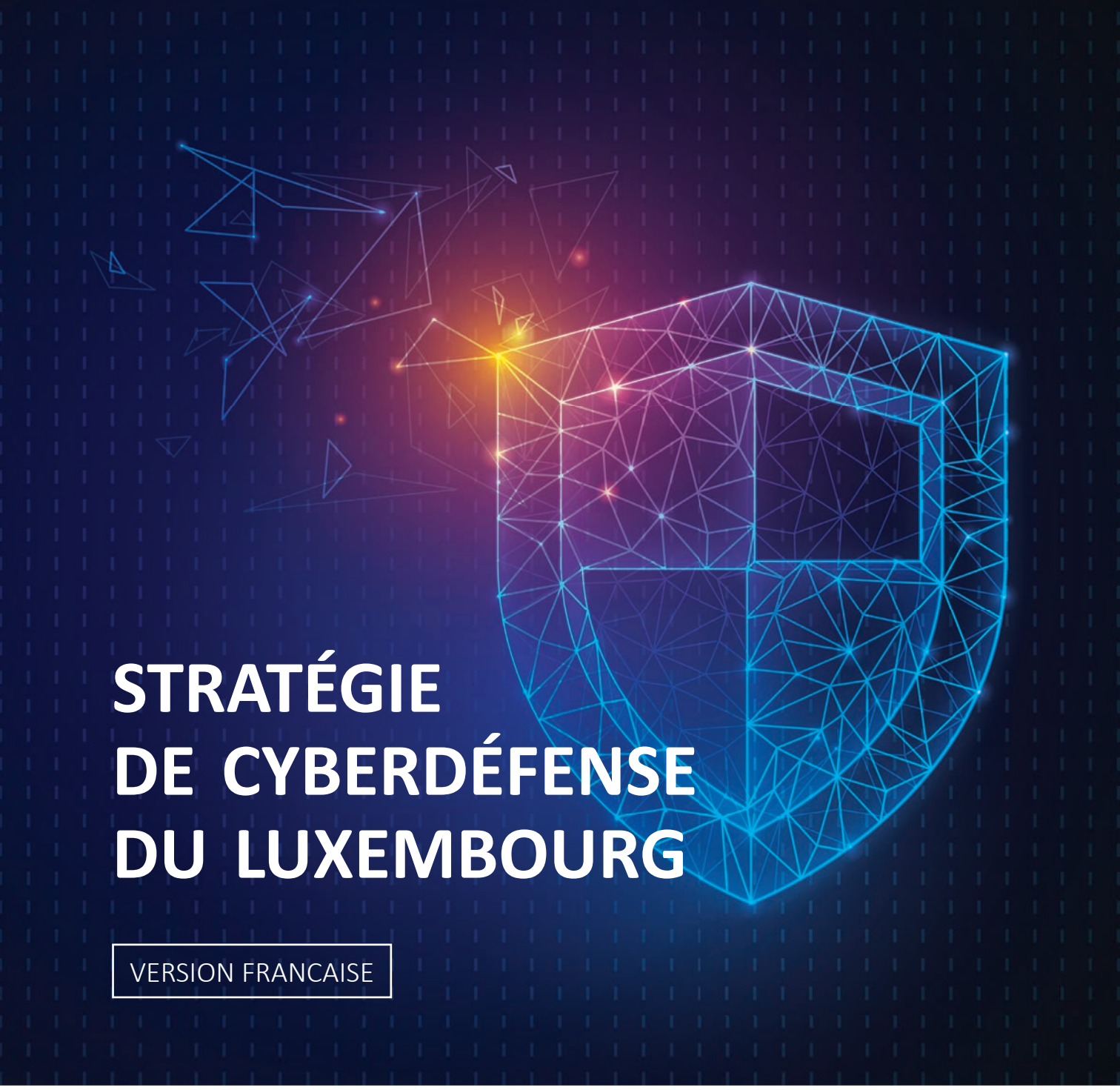


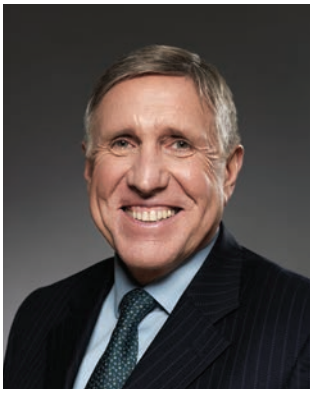
STRATÉGIE DE CYBERDÉFENSE DU LUXEMBOURG

VERSION FRANCAISE

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes

Direction de la Défense

PRÉFACE MINISTÉRIEL



SIP / Yves Kortum

Le Luxembourg a connu de nombreuses années de paix, de prospérité et de progrès grâce à la stabilité de l'ordre mondial. La numérisation et les nouvelles technologies ont donné au Luxembourg et au reste du monde de grandes possibilités de développement et de progrès, mais ont également accru notre exposition à des facteurs qui affaiblissent nos valeurs démocratiques, notre mode de vie et la stabilité de l'ordre international fondé sur des règles. Nous sommes confrontés à de nouveaux défis en raison d'activités constantes et omniprésentes en dessous du seuil de conflit qui exigent une vision plus large de la politique de sécurité et de défense, englobant les changements environnementaux mondiaux et les menaces hybrides.

C'est donc avec grand plaisir que je présente la première stratégie de cyberdéfense du Luxembourg. Cette stratégie à long terme d'une durée de 10 ans s'inscrit dans le cadre de la Stratégie nationale en matière de cybersécurité et vise à renforcer la résilience de la Défense luxembourgeoise en protégeant ses moyens