Chambre des Députés
GRAND-DUCHÉ DE LUXEMBOURG

Dossier consolidé

Date de création : 25-10-2024

Projet de loi 8167

Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

Date de dépôt : 02-03-2023
Date de l'avis du Conseil d'État : 31-03-2023
Auteur(s) : Monsieur François Bausch, Ministre de la Défense

Le document « 8167_6_Proces_verbal » n'a pu être ajouté au dossier consolidé.
Le document « 8167_7_Proces_verbal » n'a pu être ajouté au dossier consolidé.

Liste des documents

Date	Description	Nom du document	Page
02-03-2023	Déposé	8167/00	3
06-03-2023	Commission de la Sécurité intérieure et de la Défense Procès verbal (20) de la reunion du 6 mars 2023	20	20
31-03-2023	Avis du Conseil d'État (31.3.2023)	8167/01	41
11-05-2023	Commission de la Sécurité intérieure et de la Défense Procès verbal (25) de la reunion du 11 mai 2023	25	44
11-05-2023	Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile Procès verbal (33) de la reunion du 11 mai 2023	33	74
26-06-2023	Rapport de commission(s) : Commission de la Sécurité intérieure et de la Défense Rapporteur(s) : Madame Stéphanie Empain	8167/02	104
27-06-2023	Premier vote constitutionnel (Vote Positif) En séance publique n°54 Une demande de dispense du second vote a été introduite	Texte voté - projet de loi N°8167	109
27-06-2023	Premier vote constitutionnel (Vote Positif) En séance publique n°54 Une demande de dispense du second vote a été introduite	Bulletin de vote n°6 - Projet de loi N°8167	111
04-07-2023	Dispense du second vote constitutionnel par le Conseil d'Etat (04-07-2023) Evacué par dispense du second vote (04-07-2023)	8167/03	114
20-07-2023	Publié au Mémorial A n°427 en page 1	Mémorial A N° 427 de 2023	117
	Résumé du dossier	Résumé	119

8167/00

N° 8167

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

* * *

Document de dépôt

Dépôt: le 2.3.2023

*

ARRETE GRAND-DUCAL DE DEPOT

Nous HENRI, Grand-Duc de Luxembourg, Duc de Nassau,

Sur le rapport de Notre Ministre de la Défense et après délibération du Gouvernement en Conseil ;

Arrêtons :

Art. 1er. Notre Ministre de la Défense est autorisé à déposer en Notre nom à la Chambre des Députés le Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes.

Paris, le 13 février 2023

Le Ministre de la Défense,
François BAUSCH

HENRI

*

TABLE DES MATIERES

*

TEXTE DU PROJET DE LOI

Art. 1er. Le Gouvernement est autorisé à acquérir le *Luxembourg Cyber Defence Cloud*, constituée par des environnements cloud spécialisés, ainsi que de composantes et services connexes et à financer ses coûts d'exploitation, de maintenance, d'opération et de gestion.

Art. 2. Les dépenses occasionnées par la présente loi ne peuvent dépasser le montant de 250.360.323 euros, y inclus les frais liés à l'acquisition, l'exploitation, la maintenance, l'opération, la gestion du système et des composantes et services connexes du *Luxembourg Cyber Defence Cloud* à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale. Ce montant ne comprend pas la taxe sur la valeur ajoutée.

Art. 3. Les dépenses occasionnées par l'acquisition, l'exploitation, la maintenance, l'opération et la gestion du *Luxembourg Cyber Defence Cloud* sont liquidées à la charge du Fonds d'équipement militaire.

*

EXPOSE DES MOTIFS

A. Contexte
B. Présentation du projet « *Luxembourg Cyber Defence Cloud* »
C. Evaluation des besoins pour la mise en place d'un service du type « *cloud computing* » dans le domaine de la sécurité et de la défense
D. Financement du projet
E. Procédure d'acquisition

A. Contexte

En février 2021, la Défense a publié la stratégie de cyberdéfense du Luxembourg. Ce document fixe le cadre pour l'évolution de la défense luxembourgeoise dans le domaine de la cyberdéfense.

L'objectif à long-terme de cette stratégie est que le Luxembourg dispose d'une des défenses les plus cybersécurisées de l'OTAN et de l'UE et qu'il développe une expertise et des capacités qui pourront aussi être offertes aux Alliés et aux partenaires.

Le développement de telles capacités de cyberdéfense nécessite une infrastructure informatique évolutive, fiable, performante et sécurisée en termes de confidentialité, intégrité et disponibilité.

En effet, le Luxembourg possède l'un des parcs de centres de données les plus modernes et sécurisés en Europe avec des connexions les plus performantes et à faible temps de latence vers toutes les principales plates-formes Internet européennes.

La progression de la transformation digitale et par conséquence, le besoin croissant en capacités de calculs et de stockage sécurisées dans les années à venir de la Défense et d'autres acteurs étatiques sont à considérer dès aujourd'hui.

En général, la quantité de données numériques générées quotidiennement ne cesse de croître, que ce soit dans le monde civil ou militaire. Le besoin de protéger ces données s'explique du fait que ces données peuvent contenir des informations potentiellement sensibles ce qui les rend précieuses et intéressantes pour des acteurs malveillants.

En tenant compte de la progression de la transformation digitale et du besoin de protéger les informations durant tout leur cycle de vie, il convient de disposer d'un environnement performant, offrant des garanties suffisantes en termes de confidentialité, d'intégrité et de disponibilité ainsi que des capacités de calculs et de stockage facilement ajustables aux besoins évolutifs des bénéficiaires.

L'évolution progressive du Luxembourg vers un pays précurseur dans le domaine de la technologie de l'information ainsi que le développement des talents en cybersécurité sont dépendants de la mise en place des infrastructures et des technologies digitales de pointe.

Dans ce contexte, le présent projet, dénommé « *Luxembourg Cyber Defence Cloud* » (LCDC) consiste à mettre en place des environnements cloud sécurisés, qui permettront le stockage et le traitement de données au profit de bénéficiaires étatiques et de partenaires institutionnels internationaux. Ainsi, ce projet est aligné à la stratégie digitale du Luxembourg et sera un élément clé pour poursuivre la transformation digitale dans le domaine de la Défense. Le LCDC apportera une plus-value à beaucoup d'acteurs, tant au niveau national qu'international, étant donné que ces derniers ne doivent pas opérer eux-mêmes de tels environnements, mais peuvent bénéficier d'une solution sur demande.

De plus, un tel environnement cloud polyvalent et hautement sécurisé aidera non-seulement à répondre aux exigences et engagements pris au niveau international (p.ex. engagement en faveur de la cyberdéfense au niveau de l'OTAN, engagements pris dans le cadre de la coopération structurée permanente au niveau de l'UE), mais pourra aussi servir comme une contribution précieuse pour différents acteurs au niveau de la Défense comme les agences OTAN et UE, ceci notamment en vue de répondre aux défis de la transformation digitale ainsi qu'aux différents objectifs stratégiques comme ceux de la politique de cyberdéfense de l'OTAN et de la stratégie de cybersécurité de l'UE.

B. Présentation du projet « *Luxembourg Cyber Defence Cloud* »

L'informatique en nuage ou le « *cloud computing* » est la fourniture de ressources et services informatiques à la demande via un réseau de serveurs distants. Les ressources informatiques sont gérées par un fournisseur de service de sorte que le bénéficiaire peut faire abstraction de la complexité de gestion de telles ressources informatiques et pourra se concentrer sur les services qu'il veut héberger en bénéficiant des ressources informatiques mises à disposition par le fournisseur. La mise à disposition dynamique des ressources selon les besoins des bénéficiaires, est gérée par des technologies du type *cloud computing*. L'informatique en nuage présente l'avantage de pouvoir traiter les demandes des utilisateurs de manière efficace, sécurisée et flexible. Les services en nouage sont développés par des fournisseurs de solutions cloud comme Microsoft, Amazon, Google ou VMWare.

Ainsi, le projet LCDC consiste à :

- Acquérir, héberger, gérer et maintenir l'infrastructure IT nécessaire pour mettre en œuvre les différents environnements cloud.
- Créer des environnements ségrégés (« *multi-tenancy* ») pour les différents utilisateurs en assurant un taux de disponibilité élevé. Concrètement, cette ségrégation permet que plusieurs bénéficiaires peuvent utiliser la même infrastructure IT pour le stockage et traitement de leurs données en garantissant qu'un bénéficiaire ne puisse accéder aux données d'un autre bénéficiaire.
- Implémenter différents environnements cloud pour les différents niveaux de classification.
- Mettre en place les mesures de sécurité et services nécessaires pour assurer un niveau de cybersécurité élevé afin de pouvoir héberger et permettre aux bénéficiaires de traiter des données sensibles et/ou classifiées. Ceci inclut par exemple l'acquisition, la gestion et la maintenance de l'infrastructure cryptographique nécessaire pour assurer un haut niveau de sécurité des solutions informatiques hébergées et des données stockées dans ces environnements cloud.
- Offrir une plateforme compatible et interopérable avec différentes solutions technologiques provenant de différents fournisseurs. Cette approche dénommée « *multi-cloud* » vise à réduire la dépendance vers un fournisseur (enfermement propriétaire) et d'offrir la possibilité aux bénéficiaires de profiter des différentes fonctionnalités offertes par les différentes solutions cloud existantes.
- Fournir un service durable et évolutif en termes de capacités, performance et évolutions technologiques futures.

Le LCDC qui est envisagé au niveau de la Défense sera conçu pour exploiter des technologies *multi-cloud* privés[1] en offrant des services comme le stockage, le mise en réseau, ou le déploiement de machines virtuelles[2].

Le LCDC fournira une capacité de calcul et de stockage sécurisée et hautement disponible. Les bénéficiaires pourront utiliser le LCDC sous leur propre responsabilité, entre autres, pour héberger des solutions informatiques nécessitant une puissance de calcul et des capacités de stockage évolutives (exemples : solutions informatiques pour l'exécution d'exercices cyber, le traitement d'images satellitaires, la création de dessins et modèles 3D dans le domaine de l'ingénierie numérique, l'analyse d'indicateurs de compromission).

Comme la protection de l'intégrité et de la confidentialité des données hébergées et traitées dans cet environnement cloud est une préoccupation majeure, une attention particulière sera accordée aux aspects de sécurité tels que la résilience et la ségrégation des différents environnements des bénéficiaires. Il est en effet essentiel qu'un bénéficiaire soit empêché d'accéder à l'environnement cloud et par conséquent aux informations et données d'un autre bénéficiaire. Cette ségrégation forte est réalisée via le concept de la *multi-tenancy* qui permet à différents environnements cloud de partager la même infrastructure informatique (mêmes capacités de calculs et de stockage), mais de les garder en même temps suffisamment ségrégés via entres autres des moyens cryptographiques pour garantir qu'un bénéficiaire ne peut pas accéder aux données d'un autre. Par conséquent, une stratégie de gestion des identités et du contrôle d'accès ainsi qu'une gestion des clés cryptographiques et de tous les aspects connexes du cycle de vie de la gestion des clés seront définis et pris en considération dès le début du projet. De plus, des services et mesures de sécurité préventives seront considérés et le cas échéant mises en place pour pouvoir identifier des menaces cyber potentielles.

Le LCDC sera hébergé dans des centres de données sécurisés situés au Luxembourg, avec un standard de protection qui répond aux standards internationaux les plus hautes et conçus pour assurer une haute disponibilité.

