STRATÉGIE NATIONALE DE CYBERSÉCURITÉ IV

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

TABLE DES MATIÈRES

· AVANT-PROPOS DE XAVIER BETTEL, PREMIER MINISTRE, MINISTRE DES COMMUNICATIONS ET DES MÉDIAS ·

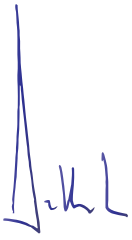
La stratégie nationale en matière de cybersécurité pour la période allant jusqu'à 2025 présente les orientations qui se trouvent à la base des projets que le Gouvernement entend mettre en œuvre pour sécuriser le cyberespace à tous les niveaux. Elle accompagne la transformation numérique qui caractérise notre économie et notre société.

Nous vivons des temps exceptionnels à plus d'un titre. Nous assistons au déploiement à large échelle de nouvelles technologies comme la cinquième génération de réseaux mobiles ou de nouvelles applications en matière d'intelligence artificielle. Les infrastructures numériques existantes au Luxembourg, en Europe et dans le monde ont été consolidées, permettant une plus grande connectivité pour plus de personnes avec des gains de fiabilité et de disponibilité indéniables, même si beaucoup reste à faire pour assurer que personne ne sera laissée pour compte dans cette révolution numérique. En même temps, des cybercriminels et d'autres acteurs de la menace profitent de ces changements et font recours aux nouveaux développements pour augmenter les tentatives d'intrusion, de sabotage ou de vols en ligne.

Prenant appui sur l'expérience acquise dans le contexte de la troisième stratégie adoptée en avril 2018 et soucieux de tenir compte des nombreuses facettes de la cybersécurité, la nouvelle stratégie a été élaborée par un groupe de travail pluridisciplinaire réunissant, sous la présidence du Haut-Commissariat à la Protection nationale, des représentants du Ministère des affaires étrangères et européennes, du Ministère de l'Economie, du GIE SECURITYMADEIN.LU, du Service des médias, des communications et du numérique, du Service de renseignement de l'Etat, de l'Institut luxembourgeois de régulation, de la Direction de la Défense, du Centre des technologies de l'information de l'Etat, du CERT gouvernemental et de l'Agence nationale de la sécurité des systèmes d'information.

La stratégie en matière de cybersécurité a pour finalité de permettre à tous les acteurs de participer pleinement à une société numérique et d'accéder aux nouvelles technologies dans un environnement sécurisé. Les mesures qui seront mises en œuvre dans ce contexte visent ainsi à assurer d'abord la prise de conscience des internautes et à renforcer leur confiance dans le monde numérique. Elles consistent ensuite à consolider et à renforcer la sécurité et la résilience des réseaux et infrastructures numériques. La stratégie cherche enfin à tenir compte de la cybersécurité comme facteur d'attractivité économique et à accompagner la stratégie de dynamisation qui caractérise le secteur du numérique en vue du développement continu d'une économie digitale performante.

Xavier Bettel



INTRODUCTION

· INTRODUCTION : TENDANCES ET MENACES PRINCIPALES ·

Le monde en 2021 est confronté à une multitude de crises internationales, de la crise sanitaire due à la pandémie COVID-19 à la crise climatique, en passant par une profonde crise du contrat social et de confiance politique dans de nombreux pays. Toutes ces crises ont des relations complexes mais indéniables avec les technologies et systèmes de l'information et de la communication : la dépendance de la société à l'égard de l'internet et la connectivité ne cesse de croître. En même temps, la surface d'attaque se diversifie avec l'introduction de nouvelles technologies tandis que les rivalités géopolitiques impactent la sécurité de l'espace numérique. Des actes malicieux sont entrepris par une multitude d'acteurs, étatiques et non-étatiques, contre des cibles diverses : administrations gouvernementales, entreprises et citoyens sont victimes de tels actes.

À l'aube de l'introduction massive de la cinquième génération de transmission de données mobiles (5G), moment qui promet de révolutionner la connectivité au niveau mondial, à la fois pour des applications industrielles et critiques, mais également pour les utilisateurs/citoyens, la société bénéficiera d'une rapidité d'accès à l'information et d'une disponibilité de données inouïes, à travers une forte augmentation des débits, une réactivité accrue grâce à une forte diminution des temps de latence ainsi qu'une nette amélioration des capacités de connectivité. La transition vers des technologies de plus en plus mobiles – l'ubiquité des smartphones et autres technologies portables, à prix sans cesse plus modique n'en est qu'un exemple – la dépendance toujours plus grande sur des solutions d'informatique en nuage, de même que le développement continu d'un internet des objets signifient que les sociétés humaines sont de plus en plus connectées, mais en même temps de plus en plus dépendantes de la disponibilité et de la fiabilité de leurs données. Les progrès de la recherche en matière de calcul quantique laissent entrevoir une continuation de la course-poursuite entre technologies de chiffrement et de déchiffrement.

Cet état de fait souligne une responsabilité collective des acteurs politiques, experts ICT et de l'industrie, tout comme celle du citoyen de tout âge à s'affranchir et à utiliser la technologie de manière avertie, voire d'exiger des services et outils de confiance, correspondant à leurs besoins.

La diffusion de désinformations, de discours de la haine ou de théories du complot mine la confiance des citoyens dans leurs gouvernements et souvent, menace la paix sociale. Les opérations d'influence – à des fins de déstabilisation politique tout comme à des fins d'augmenter des revenus privés – comme le micro-ciblage sur les réseaux sociaux étaient inimaginables il y a quelques années : elles sont devenues monnaie courante dans le paysage contemporain de la menace.

La préparation d'une nouvelle stratégie nationale de cybersécurité est l'occasion de prédilection pour revoir la posture de l'état en matière de sensibilisation à la sécurité de l'information. Dans un esprit d'ouverture et de collaboration, la nouvelle stratégie a été soumise pour consultation aux différentes parties prenantes au niveau national : Ministères et administrations concernés, entreprises privées, chercheurs professionnels en matière de sécurité de l'information et organisations de la société civile.

Si le progrès technologique est porteur de risques, il est également porteur d'opportunités à saisir. Le recours à la technologie blockchain pour de nombreuses applications différentes permet de développer des solutions de confiance dans des contextes politiques où la confiance peut être une denrée rare. La présente stratégie de cybersécurité esquisse comment une posture intégrée et complète en matière de sécurité de l'information permet à l'État, aux entreprises privées et aux citoyens de pleinement saisir les opportunités offertes par la révolution numérique. Les améliorations de performances des systèmes d'alerte et de riposte aux intrusions cyber offertes entre autres par des applications d'algorithmes avancés rendent la vie plus difficile aux groupes de menace persistante avancée ; des mesures d'atténuation des attaques par déni de service permettent de contrecarrer ou d'amortir l'effet disruptif sur les réseaux, applications ou autres services numériques.

Le Luxembourg s'engagera de manière plus proactive dans des initiatives de coopération positive au niveau mondial, comme le Plan d'Action de coopération numérique du Secrétaire général des Nations Unies. Sur le plan européen, le pôle numérique de l'UE est en phase de consolidation au Grand-Duché. L'écosystème national de la cybersécurité est en plein essor. La présente stratégie s'inscrit dans un processus continu d'amélioration de la coordination et des procédures en matière de sécurité de l'information et valorise les enseignements tirés des trois stratégies nationales précédentes.

II. STRATÉGIE NATIONALE DE CYBERSÉCURITÉ IV (2021-2025)

1. OBJECTIFS ET PRIORITÉS DE LA SNCS IV

OBJECTIFS STRATÉGIQUES

La quatrième stratégie nationale du Luxembourg se fonde sur les bases construites par les trois stratégies précédentes. Elle se décline en trois objectifs stratégiques, chacun étant assorti d'un nombre de priorités stratégiques. Sous chaque priorité sont regroupées un nombre d'actions concrètes et mesurables, reprises dans un tableau de suivi interne (disponible sur demande en s'adressant à info@hcpn.etat.lu).

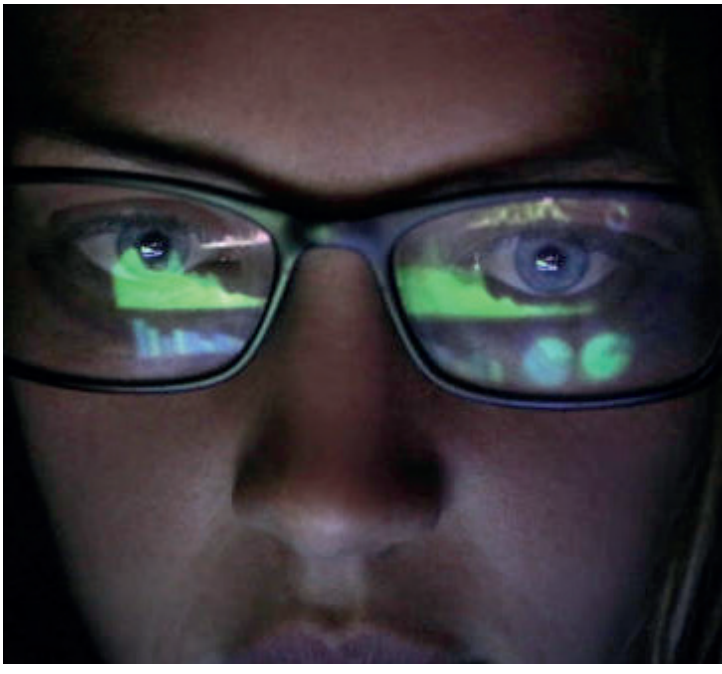
I. **Renforcement de la confiance dans le monde numérique et protection des droits humains en ligne**

II. **Consolidation de la sécurité et de la résilience des infrastructures numériques au Luxembourg**

III. **Développement d'une économie numérique fiable, durable et sécurisée**

1.1 OBJECTIF I : RENFORCEMENT DE LA CONFIANCE DANS LE MONDE NUMÉRIQUE ET PROTECTION DES DROITS HUMAINS EN LIGNE

La première obligation de l'État est la protection de ses citoyens et la garantie de leurs droits et libertés fondamentales. Dans une société connectée en permanence à internet et multi-dépendante de réseaux et systèmes informatiques, il y a de nombreux risques et menaces pour le vivre-ensemble et les droits de chaque personne. La protection de cet espace civique en ligne avec tous les droits humains – civils, politiques, économiques, sociaux, culturels et environnementaux – est le premier objectif dans la présente stratégie. Il s'agit, comme l'ont formulé les Nations Unies dans le Programme pour un développement durable à l'horizon 2030, de « ne laisser personne pour compte » : ce principe fondamental du contrat social s'applique à la fois dans le cyberespace et dans le monde physique. Ce pilier englobe autant la protection des données et de la vie privée que la sûreté des lieux de rencontre virtuels, déjà omniprésents, devenus véritablement indispensables à l'ère de la pandémie COVID-19.



I.1 PROTECTION DES DROITS HUMAINS EN LIGNE

- La coordination interministérielle sera renforcée dans les enceintes existantes pour conceptualiser et appréhender les risques pour les droits de la personne (Comité interministériel des droits de l'homme ; Groupe de travail « inclusion numérique » ; Groupe de coordination interministériel AI4GOV ; etc.) ;

- Les réflexions sur la règlementation des technologies de surveillance ou d'intrusion seront menées en tenant compte des discussions internationales, notamment au niveau de l'Union européenne et des Nations Unies, ainsi que dans le respect du droit international et communautaire ;

- Une documentation et des outils pour la sécurisation numérique (p.ex. sécurité et cryptage des communications, protection des données, etc.) à travers l'amélioration des compétences en matière de cybersécurité des organisations non-gouvernementales indépendantes qui travaillent dans le domaine de la défense des droits humains et travailleurs humanitaires (p.ex. CiviCERT) seront élaborés et mis à disposition.

I.2 PROTECTION DES DROITS DE L'ENFANT ET DES JEUNES

- Les efforts de protection des droits de l'enfant et des jeunes en ligne, notamment par la sensibilisation aux cyber-menaces, seront poursuivis, notamment par le biais de l'initiative gouvernementale BEE SECURE, fondée en 2010, qui est opérée par le 'Service National de la Jeunesse' (SNJ) et le 'Kanner a Jugendtelefon', et qui développe des mesures importantes au niveau de la sensibilisation de la population en général et des jeunes et enfants en particulier.

I.3 INCLUSION NUMÉRIQUE EN TOUTE SÉCURITÉ

- La diversité et l'inclusion seront promues dans le domaine de la cybersécurité, en appui à des initiatives comme Women In Digital Empowerment ou des projets de la société civile, notamment pour encourager des personnes issues de groupes de la population sous-représentés dans le secteur (notamment les femmes et les filles, ainsi que les personnes issues de l'immigration ou bénéficiaires de la protection internationales) à poursuivre une formation ou une carrière dans la cybersécurité.

- La cybersécurité et la sensibilisation à la sécurité en ligne trouveront leur place dans le contexte du groupe de travail interministériel pour l'inclusion numérique, qui vise notamment les publics éloignés du numérique. Le sujet est également abordé dans l'axe stratégique « confiance numérique » du plan d'action national pour l'inclusion numérique et constitue un élément fondamental de l'éducation à la citoyenneté numérique.

I.4 EDUCATION ET FORMATION PROFESSIONNELLE À LA CYBERSÉCURITÉ

- La sensibilisation, l'éducation et la formation en matière de cybersécurité seront abordées de manière plus stratégique. Le fait de développer des cursus professionnels adaptés à notre société actuelle et de sensibiliser aux métiers de la cybersécurité, rend ce domaine tangible aux citoyens. Les jeunes en voie d'entamer leurs brevets ou études, tout comme les adultes en voie de reconversion professionnelle pourront ainsi plus facilement concevoir une carrière liée au numérique et se projeter dans l'avenir. Les cursus et plans de recherche sont développés sous les points 4 et 5 de la présente stratégie

I.5 PEN-TESTING, BUG BOUNTIES ET DIVULGATION RESPONSABLE DE VULNÉRABILITÉS

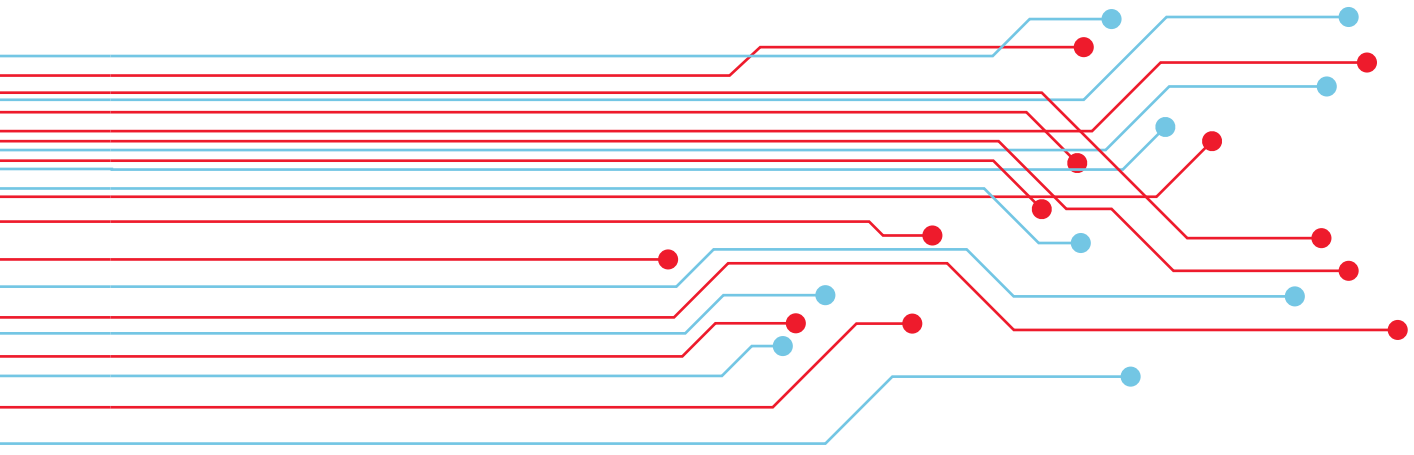
- Le Gouvernement proposera les modifications législatives et initiatives nécessaires pour rendre possible ou approfondir différentes approches pour améliorer la cybersécurité en ayant recours à l'intelligence collective des chercheurs de sécurité, entreprises privées actives dans la recherche de vulnérabilités et de tout utilisateur qui découvre une faille de sécurité. Il sera analysé la possibilité de créer à brève échéance auprès du GOVCERT.LU une plateforme incitant les chercheurs de rapporter des bogues, surtout ceux associés à des vulnérabilités.