et ses capacités contre les activités cybernétiques malveillantes. La stratégie est la base du développement de capacités de cyberdéfense pouvant être utilisées dans un contexte national et international. Une révision périodique confère à cette stratégie à long terme une flexibilité et une adaptabilité suffisante dans un domaine en constante évolution.

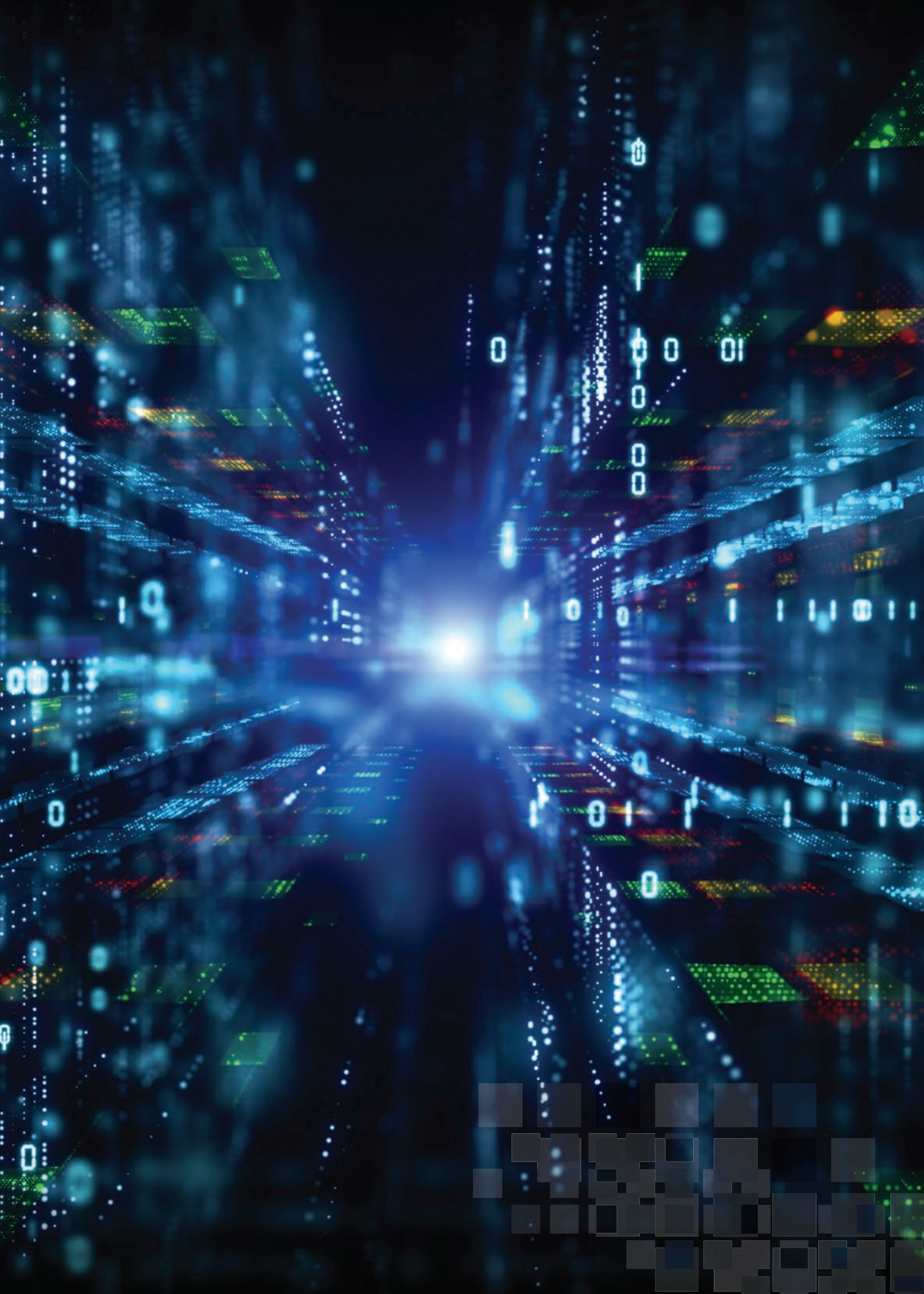
Le Luxembourg a pris des engagements concrets en vue de renforcer la défense européenne, y compris la cyberdéfense au sein de l'Union européenne (UE) et de l'Organisation du traité de l'Atlantique nord (OTAN). Le Luxembourg respectera ces engagements et a défini sa contribution à la défense commune en fonction de ses propres intérêts et objectifs. L'accent sera mis sur l'amélioration des compétences de notre personnel, sur le renforcement de la résilience nationale dans le cyberespace, sur le soutien des capacités du secteur privé et sur le renforcement de notre engagement avec nos Alliés et nos partenaires. Cela garantira une approche durablement financée vers l'intégration de la cyberdéfense dans l'ensemble de la Défense luxembourgeoise et créera les conditions permettant au Luxembourg de développer une expertise et des capacités qui pourront également être offertes aux Alliés et aux partenaires.