Le LCDC sera globalement conçu de manière à :

- être capable de stocker des informations non-classifiées ainsi que des données classifiées ;
- offrir aux bénéficiaires une puissance de calcul et des capacités de stockage pouvant être utilisées par ces derniers entres autres pour l'exploitation de capacités du domaine de la Défense ou de la cybersécurité/cyberdéfense ainsi que pour le traitement de données liées comme par exemple l'hébergement d'environnements d'entrainement utilisés pour la formation continue d'experts cyber ou l'analyse d'indicateurs indiquant une compromission potentielle d'un système informatique.

Une étude sur la faisabilité et la conformité technique a été réalisée afin de pouvoir avoir une garantie que l'environnement cloud pourra recevoir une accréditation pour le traitement et le stockage d'informations classifiées.

Pour chaque bénéficiaire, un accord/arrangement technique sera mis en place. Ces accords incluront entres autres les rôles et responsabilités du bénéficiaire et de la Direction de la Défense, les conditions d'utilisation des environnements mis à disposition et le niveau de disponibilité garanti.

C. Evaluation des besoins pour la mise en place d'un service du type « *cloud computing* » dans le domaine de la sécurité et de la défense

Afin de pouvoir répondre aux engagements pris au niveau national (stratégie de cyberdéfense, stratégie nationale de cybersécurité) et international (engagement en faveur de la cyberdéfense, mécanisme de planification de défense à l'OTAN), la Défense luxembourgeoise est en train de développer certaines capacités dont l'accès à des infrastructures informatiques évolutives, sécurisées et performantes facilite leur exploitation.

De plus, avec la transformation digitale croissante au niveau des Défenses des pays membres de l'OTAN et de l'UE ainsi que des agences OTAN et UE, mais aussi auprès des acteurs étatiques nationaux, il y aura de plus en plus de besoins de ressources informatiques. Avec le LCDC, le Luxembourg

---

1 Un cloud d'entreprise ou privé est accessible uniquement sur un réseau privé.

2 Système informatique virtuel qui apparaît comme étant à la disposition exclusive d'un utilisateur déterminé mais dont les fonctions sont accomplies par un partage des ressources d'un système informatique réel (ISO/IEC 2382 :2015).

disposera d'une capacité qu'elle pourra mettre à disposition à ses Alliés et partenaires nationaux et internationaux pour répondre à ces défis dont l'importance ne cessera de croitre.

Une telle infrastructure du type *cloud computing* aura les avantages suivants :

- Réduction de coûts auprès des bénéficiaires : Le *cloud computing* élimine la nécessité d'investir dans du matériel et des logiciels redondants, et de configurer ainsi que de gérer des centres de données sur site : racks de serveurs, alimentation électrique permanente pour l'alimentation et le refroidissement, experts informatiques pour la gestion et sécurisation de l'infrastructure.
- Évolutivité : ll est possible de mettre à disposition la quantité nécessaire de ressources informatiques, par exemple plus ou moins de puissance de calcul, de capacités de stockage ou de bande passante, selon le besoin actuel.
- Fiabilité : Le *cloud computing* simplifie la sauvegarde des données, la récupération d'urgence et la continuité des activités.
- Productivité : Les équipes informatiques des bénéficiaires n'ont plus besoin de manipuler du matériel et s'occuper de la maintenance de l'infrastructure IT. La gestion ainsi que la maintenance de l'infrastructure IT feront partie des services fournies dans le cadre du LCDC.
- Sécurité : L'infrastructure informatique hébergeant les environnements de *cloud computing* sera installée dans des centres de calculs au Luxembourg, hautement sécurisées et accrédités pour héberger des données classifiées.
- Réduction de l'empreinte écologique : En regroupant les besoins en ressources informatiques des différents bénéficiaires, il sera possible d'éviter la mise en place de multiples infrastructures informatiques et ainsi réduire la consommation totale d'énergie nécessaire pour l'opération de telles infrastructures (électricité pour l'alimentation des équipements IT, énergie pour le refroidissement des salles informatiques, etc.).
- Meilleure utilisation des investissements dans les infrastructures existantes : En se reposant sur les infrastructures existantes des centres de données et de la connectivité.

L'environnement cloud pourra être utilisé pour différents cas d'utilisations ayant besoin de capacités de stockage et/ou de calcul comme par exemple :

- Exploitation de solutions informatiques et stockage de preuves numériques pour mener des investigations numériques légales ;
- Exploitation d'une plateforme du type « *Cyber Threat Intelligence* »[3] ;
- Stockage et/ou traitement d'images satellitaires ;
- Hébergement de capacités de cyberdéfense nationales et internationales ;
- Hébergement de plateformes ayant une utilité internationale et offrant des services pour la gestion de projets multinationaux d'acquisitions et de maintien ;
- Exploitation des plateformes de formation spécialisées (p.ex. : dans le domaine de la cyber sécurité) ;
- Exploitation des futures solutions et outils numériques de la prochaine génération.

Le LCDC sera principalement conçu pour l'hébergement et l'exploitation de solutions et de projets qui :

- contribuent à la résilience du Luxembourg (p.ex. : infrastructures critiques et étatiques) contre des menaces provenant de l'espace cyber, et/ou ;
- contribuent à l'effort de défense au niveau de l'UE, de l'OTAN ou des partenaires/alliés du Luxembourg, et/ou ;
- contribuent aux objectifs stratégiques de la Défense luxembourgeoise.

Le dimensionnement des environnements cloud (volume de stockage, puissance de calcul) pourra être évolutive en elle-même. A travers une surveillance continue des ressources utilisées ainsi que sur

3 « *Cyber Threat Intelligence* » a pour objectif la collecte et l'organisation d'informations liées aux menaces du cyber-espace (cyber-attaques), afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthode utilisée, etc). Cette analyse permet de mieux se défendre et d'anticiper au mieux les différents incidents en permettant une détection aux prémices d'une attaque d'envergure.

base des indications des bénéficiaires sur leur besoin en ressources futures, il sera possible d'adapter le dimensionnement des environnements cloud.

D. Financement du projet

Le projet de loi a pour but d'autoriser un engagement financier de l'Etat luxembourgeois d'un montant total ne pouvant pas dépasser 250.360.323 euros (conditions économiques 2023) sur une période de 12 ans, frais de gestion opérationnelle et marges incluses.

Les coûts du futur contrat d'acquisition de l'infrastructure informatique, ainsi que leurs coûts d'exploitation, de maintenance, d'opération et de gestion, s'échelonneront sur douze années entre 2024 et 2035.

Les dépenses sont à charge du Fonds d'équipement militaire.

Le but principal du présent projet consiste à introduire une nouvelle capacité qui pourra aider le Luxembourg, l'UE, l'OTAN et ses partenaires et alliés à répondre aux différents défis provenant de la transformation numérique.

Dans ce contexte, une certaine retombée économique est à prévoir vu que l'infrastructure IT pour héberger les solutions cloud du LCDC sera hébergée dans des centres de calculs au Luxembourg et que des entreprises luxembourgeoises peuvent participer aux marchés publics concernant l'implémentation et l'opération du LCDC.

De plus, le LCDC permettra de réduire la nécessité d'opérer dans le futur de multiples infrastructures IT pour l'hébergement de différents projets cyber. Le LCDC permettra d'héberger différents projets sur une infrastructure IT partagée.

E. Procédure d'acquisition

Au vu des éléments qui précèdent, la Défense a chargé la « *NATO Support and Procurement Agency* » (NSPA) située à Capellen de réaliser une preuve de concept et une estimation des coûts en vue d'entamer par la suite un projet d'acquisition et de support pour la mise en place et l'opération du LCDC. Cette estimation des coûts a servi de base à l'élaboration de la fiche financière.

Etant donné l'envergure du projet et la complexité de l'infrastructure IT ainsi que de sa gestion, le projet d'acquisition et de support du LCDC est dès lors réalisé de façon étroite avec l'Agence OTAN de soutien et d'acquisition (NSPA) située à Capellen. Par ailleurs, le recours à la NSPA a permis de déterminer le budget nécessaire et a facilité la mise sur pied du projet.

La gestion du projet, l'acquisition et le support étant réalisés par l'intermédiaire de la NSPA, les coûts administratifs pour l'appui de la NSPA sont inclus dans le montant global de ce projet.

Le projet sera réalisé sous l'Association de soutien[4] MACCE[5] (matériels MIDS[6]-ACCS[7]-CCE[8]) de la NSPA dans laquelle le Luxembourg est membre depuis fin 2019.

*

---

4 Une association de soutien (« *Support Partnership* ») de la NSPA est mécanisme de coopération multinationale établi à l'initiative de deux ou plusieurs pays de l'OTAN souhaitant organiser des activités communes de soutien et de services. Les pays participants assurent la gouvernance, tandis que la NSPA développe des capacités et gère les besoins des pays. Le regroupement des besoins permet de réaliser des économies d'échelle, de réduire les coûts et l'empreinte logistique, et le cadre juridique offre un soutien commun et efficace.

5 Anglais : *MACCE SP - MACCE (MIDS-ACCS-CCE Equipment) Support Partnership.*

6 MIDS – *Multifunctional Information Distribution System.*

7 ACCS – *Air Command and Control System.*

8 CCE – *Cryptographic, Communications and Electronic Equipment.*

COMMENTAIRE DES ARTICLES

Ad. Article 1er.

L'article 1er arrête le principe, selon lequel le Gouvernement est autorisé à faire procéder à l'acquisition et à financer les coûts d'exploitation, de maintenance, d'opération et de gestion des environnements cloud spécialisés (différents environnements cloud pour les différents niveaux de classification), dénommés « *Luxembourg Cyber Defence Cloud* », ainsi que ses composantes et services connexes.

L'**acquisition** du *Luxembourg Cyber Defence Cloud*, y inclus des sous-systèmes, comprend également les dépenses occasionnées par la mise en œuvre initiale des environnements cloud, les logiciels et licences diverses, les formations initiales ainsi que les coûts d'entretien prépayés. L'acquisition inclut également les éventuelles modernisations du système ainsi que les mises à niveau des sous-systèmes respectivement des composantes connexes exploitant l'environnement du *Luxembourg Cyber Defence Cloud* pour augmenter par exemple la cyber résilience ou pour proposer des fonctions additionnelles comme la détection et l'analyse de risques cyber pour les utilisateurs.

Les **coûts d'exploitation** et de maintenance comprennent notamment les coûts liés à la maintenance de l'infrastructure informatique y compris les coûts liés aux centres de données et à la maintenance des logiciels nécessaires pour faire opérer et sécuriser les environnements cloud du *Luxembourg Cyber Defence Cloud*.

Les **coûts d'opération** comprennent notamment les services de support de contractants externes, pour la configuration et le support technique ainsi que pour le support et l'opération de services connexes nécessaires pour protéger les environnements cloud contre des attaques cyber malveillants.

Les **coûts de gestion** comprennent les coûts administratifs et les coûts liés au personnel de la « *NATO Support and Procurement Agency* » (NSPA) concernant la gestion de projet et l'assistance technique. La gestion de projet englobe notamment le suivi des procédures de marchés publics, l'évaluation des offres, la mise en place et le suivi des contrats ainsi que les services de support des bénéficiaires.

Le *Luxembourg Cyber Defence Cloud* sera opéré au profit de la Défense luxembourgeoise avec le support de la NSPA pour la gestion des contrats avec les différents contractants externes nécessaires pour l'implémentation et l'opération des environnements cloud. A part la Direction de la Défense et l'Armée luxembourgeoise, le *Luxembourg Cyber Defence Cloud* sera mis à disposition de divers acteurs intéressés étatiques, nationaux (p.ex. Police Grand-Ducale) et internationaux (p.ex. agences OTAN comme la NSPA et partenaires UE/OTAN).

Ad. Article 2.

