthode de base pour gérer la sécurité de l'information est désormais devenue la norme au Luxembourg. Plusieurs outils sont à disposition, dont l'outil MONARC qui a été publié en tant que méthode de source ouverte. Fin 2017, un vaste projet d'analyse de risques auprès des entités étatiques a été initié par l'ANSSI.

OBJECTIF 2 : RENFORCER LA COOPÉRATION INTERNATIONALE

Le Luxembourg est représenté dans les groupes et associations importants du domaine de la sécurité de l'information. Les différentes entités luxembourgeoises ont noué des contacts étroits au niveau international et ont conclu des partenariats-clé avec leurs homologues de pays partenaires. À cette fin, des accords de collaboration avec le BSI (Allemagne), l'A-SIT (Autriche) et le ISB (Suisse) ont pu être élaborés et seront signés au cours de l'année 2018. D'autres accords, notamment avec la France et la Belgique, seront finalisés durant le premier trimestre de l'année 2018. Dans le même état d'esprit, le GOVCERT et le CIRCL ont rejoint le CSIRT network et font partie du FIRST (« Forum of Incident Response and Security Teams »).

La coopération internationale a porté ses fruits, ce qui a été perceptible à l'occasion de la présidence luxembourgeoise du Conseil de l'Union européenne au cours de laquelle le GOVCERT a eu pour mission de protéger, ensemble avec ses partenaires internationaux, les infrastructures numériques étatiques.

OBJECTIF 3 : AUGMENTER LA RÉSILIENCE DE L'INFRASTRUCTURE NUMÉRIQUE

Les entités luxembourgeoises ont dorénavant plusieurs outils modernes d'analyse des risques à leur disposition.

Depuis mars 2017, la méthode MONARC est accessible à tous en « open source ». Certaines métriques nécessaires à la réalisation d'analyses de risques objectives sont publiées. En fonction du degré de maturité et de compétence des organisations, différents modèles d'analyse de risques sont proposés.

Certaines bonnes pratiques sectorielles ont pu être développées. Elles ont été publiées via des modèles de gestion de risques MONARC, respectivement via des politiques de sécurité émises par l'ANSSI. En outre, les sites d'acteurs étatiques tels que CASES proposent des bonnes pratiques spécifiques et générales.

Depuis plusieurs années, des informations sur les tendances au niveau des menaces, des vulnérabilités et de l'efficacité des mesures de sécurité sont collectées. Ces informations, ainsi que les informations acquises grâce aux diagnostics et analyses de risques, informent sur le niveau de maturité des différentes entités. Elles forment ainsi une base pour pouvoir créer des rapports de conscience situationnelle. Ceux-ci pourront servir à alimenter le volet gouvernance (gouvernance informée).

Le plan d'intervention d'urgence cyber élaboré par le HCPN est opérationnel. Ce plan a été mis à jour régulièrement par le HCPN suite aux leçons tirées des exercices et crises réelles.

Le Luxembourg a participé à l'exercice Cyber Europe 2016 organisé par l'ENISA (« European Network and Information Security Agency »). Il a en outre été associé à l'exercice Cyber Coalition 2016 de l'OTAN en tant qu'observateur, en étroite collaboration avec l'Allemagne, et a participé activement en 2017.

OBJECTIF 4 : COMBATTRE LA CYBERCRIMINALITÉ

Les travaux menés au sein du groupe de travail « cybercrime », présidé par le Parquet du Luxembourg, ont permis d'encourager la coopération nationale et de fournir des informations contextuellement importantes à toutes les entités participantes.

Les différents acteurs se sont déclarés satisfaits de la bonne collaboration mutuelle, qui a permis d'aboutir à des succès importants d'enquête. Les parties prenantes sont unanimement d'accord qu'il faudra appliquer les lois déjà existantes, les adapter à la réalité de l'environnement numérique, améliorer les procédures d'enquête sur la cybercriminalité, surtout dans le contexte de la manipulation de la preuve électronique, et faciliter le partage de l'information entre les acteurs.