En tant que Ministre de la Défense, je suis déterminé à voir cette stratégie pleinement mise en œuvre. Je travaillerai en étroite collaboration avec mes collègues du Gouvernement, du secteur public au sens large et du monde universitaire pour faire en sorte que cette ambition se concrétise.

François BAUSCH

Vice-Premier Ministre et Ministre de la Défense, de la Mobilité et des Travaux publics

SOMMAIRE



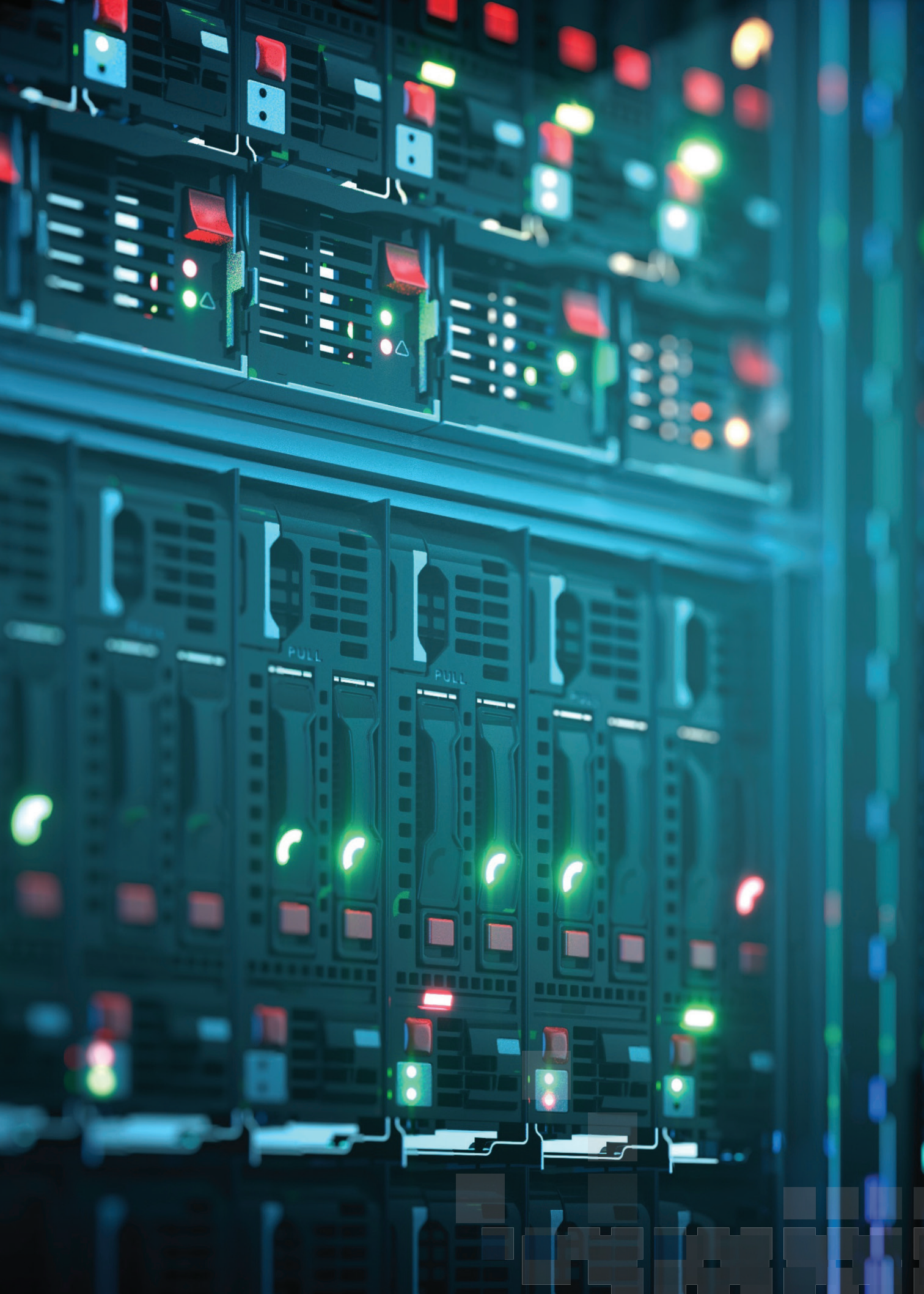
1 INTRODUCTION

Les lignes directrices de défense du Luxembourg pour 2025 et au-delà soulignent que les menaces pour les intérêts vitaux du Luxembourg ne s'arrêtent pas à la frontière physique. Le cyberespace est vital pour la sécurité du Luxembourg et essentiel pour le bon fonctionnement et pour la résilience de la dynamique du pays, son économie fondée sur l'expertise propre au Luxembourg, ouverte sur le monde. La résilience englobe toute la gamme des mesures nécessaires pour garantir que les institutions et les services publics continuent de fonctionner en toutes circonstances et pour que les populations et infrastructures critiques soient protégées. Ce vaste concept de résilience s'étend naturellement au domaine du cyberespace.