I.6 LUTTE CONTRE LA CYBERCRIMINALITÉ

- Un organe de coordination sera mis en place entre les entités répressives et celles concernées par la cybersécurité, dans le respect de leurs mandats et missions respectifs. Cette enceinte permettra notamment d'analyser sur un plan stratégique et sur un plan opérationnel les répercussions de la menace de la criminalité organisée et de la prestation de services en matière de cybercriminalité, ainsi que les imbrications entre cybercriminalité et cybersécurité. Elle permettra aussi de rechercher des synergies dans la lutte contre différentes formes de criminalité sur internet, notamment la lutte contre l'exploitation et l'abus sexuel d'enfants ;
- La coopération avec Europol/EC3, ainsi qu'avec d'autres organisations internationales pertinentes (p.ex. Interpol, ONUDC) sera renforcée, cela en tenant compte des besoins et capacités des différents acteurs concernés.

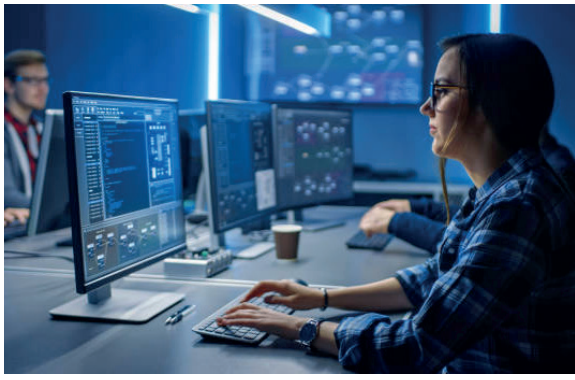
I.7 PARTICIPATION DÉMOCRATIQUE ET CIVIQUE SÉCURISÉE

- Un accent sera mis sur la prévention des opérations d'influence et de la désinformation véhiculée par voie numérique (menaces hybrides). Des guides et orientations seront élaborées à l'attention des entreprises en vue de détecter et parer les conséquences des crises engendrées par de telles campagnes.



1.2 OBJECTIF II : CONSOLIDATION DE LA SÉCURITÉ ET DE LA RÉSILIENCE DES INFRASTRUCTURES NUMÉRIQUES AU LUXEMBOURG

La disponibilité, l'intégrité et la confidentialité des données sont les objectifs de la cybersécurité : face aux nombreux incidents cyber observés quotidiennement, ainsi qu'aux risques et menaces observés à l'horizon, le Gouvernement a choisi de prioriser la consolidation de la sécurité et de la résilience des infrastructures numériques en tant que second objectif stratégique. La protection des infrastructures critiques et services essentiels fait partie des activités clé de cet objectif, tout comme la vaste panoplie d'activités des différentes entités opérationnelles.



II.1 RENFORCEMENT DE LA SÉCURITÉ ET LA RÉSILIENCE DES PROCESSUS NUMÉRIQUES ET DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION DE L'ÉTAT

- La sécurité et la résilience des processus numériques et des systèmes d'information et de communication essentiels sous-jacents seront renforcées :
  - le portail informationnel guichet.lu et myguichet.lu
  - la plateforme de messagerie électronique de l'État
  - le système de visioconférence
  - le système d'accès à distance
  - les équipements terminaux fixes et mobiles
  - le système DNS

- L'opportunité de mise en œuvre d'une solution de chiffrement d'échange de messages sensibles, respectivement classifiés jusqu'au niveau RESTREINT, sera évaluée dans le cadre d'un Proof of Concept.

- L'opportunité de mise en œuvre d'une solution nationale de messagerie instantanée sécurisée, destinée dans un premier temps aux services et agents de l'État sera étudiée dans le cadre d'un Proof of Concept. La solution « LuxChat » s'appuiera sur une architecture fédérée avec chiffrement de bout en bout des messages et sera implémentée sur la base de logiciels libres.

II.2 UTILISATION SÉCURISÉE ET MAÎTRISÉE DU CLOUD PUBLIC AU NIVEAU DE L'ETAT

- Soucieux de répondre aux enjeux du numérique de manière coordonnée et réfléchie, le Gouvernement s'est doté en 2016 d'une stratégie Cloud. L'investissement et la mise en place de services centraux au niveau de l'Etat, et rendus disponibles aux clients étatiques via des services de type cloud privé, comme par exemple « Govcloud », constituent la voie privilégiée.

Au vu des avancées du monde de la digitalisation, l'utilisation du cloud public devient incontournable dans certains domaines. Le cadre de gouvernance en matière de recours à des services Cloud publics au niveau de l'État ou dans le cadre de la fourniture de services publics sera définie en tenant compte notamment des aspects de sécurité, protection, localisation et rétention des données, de dépendances et risques d'atteinte potentiels à la souveraineté du gouvernement et aux services essentiels.

II.3 ASSURANCE DE LA SOUVERAINETÉ NUMÉRIQUE

- En coopération avec ses partenaires de l'Union européenne, le gouvernement luxembourgeois poursuivra ses efforts pour assurer la souveraineté numérique au niveau national et européen. Des réflexions à ce sujet seront menées entre toutes les parties prenantes du secteur public, en impliquant, selon les besoins et mandats des uns et des autres, des acteurs de l'industrie, du monde de la recherche ou de la société civile.

II.4 AMÉLIORATION CONTINUE DE LA DÉTECTION ET GESTION DES INCIDENTS

- Les capacités de prévention et détection d'intrusion sur les réseaux et systèmes d'information de l'État seront améliorées et progressivement étendues à l'ensemble des systèmes et réseaux névralgiques.

- Les capacités de traitement et d'analyse des logs de sécurité seront renforcées. La collecte, l'analyse et la corrélation des événements de sécurité sont indispensables pour détecter au plutôt les attaques, pour réagir rapidement en cas de compromission, respectivement, pour pouvoir réaliser les investigations à postériori en cas d'incident. L'architecture et les capacités du système de journalisation ainsi que les processus de gestion du GOVCERT seront adaptés de façon continue à l'évolution des systèmes d'information de l'État.

- Le recours systématique au télétravail augmente de façon conséquente la surface d'exposition aux attaques. En cas d'incident de sécurité et soucieux de minimiser les risques de propagation malveillante et de fuite de données, le recours à des outils d'analyse et de diagnostic à distance sera promu.

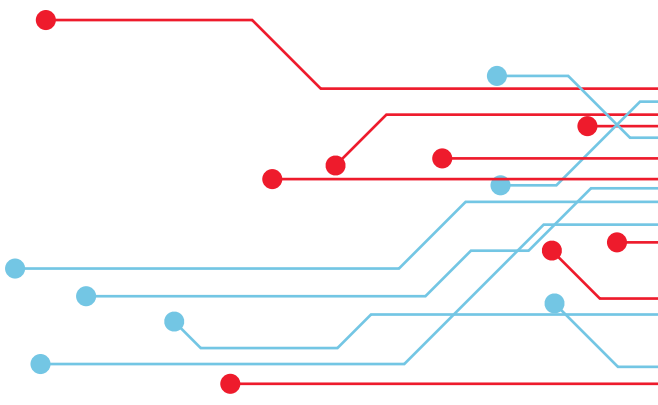
II.5 ÉTAT DES LIEUX CYBER (CYBER WEATHER) ET RENSEIGNEMENT D'INTÉRÊT CYBER

- Une meilleure conscience situationnelle partagée permettra à les toutes les parties intéressées d'agir en connaissance de cause et en concert afin d'assurer un niveau de sécurité adapté à l'état actuel de la menace.

- Dans le cadre de l'initiative Cyber Weather lancée par le GOVCERT, les CERTs luxembourgeois, sur base d'une analyse dynamique des incidents notifiés, constituent régulièrement un état des lieux cyber consolidé au niveau national. En collaboration étroite avec l'ensemble des acteurs impliqués l'état des lieux sera progressivement étoffé par le biais de l'incorporation d'informations des autres sources disponibles (ISACs sectoriels, SOCs, sondes de détection d'intrusion, analyses des risques, etc.).

- L'analyse systématique des informations récoltées, combinée à l'analyse des modes opératoires des attaques, permettra de mieux comprendre l'état de la menace (renseignement d'intérêt cyber) et de dégager des recommandations concrètes et actionnables en matière de prévention et de préparation.

- Les entités étatiques concernées assureront une diffusion cohérente et exploitable des menaces actuelles aux opérateurs publics et privés et aux professionnels du secteur des TICs d'une part et assureront la diffusion d'avertissements de sécurité avec recommandations de mitigation à l'attention du grand public d'autre part.



II.6 EVALUATION ET GESTION DES RISQUES

- Depuis la première stratégie nationale en matière de cybersécurité, le gouvernement promeut activement une culture de gestion des risques, basée sur des analyses des risques et l'application de mesures de sécurité adaptées au niveau de risque encouru. Cette approche sera étendue à tous les secteurs et les outils d'analyse des risques mis à disposition seront adaptés aux besoins spécifiques des secteurs.

- L'agrégation des évaluations des risques au niveau sectoriel et national permettra de dégager les risques systémiques au sein des secteurs et au niveau national et de définir des scénarios d'évaluation des risques systémiques. Ces scénarios seront mis à disposition des secteurs pour être intégrés dans leurs analyses des risques.

- L'identification et l'échange des scénarios de risques et métriques pertinentes est une activité collective qui sera coordonnée au niveau de l'État et documentée dans la Risk Scenario Sharing Platform (MOSP). Celle-ci sera accessible en tant que service public, qui à moyen terme, va contribuer substantiellement à augmenter la qualité de la gouvernance (« *informed governance* »), la résilience et donc l'attractivité du Luxembourg.

II.7 PROTECTION DES INFRASTRUCTURES CRITIQUES

- Le Centre national de filtrage d'attaques de dénis de service distribuées sera chargé de suivre systématiquement les évolutions et tendances DDOS au niveau national et mondial et d'élaborer des recommandations et bonnes pratiques à destination des infrastructures critiques en matière de prévention, détection et réaction aux attaques de dénis de service distribués.

- Un centre opérationnel de la sécurité pour infrastructures critiques sera mis en place. En vue de la protection contre les menaces connues et émergentes, de la diffusion systématique d'informations sur les menaces exploitables, les attaques et les tentatives d'intrusion, et de la constitution d'une connaissance partagée de la situation grâce à des métriques, il est envisagé de déployer, en partenariat avec les acteurs du secteur privé, un réseau national de sondes installées auprès des infrastructures critiques volontaires.

- Le GOVCERT continuera à renforcer ses capacités, compétences ainsi que son équipe de pentesting. Le service actuellement offert aux administrations et services de l'Etat sera étendue aux infrastructures critiques.

II.8 SÉCURITÉ DES RÉSEAUX ET SYSTÈMES D'INFORMATION DES OPÉRATEURS DE SERVICES ESSENTIELS

- L'ILR en tant qu'autorité nationale compétente et point de contact unique, veille à ce que les opérateurs de services essentiels gèrent la sécurité de leurs réseaux et systèmes d'information. En étroite coopération avec les opérateurs de services essentiels, l'ILR fera évoluer la plateforme d'analyse et de gestion des risques SERIMA, va élaborer des bonnes pratiques sectorielles, initier des campagnes de sensibilisation et organiser des exercices de gestion des incidents.

II.9 CYBERSÉCURITÉ DU SECTEUR DE LA SANTÉ

- La cybersécurité accompagnera la digitalisation accélérée des services de santé, notamment à la lumière des développements initiés dans le contexte de la pandémie du COVID-19. L'assurance de la sécurité des systèmes d'information et de communication, des dispositifs médicaux et particulièrement des données des patients (p.ex. Dossier de Soins Partagé) est devenu un enjeu stratégique.

- En concertation étroite avec les parties prenantes la collaboration avec les acteurs du secteur sera intensifiée, la sécurité et la résilience des systèmes d'information et réseaux clés seront renforcés, un système centralisé de gestion des évènements de sécurité (SIEM) sera mis en œuvre, le HealthNet CSIRT sera renforcé, le partage collaboratif d'information en matière de cybersécurité du secteur de la santé sera institutionnalisée (ISAC) et la mise en œuvre d'un centre opérationnel de gestion de la sécurité (SOC) pour l'ensemble du secteur de la santé sera envisagée.

II.10 AMÉLIORATION DES PROCESSUS ET PROCÉDURES DE GESTION DE CRISE CYBERNÉTIQUE AU NATIONAL ET INTERNATIONAL

- Le Luxembourg continuera de participer régulièrement à des exercices internationaux de gestion de crise cybernétique (e.a. de l'UE et de l'OTAN). Les leçons apprises lors des exercices seront mises en œuvre au niveau national. Les procédures et la structure décisionnelle pour la réaction diplomatique aux incidents cyber, notamment dans le contexte de la coopération au sein de l'UE et le Plan d'intervention d'urgence cyber seront revues. Au niveau national, des exercices de gestion d'incidents cybernétiques majeurs impactant les infrastructures critiques seront réalisés en mettant à profit la plateforme nationale de simulation Cyber Range.

II.11 PROMOTION DE LA COLLABORATION ET DE L'ÉCHANGE D'INFORMATIONS ENTRE LE SECTEUR PUBLIC ET LE SECTEUR PRIVÉ

- L'État va mettre en place, en étroite collaboration avec ICT Luxembourg et les fédérations y représentées un groupe de travail transversal (GTT Cyber) destiné à organiser, structurer et dynamiser les échanges et l'entraide dans le domaine cyber. Ce GTT cyber a pour but d'échanger de façon proactive et rapide des informations par rapport à des attaques ayant un grand potentiel de propagation.

  En cas de besoin, le GTT cyber se chargera aussi de coordonner les différentes équipes de gestion d'incident privées pour dynamiser l'entraide. Si nécessaire, cette coordination pourra aussi être reprise par CIRCL, ou, en cas de crise, par la cellule de crise Cyber mise en place par le HCPN.

- La Threat Intelligence Sharing Platform (MISP), la Risk Scenario Sharing Platform (MOSP) ainsi que tout autre outil ou service identifiés comme nécessaires, vont servir comme plateformes d'échange d'information et soutenir un échange dynamique et riche par rapport aux menaces, et vulnérabilités rencontrées ainsi que sur les mesures à mettre en place.

II.12 SÉCURITÉ DES RÉSEAUX ET SERVICES DE TÉLÉCOMMUNICATIONS

- La directive (UE) 2018/1972 du 11 décembre 2018 établissant le code des communications électroniques européen sera transposée dans le droit national. L'échange et la coordination avec les opérateurs de réseaux de télécommunications seront développés, notamment en vue de la mise en œuvre des mesures de sécurité de la boîte à outils 5G.

II.13 SÉCURITÉ DE LA CHAÎNE D'APPROVISIONNEMENT

- Les entités responsables de l'Etat continueront de travailler à l'amélioration des capacités de détection et de réponse aux risques et menaces tout au long de la chaîne d'approvisionnement en matériel, logiciels, ou services. Pour cela, elles se baseront sur les recommandations et bonnes pratiques pour l'État, OIC, OSE, etc. en la matière.

II.14 SÉCURISATION AU NIVEAU NATIONAL DES COMMUNICATIONS PAR COURRIER ÉLECTRONIQUE

- Le courrier électronique constitue le vecteur d'attaque majeur pour des actions spécifiques comme l'hameçonnage ciblant les utilisateurs. Un ensemble de mesures spécifiques sera mis en œuvre pour sécuriser d'avantage les services de messagerie électronique :
  - Incitation des fournisseurs de services de messagerie électronique à sensibiliser leurs clients et à leur proposer la solution de notification nationale de spam spambee.lu
  - Développement d'une offre d'évaluation de la sécurité des serveurs de messagerie électronique par le C3
  - Promotion et support à l'implémentation du standard pour la protection des domaines et d'authentification du courrier électronique DMARC

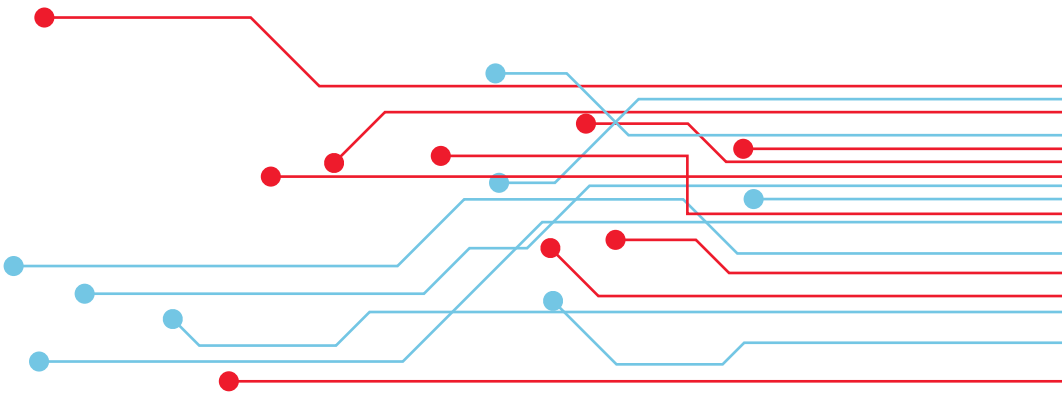
II.15 SÉCURISATION DES COMMUNICATIONS ET DES DONNÉES PAR LE RECOURS AUX TECHNOLOGIES QUANTIQUES

- En juin 2019, le Luxembourg a signé une déclaration de coopération visant à explorer ensemble avec la Commission Européenne et l'Agence Spatiale Européenne (ESA) la faisabilité de l'implémentation d'une infrastructure de communication sécurisée, basée sur la technologie quantique. Cette infrastructure sera constituée d'une partie terrestre et d'une partie spatiale. Face à la menace pour l'intégrité des communications chiffrées que représente la puissance de l'ordinateur quantique, la « Quantum Communication Infrastructure » (QCI) pourrait être la réponse, permettant d'échanger de manière sûre des clés de cryptage (quantum key distribution, QKD). Cette infrastructure sera développée et implémentée au niveau national pour ensuite être intégrée dans l'infrastructure européenne. La QCI s'adresse dans un premier temps aux usagers du secteur public avec le but de l'élargir au secteur privé. Les cas d'utilisation potentiels identifiés sont les suivants :
  - Infrastructures critiques (énergie, transport, approvisionnement en eau, etc.)
  - Centres de données
  - Niveau de protection supplémentaire pour le HPC « Meluxina »
  - Institutions européennes

II.16 OPÉRATIONNALISATION DE LA STRATÉGIE NATIONALE EN MATIÈRE DE CYBERDÉFENSE

- La Direction de la Défense du Ministère des Affaires étrangères et européennes ensemble avec l'Armée luxembourgeoise ont cartographié les obligations luxembourgeoises et les priorités nationales en matière de cyber défense afin d'établir un cadre pour faciliter la transformation de la Défense luxembourgeoise en l'une des forces armées la plus sécurisée en matière de cyber d'ici 2030.