Grâce à une bonne coopération entre les différents acteurs, soutenus également par Europol, l'intervention de la police dans le domaine de la cybercriminalité internationale est devenue plus rapide et efficace.

En prolongement des mesures initiées dans le cadre de la SNCS II, il sera indispensable de continuer à renforcer les capacités d'action des autorités judiciaires, notamment pour ce qui est de la cybercriminalité à caractère transnational. Dans le respect de leurs mandats et missions respectives, le Parquet, le cabinet d'instruction et les services spécialisés (enquête et expertise informatique) de la Police judiciaire doivent être en mesure d'enquêter et de poursuivre les cas de cybercriminalité, mais également toute autre infraction liée aux TIC. Afin d'assurer une poursuite efficace contre les actes de cybercriminalité, il sera nécessaire :

- d'adapter les instruments d'entraide judiciaire internationale à la volatilité des preuves sur internet,
- de procéder, dans la mesure du possible, à une harmonisation minimale de la durée de rétention des données qui varie fortement d'un État à l'autre,
- de tenir compte des possibilités de chiffrement offertes par les outils adéquats et de la technologie à laquelle il peut être recouru pour assurer l'anonymat, ce qui rend difficile l'identification d'un suspect (p.ex. : TOR, DARKNET),
- de trouver une réponse aux nouveaux moyens de paiement (notamment les crypto-monnaies comme Bitcoin et les dérivées) qui permettent aux criminels d'échapper facilement aux autorités et de cacher les transactions
- de se donner les possibilités de traiter le volume important de données à analyser.

OBJECTIF 5 : INFORMER, FORMER ET SENSIBILISER SUR LES RISQUES ENCOURUS

Depuis fin 2015, la formation CASES est devenue obligatoire pour les nouveaux employés et fonctionnaires de l'État, toutes carrières confondues. Cette formation contient des aspects méthodologiques généraux, tels que la classification des informations et l'analyse des risques.
Outre cette formation de base, une formation spécialisée et non obligatoire est également disponible sur demande auprès de l'INAP.

Les formations pour écoliers et lycéens sont obligatoires. Elles se concentrent sur les aspects « comportementaux » de la sécurité de l'information et expliquent les bonnes pratiques courantes.

CASES, ensemble avec ses partenaires agréés, propose un large éventail de formations aux différents publics professionnels (utilisateurs, cadres, personnel IT, formateurs, etc.).

Des formations spécifiques pour décideurs sont également proposées.

Parmi les mesures qui figuraient dans la deuxième stratégie et qui seront reprises dans la nouvelle stratégie, il y a lieu de citer le programme de formation pour opérateurs d'infrastructures critiques.

Au Luxembourg, l'accès à la sécurité de l'information est largement facilité par l'État. Des formations gratuites ou à prix abordable sont offertes pour un public très varié. De nombreux efforts ont été entrepris pour sensibiliser les citoyens, par exemple, sous forme de workshops à l'heure de midi en semaine, les soirs ou un jour de week-end.

En ligne avec la stratégie gouvernementale « Digital Luxembourg », notamment dans l'objectif de sensibiliser les élèves aux attraits des nouvelles technologies et d'encourager leur créativité, des « makerspace » ont été mis en place dans des établissements périscolaires et scolaires afin d'intéresser les jeunes aux nouvelles technologies de l'information depuis 2015. Une partie de ces espaces, dont la « Base1 » au Forum Geesseknäppchen, permettent d'accueillir des jeunes en dehors de leur horaire scolaire. Citons quelques autres projets pour souligner l'engagement du Gouvernement dans cette thématique prioritaire qu'est le développement des compétences numériques au Luxembourg : « crypto party », « coder dojo » ; « Mak@ons », « hack-4kids » et « Luxembourg Tech School ». Ces « makerspace » sont regroupés au sein de l'initiative BEE CREATIVE.