Les lignes directrices de la Défense soulignent le développement continu de l'expertise et des capacités en matière de cyberdéfense afin de renforcer la cybersécurité de la Défense luxembourgeoise et la sécurité du personnel militaire, notamment lors des déploiements. Une stratégie nationale de cyberdéfense étaiera le volet "défense" des stratégies nationales de cybersécurité actuelles et futures. L'objectif à long terme de cette stratégie est que le Luxembourg dispose d'une des défenses les plus sûres de l'OTAN et de l'UE en matière de cyberdéfense, et qu'il développe une expertise et des capacités qui pourront être offertes aux Alliés et aux partenaires. La stratégie se concentre sur quatre objectifs stratégiques qui seront revus périodiquement afin de faire preuve de suffisamment de souplesse et d'adaptabilité dans un environnement en rapide évolution.

La Défense luxembourgeoise est chargée de veiller au respect des engagements et des politiques de cyberdéfense définis par l'UE et l'OTAN. Au niveau national, la Direction de la défense fait partie du Comité interministériel de coordination pour la prévention et la cybersécurité et contribue ainsi à la stratégie nationale de cybersécurité tout en veillant conjointement à la cohérence et à la coordination des initiatives ultérieures. Cette stratégie inaugurale de cyberdéfense permettra à la Défense luxembourgeoise de faire mûrir ses capacités, de contribuer davantage aux initiatives nationales de cybersécurité et de renforcer la résilience des infrastructures nationales.