- En développant des capacités en matière de cybersécurité pour les systèmes d'information et de communication, la Défense luxembourgeoise œuvre à devenir un point de référence et à renforcer son image de partenaire fiable pour les entités nationales et organisations internationales. Cet objectif à long terme est soutenu par les objectifs stratégiques comme la cultivation de talents, le renforcement de la coopération en matière de cybersécurité aux niveaux national et international, l'intégration de la sécurité Cyber/CIS dans toutes les activités de la Défense luxembourgeoise ainsi que la recherche et le développement.



1.3 OBJECTIF III : DÉVELOPPEMENT D'UNE ÉCONOMIE NUMÉRIQUE FIABLE, DURABLE ET SÉCURISÉE

« Ouverture, dynamisme et fiabilité » : la stratégie de dynamisation et de diversification économique du Gouvernement luxembourgeois mise en grande partie sur le développement continu d'une économie digitale performante. La cybersécurité est indispensable pour le bon fonctionnement des relations, transactions, services et autres interactions qui sous-tendent l'économie numérique. Les relations de confiance jouent à plusieurs niveaux : entre Etat et citoyens, entre utilisateurs et outils technologiques, finalement entre partenaires économiques. Les différents secteurs porteurs de l'économie luxembourgeoise, industrie, finances, technologie, connaissances, logistique, s'appuient tous sur des réseaux et systèmes informatiques performants et fiables.

III.1 FÉDÉRATION DE L'ÉCOSYSTÈME DE LA CYBERSÉCURITÉ DU LUXEMBOURG

- SECURITYMADEIN.LU, en étroite collaboration avec le Ministère de l'Économie et Luxinnovation, poursuivra la gestion du répertoire des acteurs de la cybersécurité au Luxembourg afin d'identifier et promouvoir les services disponibles au Luxembourg, d'intensifier les collaborations entre acteurs et de promouvoir ce secteur au niveau international.
- Luxinnovation et le Ministère de l'Économie peuvent, de façon ciblée, attirer des sociétés qui offrent des services spécifiques qui ne sont pas encore disponibles au Luxembourg.

III.2 FÉDÉRATION DE L'ÉCOSYSTÈME DE LA RECHERCHE EN CYBERSÉCURITÉ AU LUXEMBOURG

- SECURITYMADEIN.LU, via son département C3 (Cybersecurity Competence Center) et en collaboration avec les acteurs de recherche et les acteurs étatiques concernés définira les priorités de recherche en matière de cybersécurité et coordonnera les acteurs de la recherche. Des collaborations avec les centres de recherche en grande région sont intensifiées. Ceci répondra aussi à la proposition de règlement Européen COM (2018) 630 qui prévoit une réorganisation des allocations des fonds de recherche européens dans le domaine de la cybersécurité.

III.3 DÉVELOPPEMENT DES MÉTHODOLOGIES DE CERTIFICATION, DE TESTS ET DE NORMALISATION

- L'Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) a été désigné comme autorité nationale de certification de cybersécurité[1] (NCCA – National Cybersecurity Certification Authority) au Luxembourg dans le cadre du règlement (UE) 2019/881 sur la cybersécurité (« Cybersecurity Act – CSA »). Dans ce cadre, l'ILNAS sera en charge des missions de supervision et veillera, en ce sens, à faire respecter les règles en relation avec les différents schémas de certification de cybersécurité, aux fins du contrôle du respect par les produits TIC, services TIC et processus TIC des exigences des certificats de cybersécurité européens délivrés sur le territoire national. Le cas échéant, l'ILNAS sera également chargé du contrôle du respect des obligations qui incombent aux fabricants ou fournisseurs de produits TIC, services TIC ou processus TIC qui sont établis sur le territoire national, et qui procèdent à une autoévaluation de conformité.

- Dépendant des besoins nationaux identifiés en regard, le gouvernement pourra décider de nommer une autre autorité nationale de certification de cybersécurité pour assurer les missions de certification et/ou directement en lien avec ce domaine.

- L'ILNAS participe à différentes réunions du groupe européen de certification de cybersécurité établi en 2018 par l'Acte législatif sur la cybersécurité de l'UE, pour prise en compte de toute information pertinente en regard de ses missions de supervision.

[1] **Niveaux d'assurance**
Un schéma européen de certification de cybersécurité peut préciser un ou plusieurs des niveaux d'assurance suivants pour les produits TIC, services TIC et processus TIC: « élémentaire », « substantiel » ou « élevé ». Le niveau d'assurance correspond au niveau de risque associé à l'utilisation prévue du produit TIC, service TIC ou processus TIC, en termes de probabilité et de répercussions d'un incident.

Autoévaluation
Un schéma européen de certification de cybersécurité peut permettre la réalisation d'une autoévaluation de la conformité sous la seule responsabilité du fabricant ou du fournisseur de produits TIC, services TIC ou processus TIC. L'autoévaluation de la conformité n'est autorisée que pour les produits TIC, services TIC et processus TIC qui présentent un risque faible, schéma correspondant au niveau d'assurance dit « élémentaire ». Le fabricant ou fournisseur de produits TIC, services TIC ou processus TIC garde à la disposition de l'ILNAS la déclaration de conformité de l'Union européenne, la documentation technique et toutes les autres informations pertinentes relatives à la conformité des produits TIC ou services TIC avec le schéma européen de certification concerné pendant la durée prévue dans le schéma.

Certification
Pour les niveaux d'assurance élémentaire ou substantiel, la certification est faite par un organisme d'évaluation de la conformité (CAB – conformity assessment body), sauf si un schéma prévoit (Art. 56 (5)) que seul un organisme public peut délivrer les certificats dans des cas dûment justifiés. CASES, le département de SECURITYMADEIN.LU ayant comme mission de sécuriser les PME, sera CAB pour le niveau élémentaire.

III.4 CRÉATION DU PREMIER DATA SPACE CYBERSÉCURITÉ EN EUROPE

- SECURITYMADEIN.LU créera le premier *data space* en cybersécurité en Europe et incitera ainsi les acteurs de l'écosystème luxembourgeois et de la grande région à échanger, respectivement à mettre à disposition des données pour la recherche et la création de nouveaux produits et services en matière de cybersécurité.

III.5 CAPITALISATION SUR LE CENTRE DE COMPÉTENCES EN CYBERSÉCURITÉ (C3)

- La portée de la ROOM#42, le simulateur de cyber-incidents pour des formations d'équipes de réponse aux incidents, va être étendue afin de permettre son utilisation en mode réparti, au travers d'une plateforme électronique dédiée.

- Le déploiement de la ROOM#42 sous forme de plateforme rendra possible une interconnexion avec les infrastructures de type Cyber Range, permettant la mise au point de scénarios plus complexes, amenant les équipes techniques à faire face à des incidents simulés plus proches de leurs réalités opérationnelles.

- Le C3 continuera de développer des partenariats aux niveaux national et international, suite à l'ouverture d'une première « franchise » à Toulouse en mai 2019.

- En complément de la ROOM#42, le C3 développera une méthode de création et mise en œuvre d'exercices de gestion de crise impliquant des acteurs avec des niveaux de compétence hétérogènes. Les outils correspondants seront également mis à disposition de l'écosystème.

- Un cadre de compétences en cybersécurité national (« cybersecurity skills and competence framework ») sera établi, afin de faciliter la montée en compétences de cybersécurité par les acteurs de l'économie et notamment les PME. Ce cadre décrira les rôles génériques et compétences correspondantes et comportera un outil d'aide à la décision. D'autres services en cohérence avec ce cadre seront créés.

- Le partenariat public-privé autour de la plateforme de « testing » du C3 sera développé, afin d'aider les organisations à identifier les points à améliorer d'un point de vue compétences. Elle doit permettre de tester les infrastructures, les organisations, ainsi que les individus. Elle doit également s'accompagner d'outils et documentation permettant de comprendre et interpréter les résultats des tests. Cette plateforme sera aussi mise à disposition du European Digital Innovation Hub Luxembourgeois, opéré par Luxinnovation, pour offrir le service de « test before invest ».

- Un observatoire du C3 sera mis en place, afin de :
  - centraliser tous les efforts de veille, de cyber-weather et de partage d'information et analyser les données récoltées ;
  - produire un « bulletin » régulier sur des sujets pertinents et d'actualité pour le Luxembourg ;
  - fournir une information pouvant servir de référence aux décideurs des organisations lors de leurs choix d'allocations de ressources en matière de cybersécurité.

III.6 COMMUNAUTÉ EUROPÉENNE DES COMPÉTENCES EN MATIÈRE DE CYBERSÉCURITÉ

- Désignation du centre national de coordination et contribution à l'atteinte des objectifs du Centre européen de compétences industrielles, technologiques et de recherche en matière de cybersécurité, notamment par la participation active aux activités du réseau européen en matière de compétences « cyber ».

III.7 RENFORCEMENT DES CAPACITÉS AU NIVEAU NATIONAL ET INTERNATIONAL

- Les acteurs étatiques continueront de travailler à la mise à disposition d'outils, de méthodes et de documentations destinés à faciliter l'appropriation des technologies de sécurité par le secteur économique et la société civile des pays les moins avancés, en particulier au travers de la coopération au développement des compétences locales (« *capacity building* »).

- Les efforts intra gouvernementaux « *Digital 4 Development* » seront coordonnés par la Direction de la Coopération au développement du MAEE. Le développement de l'expertise luxembourgeoise en matière de renforcement des capacités et de transfert de compétences vers les pays et régions qui en ont le plus besoin sera poursuivi via les canaux établis de la Coopération luxembourgeoise, ainsi que des partenariats public-privé ; Le C3 poursuivra sa participation active au consortium pour la mise en place de la plateforme de l'Union européenne pour le renforcement des capacités en matière de cybersécurité pour les pays en développement (EU CyberNet : https://www.eucybernet.eu).

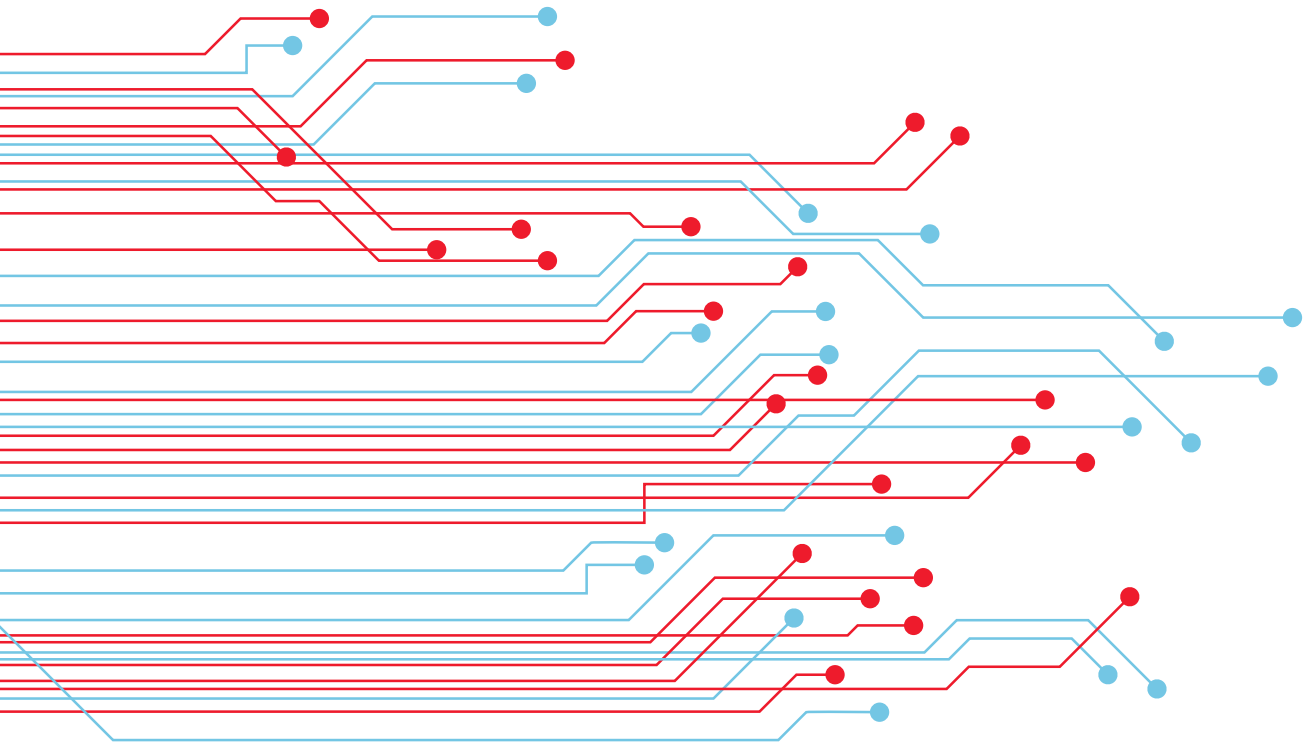
- MILCERT.LU renforce les efforts de coopération dans le réseau des CERTs militaires notamment dans le domaine de la formation à la cybersécurité du personnel militaire au Luxembourg.

- Le Luxembourg participera au *Global Forum on Cyber Expertise (GFCE)* et à d'autres coopérations internationales dans le domaine de la mise à disposition d'expertise cyber.

III.8 INTENSIFICATION DES PARTENARIATS AVEC L'INDUSTRIE, LE MONDE DE LA RECHERCHE ET LA SOCIÉTÉ CIVILE

- Des projets de recherche seront promus en vue du développement de logiciels et de matériel informatique sécurisés avec le Centre interdisciplinaire pour la sécurité, la fiabilité et la confiance (SnT) de l'Université du Luxembourg.

- Création de partenariats visant à favoriser l'émergence d'innovations en cybersécurité économiquement viables. Cela devrait passer par la mise à disposition des différents partenaires d'un portfolio de services et modèles économiques adaptés à la nature des services ou produits qu'ils comptent développer ou promouvoir.



2. CADRE DE GOUVERNANCE NATIONAL EN MATIÈRE DE CYBERSÉCURITÉ

2.1 COMITÉ INTERMINISTÉRIEL DE COORDINATION DE CYBERPRÉVENTION ET DE CYBERSÉCURITÉ

- Le 6 décembre 2017, le Conseil de gouvernement a approuvé la création d'un comité interministériel chargé d'assurer la coordination nationale en matière de cyberprévention et de cybersécurité (CIC-CPCS). Le comité a pour tâche d'assurer la coordination pragmatique et rapide des initiatives faisant partie de la cyberprévention et de la cybersécurité.

- Le CIC-CPCS, appelé à se concerter sur une base régulière sous présidence du Haut-Commissaire à la Protection nationale, a pour mission, dans le respect des compétences et responsabilités propres des entités décrites ci-après :
  - 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 cybersécurité et de cyberprévention 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 cybersécurité et de cyberprévention.