L'initiative « Kniwwelino » vient d'être lancée récemment. Il s'agit d'un micro-processeur développé au Luxembourg et distribué aux enfants et jeunes pour les familiariser avec le concept de la programmation et de la sécurité du code (pour plus de détails, voir: www.bee-creative.lu).

OBJECTIF 6 : METTRE EN PLACE DES NORMES, STANDARDS, CERTIFICATS, LABELS ET RÉFÉRENTIELS D'EXIGENCES POUR L'ÉTAT ET LES INFRASTRUCTURES CRITIQUES

L'analyse de risques selon la norme ISO/IEC 27005 est devenue la méthode de référence pour gérer la sécurité de l'information, aussi bien dans le secteur public que privé. Des analyses MONARC ont été réalisées au sein de différents secteurs prioritaires et il est prévu de répéter ces exercices selon un cycle de trois analyses par année. L'approche de gestion des risques sera progressivement généralisée et étendue à tous les secteurs.

Des standards et lignes directrices en matière de sécurité des systèmes d'information ont été mis en place. Ils sont publiés via les politiques de sécurité émises par l'ANSSI et seront finalisés suite aux conclusions relatives au projet pilote qui a été réalisé au sein du CTIE.

Un inventaire des normes et standards de la sécurité de l'information a été élaboré. Cet inventaire étant un document vivant, ce point d'action sera repris dans la nouvelle stratégie.

OBJECTIF 7 : RENFORCER LA COOPÉRATION AVEC LE MONDE ACADÉMIQUE ET DE LA RECHERCHE

Le développement d'un programme de formation cybersécurité nécessite une approche transversale. Des programmes ont été réalisés par de nombreux acteurs luxembourgeois. La coordination des initiatives prises dans ce domaine sera encore renforcée dans les années à venir.

Le renforcement de la coopération dans le cadre du développement des protocoles et algorithmes cryptographiques sera repris dans la nouvelle stratégie, en vue de clarifier les moyens à la disposition du Luxembourg pour certifier des produits dans ce domaine. En l'absence de laboratoires de certification appropriés, des partenariats avec des organismes étrangers (pays limitrophes) sont envisagés.

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

ANALYSE DES MENACES AU NIVEAU NATIONAL EN MATIÈRE DE CYBERSÉCURITÉ

Les entités ayant des responsabilités dans le domaine de la cybersécurité ont acquis au cours des dernières années une certaine expérience en observant et analysant un grand nombre d'attaques sur les systèmes informatiques. Ces observations ont permis aux acteurs d'obtenir une vue globale sur l'évolution des attaques dans le temps. La présente analyse, qui n'a pas l'ambition d'être exhaustive, permet de décrire les cybermenaces actuelles et futures.

- **FRAUDE PAR RANÇONGICIEL**

  A l'heure actuelle, les acteurs notent une augmentation sensible d'attaques ayant un but purement financier, dont notamment les attaques réalisées par rançongiciels (« ransomwares »), c'est-à-dire des logiciels malveillants introduits dans un système pour chiffrer les fichiers numériques qu'il contient, dans le but de vendre la clé de déchiffrement à la victime. Le recours à ce type d'activités illégales est facilité par l'apparition de systèmes d'échanges d'argent virtuel comme le Bitcoin, Ethereum, et autres. Une des dernières grandes attaques par rançongiciels (Notpetya) a aussi illustré la possibilité de masquer une attaque de sabotage cyber en rançongiciel.

- **ATTAQUES PAR DÉNI DE SERVICE DISTRIBUÉ (DDOS) VIA « L'INTERNET DES OBJETS »**

  L'impact des attaques par déni de service distribué est de plus en plus important. Actuellement, cette forme d'attaque a pris une ampleur jamais connue auparavant dû à « l'internet des objets ». Via des outils comme MIRAI, des objets mal sécurisés connectés à l'internet peuvent facilement être répertoriés et manipulés pour effectuer des attaques par déni de service de très grande envergure. Ces outils sont librement accessibles sur internet et ils sont souvent utilisés à des fins de chantage. De tels outils permettent également de répertorier et de compromettre des objets connectés à l'internet pour effectuer la surveillance de masse ou réaliser certaines formes d'espionnage industriel.