L'article 2 arrête le montant qui peut être engagé au titre de l'article 1er de la même loi, qui est de 250.360.323 euros. Ce montant comprend les coûts liés à l'acquisition, l'exploitation, la maintenance, l'opération, la gestion et les adaptations et modernisations du *Luxembourg Cyber Defence Cloud*, y inclus pour ses composantes et services connexes. Cet article précise également que les dépenses occasionnées par la présente loi s'entendent hors TVA et à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale.

Le montant est estimé pour une durée de 12 ans à partir de l'entrée en vigueur du présent projet de loi. En moyenne, la durée de vie du matériel IT correspond à 5 ans. Pour les estimations des coûts, un renouvellement du matériel IT après 5 ans a été inclus, ce qui équivaut donc à une durée de vie totale de l'équipement IT de 10 ans. Vu que l'acquisition du matériel IT sera réalisé principalement 2 ans après l'entrée en vigueur du présent projet de loi, une durée totale de 12 ans a été considérée pour les estimations de coûts.

Ne sont pas compris dans la présente loi, les coûts de gestion des environnements mises à disposition aux bénéficiaires, le financement des cas d'utilisation des bénéficiaires, l'interconnexion vers les sites des bénéficiaires ainsi que la connexion internet des bénéficiaires. Ces coûts sont à couvrir par les bénéficiaires eux-mêmes.

Ad. Article 3.

L'article 3 détermine que les frais occasionnés par l'acquisition, l'exploitation, la maintenance, l'opération et la gestion de l'équipement informatique et des logiciels nécessaires pour faire opérer et

sécuriser les environnements cloud du *Luxembourg Cyber Defence Cloud*, sont liquidés à la charge du Fonds d'équipement militaire.

*

FICHE FINANCIERE

1. NATURE ET DUREE DE DEPENSES PROPOSEES :

(art. 79 de la loi du 8 juin 1999 sur le Budget,
la Comptabilité et la Trésorerie de l'Etat)

Durant la phase préliminaire, des études du marché ont été réalisées et les informations nécessaires à l'élaboration des cas d'utilisation ont été collectées.

La fiche financière du présent projet de loi se base sur les estimations de coûts établies par la « *NATO Support and Procurement Agency* » (NSPA) sur base de l'étude du marché et l'élaboration des premiers cas d'utilisation lors de la preuve de concept. Les cas d'utilisation prennent en compte les besoins des bénéficiaires comme par exemple le volume et type de stockage, la puissance de calcul et les configurations spécifiques, nécessaires pour pouvoir opérer leurs logiciels pour le traitement de données.

Les coûts indiqués dans la présente fiche financière sont des estimations HTVA et à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale.

Les coûts ont été répartis sur quatre parties, présentées ci-dessous. Cette répartition a été réalisée sur base des indicateurs identifiés lors des études préliminaires. Une adaptation de la répartition des coûts n'est pas à exclure, sans néanmoins dépasser le volume totale estimé. En effet, l'environnement IT est un environnement à évolution rapide et il faut prévoir une certaine flexibilité dans la répartition des coûts pour pouvoir répondre de façon efficace et efficient à d'éventuelles changements de facteurs externes (p.ex. nouvelles mesures de sécurité à prévoir due à de nouveaux types d'attaques cyber).

Partie 1 : Infrastructure « *Luxembourg Cyber Defence Cloud* » (LCDC) partagé parmi différents cas d'utilisation

La première partie inclut les coûts d'investissement pour la mise en place de l'infrastructure de base du LCDC. Cette infrastructure de base sera utilisée pour l'hébergement des différents cas d'utilisation des bénéficiaires futurs. Différents cas d'utilisations peuvent être couverts, allant d'un simple stockage de données jusqu'à l'exploitation d'un environnement d'entraînement d'experts de cybersécurité.

Estimations totales pour la partie 1 :

Coûts d'acquisition :	72.337.511 EUR
Coûts d'exploitation et de maintenance :	33.807.423 EUR
Coûts d'opération :	14.190.793 EUR
Coûts de gestion :	6.759.944 EUR
Total :	**127.095.671 EUR HTVA**

Partie 2 : Cas d'utilisation

Cette partie 2 englobe les coûts liés à la réalisation et l'intégration des cas d'utilisation qui ont déjà été identifiés lors de l'étude de faisabilité. Pour quelques-uns de ces cas d'utilisation, il faut prévoir des acquisitions d'équipements IT dédiés ou la réalisation de configurations spécifiques, ce qui justifie la présence de coûts d'acquisition, d'exploitation et de maintenance.

L'intégration des cas d'utilisation de futurs bénéficiaires, non-encore identifiés lors de l'étude de faisabilité, sera financée via le budget de la partie 1.

Il est à noter que le nombre maximal de futurs cas d'utilisation qui pourront être hébergés sur le LCDC ne pourra pas être déterminé en avance car le nombre maximal dépend des exigences en termes de capacités de stockage et de capacités de calculs des cas d'utilisation.

Estimations totales pour la partie 2 :

Coûts d'acquisition :	9.492.194 EUR
Coûts d'exploitation et de maintenance :	23.490.003 EUR
Coûts d'opération :	319.137 EUR
Coûts de gestion :	9.466.730 EUR
Total :	**42.768.064 EUR HTVA**

Partie 3 : Services connexes

Cette partie reprend les coûts liés aux services connexes nécessaires pour des mesures de sécurité préventives afin de pouvoir protéger les environnements cloud du LCDC contre des attaques cyber malveillants. Ces mesures de sécurité s'appliquent à tous les environnements cloud du LCDC ce qui veut dire que tous les utilisateurs du LCDC vont bénéficier de ces mesures. Nonobstant l'envergure du LCDC et des coûts liés aux cas d'utilisations mentionnés dans les parties 1 et 2, les coûts liés aux services connexes restent inchangés.

Estimations totales pour la partie 3 :

Coûts d'acquisition :	0 EUR
Coûts d'exploitation et de maintenance :	2.515.578 EUR
Coûts d'opération :	19.361.551 EUR
Coûts de gestion :	143.256 EUR
Total :	**22.020.385 EUR HTVA**

Partie 4 : LCDC NSPA Private Cloud

Une partie dédiée du LCDC sera mise en place pour les besoins de la NSPA. En effet la NSPA opère actuellement déjà un environnement cloud privé pour la propres besoins et co-financé par le Luxembourg. Il est prévu de migrer cet environnement cloud privé vers le LCDC. Cette migration vers le LCDC est à considérer comme une contribution du Luxembourg vue que les coûts liés à cet environnement cloud seront pris en charge par le Luxembourg via le financement du LCDC.

Estimations totales pour la partie 4 :

Coûts d'acquisition :	40.652.793 EUR
Coûts d'exploitation et de maintenance :	5.420.372 EUR
Coûts d'opération :	12.060.497 EUR
Coûts de gestion :	342.541 EUR
Total :	**58.476.203 EUR HTVA**

Total des coûts estimés :

Le présent tableau donne une vue globale des coûts estimés par partie et types de coûts :

Partie	*Acquisition*	*Exploit./Maint.*	*Opération*	*Gestion*	*Total*
01. Luxembourg Cyber Defence Cloud	72.337.511 €	33.807.423 €	14.190.793 €	6.759.944 €	127.095.671 €
02. Cas d'utilisation	9.492.194 €	23.490.003 €	319.137 €	9.466.730 €	42.768.064 €
03. Services connexes	0 €	2.515.578 €	19.361.551 €	143.256 €	22.020.385 €
04. LCDC NSPA Private Cloud	40.652.793 €	5.420.372 €	12.060.497 €	342.541 €	58.476.203 €
Total EUR HTVA :	**122.482.498 €**	**65.233.376 €**	**45.931.978 €**	**16.712.471 €**	**250.360.323 €**

Le tableau suivant donne une vue globale des coûts estimés réparties sur la durée des 12 ans (estimation qui peut varier, notamment selon nombre de cas d'utilisation hébergés dans le LCDC et les facteurs économiques) :

Partie	*2024*	*2025*	*2026*	*2027*	*2028*	*2029*	*2030*
Acquisition	2.900.000 €	3.000.000 €	3.690.406 €	34.278.906 €	0 €	2.520.000 €	848.498 €
Exploit./Maint.	1.716.041 €	3.289.144 €	9.544.122 €	4.479.938 €	4.703.935 €	4.939.132 €	5.182.450 €
Opération	1.455.000 €	2.359.925 €	2.477.921 €	3.594.876 €	3.774.620 €	3.963.351 €	4.161.518 €
Gestion	931.500 €	1.042.125 €	1.252.996 €	1.247.923 €	1.272.030 €	1.335.631 €	1.402.409 €
Total EUR HTVA :	**7.002.541 €**	**9.691.194 €**	**16.965.445 €**	**43.601.643 €**	**9.750.585 €**	**12.758.114 €**	**11.594.875 €**

Partie	*2031*	*2032*	*2033*	*2034*	*2035*	*Total*
Acquisition	49.803.803 €	22.584.885 €	0 €	2.856.000 €	0 €	**122.482.498€**
Exploit./Maint.	5.684.823 €	5.969.065 €	6.267.518 €	6.569.869 €	6.887.339 €	**65.233.376€**
Opération	4.369.594 €	4.588.074 €	4.817.478 €	5.058.352 €	5.311.269 €	**45.931.978 €**
Gestion	1.472.533 €	1.589.530 €	1.623.467 €	1.752.457 €	1.789.870 €	**16.712.471 €**
Total EUR HTVA :	**61.330.753 €**	**34.731.554 €**	**12.708.463 €**	**16.236.678 €**	**13.988.478 €**	**250.360.323 €**

*

FICHE D'EVALUATION D'IMPACT

Coordonnées du projet

Intitulé du projet :	**Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes**
Ministère initiateur :	**Ministère des affaires étrangères et européennes – Direction de la Défense**
Auteur(s) :	**Ben Fetler, Gilles Grün**
Téléphone :	**247-82841**
Courriel :	**d7.legads@mae.etat.lu**
Objectif(s) du projet :	**Le présent projet de loi a pour objet d'autoriser le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes.**
Autre(s) Ministère(s)/Organisme(s)/Commune(s)impliqué(e)(s) :	
n.a.	
Date :	**09/01/2023**

Mieux légiférer

1. Partie(s) prenante(s) (organismes divers, citoyens, …) consultée(s) : Oui ☒ Non ☐
   Si oui, laquelle/lesquelles : NATO Support and Procurement Agency (NSPA)
   Remarques/Observations :

2. Destinataires du projet :
   – Entreprises/Professions libérales : Oui ☐ Non ☒
   – Citoyens : Oui ☐ Non ☒
   – Administrations : Oui ☒ Non ☐

3. Le principe « Think small first » est-il respecté ? Oui ☐ Non ☐ N.a.[9] ☒
   (c.-à-d. des exemptions ou dérogations sont-elles prévues suivant la taille de l'entreprise et/ou son secteur d'activité ?)
   Remarques/Observations :

4. Le projet est-il lisible et compréhensible pour le destinataire ? Oui ☒ Non ☐
   Existe-t-il un texte coordonné ou un guide pratique, mis à jour et publié d'une façon régulière ? Oui ☐ Non ☒
   Remarques/Observations :

5. Le projet a-t-il saisi l'opportunité pour supprimer ou simplifier des régimes d'autorisation et de déclaration existants, ou pour améliorer la qualité des procédures ? Oui ☐ Non ☒
   Remarques/Observations :

9 N.a. : non applicable.

6. Le projet contient-il une charge administrative[10] pour le(s) destinataire(s) ? (un coût imposé pour satisfaire à une obligation d'information émanant du projet ?) Oui ☐ Non ☒
   Si oui, quel est le coût administratif[11] approximatif total ? (nombre de destinataires x coût administratif par destinataire)

7. a) Le projet prend-il recours à un échange de données inter-administratif (national ou international) plutôt que de demander l'information au destinataire ? Oui ☐ Non ☐ N.a. ☒
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?
   b) Le projet en question contient-il des dispositions spécifiques concernant la protection des personnes à l'égard du traitement des données à caractère personnel[12] ? Oui ☐ Non ☐ N.a. ☒
   Si oui, de quelle(s) donnée(s) et/ou administration(s) s'agit-il ?