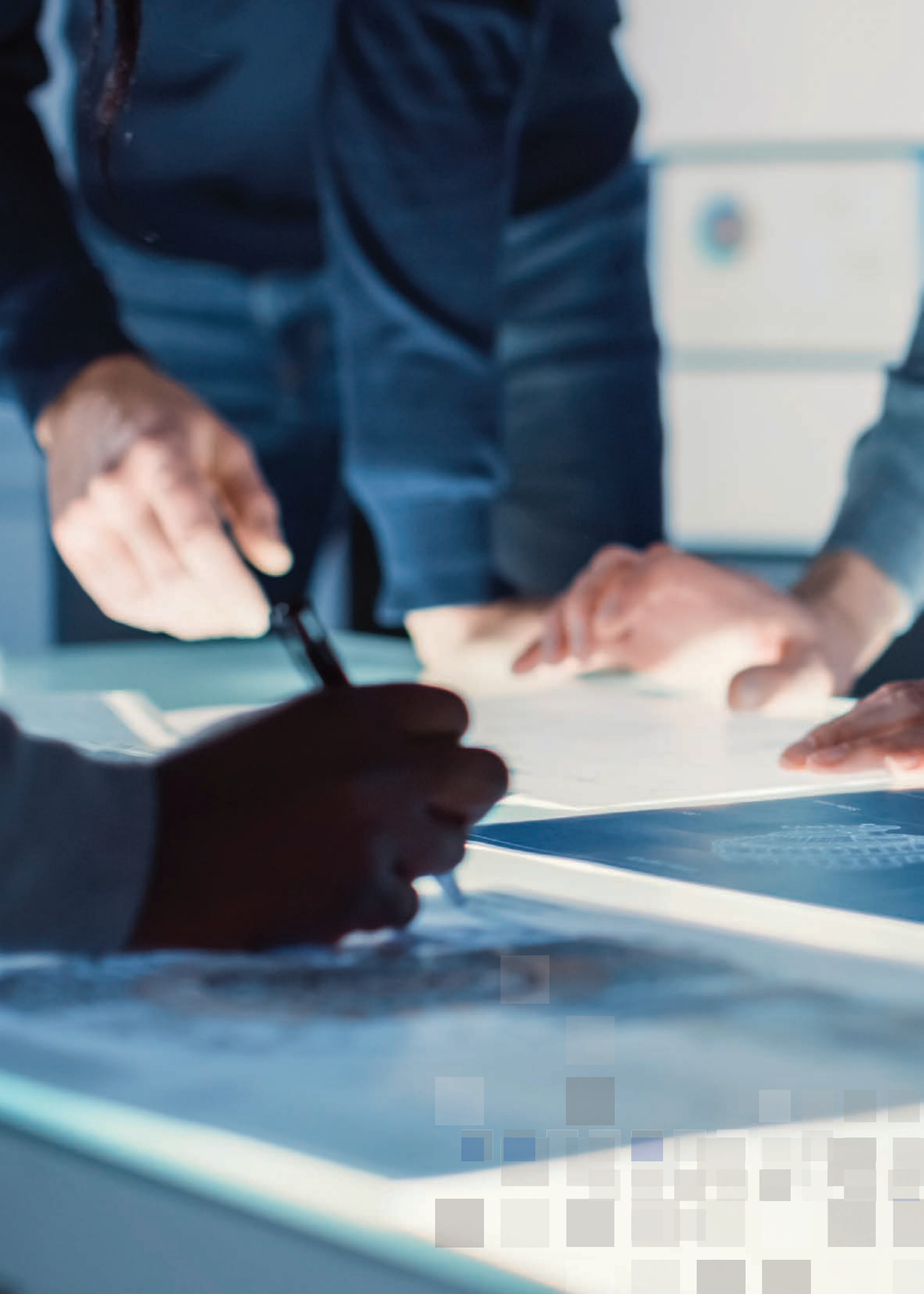
La cyberdéfense n'est pas un concept nouveau, l'OTAN ayant déjà publié sa première politique de cyberdéfense en 2008 et l'UE ayant publié son premier cadre politique de cyberdéfense en 2014. La cyberdéfense n'est pas non plus une nouveauté au Luxembourg, où des mesures ont déjà été prises pour sécuriser les ressources du pays. Pour continuer à affirmer les intérêts du Luxembourg, à faire entendre sa voix et à bénéficier de la sécurité collective assurée notamment par l'OTAN, cette stratégie intègre les engagements du Luxembourg envers les organisations internationales, en veillant à ce que le Luxembourg assume sa part de responsabilité dans les efforts et les risques inhérents à la défense collective et commune, et soit reconnu comme un partenaire apportant des contributions pertinentes.