- **« BRICKERBOT »**

  Les « BrickerBot », contrairement à d'autres attaques comme les attaques par déni de service qui empêchent les services de fonctionner un certain temps, visent à détruire des objets connectés à l'internet. Ces attaques peuvent être très furtives et sont difficiles à détecter. Elles visent des objets connectés mal protégés et essayent, après une authentification réussie, de changer des paramètres du système pour rendre l'objet inutilisable[4].

- **RISQUES INHÉRENTS AU DÉVELOPPEMENT DES « SMART CITIES » ET DE LA DOMOTIQUE**

  De plus en plus de composantes, qui font partie de notre vie quotidienne et qui sont utilisées pour offrir des services à haute valeur ajoutée, ont recours à des informations provenant en temps réel d'une infrastructure numérique. Les « smart cities » sont équipées de capteurs collectant des données et s'appuyant sur des systèmes d'information pour optimiser les services qui se caractérisent par leur haut degré de connectivité. Les attaques à l'encontre de ces infrastructures risquent de se multiplier en présence de systèmes d'authentification et de protocoles cryp-

[4] *https://arstechnica.com/security/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/*

tographiques, qui ne répondent souvent pas au plus haut niveau de sécurité.

- **NON-RESPECT DE STANDARDS MINIMAUX DE SÉCURITÉ**

  Un point inquiétant, qui est actuellement observé dans le monde de la cybercriminalité, est le non-respect, par l'éditeur d'un logiciel ou d'un outil informatique, des standards et meilleurs objectifs de sécurité au niveau du développement. La sécurité informatique n'est pas toujours l'élément prioritaire au niveau de la production de logiciels et d'outils informatiques. Ces logiciels, souvent distribués à des millions d'utilisateurs, risquent d'être piratés pour être manipulés et constituent une menace réelle pour l'économie et la sécurité d'un pays.

- **MENACES SUR LE PROCESSUS MÉTIER**

  Les attaques récentes montrent que les criminels diversifient leurs actions et cibles. Plutôt que de nuire par le chantage, l'exfiltration ou le sabotage des données, ils visent dorénavant également le processus métier. La pénurie de ressources humaines qualifiées dans le domaine informatique doit être considérée comme une vulnérabilité dans ce contexte. En effet, ce phénomène force beaucoup d'entreprises à externaliser leurs systèmes informatiques vers de grands acteurs spécialisés dans le domaine. Il s'ensuit que ces entreprises ne possèdent plus, au niveau de leur personnel, les qualifications nécessaires pour protéger les processus métiers ou industriels. Cette vulnérabilité peut être exploitée par l'intrusion d'un logiciel malveillant qui est utilisé comme outil d'espionnage pour renseigner son auteur sur les détails internes à une entreprise. Le paquet « cybersécurité », présenté par la Commission européenne en septembre 2017, cherche à pallier plusieurs de ces menaces.

- **MENACES LIÉES À LA RÉGLEMENTATION**

  Le monde entier a observé la réapparition massive de vers informatiques (« worms ») avec « WannaCry ». L'attaque en question a également montré qu'un risque peut provenir d'obligations très strictes au niveau de la régulation, qui peut donner une fausse perception de sécurité et qui lie en même temps des ressources importantes pour assurer la conformité des processus par rapport aux normes.

  Dans une autre optique, le cyberespace risque de ne pas être régulé suffisamment à certains endroits, puisque les législations n'arrivent pas toujours à suivre le rythme des nouvelles technologies, ce qui se traduit par des situations de vide juridique propices au développement d'activités malveillantes.