2.2 PRINCIPALES ENTITÉS ÉTATIQUES CONCERNÉES PAR LA GOUVERNANCE NATIONALE DE LA CYBERSÉCURITÉ

- Le Haut-Commissariat à la protection nationale (HCPN) intervient au niveau de la gestion d'une crise cybernétique. Son action est définie à travers le plan d'intervention d'urgence face aux attaques contre les systèmes d'information à partir du moment que 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 (ANSSI) qui a pour mission de définir les lignes directrices en matière de la sécurité de l'information et de veiller à ce que les mesures concernant la sécurité des systèmes d'informations soient mises en place. Le Centre gouvernemental de traitement des urgences informatiques (CERT gouvernemental / 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.

- Le Ministère de l'Economie est chargé 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 SECURITYMADEIN.LU), 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 CIRCL (services de coordination et d'ac-

tion post-incidents), ce dernier exerçant également la fonction de CERT pour les entités privées et non gouvernementales et les communes.

- Le Ministère d'Etat – Service des médias, des communications et du numérique (SMC) suit le Conseil Telecom et Société de l'Information de l'UE et ses réunions préparatoires et couvre le sujet de la stratégie de cybersécurité, notamment pour le domaine des réseaux de communications électroniques, au nom du Ministre des Communications et des Médias, pour le compte du Ministère d'Etat.

- Au sein du Ministère de la Digitalisation, le Centre des technologies de l'information de l'État (CTIE) 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'Etat ainsi que la production de documents administratifs sécurisés.

- Le Service de Renseignement de l'Etat 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, la prolifération d'armes de destruction massive ou de produits liés à la défense et des technologies y afférentes.

- Deux directions du Ministère des Affaires étrangères et européennes sont concernées :
  - La Direction des Affaires politiques coordonne les travaux en matière de cyberdiplomatie. Ceci comporte le suivi des activités du groupe de travail horizontal pour les questions cyber du Conseil de l'Union européenne, de la « boîte à outils cyber-diplomatique » et du régime de sanctions cyber, ainsi que les autres activités en matière de cyberdiplomatie au niveau international, notamment dans le cadre des Nations Unies.
  - La Direction de la Défense est concernée par le sujet dans la mesure où la cyberdéfense fait partie d'une des tâches fondamentales de l'OTAN étant donné que les cyberattaques occupent une place importante dans le cadre d'actions de guerre hybride. A noter en outre que l'OTAN et l'Union européenne ont signé en février 2016 un arrangement de coopération en matière de cyberdéfense pour répondre aux défis communs auxquelles les deux organisations ont à faire face.

- L'Institut luxembourgeois de régulation (ILR) est le point de contact unique pour le Luxembourg dans le cadre de la mise en œuvre de la Directive européenne sur les réseaux et systèmes d'information (« directive NIS ») et l'autorité compétente pour tous les secteurs visés dans la loi NIS exception faite du secteur financier qui reste sous l'égide de la Commission de surveillance du secteur financier (CSSF). Dans ce cadre, l'Institut s'est vu confier de nouvelles compétences en matière de sécurité des réseaux et systèmes d'information ainsi que dans le contexte de la cybersécurité. Concrètement, le rôle de l'Institut en tant qu'autorité compétente est d'assurer que les secteurs sous sa responsabilité (énergie, transport, santé, eau potable, infrastructure numérique et fournisseurs de services numériques) parviennent à atteindre un niveau de sécurité commun élevé pour pouvoir assumer des incidents informatiques ou des cyberattaques et prévenir ainsi des incidents ayant un impact significatif sur la disponibilité, confidentialité et intégrité des services essentiels.

2.3 CYBERSECURITY LUXEMBOURG, L'ÉCOSYSTÈME LUXEMBOURGEOIS DE LA CYBERSÉCURITÉ

L'initiative CYBERSECURITY LUXEMBOURG a été lancée par le Ministère de l'Economie pour consolider et améliorer la coopération publique-privée en matière de cybersécurité.

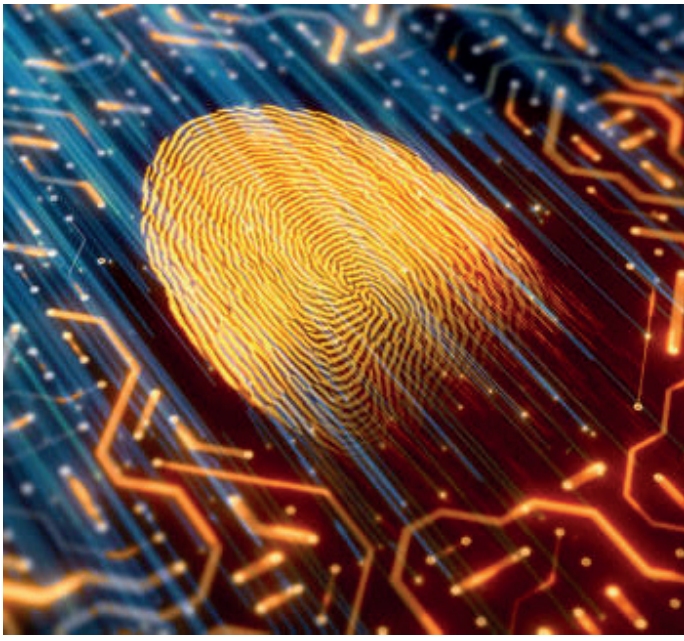
En tant que label national de l'écosystème luxembourgeois de la cybersécurité, CYBERSECURITY LUXEMBOURG rassemble et appuie tous les acteurs pertinents des secteurs privé et public dans le domaine de la cybersécurité, afin de consolider ce pilier crucial de l'économie nationale et de faciliter une ouverture internationale de l'expertise luxembourgeoise en matière de cybersécurité. Endossée par tous les acteurs du marché, la marque CYBERSECURITY LUXEMBOURG représente une plateforme commune aux niveaux national et international.

CYBERSECURITY LUXEMBOURG – est dirigée et opérée par trois entités :

- **HCPN** – en tant qu'entité présidant le comité interministériel de cybersécurité (CIC) et coordinatrice de la stratégie nationale de cybersécurité, le HCPN dirige l'initiative en l'intégrant dans la stratégie nationale et en assurant la liaison avec les autres entités publiques concernées. L'ANSSI, l'autorité nationale pour la cybersécurité du secteur public à l'exception des municipalités, qui dépend du HCPN, organisera la collecte et la récolte d'informations des entités publiques impliquées (p.ex. CTIE) et dirigera la plateforme en ligne qui couvre sa sphère de compétence.

- **SECURITYMADEIN.LU** – L'agence de cybersécurité pour l'économie et les communes luxembourgeoises sera chargée de la coordination générale de l'initiative. SECURITYMADEIN.LU organisera la collecte et le rassemblement, ainsi que la gestion des informations en matière de services indispensables mis à disposition par l'écosystème. Elle cartographiera leur disponibilité parmi les acteurs de l'écosystème et améliorera la collaboration potentielle entre eux. Elle fera également la promotion, en collaboration avec Luxinnovation, l'écosystème au sein de la Grande Région et en Europe. Elle cogérera la plateforme électronique et contribuera les outils de communication et de promotion, comme les petits déjeuners cybersécurité, la semaine de la cybersécurité, etc.

- **LUXINNOVATION** – cette agence gouvernementale met à disposition des entreprises et organisations de recherche publique un large éventail de services afin de favoriser l'innovation et de soutenir ainsi les objectifs de développement économiques du Gouvernement. L'agence fait en sorte que le Luxembourg continue d'attirer des investissements, entreprises et connaissances qui sont parfaitement adaptées au contexte du pays. Luxinnovation contribue son expertise en termes de connaissance des marchés et de promotion de l'écosystème aux niveaux national et international. En tant que coordinateur de l'initiative L-DIH (Luxembourg Digital Innovation Hub), elle fera le pont entre besoins et expertise en matière de cybersécurité (contribuant aux parties pertinentes de la plateforme en ligne).



2.4 L'INITIATIVE GOUVERNEMENTALE BEE SECURE

Fondée en 2010, l'initiative gouvernementale BEE SECURE est opérée par le 'Service National de la Jeunesse' (SNJ) et le 'Kanner-Jugendtelefon', en partenariat avec SECURITYMADEIN.LU, la Police Grand-Ducale, ainsi que le Parquet général du Grand-Duché de Luxembourg. Les ministères impliqués sont le ministère de l'Education nationale, de l'Enfance et de la Jeunesse, le ministère de l'Économie et le ministère de la Famille et de l'Intégration.

BEE SECURE est également le représentant luxembourgeois du 'Safer Internet Center' (SIC) cofinancé par la Commission européenne et en tant que tel bénéficie de l'appui d'un réseau d'homologues et partenaires au niveau international : INSAFE (centres de sensibilisation et « helplines ») et INHOPE (centres de signalement pour contenus illégaux).

De par son expérience sur le terrain luxembourgeois et grâce à son réseau établi de partenaires, BEE SECURE est en mesure de contribuer de manière concrète à l'autonomisation de l'utilisateur.

OBJECTIFS DE BEE SECURE :

Promouvoir une utilisation plus sûre, responsable et positive des nouvelles technologies de l'information auprès du grand public et, particulièrement, de 3 groupes distincts :

- Assister les enfants et les jeunes dans l'éducation de leur usage avec les nouvelles technologies.
- Soutenir les parents, enseignants et éducateurs en tant que référence / modèles des enfants/jeunes.
- Accompagner les séniors, dont la demande se développe de plus en plus (https://silversurfer.lu/).

DOMAINES D'ACTION :

1. Sensibilisation et information : BEE SECURE diffuse des informations et conseils en matière d'une utilisation responsable d'Internet. Ainsi BEE SECURE organise de manière systématique des formations dans les écoles et les lycées. BEE SECURE publie régulièrement des dossiers d'information sur des sujets d'actualité (dont le cyber mobbing, la désinformation, les cyber risques, les tendances extrémistes, l'apprentissage d'un usage équilibré des outils informatiques...) ainsi que des guides pratiques pour enfants, jeunes et leur entourage. BEE SECURE met ces informations à disposition du grand-public à travers ses sites Internet, les réseaux sociaux et la presse nationale.
2. Orientation et conseil : La BEE SECURE « Helpline » est un point de contact pour les questions relatives à la sûreté en ligne et un usage responsable des nouvelles technologies de la communication. Elle s'adresse au grand public et surtout aux enfants, jeunes, parents, seniors ainsi qu'aux enseignants et éducateurs. La « Helpline » est un service gratuit, avec un traitement des informations anonyme et confidentiel.
3. Signalement de contenus illégaux : A travers la BEE SECURE « Stopline », des contenus illégaux en ligne peuvent être signalés de manière anonyme et confidentielle. Ces signalements peuvent être classés dans l'une des trois catégories : matériel d'abus sexuel de mineurs (« Child sexual abuse matériel/CSAM ») ; discrimination, racisme ou révisionnisme ; respectivement terrorisme. Les signalements sont analysés et, le cas échéant, seront transmis aux autorités compétentes.
4. Veille : L'échange régulier avec les enfants et les jeunes lors des formations, l'analyse des demandes sur la « BEE SECURE Helpline » et la collaboration avec les groupes de discussion « Youth et Kids Panels » permet à BEE SECURE de suivre les tendances de près. L'échange avec différents partenaires nationaux et internationaux permet de compléter le « trend monitoring ». Les résultats du « trend monitoring » seront partagés à travers le BEE SECURE 'RADAR'.

3. MESURES EN MATIÈRE DE PRÉPARATION, D'INTERVENTION ET DE RÉCUPÉRATION

3.1 PRÉSENTATION DU PLAN D'INTERVENTION D'URGENCE CYBER

La situation d'urgence cyber désigne une situation qui découle d'un incident ou d'une attaque risquant d'entraîner un dysfonctionnement majeur, voire une indisponibilité de systèmes de communication et de traitement de l'information qui menace les intérêts vitaux ou les besoins essentiels de tout ou partie du pays ou de la population du Grand-Duché de Luxembourg.

La prise de connaissance d'un incident ou d'une attaque cyber par les organes de gestion de crise se fait en principe soit par l'analyse d'informations disponibles au niveau national, soit par des acheminements internationaux suivants des accords en vigueur.

Dès la prise de connaissance d'un incident cyber, la Cellule d'évaluation du risque cyber (CERC) est alertée et procède à une évaluation des informations disponibles. Si l'incident est de nature à engendrer un impact significatif, le Haut-Commissaire à la protection nationale est alerté et en informe le Premier ministre, ministre d'État, qui décide de l'opportunité d'activer la Cellule de crise.

La Cellule de crise peut déléguer à une cellule opérationnelle notamment l'exécution, la mise en œuvre et le contrôle des mesures et activités ordonnées.

Dans le contexte cyber, les fonctions de Cellule opérationnelle sont en règle générale assumées par la Cellule d'évaluation du risque cyber (CERC).

3.2 PRÉSENTATION DES ACTIVITÉS DES CERTS

Le Luxembourg dispose d'une communauté active de centres d'alerte et de réaction aux attaques informatiques (CERT/CSIRT) publics et privés, qui coopèrent au niveau national et international pour réagir rapidement à des incidents.

Le CERT gouvernemental est intégré au Haut-Commissariat à la protection nationale (Ministère d'Etat) et assure une panoplie de services pour le secteur public et les infrastructures critiques afin d'augmenter davantage la résilience des systèmes informatiques dans sa constituante. Le CERT gouvernemental opère aussi un CERT militaire valorisant les synergies surtout dans le domaine des exercices de cybersécurité et dans les tests de vulnérabilité et d'intrusion.

Le CIRCL (*Computer Incident Response Centre Luxembourg*), CERT pour le secteur privé géré par le Ministère de l'Economie, opère un nombre de services en matière de prévention, de détection et de mitigation de la menace, notamment la plateforme de partage d'informations sur les malware (MISP).

CIRCL agit comme un centre de partage d'informations sur les cyber-menaces pour divers secteurs, en fournissant les outils, le leadership communautaire, les meilleures pratiques, les normes d'échange ainsi que des données pour un large éventail de communautés, plaçant le Luxembourg dans une position centrale pour ce partage d'informations sur les menaces à l'échelle mondiale. En outre, le CIRCL agit également en tant qu'hôte de confiance pour plusieurs communautés de partage d'informations de premier plan, en offrant l'hébergement et la gestion de hubs centraux dédiés ainsi que des opportunités de soutien et de formation pour ces communautés.

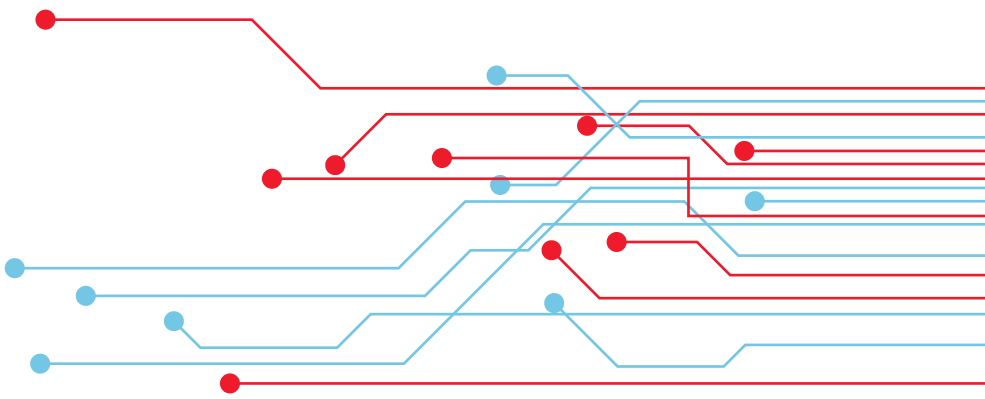
3.3 LE « SCRUBBING CENTRE »

En 2018, le Luxembourg a créé un partenariat public-privé ambitieux pour la mise en place d'un centre pour la protection contre les attaques sophistiquées de déni de service distribué (DDoS). Ce partenariat public-privé assure une détection avancée d'incidents DDoS et permet de filtrer des requêtes non légitimes afin d'assurer la continuité des services informatiques et l'accessibilité et la fiabilité des données en cas d'attaque.

3.4 EXERCICES EN MATIÈRE DE CYBERSÉCURITÉ

Le Luxembourg participe aux exercices à large échelle organisés par ses partenaires multilatéraux, notamment au niveau de l'Union européenne (CyberEurope) et de l'OTAN (Locked Shields et Cyber Coalition).

Une plateforme Cyber Range sera introduite pour conduire des exercices nationaux et internationaux et pour compléter le programme de formation cyber en développant un centre de formation avancé.