PULL
PULL

2 OBJECTIF À LONG TERME DU LUXEMBOURG EN MATIÈRE DE CYBERDÉFENSE

D'ici 2030, le Luxembourg disposera d'une des Défenses les plus sûres de l'OTAN/UE, grâce à la maximisation de ses capacités de cyberdéfense.

En développant des capacités de cyberdéfense et en contribuant à la résilience du cyberespace national, la Défense luxembourgeoise vise à devenir un partenaire fiable pour les organisations internationales telles que l'OTAN et l'UE, ainsi qu'un point de référence pour les acteurs nationaux concernés dans le domaine du cyberespace. En investissant dans les ressources humaines, la technologie, ainsi que dans la recherche et le développement, le Luxembourg développera une expertise et des capacités qui pourront également être offertes aux Alliés et aux partenaires.



3 OBJECTIFS STRATÉGIQUES

La cyberdéfense du Luxembourg est jeune et a besoin de mûrir. Elle doit se faire une place dans les forces armées du Luxembourg et dans le paysage de la cybersécurité luxembourgeoise tout en développant des capacités de base de la cyberdéfense. Les objectifs stratégiques (OS) pour la mise en œuvre de cette stratégie couvrent donc un large éventail de facteurs :

- **OS1 Une main-d'œuvre qualifiée et motivée**
- **OS2 Une forte coopération nationale et internationale dans le domaine cyber**
- **OS3 Cyberdéfense intégrée dans l'ensemble des activités, des actifs et de la culture de la Défense luxembourgeoise**
- **OS4 Un paysage "CyberFutures" cartographié, priorités identifiées et programmes de recherche enclenchés**

L'objectif est de **développer les bonnes capacités, de les gouverner et de les utiliser de manière appropriée, d'intégrer la cyberdéfense dans la Défense luxembourgeoise et d'établir la cyberdéfense luxembourgeoise comme un partenaire de renom tant au niveau international que national.**

La réalisation des objectifs stratégiques dépend de la mise en œuvre de différentes capacités. Les sections suivantes définissent ces objectifs stratégiques et les capacités sous-jacentes.

3.1 OBJECTIF STRATÉGIQUE 1 – Une main-d'œuvre qualifiée et motivée

La première condition préalable à l'objectif à long terme est de disposer d'une main-d'œuvre instruite dans le domaine cyber, qualifiée et motivée. La main-d'œuvre existante à la Défense luxembourgeoise sera plus compétente et de nouveaux talents en matière de cyber seront attirés en augmentant la visibilité de la cyberdéfense luxembourgeoise. En outre, la Défense luxembourgeoise contribuera à renforcer les compétences nationales en matière de cyberdéfense afin d'accroître la résilience du cyberespace national dans les secteurs privé et public.

CAPACITÉ 1 : Personnel de défense bien informe et expérimenté

La Défense luxembourgeoise établira et promouvra une formation interne en matière de cybersécurité et sensibilisera à l'importance d'intégrer la cybersécurité dans les processus existants. La Défense luxembourgeoise enverra du personnel pour participer à des exercices et des formations nationaux et internationaux sur la cybersécurité. Les aspects cybernétiques seront intégrés dans les exercices militaires et pris en compte dans les opérations.

CAPACITÉ 2 : Perception publique positive accrue de la cyberdéfense luxembourgeoise, y compris en tant qu'employeur

Grâce à une présence aux conférences nationales sur la cybersécurité et aux salons de l'emploi, à la promotion des initiatives luxembourgeoises en matière de la cyberdéfense via les médias sociaux et la diplomatie publique et à la coopération avec le secteur de l'éducation luxembourgeois, la perception de la Défense luxembourgeoise en tant qu'employeur sera améliorée.

CAPACITÉ 3 : Mise en place et renforcement des principaux organes de cyberdéfense

La cyberdéfense est un domaine en pleine expansion et nécessite le renforcement des capacités des structures existantes et nouvelles. Les ressources humaines seront augmentées, des capacités MilCERT dévouées seront mises en place et la Défense luxembourgeoise est en faveur à la création d'une cyber-réserve nationale, en soutenant sa mise en place.