- **DIVULGATION D'INFORMATIONS SUR LES RÉSEAUX SOCIAUX ET « SOCIAL ENGINEERING »**

  De nos jours, la fréquentation des réseaux sociaux devient de plus en plus importante. Les utilisateurs y divulguent de nombreuses informations relatives à leur vie privée. La technique de l'ingénierie sociale vise à accéder à ces informations confidentielles qui sont stockées par les entreprises afin de les utiliser à des fins criminelles ou même d'espionnage ou de sabotage. Certaines entreprises « all-cloud » en sont un exemple : elles migrent toutes les données dans un « cloud », mais n'ont pas de procédures sécurisées pour entrer en contact avec le fournisseur du service cloud. Ces failles sont facilement exploitables par des criminels via le « social engineering », alors que les systèmes d'authentification forte qui l'éviteraient ne sont pas encore vraiment répandus dans les environnements cloud.

- **MENACES PROVENANT DU GRAND NOMBRE D'OUTILS D'ACCÈS À L'INTERNET**

  Aujourd'hui, les utilisateurs recourent fréquemment au téléphone portable pour accéder à l'internet et pour réaliser des opérations en ligne. Certains smartphones sont malheureusement difficiles à protéger et représentent dès lors une cible idéale.

- **UTILISATION DES OUTILS NUMÉRIQUES COMME MOYEN DE DÉSTABILISATION**

  L'une des menaces ayant eu un grand impact récemment réside au niveau des outils numériques utilisés comme moyen de déstabilisation. Citons le groupe de hackers Shadow-brokers, qui a réussi à voler un nombre important d'outils informatiques d'une autorité de sécurité, outils utilisés par celle-ci pour accéder à certains systèmes et réseaux. Les conséquences liées à l'utilisation d'une telle arme pourraient être très lourdes. Cette nouvelle menace s'aligne à des situations qui risquent de paralyser des pays, voire des régions entières. Le sabotage numérique et la mise à l'arrêt d'un pays entier par des moyens numériques deviennent de plus en plus réalistes : les forces armées du monde entier se préparent à de tels scénarios. La manipulation d'élections par des révélations émanant d'attaques numériques ou la diffusion de fausses informations sur les réseaux sociaux ont pu être observées dans certains pays au cours des dernières années, dans le cadre d'attaques hybrides, relevant en partie de la cybersécurité.

- **MENACES INHÉRENTES AU DÉVELOPPEMENT DE L'INTELLIGENCE ARTIFICIELLE**

  De manière générale, l'intelligence artificielle fera son apparition dans la conception et l'exécution des logiciels malveillants. Ce qui pour le moment est un sujet de recherche dans les universités sera bientôt assez mature pour être mis en œuvre dans des malwares réels, qui posséderont la capacité de s'adapter, de façon dynamique, aux mesures de sécurité mises en place par les équipes défendant les réseaux et infrastructures d'une organisation.

GLOSSAIRE

AIL
« Analysis of Information Leaks » *(analyse des fuites d'information)*

ANSSI
« Agence nationale de la sécurité des systèmes d'information » *: autorité nationale en matière de sécurité des systèmes d'information classifiés et non-classifiés installés et exploités par l'État et les opérateurs d'infrastructures critiques pour leurs besoins propres.*

BEESECURE stopline
Centre pour rapporter des contenus illicites et/ou préjudiciables en ligne.

CASES
« Cyberworld Awareness & Security Enhancement Services » *: programme du groupement d'intérêt économique SMILE g.i.e.*

CC
« Cyber Coalition » *: exercice de cyberdéfense annuel de l'OTAN.*

CCDCoE
« Cooperative Cyber Defence Centre of Excellence » *: Centre d'excellence pour la cyberdéfense de l'OTAN à Tallinn (Estonie).*

CDMB
« Cyber Defence Management Board » *: organe de l'OTAN chargé des affaires relevant de la cyberdéfense de l'alliance.*