3.5 COOPÉRATION INTERNATIONALE ET CYBERDIPLOMATIE

Sur le plan de la diplomatie et des relations internationales, le Luxembourg est un défenseur de longue date de la méthode multilatérale et œuvre en faveur d'une coopération internationale positive dans le cadre du droit international et du droit international humanitaire. La coopération internationale dans le domaine normatif permet de discuter et d'approfondir les normes de comportement responsable des états dans le cyberespace, à l'instar des efforts actuellement en cours au niveau des Nations Unies : l'engagement en bonne foi dans ces négociations internationales est l'un des éléments stratégiques en faveur d'une plus grande sécurité collective.

- Au niveau des Nations Unies, le Luxembourg suit notamment les activités qui sont actuellement en cours à l'Assemblée générale, au sein de deux organes mis en place en 2019 : d'une part, par une participation active aux travaux du Groupe de travail à composition non limitée sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale, d'autre part en suivant les travaux du Groupe d'experts gouvernementaux sur la promotion du comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale.

- L'Union européenne est l'organisation d'intégration régionale la plus avancée au monde : le Luxembourg participe aux différents mécanismes de coopération mis en place dans le cadre de la directive (UE) 2016/1148 sur la sécurité des réseaux et des systèmes d'information, ainsi qu'aux enceintes de coopération en matière de formulation des politiques et de gestion des crises.
  - La SNCS IV devra reprendre sur le métier la transposition des obligations européennes au niveau national, notamment en matière de l'utilisation de la boîte à outils diplomatique de l'UE pour répondre aux actes cyber malicieux, ainsi qu'en matière de l'opérationnalisation du plan d'action (« Blueprint ») de l'UE pour les réponses aux cyber-incidents de large ampleur.
  - Le Luxembourg devrait se doter d'une politique nationale et des procédures nécessaires en matière d'attribution de la responsabilité pour un incident cyber.

- L'Organisation pour la sécurité et la coopération en Europe (OSCE) est l'une des organisations régionales les plus avancées en matière de mise en place de mesures de confiance et de coopération cyber.

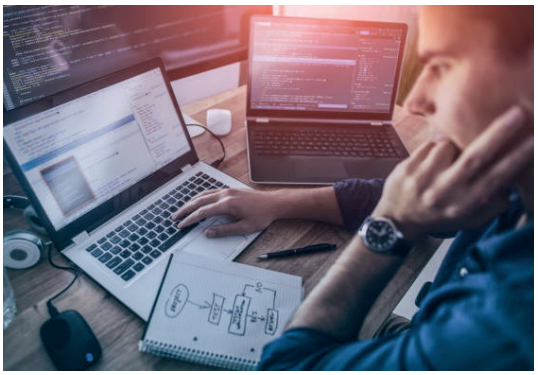
- L'Organisation du Traité de l'Atlantique du Nord (OTAN) a un dispositif sophistiqué en matière de cyberdéfense coopérative.

3.6 ACCORDS DE COOPÉRATION AU NIVEAU BENELUX

- Le HCPN envisage de renforcer la coopération stratégique en matière de gestion de crises cyber et de développement des capacités cybersécurité avec ses homologues du Benelux.

4. PROGRAMMES D'ÉDUCATION, DE FORMATION ET DE SENSIBILISATION

Dans un effort pour disposer d'experts de cybersécurité dans le futur, des cursus de formations doivent être mis à jour et inclure le sujet de la Cybersécurité. Au commencement de l'école secondaire ou même du cycle 4, de premières introductions doivent être faites pour diriger d'entrée les futurs experts dans la bonne direction.



4.1 ÉDUCATION FORMELLE

- Éducation nationale et inclusion dans les curricula nationaux :
  - Cadre général pour l'éducation aux et par les médias : le *Medienkompass* https://www.edumedia.lu/medienkompass/medienkompass/

- BEE-SECURE
  Parmi les objectifs et domaines d'actions de BEE SECURE figure la promotion d'une utilisation plus sûre, responsable et positive des nouvelles technologies de l'information auprès du grand public (enfants, jeunes, parents, enseignants, éducateurs, seniors). Pour cela, BEE SECURE :
  - diffuse des informations et conseils en matière d'une utilisation responsable d'Internet ;
  - organise de manière systématique des formations dans les écoles et les lycées ;
  - publie régulièrement des dossiers d'information sur des sujets d'actualité ainsi que des guides pratiques pour enfants, jeunes et leur entourage.

- BTS (Brevet Technique Supérieur) :
  - BTS « Cloud computing » - http://bts.lu/domaines/services/cloud-computing/
  - BTS « Internet of Things » - http://bts.lu/domaines/services/internet-things/
  - BTS Informatique - http://bts.lu/domaines/services/informatique
  - 2021/2022 : création d'un BTS dans le domaine de la cybersécurité, ayant l'objectif de former des professionnels qui possèdent un profil technique et qui peuvent occuper des postes opérationnels tel qu'opérateur SOC, analyste d'incidents, officier de cybersécurité ou junior « *penetration tester* ».

- Université du Luxembourg :
  - Bachelor in Applied Information Technology (https://wwwen.uni.lu/studies/fstm/bachelor_in_applied_information_technology)
  - Master in Information System Security Management (https://wwwen.uni.lu/studies/fstm/master_in_information_system_security_management)

4.2 FORMATIONS INITIALES ET CONTINUES ; RE-SKILLING ET UPSKILLING

L'essor du marché numérique va de pair avec une forte croissance des besoins en formateurs et en professionnels de la cybersécurité. Les formations et métiers sont généralement encore peu connus ou méconnu par le grand public et les jeunes lors du choix de leurs études. Ils ne sont pas non plus vraiment considérés en tant qu'option lors d'un choix de reconversion pour l'adulte pendant sa vie active. Et pourtant en réalité, la panoplie des métiers cyber est vaste; elle est en continuel changement, dû à la nature évolutive de la société numérique, et les formations et l'accès aux professions sont ouvertes à tout genre.

INAP

- La cyberattaque et la fuite d'information sont une réalité… Comment se préparer? (Room #42)
- Sécurité de l'information - formation pour les directions des administrations
- Sécurité de l'information - formation sur mesure par administration
- Sécurité de l'information – Initiation
  - Ce cours sera prochainement disponible en e-Learning. Il fait partie de la Formation générale de l'État et est suivi par chaque fonctionnaire-stagiaire et chaque employé en service provisoire.
- Formation au signalement d'incidents de sécurité de l'information auprès du CERT gouvernemental
- ECDL Base - L'essentiel sur le Web et la Communication
- ECDL Standard - Collaboration en ligne
- ECDL Standard - Sécurité informatique

HOUSE OF TRAINING

- La House of training (https://www.houseoftraining.lu/) offre un nombre de formations aux entreprises, dont certaines en partenariat avec SECURITYMADEIN.LU :
  - Données personnelles et sécurité de l'information - Enjeux juridiques et nouvelles règles européennes
  - Cybersécurité - Sensibilisation des collaborateurs
  - Cybersécurité et PME - Comment protéger son entreprise
  - Ethical Hacking – Fundamentals
  - Room#42 - Experience and learn to manage cyber incidents
  - Room#42 - Experience and cyber crisis management training

C3

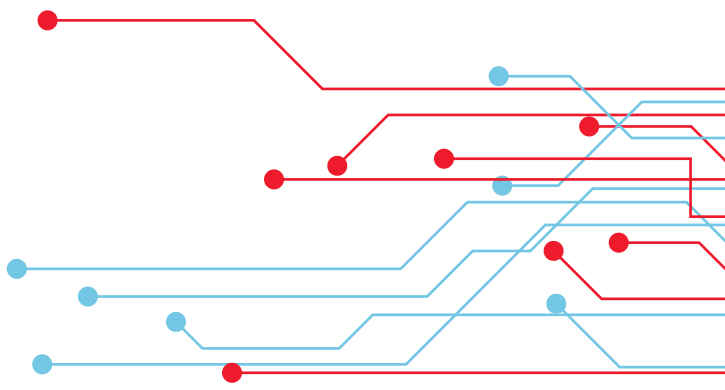
- Le C3 soutient le développement d'un BTS Cybersécurité au Lycée des Arts et Métiers.
- Le C3 renforce le programme de simulation ROOM#42 en en développant une version « plateforme » permettant de former et tester des équipes réparties géographiquement sur plusieurs sites.
- Le C3 accroît l'interactivité des formations de sensibilisation afin d'aider les personnels formés à acquérir des gestes élémentaires d'autoprotection, notamment en matière d'utilisation des plateformes mobiles (téléphone, tablette, véhicule personnel, appareils ménagers) et des réseaux sociaux.

4.3 RE-SKILLING / UPSKILLING

- Cyberwayfinder.com

4.4 ÉDUCATION NON-FORMELLE

- BEE CREATIVE / Maker Spaces
- Hack4kids.lu



4.5 ACTIVITÉS DE SENSIBILISATION :

BEE-SECURE
https://www.bee-secure.lu/fr/

MOIS EUROPÉEN DE LA CYBERSÉCURITÉ

- Le Mois européen de la cybersécurité, ou ECSM, est un événement européen de sensibilisation organisé chaque année en octobre à l'initiative de l'ENISA, l'agence européenne chargée de la sécurité des réseaux et de l'information. Au Luxembourg le point de contact pour ECSM est le ministère de l'Economie ; les évènements ont lieu lors de la 'semaine luxembourgeoise' organisée par l'écosystème de la cybersécurité luxembourgeoise « Cybersecurity Luxembourg » et différents partenaires locaux.

CYBERSECURITY WEEK LUXEMBOURG :
https://www.cybersecurityweek.lu/

- La Cybersecurity Week Luxembourg est une semaine de campagne composée de différents évènements, qui vise à sensibiliser aux menaces de cybersécurité, à promouvoir la cybersécurité auprès des citoyens et des professionnels, et à fournir les dernières informations disponibles dans ce domaine à travers l'éducation et le partage de bonnes pratiques. Au cours de la campagne sont notamment désignés par un jury de pairs les CISO et DPO de l'année.

TRUSTBOX CASES :
https://trustbox.cases.lu

- Fournir les ressources sous forme digitale, comme les formations, les documents, tutoriels et ateliers permets de mieux protéger la vie privée comme la vie professionnelle des différents acteurs. C'est un ajout important dans certaines situations, qui contient des documents, des formations vidéoludiques, des diffusions et cours en ligne, avec le but d'approfondir les connaissances et distribuer le message de la cybersécurité.

PORTAIL DE LA CYBERSÉCURITÉ DE L'ANSSI :
https://cybersecurite.public.lu/fr.html

PORTAIL EXTRANET DE L'ANSSI RÉSERVÉ AUX UTILISATEURS DES SYSTÈMES D'INFORMATION DE L'ÉTAT :
https://anssi.extranet.etat.lu

CAMPAGNES « NATIONALES »

- IoT - une campagne aussi importante que son sujet
  - Dans la dernière stratégie de cybersécurité, la campagne concernant l'internet des objets (IoT) et les bâtiments intelligents (Smart buildings) a été définie et commencée. Cependant, cela reste une campagne importante qui restera active pour une période plus longue au vu du nombre de sujets à aborder. De plus, même si l'ANSSI et CASES ont commencé la campagne, plus d'acteurs vont rejoindre et continuer la sensibilisation pour expliquer une vision plus générale concernant la cybersécurité pour les équipements intelligents.

- Nouvelle campagne de cybersécurité sur la mise au rebut de matériel
  - Même si cette campagne n'est pas aussi large que l'internet des objets (IoT), beaucoup de confusions sont encore faites en ce qui concerne la mise au rebut d'équipements intelligents, et comment effacer correctement les données du stockage avant leur destruction ou leur redistribution et réutilisation. Plusieurs acteurs peuvent rejoindre cette campagne, comme Digital Inclusion, CASES, SuperDrecksKescht, ou d'autres organisations et entreprises de la sécurité de l'information et de destruction pour fournir les connaissances et les bonnes pratiques pour chaque entreprise, pour qu'ils puissent recycler leur équipement sans donner leurs informations à des tiers.

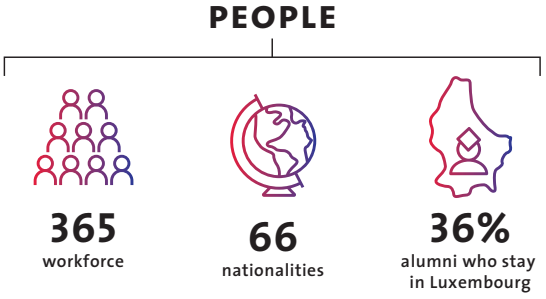
5. PLANS DE RECHERCHE ET DE DÉVELOPPEMENT

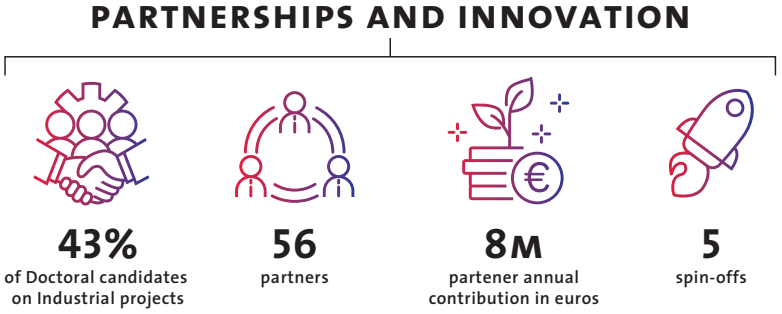
5.1 UNIVERSITÉ DU LUXEMBOURG : INTERDISCIPLINARY CENTRE FOR SECURITY, RELIABILITY AND TRUST (SNT)

Le *Interdisciplinary Centre for Security, Reliability and Trust* (SnT) de l'Université du Luxembourg mène des recherches compétitives à l'échelle internationale dans les technologies de l'information et de la communication (TIC), en mettant l'accent sur la sécurité, la fiabilité et la confiance de ces technologies. Le centre attire des chercheurs talentueux du monde entier pour travailler sur des projets coopératifs avec l'industrie et le secteur public, créant par ce biais un impact socio-économique. Depuis son lancement en 2009, le SnT a établi des partenariats avec plus de 50 organisations.

Les priorités en matière de recherche stratégique du SnT sont : véhicules autonomes, cybersécurité, technologie financière, Internet des objets, gestion de données sécurisée et conforme, systèmes spatiaux et ressources.

CHIFFRES-CLÉS





DOMAINES DE RECHERCHE STRATÉGIQUE

Le SnT a six domaines de recherche définissant son travail. Si la cybersécurité est l'un des domaines cibles du SnT, il s'agit aussi d'un sujet de nature transversale dans les branches les plus pertinentes au Luxembourg.

Technologie financière :
La règlementation devenant toujours plus complexe, les outils des TIC sont nécessaires pour des solutions rentables et conformes à destination des secteurs financier, juridique et de l'assurance. Nos équipes dédiées à la recherche développent des solutions pour assurer la sécurité et la confiance dans ces secteurs.

Systèmes spatiaux :
La révolution des technologies spatiales est à l'origine de nouveaux modèles d'affaires innovants. Notre expertise dans les télécommunications par satellite, les opérations autonomes et les logiciels stratégiques nous positionnent idéalement pour travailler avec les acteurs mettant en place des activités de R&D au Luxembourg.

Véhicules autonomes :
La conduite autonome promet d'être plus efficace que le transport traditionnel, engendrant une nouvelle ère de changement disruptif dans la mobilité. Nous nous concentrons sur la création de solutions d'infrastructure sécurisées et sûres pour cette technologie hautement complexe et dynamique.

Cybersécurité :
La sécurité et la confiance sont les mots-clés associés à la conduite des affaires au Luxembourg, permettant au pays d'édifier une place financière gérant des actifs de plusieurs fois la taille du PIB national. Les infrastructures basées sur le cloud sont l'avenir d'une grande partie de l'économie axée sur les services, offrant flexibilité, évolutivité et abordabilité. Ces systèmes doivent être conçus pour assurer la résilience contre les défaillances et les erreurs humaines ainsi que pour résister aux cyber-attaques. Les infrastructures critiques présentent un défi particulier, permettant aux chercheurs de repousser les limites en matière de sécurité et de résilience. La cybercriminalité et d'autres formes de menaces persistantes ciblées et avancées représentent un risque permanent pour ces systèmes, et le Luxembourg doit être à la pointe de la cybersécurité s'il veut conserver et renforcer sa position sur le plan international.

Internet des objets :
Qu'il soit utilisé pour les maisons intelligentes, les villes ou l'industrie manufacturière, l'IdO offre de formidables opportunités dans la création de services pour améliorer nos vies. Pour en faire une réalité, nous développons des solutions IdO et des analyses de données intelligentes, sécurisées et confidentielles.

Gestion des données sécurisée et conforme :
La nouvelle économie est axée sur les données et les règlementations actuelles en matière de protection des données et de confidentialité créent une opportunité pour le Luxembourg de s'établir dans ce domaine. Nos recherches sur l'évolutivité, la sécurité, l'accessibilité et la conformité pour la gestion et la protection des données sont cruciales pour cette initiative.