CAPACITÉ 4 : Renforcement des compétences nationales non militaires/non liées à la défense en matière de cyberdéfense

La cyberdéfense fait partie intégrante de la posture de la Défense luxembourgeoise qui fournira des formations et des exercices pour le personnel concerné, par exemple en utilisant la plate-forme Cyber Range du Luxembourg.

3.2 OBJECTIF STRATÉGIQUE 2 – Une cybercoopération nationale et internationale forte

Étant donné que le cyberespace n'a pas de frontière, le Luxembourg s'efforcera, au niveau national et international, de faire respecter l'ordre international fondé sur des règles, de remplir les engagements pris, entre autres, sous les auspices de l'OTAN et de l'UE.

CAPACITÉ 1 :
Identification des besoins et capacités mutuels et des facteurs favorables

La Défense luxembourgeoise entreprendra des missions d'enquête et commandera des études comparatives régulières, ainsi qu'un catalogage des capacités de l'industrie de la cyberdéfense luxembourgeoise afin d'identifier les besoins futurs. Ce travail aidera également les entreprises luxembourgeoises à accéder au marché international de la cyberdéfense.

CAPACITÉ 2 :
Échange continu d'expertise et de ressources

La Défense luxembourgeoise va promouvoir l'expertise luxembourgeoise et l'échange de bonnes pratiques en construisant des réseaux nationaux et internationaux, en devenant membre du Centre d'excellence pour la cyberdéfense en coopération de l'OTAN (NATO CCD COE) et en participant à d'autres activités pertinentes, comme des exercices internationaux. Le Luxembourg participera également au partage international de renseignements sur les menaces afin d'améliorer la connaissance de la situation avec et entre les Alliés et partenaires de l'OTAN et les États membres de l'UE.

CAPACITÉ 3 :
Renforcement de la coopération avec les acteurs nationaux

La Défense luxembourgeoise continuera à participer au Comité interministériel de coordination en matière de cyberprévention et de cybersécurité, à renforcer la collaboration avec les acteurs nationaux et à prendre part à des projets nationaux liés à la cybersécurité.

3.3 Objectif stratégique 3 – Cyberdéfense intégrée dans l'ensemble des activités, des moyens et de la culture de la défense luxembourgeoise

La numérisation des sociétés modernes a offert de grandes possibilités, mais a également accru l'exposition aux risques, et la Défense ne fait pas exception à la règle. La sensibilisation et la prise en compte du cyber dans les activités, les ressources et au niveau culturel de la Défense luxembourgeoise seront généralisées. La résilience de la Défense et des forces armées luxembourgeoises dans le cyberespace en particulier sera accrue, tant au niveau national que dans les opérations.

CAPACITÉ 1 :

La cybersécurité ancrée dans la culture organisationnelle

La Défense luxembourgeoise mettra en œuvre les meilleures pratiques et lignes directrices de l'industrie et des organisations internationales pour intégrer la cybersécurité dans la culture organisationnelle. La Défense luxembourgeoise introduira également une identité visuelle de cyberdéfense.

CAPACITÉ 2 :

Gouvernance, mise en œuvre et exécution

Grâce à un cadre de gouvernance, de mise en œuvre et d'évaluation, la Défense luxembourgeoise assurera l'intégration des meilleures pratiques en matière de cybersécurité par la mise en œuvre d'un Système de Management de la Sécurité de l'Information. En outre, la Défense luxembourgeoise mettra en œuvre des projets tels que le Cyber Range, des exercices d'entraînement et contribuera aux opérations dans le cyberespace. L'Armée luxembourgeoise cherchera en permanence à améliorer la résilience du cyberespace, de son personnel, de ses infrastructures, de ses capacités et de ses systèmes.

3.4 OBJECTIF STRATÉGIQUE 4 – Cartographie du paysage des "cyberfutures", identification des priorités et programmes de recherche en cours

La Défense luxembourgeoise dressera une carte des défis émergents et futurs afin d'identifier les menaces et de tirer le meilleur parti des développements technologiques pour améliorer la cyberdéfense. Cela devrait particulièrement profiter aux forces Armées luxembourgeoises dans leur rôle opérationnel.