8. Le projet prévoit-il :
   – une autorisation tacite en cas de non réponse de l'administration ? Oui ☐ Non ☐ N.a. ☒
   – des délais de réponse à respecter par l'administration ? Oui ☐ Non ☐ N.a. ☒
   – le principe que l'administration ne pourra demander des informations supplémentaires qu'une seule fois ? Oui ☐ Non ☐ N.a. ☒

9. Y a-t-il une possibilité de regroupement de formalités et/ou de procédures (p.ex. prévues le cas échéant par un autre texte) ? Oui ☐ Non ☐ N.a. ☒
   Si oui, laquelle :

10. En cas de transposition de directives communautaires, le principe « la directive, rien que la directive » est-il respecté ? Oui ☐ Non ☐ N.a. ☒
    Sinon, pourquoi ?

11. Le projet contribue-t-il en général à une :
    a) simplification administrative, et/ou à une Oui ☐ Non ☒
    b) amélioration de la qualité réglementaire ? Oui ☐ Non ☒
    Remarques/Observations :

12. Des heures d'ouverture de guichet, favorables et adaptées aux besoins du/des destinataire(s), seront-elles introduites ? Oui ☐ Non ☐ N.a. ☒

13. Y a-t-il une nécessité d'adapter un système informatique auprès de l'Etat (e-Government ou application back-office) ? Oui ☐ Non ☒
    Si oui, quel est le délai pour disposer du nouveau système ?

---

10 Il s'agit d'obligations et de formalités administratives imposées aux entreprises et aux citoyens, liées à l'exécution, l'application ou la mise en oeuvre d'une loi, d'un règlement grand-ducal, d'une application administrative, d'un règlement ministériel, d'une circulaire, d'une directive, d'un règlement UE ou d'un accord international prévoyant un droit, une interdiction ou une obligation.

11 Coût auquel un destinataire est confronté lorsqu'il répond à une obligation d'information inscrite dans une loi ou un texte d'application de celle-ci (exemple: taxe, coût de salaire, perte de temps ou de congé, coût de déplacement physique, achat de matériel, etc.).

12 Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (www.cnpd.lu)

14. Y a-t-il un besoin en formation du personnel de l'administration concernée ? Oui ☐ Non ☐ N.a. ☒

Si oui, lequel ?

Remarques/Observations :

Egalité des chances

15. Le projet est-il :
- principalement centré sur l'égalité des femmes et des hommes ? Oui ☐ Non ☒
- positif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒

  Si oui, expliquez de quelle manière :
- neutre en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒

  Si oui, expliquez pourquoi :
- négatif en matière d'égalité des femmes et des hommes ? Oui ☐ Non ☒

  Si oui, expliquez de quelle manière :

16. Y a-t-il un impact financier différent sur les femmes et les hommes ? Oui ☐ Non ☐ N.a. ☒

Si oui, expliquez de quelle manière :

Directive « services »

17. Le projet introduit-il une exigence relative à la liberté d'établissement soumise à évaluation[13] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire A, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

18. Le projet introduit-il une exigence relative à la libre prestation de services transfrontaliers[14] ? Oui ☐ Non ☐ N.a. ☒

Si oui, veuillez annexer le formulaire B, disponible au site Internet du Ministère de l'Economie et du Commerce extérieur :

www.eco.public.lu/attributions/dg2/d_consommation/d_march_int_rieur/Services/index.html

13 Article 15, paragraphe 2 de la directive « services » (cf. Note explicative, p. 10-11)

14 Article 16, paragraphe 1, troisième alinéa et paragraphe 3, première phrase de la directive « services » (cf. Note explicative, p. 10-11)

Impression: CTIE – Division Imprimés et Fournitures de bureau

20

Session ordinaire 2022-2023

MW/PR P.V. SID 20

Commission de la Sécurité intérieure et de la Défense

Procès-verbal de la réunion du 6 mars 2023

(La réunion a eu lieu par visioconférence.)

Ordre du jour :

8167 Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

- Présentation du projet de loi

*

Présents : Mme Nancy Arendt épouse Kemp, M. André Bauler, M. François Benoy, M. Dan Biancalana, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, M. Gusty Graas, M. Max Hahn, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Georges Mischo, Mme Octavie Modert (en rempl. de Mme Diane Adehm), Mme Lydia Mutsch, Mme Jessie Thill (en rempl. de Mme Semiray Ahmedova)

M. Emile Eicher, Mme Lydie Polfer, observateurs

M. François Bausch, Ministre de la Défense

Mme Nina Garcia, Coordination générale ; M. Gilles Grün, M. Ben Fetler, Col Guy Hoffmann, Direction de la Défense, du Ministère des Affaires étrangères et européennes

Mme Marianne Weycker, de l'Administration parlementaire

Excusée : Mme Nathalie Oberweis, observatrice déléguée

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission

*

Suite à quelques paroles introductives de Madame la Présidente, Monsieur le Ministre indique que le présent projet est, après la plateforme « Cyber Range » déjà opérationnelle, le deuxième grand projet de la stratégie de cyberdéfense du Luxembourg, dont les objectifs

à long terme sont de disposer d'une défense les plus cyber-sécurisées de l'OTAN[1] et de l'UE[2] et de développer une expertise et des capacités qui pourront aussi être offertes aux Alliés et aux partenaires. Le projet suscite un vif intérêt de petits pays, tels les pays baltes, mais aussi de grands pays comme l'Allemagne.

Une « Cyber Range » est une plateforme de simulation qui permet aux responsables de sécurité informatique de s'entraîner contre les cyberattaques. Un « cloud » ne permet pas seulement de stocker des données, mais aussi de les traiter et d'héberger des services informatiques.

La stratégie de cyberdéfense nécessite une infrastructure informatique évolutive, fiable, performante et sécurisée. Pour des raisons de sécurité, ni le nombre de sites ni leur emplacement au Luxembourg ne peuvent être précisés.

Outre les objectifs à long terme de la stratégie de cyberdéfense, le Luxembourg doit pouvoir répondre à ses engagements au niveau international (OTAN, UE). Monsieur le Ministre souligne que le présent projet est proactif, puisque le Luxembourg devance les exigences d'aujourd'hui de l'OTAN et, les exigences futures s'annonçant considérables, notre pays créera le cadre qui permettra aussi à ses Alliés et partenaires d'y avoir recours pour satisfaire celles-ci. Comme dans les domaines de la reconnaissance et de l'espace, le Luxembourg peut ici se spécialiser dans un troisième domaine de sa Défense.

Le projet aura des retombées économiques pour le Luxembourg et renforcera l'image de notre pays, dont le côté fort peut consister justement dans de tels projets qui ne nécessitent pas la mise à disposition d'importants effectifs militaires, mais une équipe de spécialistes.

À côté de ses engagements au niveau international, le Luxembourg doit aussi pouvoir répondre de façon adéquate, comme le décrit l'exposé des motifs, aux défis de la transformation digitale croissante au niveau des Défenses des États membres de l'OTAN et de l'UE, ainsi que des agences OTAN et UE, et auprès des acteurs étatiques nationaux. Cette digitalisation fait augmenter les besoins de ressources informatiques qui doivent en plus satisfaire en matière de défense à des conditions spécifiques de sécurité.

Le « Luxembourg Cyber Defence Cloud » (LCDC) se traduira par des environnements cloud privés et hautement sécurisés de la Défense luxembourgeoise qui permettent le stockage et le traitement de données.

L'exposé des motifs du projet de loi explique que « L'informatique en nuage ou le « *cloud computing* » est la fourniture de ressources et services informatiques à la demande via un réseau de serveurs distants. Les ressources informatiques sont gérées par un fournisseur de service de sorte que le bénéficiaire peut [puisse] faire abstraction de la complexité de gestion de telles ressources informatiques et pourra [puisse] se concentrer sur les services qu'il veut héberger en bénéficiant des ressources informatiques mises à disposition par le fournisseur. ».

Un expert du ministère précise la différence entre « public clouds » et « private clouds » : les premiers fonctionnent et sont joignables par Internet, tandis que les seconds ne sont pas joignables par Internet, mais par des lignes sécurisées reliant le fournisseur (pour le LCDC la Défense luxembourgeoise) à l'utilisateur final (par exemple une armée ou un pays étranger ayant recours au LCDC), lequel est le seul à avoir accès. Le LCDC étant hébergé sur plusieurs sites au Luxembourg, il est garanti contre une défaillance.

[1] Organisation du Traité de l'Atlantique Nord (NATO - North Atlantic Treaty Organization)
[2] Union européenne

La Défense luxembourgeoise sera le propriétaire du LCDC ; pour l'acquisition de l'infrastructure IT, elle collabore étroitement avec la NSPA[3], comme elle le fait depuis 2019 dans le cadre d'un programme de partenariat. Le LCDC pourra stocker des données classifiées (OTAN, UE, et éventuellement aussi des données nationales) et non-classifiées. Les auteurs du projet de loi précisent à l'exposé des motifs que le stockage se fait dans des centres de données sécurisés, dont le standard de protection répond aux standards internationaux les plus hauts et conçus pour assurer une haute disponibilité. Une panoplie de mesures de sécurité est exigée pour pouvoir résister contre des attaques cyber, ces mesures variant en fonction du niveau de sécurité. Le niveau de protection visé pour le LCDC est « NATO Restricted », voire « NATO Secret » ; ce dernier exige par exemple des gardiens armés et des mécanismes de cryptage spécifiques.

Aussi une étude sur la faisabilité et la conformité technique a-t-elle été réalisée pour garantir que l'environnement cloud pourra recevoir une accréditation pour le traitement et le stockage d'informations classifiées.

S'agissant de l'envergure du projet LCDC, celui-ci consiste d'abord en l'acquisition, l'hébergement, la gestion et la maintenance de l'infrastructure IT nécessaire pour les différents environnements cloud.

Ensuite, fait partie du projet la création des environnements cloud pour les différents pays ou projets cyber. Ces environnements sont ségrégés ; les auteurs expliquent à l'exposé des motifs que « Cette ségrégation forte est réalisée via le concept de la *multi-tenancy* qui permet à différents environnements cloud de partager la même infrastructure informatique (mêmes capacités de calculs et de stockage), mais de les garder en même temps suffisamment ségrégés via entre autres des moyens cryptographiques pour garantir qu'un bénéficiaire ne peut pas accéder aux données d'un autre. Par conséquent, une stratégie de gestion des identités et du contrôle d'accès ainsi qu'une gestion des clés cryptographiques et de tous les aspects connexes du cycle de vie de la gestion des clés seront défini[e]s et pris[es] en considération dès le début du projet. De plus, des services et mesures de sécurité préventives seront considérés et le cas échéant mis[~~es~~] en place pour pouvoir identifier des menaces cyber potentielles. ». Le bénéficiaire obtient la clé cryptographique de son environnement cloud ; il en a la responsabilité et est le seul à avoir accès à cet environnement cloud. En cas de perte de la clé, aucun accès ne sera plus possible, mais il existe des techniques destinées à empêcher la perte de la clé.