PROGRAMMES DE PARTENARIAT

Le SnT est guidé par le principe qu'une recherche scientifique excellente peut relever les défis les plus pressants auxquels la société est confrontée et aider l'industrie à développer des solutions. Cette fondation définit sa structure. Le SnT dispose d'un modèle de partenariat qui permet une recherche collaborative avec des acteurs du secteur privé et du secteur public, relevant les défis correspondants qui reposent sur des données et des systèmes réels. Cette approche crée un écosystème vivant qui alimente le vivier local de talents et soutient l'économie locale.

Dans le domaine de la cybersécurité, le SnT a établi des partenariats avec CREOS, VAIL, Proximus, QRA, le ministère des Affaires étrangères - Direction de la coopération et MEGENO.

Un exemple récent d'un partenariat dans la cybersécurité est le *Luxembourg/West Africa Lab for Higher Education Capacity Building in Cybersecurity* (LuxWAyS). LuxWAyS est un projet ambitieux de coopération dans l'enseignement supérieur entre le Luxembourg et les pays cibles de la coopération luxembourgeoise. LuxWAyS vise à former des experts en cybersécurité (1,5 M € – 10 doctorants sur 5 ans) dans la sous-région de l'Afrique de l'Ouest en collaboration avec l'Université Cheikh Anta Diop de Dakar (UCAD), Sénégal ; l'Université Joseph Ki-Zerbo (UJKZ), Burkina Faso ; et l'Université virtuelle du Burkina Faso (UVBF), Burkina Faso.

GROUPES DE RECHERCHE

Les équipes du SnT travaillent actuellement sur plus de 40 projets touchant à la cybersécurité.

Par ailleurs, le SnT est le seul centre de recherche en Europe à être présent dans trois des quatre réseaux H-2020, mettant en exergue sa réputation dans le domaine (CONCORDIA, Cyber Security for Europe, SPARTA).

Parmi les 15 groupes de recherche du SnT, 5 groupes se concentrent sur la cybersécurité :

CRITICAL AND EXTREME SECURITY AND DEPENDABILITY (CRITIX - SÉCURITÉ ET FIABILITÉ CRITIQUES ET EXTRÊMES)

Prof Marcus Voelp

CritiX poursuit des recherches de pointe dans un domaine problématique qui peut être qualifié d'extreme computing (informatique de l'extrême) – l'informatique et l'ingénierie poussées à l'extrême des propriétés fonctionnelles et non fonctionnelles des systèmes. Sont en particulier étudiés les architectures, les intergiciels, les algorithmes et les protocoles pouvant trouver une applicabilité dans les systèmes et réseaux distribués, qui, par exemple :

- déploient des ensembles de données, des flux et des calculs à très grande échelle, en tenant compte du cloud, du Big Data et du traitement d'événements complexes,
- résistent à des niveaux extrêmes de menaces, comme les menaces persistantes avancées, en tenant compte des infrastructures d'information critiques,
- ont besoin d'avoir une probabilité de défaillance extrêmement basse --- compte tenu des domaines de haute criticité tels que la finance, l'énergie, la mise en réseau (SDN) ou l'aérospatiale et les véhicules autonomes,
- présentent des exigences extrêmes en matière de confidentialité et d'intégrité des données – à l'égard de la cybersanté, de la génomique ou du commerce/de la finance.

La programmation informatique modulaire et distribuée résiliente est une réponse à la nécessité d'un changement de paradigme permettant une approche globale de ces défis extrêmes, à partir des premiers principes : architecture et conception pour faire face simultanément aux défaillances accidentelles et malveillantes ; fournir une protection de manière graduelle et s'adapter automatiquement à une dynamique d'échelle, de gravité et de persistance des menaces, dont certaines peuvent être inconnues à priori. Les paradigmes et techniques émergeant de cette recherche devraient doter les systèmes de la capacité de vaincre une puissance antagoniste extrême, accidentelle ou malveillante (menaces graves et continues) et de maintenir un fonctionnement constant et sans surveillance (de manière systématique et automatique).

CRITIX prévoit de s'attaquer à ce niveau de menace en s'inspirant et en s'appuyant sur des recherches récentes sur des techniques de sécurité et de fiabilité automatiques puissantes et innovantes, telles que la tolérance aux pannes et aux intrusions ou la tolérance aux pannes byzantines (BFT), l'informatique dite de confiance et l'hybridation architecturale, le secret réparti et les calculs multipartis sécuritaires, l'auto-réparation et la diversité ou la sécurité post-compromis. En outre, la recherche s'appuiera sur des techniques de vérification officielles améliorées telles que la démonstration interactive de théorèmes, en vue d'atteindre une très grande dépendance à l'égard des logiciels utilisés derrière les certificats roots-of-trust ou TCB.

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement	Groupe de recherche du SnT
HyLIT	Architectural Support for Intrusion Tolerant Operating-System Kernels	M. Volp	FNR	CritiX
CyberSec4Europe	Cyber Security Network of Competence Centres for Europe	P. Esteves Verissimo	CE	CritiX
ADMORPH	Towards Adaptively Morphing Embedded Systems	M. Volp	CE	CritiX
GenoMask - PoC	Early stage read filtering and masking of genomic information POC	J. Decouchant	FNR	CritiX
IISD	Strategic RTnD Program on Information Infrastructure Security and Dependability	P. Esteves Verissimo	FNR	CritiX
SPARTA	Special projects for advanced research and technology in Europe	P. Esteves Verissimo	CE	CritiX
ByzRT	ByzRT : Intrusion resilient real-time communication and computation in autonomous systems	P. Esteves Verissimo	FNR	CritiX
ThreatAdapt	Adaptive Byzantine Fault and Intrusion Tolerance	P. Esteves Verissimo	FNR	CritiX
CritiX-CARS	Architectural Support for Efficient Domain-Specific Byzantine Fault and Intrusion Tolerance	P. Esteves Verissimo		CritiX

CRYPTOLUX

Prof. Dr. Alex Biryukov

CryptoLUX est un groupe de recherche en cryptologie dirigé par le professeur Alex Biryukov.

La mission du groupe CryptoLUX est de définir, de mener et de diffuser des recherches de pointe en cryptologie (et dans des domaines étroitement liés) et de transmettre les connaissances acquises grâce à la recherche aux étudiants et aux partenaires du secteur. CryptoLUX est l'une des rares équipes dédiées à la recherche universitaire au monde à posséder une expertise dans l'éventail complet de la cryptologie, allant des fondements théoriques aux aspects de la mise en œuvre et aux applications. Leurs missions et objectifs sont élaborés conformément aux trois objectifs principaux de l'Université du Luxembourg, à savoir l'enseignement, la recherche et le transfert de connaissances au plus haut niveau international. Les membres de CryptoLUX collaborent avec les plus éminents groupes de recherche du monde entier et participent aux activités d'ECRYPT, le réseau européen d'excellence en cryptologie (European Network of Excellence in Cryptology). Les projets de recherche actuels couvrent une grande variété de sujets, notamment la conception d'algorithmes (chiffrements par blocs, fonctions de hachage, etc.), la cryptanalyse, la sécurité des communications et l'anonymat, les applications effectives, les attaques par canaux cachés et l'ingénierie inverse.

Les technologies de l'information et de la communication émergentes, telles que le cloud computing (informatique en nuage) ou l'Internet des objets, posent un certain nombre de défis uniques liés à la conception et à la mise en œuvre de primitives cryptographiques, ce qui a permis de lancer un grand nombre de recherches dans ces domaines. Néanmoins, le nombre d'attaques cryptanalytiques (tant les attaques classiques que les attaques par canaux cachés) augmente constamment, et bon nombre de ces attaques ont conduit à des failles de sécurité dévastatrices aux conséquences fatales. CryptoLUX est à l'avant-garde d'une communauté de recherche internationale qui s'intéresse à ces défis et développe des solutions innovantes pour des problèmes de sécurité complexes reposant sur une base cryptographique solide. Pour y parvenir, l'équipe s'efforce de mieux comprendre comment les cryptosystèmes tombent en panne (ou se brisent) dans le monde réel, comment ils peuvent être conçus et mis en œuvre pour mieux résister aux attaques et comment ils devraient être utilisés pour développer des systèmes et des réseaux sécurisés.

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement
FinCrypt	Security, Scalability, and Privacy in Blockchain Applications and Smart Contracts	A. Biryukov	FNR
APLICA	Analysis and Protection of Lightweight Cryptographic Algorithms	A. Biryukov	FNR

APPLIED SECURITY AND INFORMATION ASSURANCE (APSIA)

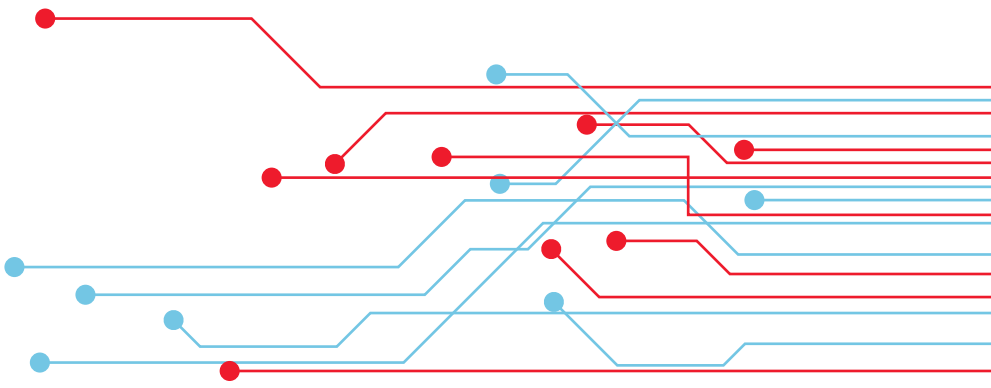
Prof Dr Peter Y.A. Ryan

L'*Applied Security and Information Assurance Group* - APSIA (groupe de sécurité appliquée et d'assurance de l'information) est dirigé par le professeur Peter Y. A. Ryan, professeur de sécurité appliquée.

Le groupe APSIA est spécialisé dans la conception et l'analyse de systèmes sécurisés :

- Protocoles de cryptographie (classique et quantique)
- Algorithmes et primitives cryptographiques
- Flux d'information
- Modalités de vote vérifiables
- Analyse socio-technique de la sécurité
- Technologies améliorant la protection de la vie privée

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement
Q-CoDe	Quantum Communication with Deniability	P. Ryan	FNR
EquiVox	Secure, Quantum-Safe, Practical Voting Technologies	P. Ryan	FNR
FutureTPM	Future Proofing the Connected World : A Quantum-Resistant Trusted Platform Module	P. Ryan	CE
STV	Socio-Technical Verification of Information Security and Trust in Voting Systems	P. Ryan	FNR
SZK	Stateful Zero-Knowledge	A. Rial	FNR
SmartExit	Facilitating optimal containment and exit strategies with minimal disclosure access control and tracking	P. Ryan	FNR
SURCVS	Secure, Usable, Robust Cryptographic Voting Systems	P. Ryan	FNR



SOCIO-TECHNICAL CYBERSECURITY (IRISC - CYBERSÉCURITÉ SOCIO-TECHNIQUE)

Prof Dr Gabriele Lenzini

Le groupe de recherche positionne ses recherches dans le domaine de la *cybersécurité socio-technique*. Aujourd'hui, la sécurisation d'un système nécessite de comprendre non seulement les communications et les protocoles numériques, mais aussi la réalité humaine et juridique dans laquelle le système est déployé.

Les recherches de l'équipe IRiSC identifient ce changement de perspective : l'accent mis sur la conception et l'analyse de systèmes sécurisés prend en compte globalement les cadres technique, social et juridique. Les recherches du groupe portent, mais sans s'y limiter, sur les domaines suivants :

- Cybersécurité centrée sur l'humain
- Sécurité d'utilisation et expérience utilisateur
- Cyberattaques et cyberdéfenses
- Sécurité des informations et des systèmes
- Protection des données et conformité légale
- Éthique et droits de l'homme

Les chercheurs du groupe IRiSC suivent des méthodologies qui incluent des méthodes de calcul officielles, ainsi que des méthodes de recherche quantitatives et qualitatives. Ils ont une formation interdisciplinaire, combinant sécurité de l'information et sciences sociales, sciences physiques ou droit, et participent tous aux recherches de nature interdisciplinaire.

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement
NoCry PoC	No More Cryptographic Ransomware, Proof of Concept	G. Lenzini	FNR
ConGenIAL	CONsent to turn GENome into Individual's Asset for a Lifetime	G. Lenzini	FNR
LEGAFIGHT	Legally Fighting COVID-19 - LEGAFIGHT	E. Poillot	FNR
LeADS - Resubmission 2	Legality Attentive Data Scientists - Resubmission 2	G. Lenzini	CE
SSh	Security in the Shell	J. Lagerwall	FNR

TRUSTWORTHY SOFTWARE ENGINEERING (TRUX - INGÉNIERIE LOGICIELLE FIABLE)

Prof Dr Jacques Klein

TruX est un groupe de recherche spécialisé en génie logiciel et sécurité logicielle qui développe des approches et des outils innovants visant à soutenir les communautés de recherche et de pratique dans l'élaboration de logiciels fiables. Trustworthy Software a atténué les vulnérabilités ; quand il tombe en panne, il peut être réparé automatiquement ; lorsqu'il fonctionne, il peut étayer ses commandes d'exécution.

TruX explore l'immensité des données sur les artefacts de développement logiciel (y compris le code source et les informations textuelles dans les registres, tels que les rapports d'erreurs, les analyses, etc.) pour obtenir des connaissances sur la façon d'automatiser l'analyse, l'élaboration et la réparation des programmes logiciels. En particulier, TruX mène des recherches selon trois axes principaux :

1. Sécurité logicielle : en développant de nouveaux outils et approches pour évaluer et garantir les propriétés de sécurité et de confidentialité des applications logicielles. Parmi les exemples d'activités de recherche figurent la détection de fuites en matière de confidentialité dans les applications Android ou la détection de vulnérabilités dans les logiciels open source au moment de la validation.

2. Réparation logicielle : en concevant et en mettant en œuvre de nouveaux algorithmes, méthodologies et support d'outils pour la réparation automatique des programmes. Cela s'effectue en identifiant les emplacements de bug ou de vulnérabilité et en appliquant des opérations de changement de code qui permettront aux programmes de répondre aux critères d'exactitude. Au sein de TruX, les chercheurs s'attachent particulièrement à inventer des solutions de réparation logicielle en adéquation avec les contraintes des spécialistes.

3. Logiciels explicables : en veillant à ce que les solutions d'ingénierie logicielle aux problèmes commerciaux ne soient pas des solutions dites « black-box », mais véhiculent plutôt des explications et des informations contextuelles pour aider les utilisateurs finaux. Cette orientation de la recherche va de pair avec une exigence émergente dans le domaine de l'intelligence artificielle où les modèles et les techniques doivent être conçus de sorte que les résultats d'une solution d'IA puissent être compris par des experts humains. Compte tenu de l'utilisation d'algorithmes d'IA dans plusieurs de leurs axes de recherche, les chercheurs TruX étudient également des pistes pour rendre les analyses traitables.

Outils pour les spécialistes : TruX vise à développer des solutions de recherche à la fois pratiques et fondamentales. « Pratique », car TruX cible directement les professionnels ayant l'ambition de lancer des outils pertinents pour les développeurs. « Fondamental », car TruX étudie les principaux problèmes d'ingénierie logicielle ouverte et matérielle tels que la définition de la similarité de code (p. ex. les techniques d'apprentissage de représentation pour l'identification d'un clone de code sémantique), la dérivation d'opérateurs de réparation abstraits qui sont moins enclins à tester le surapprentissage, etc.