CAPACITÉ 1 : Cartographie continue des défis et opportunités futurs, définition des priorités en matière de recherche, de développement et de technologie (moyen terme)

Une analyse prospective régulière sera entreprise afin d'identifier les défis et les opportunités qui influenceront probablement la position du Luxembourg en matière de cybersécurité et de cyberdéfense dans les années à venir. Les résultats de cet exercice récurrent permettront d'identifier les "CyberFutures" les plus pertinents pour la Défense luxembourgeoise.

CAPACITÉ 2 : Alignement des moyens et des capacités de cyberdéfense (court terme)

Grâce à ces résultats de l'analyse prospective ("CyberFutures"), la Défense luxembourgeoise alignera ses ressources et ses capacités sur les défis à venir. Étant donné que la plupart des innovations de pointe ont lieu dans le secteur privé, l'expertise et le potentiel appropriés du Luxembourg seront utilisés pour contribuer aux programmes de développement et d'acquisition requis.

Des revues régulières auront lieu afin de s'assurer que les "CyberFutures" précédemment identifiés sont toujours pertinents pour la Défense luxembourgeoise.

CAPACITÉ 3 : Intégration du cyber dans la R&D de défense luxembourgeoise

Les résultats pertinents de l'analyse prospective du cyberdomaine seront priorisés pour orienter la recherche soutenue au niveau national.

4 SUIVI ET ÉVALUATION

4.1 Activités et programmes

Les activités et les programmes sous-jacents aux objectifs stratégiques et capacités feront l'objet d'une revue annuelle en fonction d'indicateurs de performance clés (KPI) convenus au préalable qui pourront alors mener à un ajustement des KPI, du contenu ou des objectifs.

4.2 Objectifs stratégiques et capacités

À la lumière de la revue et de l'ajustement des activités et programmes sous-jacents, les objectifs stratégiques et les capacités seront réexaminés périodiquement.

GLOSSAIRE ET DÉFINITIONS

SIC	Systèmes d'Information et de Communication
CyberFutures	Défis et opportunités émergents et futurs en matière de cyberdéfense pouvant intéresser la Défense luxembourgeoise
UE	Union européenne
Défense luxembourgeoise	L'Armée luxembourgeoise et la Direction de la défense du Ministère des Affaires étrangères et européennes
Cyberdéfense luxembourgeoise	Les entités responsables de la cyberdéfense au sein des forces Armées luxembourgeoises et la Direction de la défense du Ministère des Affaires étrangères et européennes
KPI	Indicateur de performance clé
MilCERT	Équipe militaire d'intervention en cas d'urgence informatique (CERT)
OTAN	Organisation du traité de l'Atlantique nord
R&D	Recherche et développement
OS	Objectif stratégique

Cyberdéfense[1]	Moyens mis en place pour mener à bien et exécuter des mesures défensives contre des cybermenaces et en atténuer les effets et, ainsi, préserver et restaurer la sécurité des systèmes d'information et de communication ou autres systèmes électroniques, ou encore des données stockées, traitées ou transmises à l'aide de ces systèmes.
Cybersécurité[1]	Application de mesures de sécurité destinées à protéger les systèmes d'information et de communication et autres systèmes électroniques, ainsi que les données stockées, traitées ou transmises à l'aide de ces systèmes, eu égard aux critères de confidentialité, d'intégrité, de disponibilité, d'authentification et de non-répudiation. Selon les publications de l'OTAN "Technical and Implementation Directive for CIS Security" (page 1-7) et "Allied Joint Doctrine for Cyberspace Operations" (page 4), une équivalence des termes sécurité CIS (Communication and Information System) et cybersécurité a été établie. C'est pourquoi la présente stratégie utilise le terme de cybersécurité qui englobe également la sécurité du CIS.
Résilience du cyberespace [1]	La capacité technique et procédurale globale des systèmes, des organisations et des opérations à résister aux incidents cyber et, lorsqu'un dommage est causé, à s'en remettre sans impact ou avec un impact acceptable sur l'assurance ou la continuité de la mission.
Cyber opération[2]	Ensemble d'actions menées dans ou via le cyberespace dans le but de préserver la liberté d'action de ses propres forces ou des forces amies dans le cyberespace ou de créer des effets permettant d'atteindre les objectifs militaires.

1 Définition de l'OTAN selon AAP-06 (2019)

2 Définition de l'OTAN selon l'AJP 3.20

ENGLISH VERSION ▶

https://gd.lu/6Bn6xL