CE2012
« Cyber Europe 2012 » *: exercice biannuel de l'UE.*

CERC
« Cellule d'Evaluation du Risque Cyber » *: groupe d'experts en matière cyber constitué dans le contexte du PIU Cyber*

STRATÉGIE NATIONALE EN MATIÈRE DE CYBERSÉCURITÉ III

CERT
« Computer Emergency Response Team » *: équipe prenant en charge des incidents de cybersécurité.*

CIRCL
« Computer Incident Response Center Luxembourg » *: CERT en charge des incidents cybers au niveau des secteurs privés et communaux, opéré par le groupement d'intérêt économique SMILE.*

CNPD
« Commission nationale pour la protection des données »

CSB
« Cybersecurity Board » *: créé par décision du Conseil de gouvernement le 18 juillet 2011. Le Cybersecurity Board luxembourgeois a pour mission d'élaborer le plan stratégique national de lutte contre les cyberattaques. Il est présidé par le Ministre des Communications et des Médias.*

CSIRT
« Computer Security Incident Response Team », *synonyme de CERT.*

CSSF
« Commission de surveillance du secteur financier »

CTIE
« Centre des technologies de l'information de l'État »

EC3
« European Cybercrime Centre »

ENISA
« European Network and Information Security Agency »

EUCTF
« European Cybercrime Task Force »

FIRST
« Forum of Incident Response and Security Teams »

FOP
« Friends of the Presidency »

FSI
« Fournisseur de Services Internet »

GOVCERT
« CERT gouvernemental » *: CERT prenant en charge des incidents de cybersécurité du secteur public et des infrastructures critiques. Créé par l'arrêté grand-ducal du 30 juillet 2013 déterminant l'organisation et les attributions du Centre gouvernemental de traitement des urgences informatiques, aussi dénommé « Computer Emergency Response Team Gouvernemental ».*

GT
« Groupe de travail »

HCPN
« Haut-Commissariat à la protection nationale »

ICP
« Infrastructure de clés publiques », *en l'occurrence LUXTRUST.*

ILNAS
« Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et de la qualité des produits et services »

ILR
« Institut Luxembourgeois de Régulation »

MISP
« Malware Information Sharing Platform » *: plateforme d'échange d'informations sur les logiciels malveillants.*

Menace hybride
En général, une menace hybride consiste en une combinaison de différents types de menaces, utilisées ensemble pour atteindre un objectif commun. Dans ce document, le terme adresse exclusivement les menaces hybrides incluant un aspect cyber.

MONARC
« Méthodologie d'analyse des risques de CASES »

MoU
« Memorandum of Understanding » *: mémorandum d'accord.*

NCSS II
« National Cyber Security Strategy 2 » *(stratégie nationale de cybersécurité 2).*

PGD
« Police grand-ducale »

PIU
« Plan d'intervention d'urgence »

PSI-LU
« Politiques de sécurité de l'information du Luxembourg »

POM
« Plans opérationnels par mesure »

RESTENA
« Réseau téléinformatique de l'éducation nationale et de la recherche »