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement
CHARACTERIZE	Characterization of Malicious Code in Mobile Apps : Towards Accurate and Explainable Malware Detection	J. Klein	FNR
CatchMe	Android Malicious code Localisation : Catch Me if You can !	J. Klein	FNR
HitDroid	Hinting at Malicious Code in Android Apps Identifying Malicious Payloads in Malware at Market Scale with Graph and Data Clustering Techniques	J. Klein	UL
LuxWAys	Luxembourg/West Africa Lab for Higher Education Capacity Building in Cyber Security and Emerging Topics in ICT4Dev	T.F.D.A. Bissyande	

D'autres équipes mènent également des projets de recherche dans le domaine de la cybersécurité et la liste figurant ci-dessous donne un aperçu de ces projets :

Acronyme du projet	Nom du projet	Chercheur principal	Organisme de financement
CLOUDMAP	Cloud Computing via Homomorphic Encryption and Multilinear Maps	J. Coron	CE
SWITECH	Secure Software using Whitebox Technology - resubmission	J. Coron	FNR
PrivDA	Privacy-preserving Publication of Dynamic Social Network Data in the Presence of Active Adversaries	Y. Ramirez-Cruz	FNR
PriML	Privacy Attacks and Protection in Machine Learning as a Service	J. Pang	FNR
PandemicGR	Information Diffusion in Twitter during the COVID-19 Pandemic: the Case of the Greater Region	J. Pang	FNR
DGAP	Real time prediction and detection of malicious activities	R. State	FNR
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion	R. State	CE
FIN-TECH	A FINancial supervision and TECHnology compliance training programme	R. State	CE
STARTS	Security Assessment of TrustZone-M enabled Software	A.K. Iannillo	FNR
Incident Management and Sofware testing	Incident Management and Sofware testing	Y. Le Traon	UL
SATOCROSS	Support of Advanced Test cOverage Criteria for RObust and Secure Software	M. Papadakis	FNR
Fb testing and verification	Detecting (flaky) test failures of system user interactive tests	M. Papadakis	Autre organisme de financement
ONNIVA	Automatic Detection and Prevention of Deserialization Vulnerabilities	A. Bartel	FNR
EQUACS	Early Quality Assurance of Critical Systems	M. Sabetzadeh	FNR
FAQAS	Fault-based, Automated Quality Assurance Assessment and Augmentation for Space Software	F. Pastore	ESA
COSMOS	DevOps for Complex Cyber-physical Systems	L. Briand	CE

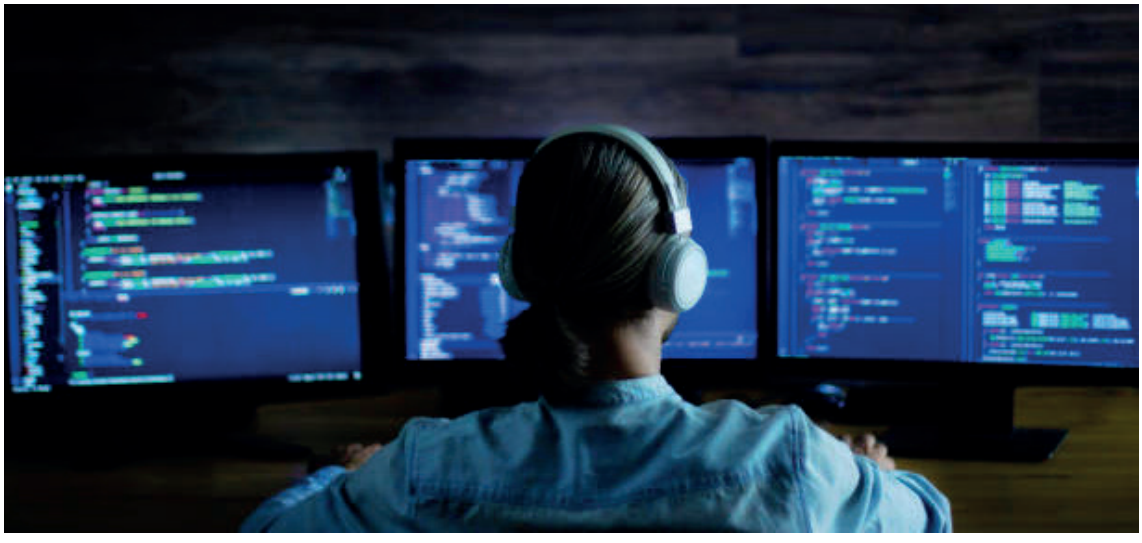
5.2 LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY (LIST)

Le département « IT for Innovative Services » (ITIS) du Luxembourg Institute of Science and Technology (LIST) combine des activités de recherche scientifique et appliquée grâce à la présence de quelque 120 ingénieurs chevronnés et chercheurs hautement qualifiés. Au sein d'ITIS, l'équipe impliquée dans la cybersécurité se concentre sur la confidentialité et la sécurité des données, la sécurité des cybersystèmes et la gestion de la sécurité de l'information. Elle est composée de 10 chercheurs avec une combinaison équilibrée d'ingénieurs, de chercheurs titulaires d'un doctorat ainsi que de collaborateurs travaillant sur leurs projets de thèse.

Sur le plan scientifique, l'équipe se concentre sur la modélisation, la conception et l'analyse de nouveaux algorithmes, protocoles et systèmes pour la cyber-résilience. Les activités de recherche sont principalement soutenues par le financement des programmes FNR CORE / INTER et Horizon 2020 de l'UE.

Du côté appliqué, la recherche se concentre sur les défis pratiques de la cybersécurité, p. ex. l'application et le développement d'outils cryptographiques et de technologies de protection des données personnelles, la conception et la mise en œuvre de technologies blockchain pour résoudre les problèmes de sécurité et de confidentialité, l'assistance aux régulateurs/entités régulées pour appliquer les règlementations nouvelles et multiples (gestion des risques, conformité, analyse de données). Ces activités de recherche sont soutenues par des partenaires privés et publics, FNR CORE/INTER, EU Horizon 2020 et Erasmus+, Connecting Europe Facility (CEF), la loi RDI au niveau national, ainsi que par des collaborations avec des partenaires industriels. De plus, les chercheurs s'engagent dans des formations universitaires, dispensant des cours en cybersécurité au niveau Master (Université du Luxembourg, Université de Lorraine, etc.) ainsi que dans des formations professionnelles.

Les activités de recherche précédemment mentionnées d'ITIS contribuent à l'ensemble de la stratégie nationale de cybersécurité. Cependant, un effort particulier est fourni actuellement à l'égard de la directive n°2 de la stratégie nationale en matière de cybersécurité concernant la protection des infrastructures numériques. Néanmoins, les autres points sont également abordés, conformément aux objectifs tels que la création de nouveaux produits et services, la gestion des risques, la formation, etc.



DOMAINES DE RECHERCHE SÉCURITÉ ET CONFIDENTIALITÉ DES DONNÉES

Le LIST possède une vaste expertise dans les fondements de la sécurité et de la confidentialité des données. Ce savoir-faire comprend des algorithmes et des protocoles cryptographiques ainsi que des technologies standards et émergentes améliorant la protection de la vie privée, illustrés par le contrôle de la divulgation de données statistiques et de la confidentialité différentielle. À cette fin, le LIST publie régulièrement de nouveaux résultats scientifiques lors de conférences et dans des revues. De par sa nature de RTO (*Research and Technology Organisation*), le LIST a utilisé ces connaissances dans des domaines d'application pratiques, notamment dans :

- la conception de protocoles d'authentification et de gestion efficaces des clés cryptographiques spécifiques pour les dispositifs IoT (Internet des Objets),
- la fiabilité des solutions d'apprentissage automatique en privilégiant les aspects axés sur les données (par exemple, la pollution des données et les exemples contradictoires),
- et les problèmes de sécurité et de confidentialité pour les écosystèmes de la 5G avec un accent sur la sécurité des interfaces de programmes d'application (API).

En outre, le LIST travaille également sur les aspects de sécurité et de confidentialité des technologies en matière de registre distribué (Distributed Ledger Technologies ou DLT) et des solutions blockchain, ainsi que sur les applications de ces technologies dans des domaines tels que le transport des marchandises dangereuses, les assurances ou le logement.

Les travaux menés par le LIST ont permis :

- d'évaluer les problèmes de sécurité et de confidentialité (et plus généralement la fiabilité) des systèmes TIC existants,
- d'améliorer les systèmes actuels avec de nouveaux algorithmes (p. ex. chiffrement homomorphe), protocoles (p. ex. apprentissage automatique préservant la vie privée) et processus (p. ex. comment la recherche des contacts est effectuée),
- de mettre en application les nouvelles technologies telles que l'apprentissage automatique et la DLT/blockchain à de nouveaux scénarios d'application de manière transparente et responsable,
- de déposer un brevet (LU100580 - 12/2017) sur une solution dédiée à la protection et à la valorisation des profils des internautes.

SÉCURITÉ ET RÉSILIENCE DU SYSTÈME CYBERNÉTIQUE

La recherche effectuée dans le cadre de cette thématique est double. D'une part, les activités sont centrées sur une sensibilisation totale à la cybersécurité. Le LIST travaille sur une approche de modélisation des services, des organisations et des infrastructures pour permettre le partage des connaissances liées à la sécurité, l'intégration et une meilleure résilience des infrastructures critiques et de leurs services-clés associés. Cette approche repose sur les résultats de la gestion de la sécurité de l'information pour permettre la prévention, la détection, la réaction et l'atténuation des incidents en temps réel. Cela permet d'accroître la résilience face aux menaces de cybersécurité et aux évènements en cascade potentiels, tout en garantissant un alignement continu vis-à-vis des exigences de cybersécurité et en alimentant de manière ultime les analyses des risques de sécurité de l'information. Cette approche repose sur le développement d'artefacts technologiques distribués, l'exploitation massive de données et l'utilisation de technologies d'intelligence artificielle pour la protection de la cybersécurité en temps réel.

D'autre part, le LIST travaille sur des infrastructures intelligentes avec leurs dispositifs IoT (Internet des Objets : IdO) qui sont intégrés dans un concept d'informatique en périphérie, géodistribuée et en nuage, pour lesquelles

une garantie élevée de résilience contre divers types d'attaques est primordiale. En ce sens, le LIST identifie et précise les composants clés, leurs fonctions et services, en tant qu'éléments d'un cadre d'orchestration qui sont nécessaires pour garantir des niveaux de sécurité prédéfinis, et qui prennent en compte la configuration hétérogène des infrastructures IdO) potentielles. En outre, un nouveau mécanisme cryptographique qui mettra en œuvre le concept du respect de la vie privée dès la conception dans le domaine des infrastructures intelligentes et des réseaux IdO est évalué et proposé. Les technologies blockchain / DLT sont considérées comme le fondement potentiel d'infrastructures résilientes qui ciblent les applications distribuées dans un environnement de partenaires qui ne sont pas nécessairement entièrement fiables. Nous étudions les cas d'utilisation qui pourraient bénéficier le plus des propriétés fondamentales des technologies blockchain / DLT et tentons de créer des solutions résilientes sur la base des derniers cadres existants.

Les travaux menés par le LIST ont permis de :

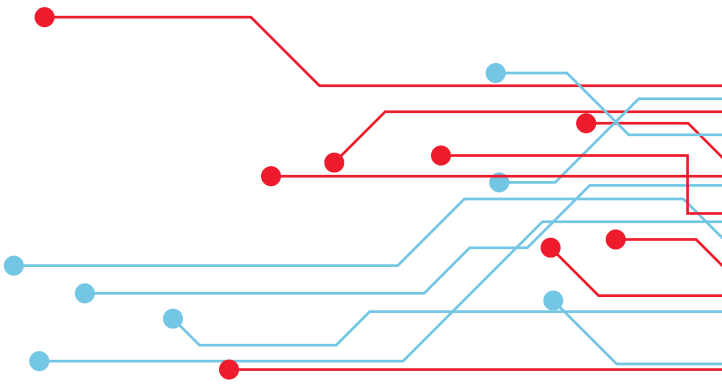
- développer une méthodologie basée sur les risques pour la surveillance de la sécurité en temps réel des services interdépendants dans les infrastructures critiques,
- développer une architecture distribuée permettant la prévention, la détection, la réaction et l'atténuation des incidents en temps réel de manière continue pour les infrastructures critiques,
- mettre en application de nouvelles technologies telles que la DLT/la blockchain pour créer des infrastructures résilientes à destination de certains cas d'utilisation.

Directement en lien avec les travaux sur la résilience, le LIST travaille sur un cadre de gestion des risques de sécurité couvrant l'ensemble du cycle règlementaire, de l'évaluation au traitement des risques de sécurité par les entités régulées à la collecte et à l'analyse des données relatives aux risques par le régulateur. L'objectif est d'adopter un cadre permettant d'intégrer les spécificités de la gestion des risques issues des différentes règlementations et de les traiter de manière intégrée. Ce cadre a été mis en œuvre dans la plateforme technologique intitulée SERIMA qui englobe des modules de gestion des risques, de notification des incidents et d'analyse des données. Ces travaux ont permis une amélioration de la qualité des résultats de la gestion des risques et la réduction des coûts liés à la conformité. Une gouvernance sectorielle et systémique de la cybersécurité fait aussi partie des principaux avantages de cette approche.

Un accent particulier sera mis au cours des deux prochaines années sur l'extension des modèles et des meilleures pratiques à l'émergence de la 5G et à la publication du Code des communications électroniques européen (CCEE). En 2021, la plateforme règlementaire accueillera une centaine d'entreprises issues de tous les secteurs. Une feuille de route pour l'amélioration des méthodologies et des fonctionnalités sera également développée au cours des trois prochaines années en collaboration avec un partenaire industriel, les régulateurs (l'ILR au Luxembourg, l'IBPT en Belgique) et les entreprises concernées.

Les travaux menés par le LIST ont permis d'élaborer :

- un ensemble de modèles standard d'analyse des risques,
- une plateforme de régulation permettant à toutes les entreprises des secteurs concernés de gérer leurs risques, de signaler leurs risques au régulateur et de notifier les incidents,
- des capacités d'analyse des données au niveau sectoriel et national pour les régulateurs.



PROJETS ET PARTENAIRES

PROJETS :

PROJETS DE L'UE

- **SPARTA (H2020)** : Développement d'une méthodologie permettant la prévention, la détection, la réaction et l'atténuation des incidents liés aux infrastructures critiques en temps réel, ainsi que des panoplies d'outils et des cadres étayant la conception, le développement et la vérification de systèmes distribués à grande échelle et critiques pour la sécurité formant une infrastructure intelligente.

- **TOKEN (H2020)** : Fournir des ressources pour l'introduction de technologies disruptives (à savoir la DLT et la blockchain) qui contribuent à accélérer la transformation des services publics vers un modèle de gouvernement ouvert basé sur les principes de collaboration, de transparence et de participation.

- **NISDUC (CEF)** : Développement d'un panel d'activités visant à accroître la sensibilisation, les compétences et les capacités des acteurs de la directive NIS (autorités compétentes, opérateurs de services essentiels et fournisseurs de services numériques) en collaboration avec SECURITYMADEIN.LU, l'ILR et l'IBPT.

- **Housing+ (Erasmus+)** : Améliorer la formation universitaire dans le domaine du logement et de l'immobilier auprès des professionnels, des parties prenantes, des décideurs politiques et des chercheurs grâce à des documents de formation dotés d'un contenu interdisciplinaire, international et axé sur les nouvelles technologies (p. ex. DLT et blockchain), de vidéos et d'une gamification (ludification).

FNR :

- **DECEPTICON** : Développer des procédures et des outils pour aider diverses parties prenantes à évaluer la présence d'interfaces truquées dans les services en ligne.

- **CATALYST** : Financement d'une thèse dédiée à la conception de protocoles d'échange de clés et d'authentification efficaces pour les dispositifs IdO et conception de protocoles d'analyse des données IdO préservant la confidentialité des données échangées.

- **5G INSIGHT** : Concevoir de nouveaux mécanismes de sécurité allant de la détection d'attaques à l'atténuation des attaques en tirant parti d'outils et de paradigmes novateurs tels que ceux basés sur l'apprentissage automatique (ML), en particulier l'apprentissage fédéré et profond, jusqu'aux blockchains et à la technologie de la tromperie (deception security), tout en prenant en compte le cas spécifique mais très sensible (en termes de sécurité) des zones transfrontalières (frontière franco-luxembourgeoise).

- **REGTECH4ILR** : Développement d'un cadre de gestion des risques de sécurité, composé d'une partie dédiée aux autorités de régulation et d'une autre pour les entités régulées.

PROJETS COLLABORATIFS :

- **DG-SEC (DoD)** : Développement d'un système basé sur la technologie blockchain pour appuyer l'autorisation et améliorer la sécurité dans le déroulement du transport de déchets dangereux à travers l'Europe.

- **NIS Collaboration (ILR)** : Travail sur l'évolution et l'adaptation du cadre de gestion des risques de sécurité pour inclure les secteurs de la loi du 28 mai 2019 transposant la directive NIS et prendre en compte les risques systémiques dans et entre les secteurs.

PROJET DE LOI RDI :

- **POST 5G Secure Experience** : Développer une plate-forme de sécurité de télécommunications 5G (un système complet de détection d'intrusion télécom) sur trois ans pour protéger le réseau POST et ses utilisateurs des exploitations au niveau de l'infrastructure contre les attaques télécoms telles que l'usurpation de SMS, l'interception d'appels et de SMS, la détection d'intrusion.