Une autre partie du projet est de satisfaire aux exigences de sécurité afin d'atteindre les différents niveaux de classification.

La sécurité cyber en général est un autre volet. Des mesures de sécurité et services seront mis en place pour découvrir si d'autres pays attaquent le cloud à partir d'Internet ou d'autres voies (OSINT – Open Source Intelligence/ROSO – Renseignement d'origine source ouverte).

Le LCDC ne sera pas dépendant d'un fournisseur de service cloud, mais offrira une plateforme compatible et interopérable avec différentes solutions technologiques provenant de différents fournisseurs (approche « multi-cloud »). En effet, la dépendance d'un seul fournisseur comporte le risque d'une hausse considérable des prix ; en outre, il n'y a pas de garantie qu'un fournisseur offre les mêmes fonctionnalités encore dans une dizaine d'années.

Finalement, le projet fournira un service durable et évolutif. Il y a un certain nombre de projets déjà annoncés qui seront hébergés sur le LCDC. Comme de futurs projets ne sont

[3] NATO Support and Procurement Agency

pas encore connus, il est veillé à ne pas acquérir de matériel inutile qui consommerait inutilement de l'énergie. Si les besoins en capacités de stockage et de performance augmentent effectivement, l'infrastructure IT sera adaptée de manière dynamique.

Les avantages du LCDC pour les besoins de la Défense sont les suivants :

- une réduction des coûts pour les bénéficiaires : pour les futurs projets cyber, il ne sera plus nécessaire de mettre en place pour chacun une infrastructure IT, donc d'acquérir du matériel, de créer un réseau, etc., mais ces projets pourront être hébergés sur le LCDC, ce qui signifie une réduction des coûts, mais aussi du temps nécessaire pour démarrer un projet ; ceci représente également un avantage considérable pour nos partenaires OTAN et UE, sachant qu'il y a en outre une pénurie d'experts IT et que les frais de rémunération de ceux-ci sont extrêmement élevés ;

- l'évolutivité : si un bénéficiaire a besoin de plus de capacités qu'initialement, le LCDC permet de les lui mettre à disposition ;

- la fiabilité et la sécurité : comme il vient d'être expliqué, le LCDC se traduira par des environnements cloud hautement sécurisés et sera à l'abri d'une défaillance du fait de l'hébergement sur plusieurs sites ;

- la productivité : comme décrit à l'exposé des motifs du projet de loi, le bénéficiaire de l'informatique en nuage peut faire abstraction de la complexité de gestion de ressources informatiques et peut se concentrer sur les services qu'il veut héberger en utilisant les ressources informatiques mises à disposition par le fournisseur de celles-ci ;

- la contribution au développement de compétences : le LCDC attire des entreprises au Luxembourg, avec lesquelles est conclu un contrat de sous-traitance pour faire fonctionner le cloud; l'attractivité ainsi croissante du Luxembourg dans ce domaine va de pair avec le développement, notamment en matière de défense, de notre stratégie de digitalisation ;

- la réduction de l'empreinte écologique : en regroupant les besoins en ressources informatiques des différents bénéficiaires, la mise en place de nombreuses infrastructures informatiques est évitée et la consommation d'énergie (électricité, eau pour le refroidissement des salles informatiques) réduite. En outre, les sites utiliseront de l'énergie verte.

Concernant les objectifs du LCDC, celui-ci hébergera principalement des projets qui contribuent

- à la résilience du Luxembourg face aux menaces cyber, par exemple des projets profitant à des infrastructures critiques et étatiques ; un tel projet est la plateforme « Cyber Range » destinée à former des experts IT contre les attaques cyber ; un autre exemple est le « National Sensory Network », un projet qui vise à découvrir, au moyen de détecteurs installés dans des infrastructures critiques, des attaques cyber qui s'annoncent ; les indications seront centralisées via le LCDC et les autres infrastructures critiques seront prévenues pour leur permettre de prendre des contre-mesures ;
- à l'effort de défense luxembourgeois au niveau de l'OTAN, de l'UE ou de partenaires ou Alliés ; comme il vient d'être dit, le présent projet est proactif et, compte tenu de la digitalisation croissante dans le domaine de la défense, permettra au Luxembourg d'être préparé aux exigences futures en disposant de la plateforme nécessaire pour héberger les futurs projets ;
- aux objectifs stratégiques de la Défense luxembourgeoise.

Un accord technique conclu par la Défense avec chaque bénéficiaire déterminera les modalités et responsabilités respectives en fonction des besoins du bénéficiaire.

Quelques exemples de cas d'utilisation du LCDC :

- exploitation de solutions informatiques et stockage de preuves numériques pour mener des investigations numériques légales : si un incident cyber s'est produit, le LCDC peut héberger la software pour procéder à une investigation digitale de l'incident ; plus concrètement, s'agissant de cybercriminalité, les outils nécessaires pour l'investigation ont besoin d'importantes capacités numériques pour un laps de temps très court et le LCDC pourra fournir ces capacités pendant ce temps ;

- exploitation d'une plateforme du type « Cyber Threat Intelligence »[4] : le LCDC met à disposition les infrastructures IT pour détecter les acteurs étatiques ou autres qui préparent une attaque contre notre pays, l'UE ou l'OTAN (cf. p. 4 sous « résilience du Luxembourg face aux menaces cyber ») et donc aussi pour protéger le cloud ;

- stockage et/ou traitement d'images satellitaires : de plus en plus de projets génèrent des images satellitaires, lesquelles ne sont souvent pas analysées manuellement, mais par une intelligence artificielle ; le stockage et l'analyse des images requièrent de grandes quantités de capacités de stockage et de calcul ;

- hébergement de capacités de cyberdéfense nationales et internationales ; un exemple au niveau national est la plateforme « Cyber Range » qui pourra être migrée vers le LCDC en cas de vétusté des serveurs actuels ;

- hébergement de plateformes ayant une utilité internationale et offrant des services pour la gestion de projets multinationaux d'acquisitions et de maintien ; un projet concret, déjà annoncé, est celui avec les Pays-Bas et la Suède, avec le support de la NSPA, qui consiste à installer sur le cloud une plateforme « Digital Engineering » : en prenant l'exemple de l'achat d'un hélicoptère, tout, c'est-à-dire l'acquisition, le prototypage, le financement et à la fin la mise au rebut, se fait à l'heure actuelle manuellement et dans différents services, dont chacun dispose de ses propres outils. Afin d'être plus performant et de permettre à chaque personne d'être à jour sur l'état du prototype, le traitement entier se fera sur une plateforme digitale.

Pour ce qui est de l'échéancier du LCDC, la durée du projet s'étend de 2024 à 2035 : les deux premières années sont destinées à l'acquisition de l'infrastructure et à la mise en opération progressive jusqu'au niveau de capacité 1. Ensuite, après cinq ans d'opération, les équipements informatiques sont à remplacer pour une nouvelle durée de cinq ans, la durée de vie de ces équipements étant de cinq ans. En cas de succès, la capacité sera en outre augmentée de 50% au maximum (niveau de capacité 2).

En ce qui concerne le financement, le projet a débuté en 2019 par une étude auprès des fournisseurs de « clouds » pour voir si un tel projet est réalisable en dehors d'Internet, certains fournisseurs n'offrant que des « public clouds ».

Par ailleurs, des études sur le financement ont été lancées avec la NSPA. Ces études viennent seulement d'être terminées, puisque les coûts du projet LCDC ont dû être adaptés en cours de route suite à l'augmentation des taux d'intérêts et des frais d'énergie.

[4] Wikipedia : « La **Threat Intelligence**, ou **Cyber Threat Intelligence** (**CTI**) est une discipline basée sur des techniques du renseignement, qui a pour but la collecte et l'organisation de toutes les informations liées aux menaces du cyber-espace (cyber-attaques), afin de dresser un portrait des attaquants ou de mettre en exergue des tendances (secteurs d'activités touchés, méthode utilisée, etc). Ce profiling permet de mieux se défendre et d'anticiper au mieux les différents incidents en permettant une détection aux prémices d'une attaque d'envergure (APT). »

Aux conditions économiques de 2023, le LCDC coûtera au total 250 360 323 euros sur une durée de 12 ans. Cette somme inclut les frais d'acquisition, d'exploitation, de maintenance, d'opération et de gestion du système et des composantes et services connexes (comme pour la sécurisation du cloud). Est également inclus le financement d'un environnement cloud pour la NSPA qui s'élève à 58 476 203 euros, ce qui représente une importante contribution à l'effort de défense au niveau de l'OTAN, le Luxembourg étant par ailleurs la « host nation » de la NSPA. Déjà aujourd'hui, le Luxembourg finance en partie l'infrastructure IT et les centres de données IT de la NSPA.

Le financement autorisé par le présent projet de loi exclut
- les coûts de gestion des environnements mis à disposition aux bénéficiaires,
- les cas d'utilisation des bénéficiaires,
- l'interconnexion vers les sites des bénéficiaires et la connexion internet des bénéficiaires.

Ces coûts sont à charge des bénéficiaires et déterminés dans l'accord technique conclu avec chaque bénéficiaire.

Le budget se répartit comme suit :
- coûts de l'infrastructure (serveurs, réseaux, configuration) : 127 095 671 euros ;
- projets déjà identifiés à héberger dans le LCDC : 42 768 064 euros ;
- services connexes (mesures spécifiques de sécurité, services IT de fournisseurs externes (monitoring de la performance du LCDC)) : 22 020 385 euros ;
- financement d'un environnement cloud pour la NSPA : 58 476 203 euros.

Discussion

▪ Pour M. Marc Goergen (Piraten), le LCDC donne lieu aux questions et observations suivantes :

1) De quelle taille est le risque pour le Luxembourg de devenir la cible d'attaques, physiques ou virtuelles, en raison de l'installation de tels centres de données dans notre pays ?
2) Les coûts du LCDC s'élèvent à 250 millions d'euros sur une durée de 12 ans. Avec les 195 millions d'euros sur 10 ans pour la fourniture de capacités de communication satellitaire sur une orbite terrestre moyenne (« Medium Earth Orbit » (MEO))[5], investissement prévu dans le cadre d'un partenariat récemment lancé avec les États-Unis d'Amérique, des dépenses de plus de 400 millions d'euros seront effectuées en peu de temps dans le domaine de la Défense, alors que pour d'autres domaines, des mesures, dont les coûts ne représentent qu'une fraction de ces montants, ne sont pas réalisées faute de budget. Sans s'opposer aux investissements en matière de défense, l'orateur voudrait toutefois obtenir des précisions sur l'ordre de priorité des dépenses budgétaires.
3) Quant à l'empreinte écologique, quelle est la consommation réelle des centres de données ?
4) Est-ce que le Luxembourg ne se rend pas dépendant en faisant passer tous ces projets par la NSPA ?

Ad 4) : Monsieur le Ministre rappelle que la NSPA est une agence publique qui se compose des États membres de l'OTAN et dont le siège se trouve au Luxembourg, ce qui renforce la crédibilité de notre pays au sein de l'OTAN.

[5] Dossier parlementaire 8157

Ad 2) : Les dépenses élevées ne devraient pas surprendre, comme les projets sont toujours annoncés, et elles sont nécessaires pour atteindre un effort de défense de 1% du PIB en 2028. Celui-ci se situe actuellement autour de 0,69% du PIB et doit donc augmenter significativement au cours des prochaines années. De surplus, les projets sont choisis de manière à être également utiles à notre économie.

Monsieur le Ministre souligne que d'autres projets coûteux devront suivre pour maintenir l'effort de défense à 1% du PIB à partir de 2028, à moins que la Chambre des Députés n'en décide autrement.