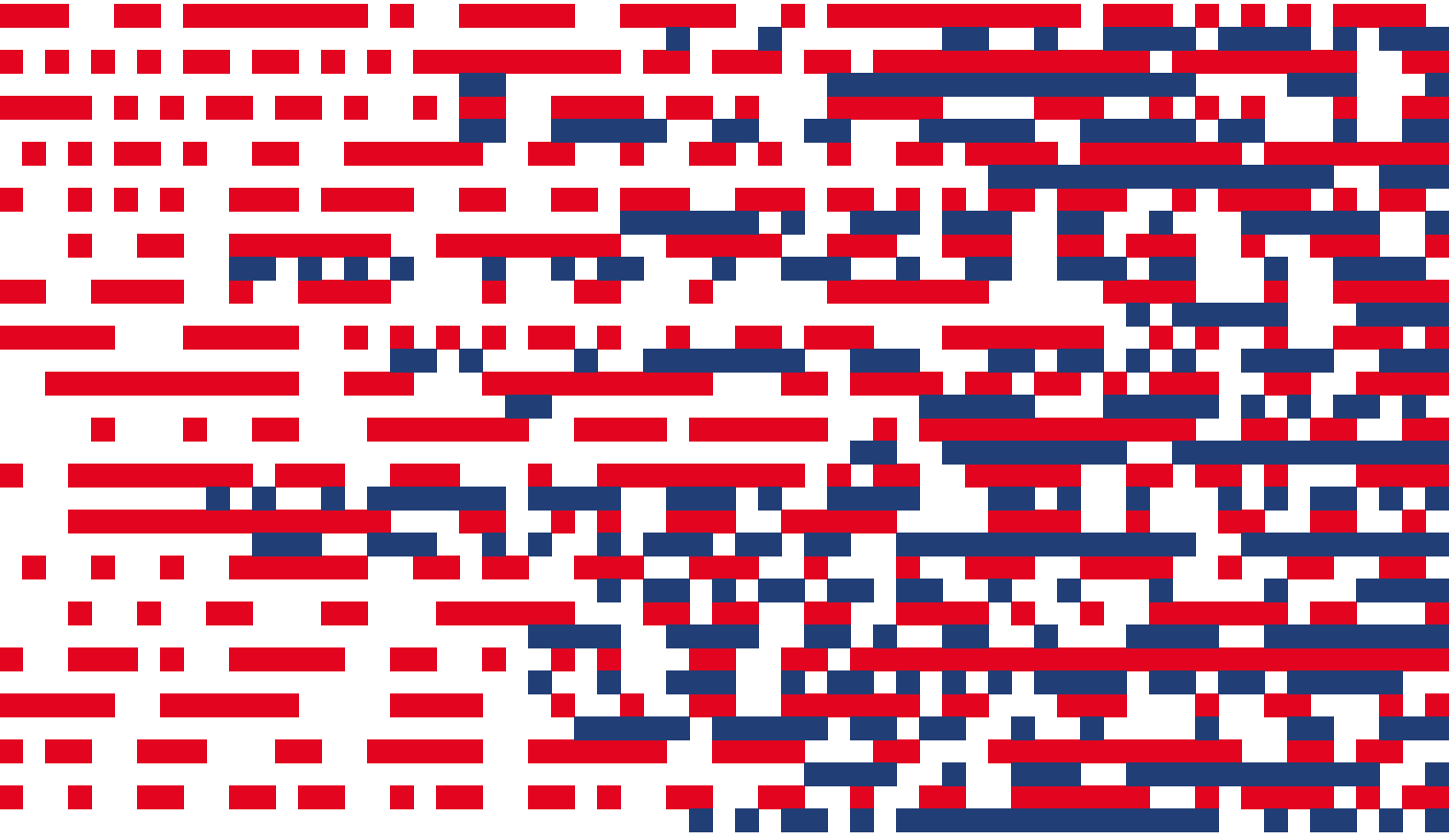
RGPD
« Règlement général sur la protection des données personnelles »

Smart nation
« Une nation polyglotte, cosmopolite, hyperconnectée, entreprenante et très bien formée »

SMC
« Service des Médias et des Communications »

SMILE
« Security Made in Lëtzebuerg » *g.i.e. : opérateurs majeurs des initiatives gouvernementales BEE SECURE, CASES et CIRCL. SMILE est constitué de 3 membres : l'État (représenté par trois ministères : Ministère de l'Économie, Ministère de la Famille, de l'intégration et à la Grande Région, Ministère de l'Education nationale, de l'Enfance et de la Jeunesse), le SYVICOL (Syndicat des villes et communes luxembourgeoises) et le SIGI (Syndicat intercommunal de gestion informatique).*

SSI
« Sécurité des systèmes d'information »

TIC
« Technologie de l'information et de la communication »

ENGLISH VERSION