SERVICES ET FORMATIONS :

- **Conseil sur la Blockchain pour INFRACHAIN** incluant la mise en place d'un nœud de l'infrastructure EBSI (European Blockchain Service Infrastructure) pour le Luxembourg.
- **Formations professionnelles sur la sécurité dans le cadre du Professional Master conjointement organisé avec Uni.lu.**

PROJETS FINANCÉS EN INTERNE :

- **Thèse de doctorat sur la blockchain dans le transport des marchandises dangereuses.**

PARTENAIRES :

PARTIES PRENANTES :

- **Écosystème de régulation** (régulateurs, entités régulées et fournisseurs de RegTech)
- **Organisations TIC**

PARTENAIRES DE COOPÉRATION (AU NIVEAU NATIONAL) :

- **Autorités** (Ministère des Affaires étrangères et européennes - Défense, CIRCL)
- **Régulateurs** (ILR au Luxembourg et IBPT en Belgique)
- **Milieu universitaire** [Uni.lu (Master en Management de la Sécurité des Systèmes d'Information, supervision de doctorats), SnT]
- **Fournisseurs de technologie** (Westpole, RoamsysNext, Post, Compellio)
- **Initiatives/Associations/Réseaux** (Infrachain, Luxembourg Blockchain Lab, CLUSIL, SDAM alliance)

PARTENAIRES DE COOPÉRATION (AU NIVEAU INTERNATIONAL) :

- **Consortiums H2020** à travers l'Europe
- **Milieu universitaire** [Université de Vienne et AIT, TNO (Pays-Bas), SUTD (Singapour), Université Paris-Saclay (France)]

III. EVALUATION ET EXPÉRIENCES DE LA SNCS II

La troisième Stratégie nationale de cybersécurité (SNCS III) était structurée suivant trois lignes directrices et son plan d'action énumérait 61 actions concrètes, qui ont pour la grande majorité pu être mises en œuvre. Voici une sélection de résultats :

1ÈRE LIGNE DIRECTRICE : RENFORCEMENT DE LA CONFIANCE PUBLIQUE DANS L'ENVIRONNEMENT NUMÉRIQUE

- Pour renforcer la confiance publique dans l'environnement numérique, la SNCS III a mis l'accent sur la collecte et le partage des informations pertinentes dans le domaine de la cybersécurité.

- Du côté de la collecte des informations sur les incidents et le paysage de la menace, les CSIRT nationaux ont coopéré au sein du réseau national CERT.LU. Ceci a permis de rassembler et de partager les informations en relation avec les incidents au niveau national et de les partager dans les constituantes respectives.

- Plusieurs volets d'activités au niveau internationale (FIRST.org, TF-CSIRT, CiviCERT, OASIS Open, IETF, NIS CSIRT network, Europol) ont été poursuivis avec un focus sur les questions techniques et pratiques du partage d'information, la réponse aux incidents et l'automatisation des processus pertinents.

- Les problématiques de la cybercriminalité et les campagnes de désinformations furent adressées dans des groupes de travail pluridisciplinaires, mis en place de manière ad-hoc et en fonction de l'actualité et de la coopération internationale, notamment au sein de l'Union européenne. La sécurisation des élections européennes ou encore la riposte aux tendances extrémistes sur les réseaux sociaux sont deux exemples de coopérations. Les organismes qui ont contribué à l'atteinte des objectifs sous cette ligne directrice sont principalement le Ministère d'Etat, le Service national de la Jeunesse, le Ministère de l'Education nationale, le Ministère de l'Economie, Security Made in Luxembourg, le Kanner- a Jugendtelefon, le Ministère de la Famille, BEE SECURE, le GOVCERT, le Haut-Commissariat à la Protection nationale, le Ministère des Affaires européennes et étrangères, la Police et le Parquet.

2ÈME LIGNE DIRECTRICE : PROTECTION DES INFRASTRUCTURES NUMÉRIQUES

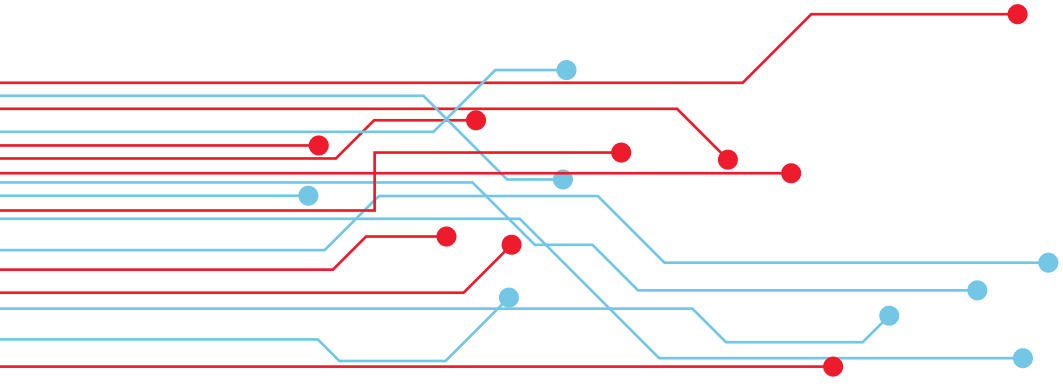
- Avec la transposition de la directive sur les réseaux et systèmes d'information (NIS) et le recensement des infrastructures critiques par le HCPN, une nouvelle fondation pour le renforcement de la résilience de l'infrastructure numérique de l'État fut établie sous la SNCS III. Sur le terrain, l'un des résultats concrets a été la mise en œuvre du centre de filtrage contre les attaques de déni de service distribuées (DDoS) permet de mitiger de telles attaques à des volumétries élevées. Ainsi, une protection supplémentaire pour les infrastructures numériques et une augmentation de la résilience du secteur des ICT au niveau national a été réalisée.

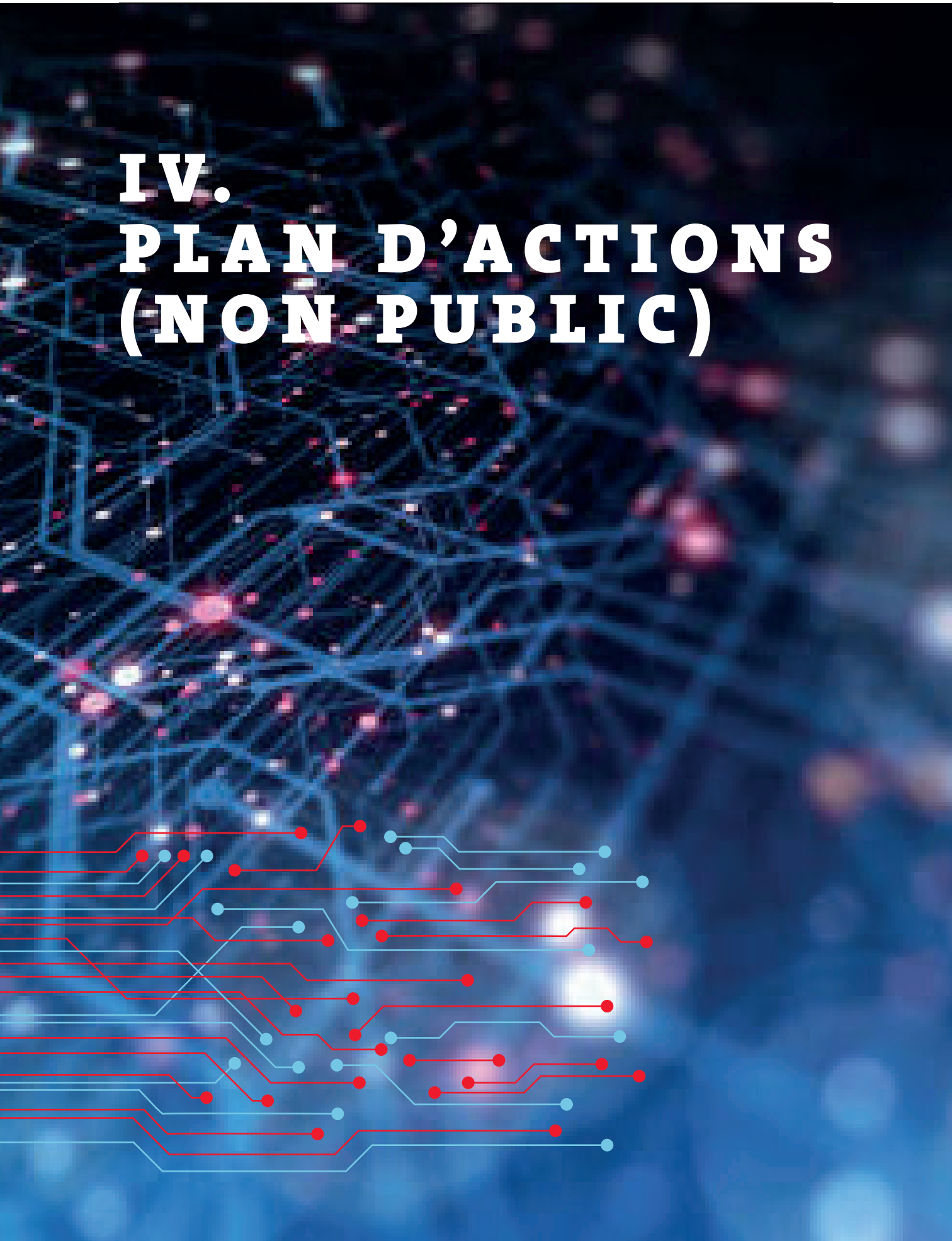
- Dans le contexte de l'affinement de nos procédures de la gestion de crise cyber les acteurs concernés ont participé aux principaux exercices cyber internationaux organisés par l'Union européenne et l'OTAN.

3ÈME LIGNE DIRECTRICE : PROMOTION DE LA PLACE ÉCONOMIQUE

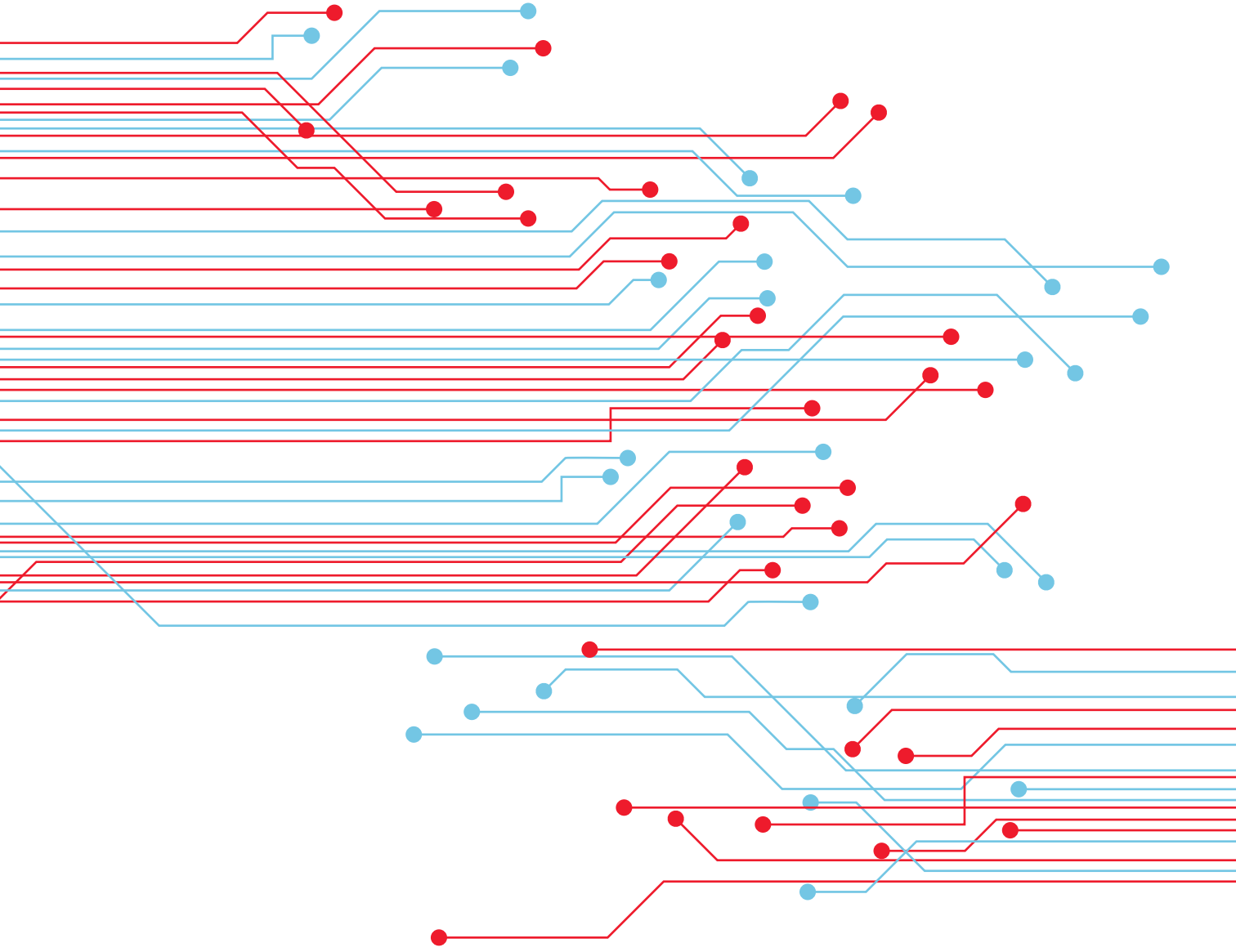
- Le Ministère de l'Economie a préparé en 2018 une stratégie de « data-driven economy » (approuvée par le Gouvernement en conseil du 26 avril 2019). Une analyse juridique a été réalisée par rapport aux travaux légistiques qui doivent encore être réalisés. Depuis lors, le ministère a lancé les travaux par rapport à la mise en place d'un tiers de confiance dans le domaine de la pseudonymisation et de l'anonymisation. Ces travaux sont coordonnés avec la mise en place du High Performance Computing Competence Centre européen (EuroHPC). Une coopération avec la Commission nationale de protection des données (CNPD) a été entamée pour mettre à disposition au Luxembourg un code de conduite RGPD pour la pseudonymisation et l'anonymisation.

- Une nouvelle version de la plateforme MONARC a été élaborée et comporte dorénavant aussi la possibilité de lier l'analyse des risques à des référentiels d'exigences et de créer automatiquement des SOA (statement of applicability), tels que prévus dans la norme ISO/IEC 27001.





IV. PLAN D'ACTIONS (NON PUBLIC)



GLOSSAIRE

ANSSI

« Agence nationale de la sécurité des systèmes d'information » : *autorité nationale en matière de sécurité des systèmes d'information classifiés et non classifiés et exploités par l'État. L'ANSSI a pour principales missions de définir la politique générale de sécurité de l'information de l'État, de définir, en concertation avec les acteurs concernés, les politiques et lignes directrices de sécurité de l'information pour les domaines spécifiques, de définir l'approche de gestion des risques et de promouvoir la sécurité de l'information par le biais de mesures de sensibilisation. La fonction d'Agence nationale de la sécurité des systèmes d'information est assurée par le Haut-Commissariat à la protection nationale.*

CASES

« Cyberworld Awareness & Security Enhancement Services » : *département de SECURITYMADEIN.LU*

CERC

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

CERT

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

CIRCL

« Computer Incident Response Center Luxembourg » : *département de SECURITYMADEIN.LU*

CNPD

« Commission nationale pour la protection des données »

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 »

FIRST
« Forum of Incident Response and Security Teams »

GOVCERT
« CERT gouvernemental » : *a pour principales missions de constituer le point de contact unique dédié au traitement des incidents de sécurité d'envergure affectant les réseaux et les systèmes d'information des administrations et services de l'État, d'assurer un service de veille, de détection, d'alerte et de réaction aux attaques informatiques et aux incidents de sécurité d'envergure ainsi que d'assurer les fonctions de centre national de traitement des urgences informatiques (CERT national) et de centre militaire de traitement des urgences informatiques (CERT militaire). Le CERT gouvernemental est soumis à l'autorité du Haut-Commissariat à la protection nationale.*

HCPN
« Haut-Commissariat à la protection nationale »

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 »

MOSP
« MONARC Objects Sharing Platform »

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

PIU
« Plan d'intervention d'urgence »

RGPD
« Règlement général sur la protection des données personnelles »

SECURITYMADEIN.LU
« Security Made in Lëtzebuerg » *g.i.e. est l'Agence de Cybersécurité pour les Communes et l'Économie luxembourgeoise. Le groupement exerce sa mission publique au bénéfice du secteur privé, des communes et des entités non gouvernementales du Luxembourg, couvrant les domaines suivants :*
- *détection et réaction aux attaques « cyber » (CRICL) ;*
- *gouvernance et gestion des risques (CASES) ;*
- *renforcement des compétences et capacités (C3) ;*
- *fédération et promotion de l'écosystème (CYBERSECURITY Luxembourg).*

SMC
« Service des médias, des communications et du numérique »

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