Ad 1) : L'expert ministériel explique que le risque d'attaques augmente, mais le LCDC a un effet dissuasif, comme il s'agit d'un projet de l'OTAN hébergeant des données et services informatiques de l'OTAN et de ses pays membres. En cas d'attaque, l'article 5 du Traité de l'Alliance pourrait être invoqué ; en vertu de cette disposition, une attaque armée contre un membre de l'Alliance est considérée comme une attaque contre tous les membres.

Par ailleurs, toutes les mesures de sécurité seront prises et constamment actualisées. Le LCDC sera sécurisé de manière proactive pour devancer les attaques. S'agissant en outre d'un « private cloud », une attaque à travers Internet n'est pas possible, mais devrait passer par un utilisateur ; or, les accès des utilisateurs sont à leur tour hautement sécurisés.

Monsieur le Ministre tient à ajouter qu'en tant que membre d'une alliance internationale, le Luxembourg ne peut pas se limiter à se tenir sous le bouclier, alors que ses partenaires supportent les risques.

Ad 3) : Le LCDC sera hébergé dans des centres de données existants, ce qui signifie qu'il ne causera pas de consommation d'énergie supplémentaire. Pour savoir néanmoins quelle serait la consommation d'énergie propre du LCDC, une étude a révélé qu'elle correspondrait au maximum, donc pour le niveau de capacité 2, à la consommation annuelle de 125 ménages.

- Tout en étant conscient de la nécessité de ne pas divulguer le nombre et l'emplacement des sites, M. Gusty Graas (DP) estime néanmoins important de prendre contact avec les autorités locales concernées pour éviter des discussions inutiles par après. En effet, dans d'autres dossiers sensibles, les communes n'avaient pas été associées à temps.

Le ministère assure que les communes seront contactées et informées autant que nécessaire, dans les limites imposées du fait qu'on se trouve dans un domaine très sensible qui concerne la sécurité de notre pays. Comme les centres de données hébergent déjà maintenant des projets de l'OTAN et de l'UE, ils répondent déjà aux exigences de sécurité. Le LCDC est un projet supplémentaire.

- Mme Stéphanie Empain (déi gréng) s'informe sur les points suivants :

1) Où sont actuellement stockées les données secrètes de l'OTAN – également dans des clouds ou sur des serveurs informatiques ? Comment savoir où accéder à des données déterminées et est-ce que ces données sont interconnectées ?
2) Le stockage de données d'un État constitue-t-il un back-up ou s'agit-il du seul emplacement pour ces données ?
3) Comment fonctionne l'approche « multi-cloud » du point de vue technique ?
4) Le projet « National Sensory Network » est-il lié au LCDC ou ne faudrait-il pas réaliser un tel projet déjà maintenant, comme le risque de cyberattaques existe déjà ?
5) Est-il déjà possible de chiffrer les besoins budgétaires pour le remplacement des équipements après les premiers cinq ans d'opération ?

Ad 1) : Les données secrètes OTAN actuelles sont hébergées sur des serveurs. La transformation digitale engendre constamment de nouvelles données et de nouveaux projets, ce qui rend nécessaire de plus en plus de capacités de stockage. En outre, il n'existe souvent pas de back-up pour ces données et projets. Le LCDC offre aussi bien les capacités requises que le back-up.

Ad 2) : L'utilisateur formule sa demande selon ses besoins. Le Luxembourg examine le projet, s'assurant notamment qu'il ne va pas à l'encontre de l'idéologie luxembourgeoise, et met à disposition les capacités nécessaires. Le LCDC est largement ouvert aux projets et idées, il ne pose pas dès le début des limites.

Ad 3) : Le LCDC offrira une plateforme neutre. Les technologies cloud proviennent de fournisseurs extérieurs ; le Luxembourg ne retiendra que ceux qui offrent des fonctionnalités « private clouds ». Pour le LCDC, il est fait en quelque sorte une copie du « public cloud » destiné par le fournisseur au public ; cette copie est ensuite installée dans les environnements cloud privés et hautement sécurisés du LCDC. Pour l'actualisation des fonctionnalités et l'installation de nouvelles fonctionnalités, le fournisseur doit le faire sur le LCDC, donc se rendre sur le site, puisque les « private clouds » ne sont pas accessibles de l'extérieur par Internet. Le LCDC débutera avec la solution d'un fournisseur et s'élargira par la suite en utilisant les solutions technologiques de plusieurs fournisseurs pour ne pas dépendre d'un seul (approche « multi-cloud »).

Ad 5) : Le montant de 250 millions d'euros inclut l'augmentation de la capacité jusqu'au niveau 2. Au cas où il ne serait pas procédé à cette augmentation, le budget serait utilisé pour la continuation du LCDC au niveau de capacité 1 au-delà de 12 ans.

En cas de succès et donc d'augmentation, le niveau de capacité 2 constitue la limite. Un dépassement pour de nouveaux projets de l'OTAN ou de l'UE devrait être discuté. Une réserve de capacité sera toujours disponible pour les projets luxembourgeois.

Ad 4) : Les cyberattaques se font au Luxembourg encore manuellement, mais avec des instruments IT[6]. Le domaine cyber en matière de défense est seulement en train de se construire, le renseignement d'origine source ouverte (OSINT – cf. supra) n'existant pas encore ici. Les projets correspondants sont en train d'être mis en place. La collecte et l'analyse des informations se font à l'aide de solutions IT. Ces informations doivent être stockées afin de pouvoir faire l'historique en cas d'attaque ultérieure par une voie nouvelle et afin de pouvoir s'y adapter. Le LCDC offre les capacités pour héberger les services nécessaires.

Concernant l'article 5 du Traité de l'Atlantique Nord, Monsieur le Ministre souligne que les attaques cyber en matière de défense sont mises sur un pied d'égalité avec les attaques armées. Le Luxembourg bénéficie en tant que membre de l'OTAN de la protection de la défense collective de l'article 5 ; en plus, le LCDC représente une contribution luxembourgeoise à l'effort de défense collectif.

Procès-verbal approuvé et certifié exact

Annexe : Luxembourg Cyber Defence Cloud (Présentation)

[6] Information Technology

LUXEMBOURG CYBER DEFENCE CLOUD

- 06/03/2023 -

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

Direction de la défense

Agenda

01 Contexte

02 Le projet: Luxembourg Cyber Defence Cloud

03 Questions - Réponses

Contexte

Stratégie de cyberdéfense du Luxembourg
- Objectifs à long terme -

1. Disposer d'une des défenses les plus cybersécurisées de l'OTAN et de l'UE
2. Développer une expertise et des capacités qui pourront aussi être offertes aux Alliés et aux partenaires

Nécessite une infrastructure informatique **évolutive, fiable, performante et sécurisée**.

Contexte

- Outre les objectifs à long terme de la stratégie de cyberdéfense, il faut pouvoir répondre de façon adéquate:
  - **aux exigences et engagements pris au niveau international** (OTAN et UE);
  - **aux défis de la transformation digitale** auprès des défenses des États membres de l'OTAN et de l'UE.

La Défense luxembourgeoise entend répondre à ces défis en développant le:

Luxembourg Cyber Defence Cloud

Environnements cloud privés et hautement sécurisés de la Défense luxembourgeoise permettant le stockage et le traitement de données.

Luxembourg Cyber Defence Cloud

Un **environnement cloud privé hébergé au Luxembourg**

Offre la possibilité de **stocker et traiter des données sensibles et classifiées**

Capacités de calcul et de stockage évolutives afin de s'adapter à la demande et de supporter des cas d'utilisation futurs.

Opéré au profit de la Défense luxembourgeoise avec le support de la NSPA, contractée pour la partie acquisition, implémentation et exploitation.

Luxembourg Cyber Defence Cloud

ENVERGURE DU PROJET

- **Acquérir, héberger, gérer et maintenir** l'infrastructure IT nécessaire pour les différents environnements cloud.
- **Créer des environnements ségrégés** (« multi-tenancy ») pour les bénéficiaires **en assurant un taux de disponibilité élevé**.
- Implémenter **différents environnements cloud pour les différents niveaux de classification**.
- Mettre en place les mesures de sécurité et services nécessaires pour **assurer un niveau de cybersécurité élevé**.
- Offrir une **plateforme compatible et interopérable avec différentes solutions technologiques** provenant de différents fournisseurs (approche « multi-cloud »).
- **Fournir un service durable et évolutif** en termes de capacités, performance et évolutions technologiques futures.

Luxembourg Cyber Defence Cloud

AVANTAGES POUR LES BESOINS DE LA DÉFENSE

- Réduction des coûts pour les bénéficiaires
- Fiabilité
- Sécurité
- Réduction de l'empreinte écologique
- Évolutivité
- Productivité
- Contribution au développement de compétences

Luxembourg Cyber Defence Cloud

OBJECTIFS

- LCDC **principalement conçu pour l'hébergement de projets** qui :
  - **contribuent à la résilience du Luxembourg** (p.ex. : infrastructures critiques et étatiques) face aux menaces cyber
  - **contribuent à l'effort commun en matière de défense collective** au niveau de l'UE, de l'OTAN ou des partenaires du Luxembourg
  - **contribuent aux objectifs stratégiques** de la Défense luxembourgeoise

Pour chaque bénéficiaire, un accord/arrangement technique sera mis en place

Luxembourg Cyber Defence Cloud

EXEMPLES DE CAS D'UTILISATIONS

- Exploitation de solutions informatiques et stockage de preuves numériques pour mener des investigations numériques légales ;
- Exploitation d'une plateforme du type « Cyber Threat Intelligence » ;
- Hébergement de plateformes ayant une utilité internationale et offrant des services pour la gestion de projets multinationaux d'acquisitions et de maintien.
- Stockage et/ou traitement d'images satellitaires ;
- Hébergement de capacités de cyberdéfense nationales et internationales ;

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères
et européennes
Direction de la Défense

Luxembourg Cyber Defence Cloud

TIMELINE

Durée du projet: 12 ans (2024 – 2035) y inclus les renouvellements nécessaires après 5 ans et extension de capacité future du LCDC.

2024 - 2027 - 2031 - 2035

Acquisition de l'infrastructure et mise en opération progressive jusqu'au niveau de capacité 1.

Opération, maintenance et support. Intégration des cas d'utilisation supplémentaires suivant demande.

Intégration des premiers cas d'utilisation.

Renouvellement et en cas de succès: augmentation de la capacité de max 50% (niveau de capacité 2).

★ *Étape clef du projet*

Luxembourg Cyber Defence Cloud

FINANCEMENT

- Durant la **phase préliminaire** (2019-2022):
  - Réalisation d'une étude de marché
  - Identification de premiers cas d'utilisation
  - Initiation d'une preuve de concept

- Coûts totaux: **250.360.323€ sur une durée de 12 années** (conditions économiques de 2023).
  - Y inclus sont:
    - **les frais liés à l'acquisition, l'exploitation, la maintenance, l'opération et la gestion** du système et des composantes et services connexes,
    - **le financement d'un environnement cloud dédié pour la NSPA** (58.476.203 €).
  - Coûts à couvrir par les utilisateurs:
    - les **coûts de gestion des environnements** mises à disposition aux bénéficiaires,
    - le **financement des cas d'utilisation** des bénéficiaires,
    - **l'interconnexion vers les sites** des bénéficiaires ainsi que la **connexion internet** des bénéficiaires.

LUXEMBOURG CYBER DEFENCE CLOUD

Questions - Réponses

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

Direction de la défense

8167/01

N° 8167[1]

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « *Luxembourg Cyber Defence Cloud* », ainsi que ses composantes et services connexes

* * *

AVIS DU CONSEIL D'ETAT

(31.3.2023)

Par dépêche du 6 mars 2023, le Premier ministre, ministre d'État, a soumis à l'avis du Conseil d'État le projet de loi sous rubrique, élaboré par le ministre de la Défense.

Au texte du projet de loi étaient joints un exposé des motifs, un commentaire des articles, une fiche d'évaluation d'impact ainsi qu'une fiche financière.

Le ministre de la Défense a fait préciser, dans la lettre de saisine, qu'« aucun avis n'a été demandé à une chambre professionnelle, étant donné que le présent projet de loi ne rentre pas dans leurs champs de compétences respectifs ».

*

CONSIDERATIONS GENERALES

Le projet de loi vise à autoriser le Gouvernement à financer le projet « Luxembourg Cyber Defence Cloud », constituée par des environnements « cloud computing » spécialisés, ainsi que de composantes et services connexes et à financer ses coûts d'exploitation, de maintenance, d'opération et de gestion. Selon l'exposé des motifs, ce projet fait partie de la stratégie de cyberdéfense du Luxembourg et doit permettre, dans les centres de données situés au Luxembourg, le développement d'une « infrastructure informatique évolutive, fiable, performante et sécurisée en termes de confidentialité, intégrité et disponibilité », ainsi que d'une expertise et des capacités de cyberdéfense qui seront mises au service des pays membres de l'OTAN et de la coopération européenne en matière de cyberdéfense. Le coût du projet « Luxembourg Cyber Defence Cloud » à financer ne peut dépasser le montant de 250 360 323 euros, hors TVA, sur une période de douze ans, frais de gestion opérationnelle et marge incluses. Les dépenses afférentes seront liquidées à la charge du Fonds d'équipement militaire.

*

EXAMEN DES ARTICLES

Article 1er à 3

Sans observation.

*

OBSERVATIONS D'ORDRE LEGISTIQUE

Observation générale

Le Conseil d'État tient à relever que les termes rédigés en italiques sont à omettre dans les textes normatifs et suggère de faire figurer les termes « Luxembourg Cyber Defence Cloud » systématiquement entre guillemets.

Intitulé

L'intitulé n'est pas à faire suivre d'un point final, étant donné que les intitulés ne forment pas de phrase.

Article 2

À la première phrase, il est signalé que les tranches de mille sont séparées par une espace insécable. Par conséquent, il y a lieu d'écrire « 250 360 323 euros ».

Ainsi délibéré en séance plénière et adopté à l'unanimité des 15 votants, le 31 mars 2023.

Le Secrétaire général, — *Le Président,*

Marc BESCH — Christophe SCHILTZ

Impression: CTIE – Division Imprimés et Fournitures de bureau

25

Session ordinaire 2022-2023

MW/PR

P.V. SID 25
P.V. AEECA 33

Commission de la Sécurité intérieure et de la Défense

Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

Procès-verbal de la réunion du 11 mai 2023

Ordre du jour :

1. Présentation des nouvelles Lignes directrices de la défense

2. Uniquement pour les membres de la Commission de la Sécurité intérieure et de la Défense

   8157 Projet de loi autorisant le Gouvernement à financer le programme « Medium Earth Orbit Global Services » (MGS)
   - Rapportrice : Madame Stéphanie Empain

   - Adoption d'un projet de rapport

3. 8167 Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

   - Désignation d'un rapporteur
   - Examen de l'avis du Conseil d'État

*

Présents : Mme Diane Adehm, M. André Bauler, M. François Benoy, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, M. Max Hahn, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, Mme Lydia Mutsch, membres de la Commission de la Sécurité intérieure et de la Défense

Mme Nathalie Oberweis, observatrice déléguée

Mme Simone Beissel, Mme Djuna Bernard, M. Yves Cruchten, M. Emile Eicher, Mme Stéphanie Empain, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Laurent Mosar, Mme Lydia Mutsch, Mme Nathalie Oberweis, Mme Lydie Polfer, M. Claude Wiseler, membres de la Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

M. François Bausch, Ministre de la Défense

Mme Nina Garcia, Coordinatrice générale Défense, M. Tom Köller, Directeur, LtCol Tom Schons, Chef du Département Planification stratégique, M. Alain Charlier, M. Ben Fetler, M. Michael Schuster, Direction de la Défense, du Ministère des Affaires étrangères et européennes

Lëtzebuerger Arméi :

Gen Steve Thull, Chef d'État-Major

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : Mme Nancy Arendt épouse Kemp, membre de la Commission de la Sécurité intérieure et de la Défense

M. Marc Spautz, membre de la Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

M. Jean Asselborn, Ministre des Affaires étrangères et européennes

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission de la Sécurité intérieure et de la Défense

*

1. Présentation des nouvelles Lignes directrices de la défense

Après quelques mots introductifs de Madame la Présidente, Monsieur le Ministre présente les Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 (désignées ici par « les Lignes directrices »), document adopté par le Conseil de gouvernement le 28 avril 2023. L'élaboration a pris deux ans, certains éléments importants ayant nécessité du temps pour devenir réalité et visant aussi un horizon plus lointain. Suivant l'accord de coalition 2018-2023 :

« La continuité de la politique de défense nationale contribue à assurer la confiance légitime que le Luxembourg doit susciter auprès de ses partenaires européens. La poursuite de la mise en œuvre des « Lignes Directrices de la Défense à l'horizon 2025 et au-delà » constituera le fil rouge du développement de l'Armée luxembourgeoise. Cette stratégie ambitieuse consacre la continuité des missions de l'Armée, assure la participation du secteur privé, s'oriente sur les priorités des lacunes capacitaires européennes et prend en compte les capacités à double-usage civile et militaire. Elle sera mise à jour à mi-mandat afin de tenir compte de l'évolution des contextes national et international. ».

Les Lignes directrices revêtent également une importance particulière en raison de la situation de sécurité moins bonne par rapport à celle en 2017, où les « Lignes directrices de la défense luxembourgeoise à l'horizon 2025 et au-delà » ont été présentées. Par ailleurs, l'OTAN[1] a adopté en automne 2021 des objectifs capacitaires qui engendrent, entre autres, comme conséquence pour le Luxembourg la création du bataillon de reconnaissance belgo-luxembourgeois.

[1] Organisation du Traité de l'Atlantique Nord

La situation de sécurité est marquée principalement par la guerre en Ukraine. S'y ajoutent notamment les relations conflictuelles entre l'OTAN et la Chine, de même que le changement climatique qui génère des conflits pour l'accès à des ressources, telles l'eau ou des énergies fossiles.

La discussion sur l'effort de défense continue. En 2014, l'OTAN a recommandé dans sa déclaration du sommet du Pays de Galles un niveau minimum de dépenses de défense de 2% du PIB[2]. Les Alliés, dont la part du PIB est inférieure à ce niveau recommandé par la directive OTAN, « - cesseront toute diminution des dépenses de défense ; - chercheront à augmenter leurs dépenses de défense en termes réels à mesure que croîtra leur PIB ; - chercheront à se rapprocher dans les dix années à venir des 2% recommandés, en vue d'atteindre leurs objectifs capacitaires OTAN et de combler les insuffisances capacitaires de l'OTAN ». Aujourd'hui, 2% du PIB sont considérés plutôt comme minimum et certains pays sont d'avis que l'effort de défense devrait augmenter jusqu'à 2,5%, voire 3%. Monsieur le Ministre regrette que la discussion soit menée sans poser la question, en ce qui concerne certains pays, de l'objectif des dépenses et sans tenir compte de la situation spécifique de notre pays.

Les « Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 » sont d'abord le résultat d'une bonne coopération entre la Direction de la Défense et la Lëtzebuerger Armée et ensuite aussi avec le Ministère des Affaires étrangères et européennes, la Représentation Permanente du Luxembourg auprès du Conseil de l'Atlantique Nord (OTAN) et le Haut-Commissariat à la Protection nationale (HCPN).

Monsieur le Ministre souligne que des Lignes directrices s'étendant sur 12 ans donnent à l'Armée une sécurité de planification. Le fait que le Luxembourg est le pays le plus riche de l'Union européenne (UE), en ce qui concerne le PIB et le revenu par habitant, lui confère une situation exceptionnelle. La croissance exceptionnelle au cours des dernières décennies n'était possible que grâce à l'intégration dans une architecture sécuritaire formée par des collectivités comme l'OTAN, les Nations unies, l'OSCE[3], l'UE, etc., dont le Luxembourg est membre. L'orateur met dès lors l'accent sur la solidarité du Luxembourg et la promotion de nos valeurs à l'échelle mondiale. De même, une autre finalité de la politique de défense luxembourgeoise est la préservation des intérêts essentiels de notre sécurité à travers le multilatéralisme basé sur le droit international. Dans ce contexte, le Luxembourg doit agir en tant que partenaire solidaire ; une politique crédible de défense et de dissuasion est essentielle pour préserver la paix. Tout aussi important est le soutien des mesures de confiance et de sécurité, celles-ci étant actuellement négligées (« Confidence and Security Building Measures »), alors qu'un rôle primordial revient à la prévention, puisque le but doit être l'empêchement de conflits.

Au cœur de la transformation de la défense luxembourgeoise se trouve la mise en place du bataillon binational mentionné ci-dessus. Ensuite, il y a trois domaines nouveaux, dans lesquels le Luxembourg se spécialise depuis quelques années : l'Espace, l'Air et le Cyber. Un autre chantier important constitue la future nouvelle loi-cadre sur l'Armée.

La défense se voit confrontée à de multiples défis qui risquent d'évoluer de plus en plus vite, ces défis ne provenant pas seulement du contexte géopolitique, mais aussi de la remise en cause, au moins en Europe, de l'ordre international fondé sur des règles.

Les menaces deviennent de plus en plus complexes : aux menaces conventionnelles et nucléaires s'ajoutent des menaces asymétriques et hybrides[4] et des menaces cyber. Les

[2] Produit intérieur brut
[3] Organisation pour la sécurité et la coopération en Europe
[4] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 20 : « Les actions hybrides sont un mélange d'activités coercitives et subversives, de méthodes traditionnelles (comme p.ex. diplomatiques, militaires, économiques) et non

changements environnementaux ont un double effet sur la sécurité : un effet sur le fonctionnement des armées, plus précisément sur leur manœuvrabilité, et sur les installations[5] et un effet d'aggravation des conflits pour l'accès aux ressources (cf. supra), engendrant aussi des afflux de réfugiés. En conséquence, il importe de procéder en matière de défense à des transformations et à une adaptation des objectifs stratégiques.

Afin d'atteindre les objectifs, la politique de défense suit les principes structurants suivants :

- la solidarité envers les partenaires ;
- l'autonomie décisionnelle, laquelle « porte d'abord sur la liberté des choix politiques stratégiques et ensuite sur le contrôle des activités opérationnelles et du cycle de vie des capacités » ;
- le partenariat transatlantique ;
- l'adaptabilité et la spécificité militaire ; il convient de rappeler que « L'adaptabilité et la spécificité du métier militaire impliquent que les forces armées ne peuvent pas être soumises en totalité aux mêmes règles et lois que celles applicables aux fonctionnaires et autres agents de l'État. Cela est dû à la nature unique de leurs missions, qui comprennent la maîtrise de situations d'urgence, l'engagement dans des opérations de maintien de la paix ainsi que la préparation au combat. Par conséquent, une législation spécifique est nécessaire pour réglementer les activités de l'Armée et garantir qu'elle puisse remplir ses obligations de manière efficace conformément aux normes éthiques et juridiques internationales applicables. Cette législation doit inclure des lois spécifiques sur le régime de travail, la discipline militaire, les procédures de conduite des opérations et les procédures de justice militaire. Il est important que cette législation soit révisée régulièrement pour qu'elle reste pertinente par rapport au milieu en constante mutation dans lequel l'Armée opère. » ;
- les partenariats et la mutualisation des ressources (« pooling and sharing »), ce qui se révèle aussi plus rentable et efficace ;
- l'engagement pour la société luxembourgeoise ;
- la politique étrangère et de sécurité des « 3D » : diplomatie, défense, développement.

L'objectif général est le développement des capacités, tout d'abord des forces, ensuite celles dans les domaines aérien, spatial et cyber. Les objectifs « pourront évoluer en fonction de la volatilité de l'environnement sécuritaire, que ce soit sur le plan international ou national, ceci dans la limite des contraintes légales – lois d'acquisitions – et budgétaires ».[6]

S'agissant en particulier de l'effort de défense, une augmentation substantielle est prévue pour atteindre 1% du PIB en 2028, ce qui fait une dépense d'1 milliard d'euros. Il ne s'agit pas d'une dépense unique, mais il importe de maintenir l'effort de défense à ce niveau. Dès l'année en cours, 2% de l'effort de défense sont consacrés à la recherche et au développement, spécialement dans le domaine des matériaux et des systèmes de propulsion.

Dans le cadre de la prévention des risques sécuritaires liés aux changements environnementaux, le niveau « net zero » d'ici 2050 est visé, tout en veillant à maintenir l'efficacité opérationnelle, militaire et économique.

---

conventionnelles (comme p.ex. utilisation abusive des réseaux sociaux, informations manipulées) utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs politiques, sans que le seuil d'une guerre officiellement déclarée ne soit atteint. La caractéristique de ces actions hybrides est que celles-ci sont difficilement attribuables à un acteur précis. En conséquence, le choix de réponse sera limité. Le fait que ces menaces ne peuvent être contrées dans leur totalité à tout moment, souligne l'importance de la résilience des outils étatiques, en particulier de la défense. »

[5] p. ex. inondation de la base aérienne d'Offutt (Nebraska) par la crue du Mississippi en 2019 ou encore dévastation de la base aérienne de Tyndall (Florida) par l'ouragan Michael en 2018

[6] Les objectifs sur le plan organisationnel, capacitaire et opérationnel sont détaillés aux pages 9 et 10 de l'annexe et aux pages 33 à 43 des Lignes directrices de la Défense luxembourgeoise à l'horizon 2035.

L'accroissement du taux de femmes dans l'Armée est un autre objectif. Les Lignes directrices indiquent que « La Défense appuie les programmes relatifs au développement du rôle des femmes dans la résolution des conflits. L'ONU[7] note que : « les femmes jouent un rôle déterminant dans la consolidation de la paix et notant que la participation pleine et concrète des femmes aux activités de prévention et de règlement des conflits et de reconstruction est intimement corrélée à l'utilité et à la viabilité à long terme de ces efforts, et soulignant à cet égard qu'il importe que les femmes participent sur un pied d'égalité avec les hommes à tout ce qui est entrepris pour maintenir et promouvoir la paix et la sécurité, et qu'il faut les associer davantage à la prise des décisions qui intéressent la prévention et le règlement des conflits et la consolidation de la paix, S/RES/2282 (2016) ». ».

Le « NATO Defence Planning Process » (NDPP) et le « Capability Development Plan » (CDP) de l'UE sont les principales références pour orienter le développement capacitaire national qui se compose de quatre axes prioritaires :

- Land (Terre) :
  - développement des capacités de reconnaissance terrestres
  - accent mis sur le bataillon binational (belgo-luxembourgeois) de reconnaissance de combat médian en coopération étroite avec la France

  Pour cela, l'Armée a besoin de renforts, dont du matériel plus lourd, en ce qui concerne les véhicules et l'armement → systèmes modernes antichar, remplacement des Dingos par les CLRV[8].
  - introduction de nouvelles capacités de reconnaissance, tels le contrôle aérien avancé (JTAC[9] - assure la coordination des systèmes d'armement dans l'espace aérien pour soutenir les troupes au sol (contrôle de l'appui aérien)) et les systèmes contre drone (protection des unités contre les attaques par drones)
  - remplacement des drones tactiques et des capacités de purification d'eau
  - mise en conformité de la capacité de déminage aux exigences OTAN

- Air :
  - axe en développement et significatif pour atteindre les objectifs de défense, dont la croissance de l'effort de défense et de contributions opérationnelles à haute plus-value
  - capacités stratégiques A400M[10] et MRTT[11]
  - remplacement des aéronefs AWACS[12] par la capacité AFSC (« Alliance Future Surveillance and Control »)[13]
  - maintien du soutien substantiel de la Défense au programme drone AGS[14]
  - études d'opportunités de renforcement de la défense anti-aérienne « Anti-Access/Area Denial » (A2/AD)
  - contribution aux missions « Search and Rescue » (SAR) - missions de recherche et de sauvetage d'aéronefs en détresse – avec les hélicoptères H-145M

- Space (Espace) :
  - mise en œuvre de la stratégie sectorielle décrite dans la première stratégie spatiale de défense de 2022 autour de quatre axes de développement :

  1. consolider les capacités spatiales actuelles, 2. soutenir une liberté d'action dans et à partir de l'espace, 3. favoriser la coopération nationale et internationale, 4. attirer et fidéliser une main d'œuvre qualifiée et motivée

[7] Organisation des Nations unies
[8] Véhicules de commandement, de liaison et de reconnaissance – cf. dossier parlementaire 7852
[9] Joint Terminal Attack Controller
[10] Avion de transport militaire polyvalent Airbus A400M Atlas – cf. dossier parlementaire 7979
[11] Multi-Role Tanker Transport – avion militaire de transport et de ravitaillement Airbus A330 – cf. dossier parlementaire 7513
[12] Airborne Warning and Control System – Système aéroporté de détection et de contrôle
[13] https://www.nato.int/cps/en/natohq/news_195803.htm
[14] Alliance Ground Surveillance – Capacité alliée de surveillance terrestre ; https://www.nato.int/cps/fr/natohq/topics_48892.htm

- poursuite des programmes existants, tels que WGS[15], GovSat[16] et LUXEOSys[17]
- développement du nouveau programme MGS[18], lequel sera réalisé avec les États-Unis d'Amérique avec, comme prestataire de services, la SES[19]

- Cyber :
  - mise en œuvre de la stratégie sectorielle de 2021, qui s'étend sur dix ans et se situe dans le cadre de la stratégie nationale de cybersécurité, visant notamment à renforcer la résilience de la Défense luxembourgeoise : « Dans cette perspective, la stratégie met l'accent sur l'amélioration des compétences du 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.

    L'objectif à long terme de la stratégie consiste à garantir que le Luxembourg dispose d'une des défenses les plus cybersécurisées grâce à la maximisation des capacités de cyberdéfense.

    La cyberdéfense est en train de forger sa place dans les forces armées ainsi qu'au sein du paysage de la cybersécurité du Grand-Duché. Les objectifs stratégiques suivants ont été retenus en matière de mise en œuvre : - attirer et fidéliser une main d'œuvre qualifiée et motivée ; - renforcer davantage la coopération nationale et internationale dans le domaine cyber ; - intégrer la cyberdéfense dans l'ensemble des activités, des actifs et de la culture de la Défense luxembourgeoise ; - cartographier un paysage « Cyber Futures », identification des priorités identifiées et programme de recherche enclenchés. » [20]
  - En étroite coopération avec la NSPA[21] a été lancé le projet « Luxembourg Cyber Defence Cloud » (LCDC)[22].
  - La Défense et l'Université du Luxembourg, avec d'autres collaborateurs publics et privés, ont lancé un projet de mise en place d'un Centre national de compétences en recherche sur la cybersécurité et la cyberdéfense (« National Competence Hub in Research in Cybersecurity and Cyber Defence »).

Des efforts additionnels et complémentaires sont nécessaires pour la réalisation des objectifs fixés dans le cadre des axes prioritaires du développement capacitaire :

- développement de la communication stratégique, laquelle « contribuera activement aux efforts de dissuasion en véhiculant le message d'une défense crédible »
- développement de la présence de cadres dans des États-majors internationaux et des organismes multinationaux : « L'insertion de cadres dans différentes structures de commandement et de contrôle, que ce soit au niveau de l'OTAN, de l'UE, de l'ONU ou d'autres organes, tels que le Corps européen, l'EATC[23], ou encore le Centre d'excellence Espace de l'OTAN, est une obligation découlant directement des missions de l'Armée sur le plan internationales telles qu'arrêtées par la loi. »[24]
- vérification et contrôle de l'exécution des traités multinationaux par l'Agence de contrôle des armements du Benelux (BACA)

[15] Wideband Global Satellite Communications System
[16] https://govsat.lu/
[17] Luxembourg Earth Observation System – dossier parlementaire 7542
[18] Medium Earth Global Services – dossier parlementaire 8157
[19] Société Européenne des Satellites - https://www.ses.com/fr/press-release/le-luxembourg-annonce-son-intention-dexploiter-le-systeme-o3b-mpower-de-ses-pour
[20] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, pp. 52 et 53
[21] NATO Support and Procurement Agency
[22] Dossier parlementaire 8167
[23] European Air Transport Command, https://eatc-mil.com/en
[24] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 55

- développement de la médecine militaire, d'une capacité « medical surgical team » (Med-ST) en réponse aux exigences de l'OTAN, en étroite collaboration avec la Belgique et la France
- mobilité militaire : « Outre la dimension du soutien logistique au profit du bataillon binational, la démarche de la création d'un hub militaire multimodal (M3H) s'inscrira dans le cadre du mécanisme de développement capacitaire de l'UE, où la mobilité militaire renforcée, tant à l'extérieur qu'au sein du territoire de l'UE, figure comme secteur prioritaire (focus area). Dans le sillage de cette logique, le Luxembourg s'engage dans le projet PESCO « Network of Logistic Hubs in Europe and Support to Operations». L'objectif central de ce projet est d'établir et d'exploiter un réseau de plate-formes logistiques (« Logistics Hubs » ou « LogHubs ») en Europe. Dans un contexte plus large encore, agencé par la refonte des mécanismes de dissuasion et de défense sur le continent européen, un M3H luxembourgeois se destine potentiellement comme maillon clé en termes d'appuis de la nation hôte ou de transit au sein du réseau de renforcement et de soutien établi au profit des forces de l'OTAN. Concrètement, cette capacité visera à faciliter l'activation, le renforcement et le maintien en puissance des forces de l'Alliance en cas de besoin. »[25]
- rénovation des infrastructures militaires nationales, de la WSA[26] et de la NSPA, dont le Luxembourg est le pays hôte.

Pour réussir les défis, les Lignes directrices soulignent l'importance « de montrer un engagement politique avec une vision claire sur le long terme et d'arbitrer en continu entre les objectifs et les ressources disponibles. (…) La Défense continuera à évoluer à travers différentes formes de coopération dans les grands ensembles multinationaux. » et harmonisera son horizon stratégique avec celui de ses partenaires. « La Défense continuera à s'appuyer sur les mécanismes de planification de l'OTAN et de l'UE. »

- Les efforts à faire nécessitent une augmentation du personnel et des qualifications de celui-ci en raison de la complexité croissante du métier militaire.
- Il importe de veiller à préserver une autonomie décisionnelle suffisante. L'objectif capacitaire primaire de l'Armée, le bataillon de reconnaissance belgo-luxembourgeois, répond au principe de solidarité, mais entraîne aussi une réduction de l'autonomie décisionnelle.
- L'augmentation significative de l'effort de défense exige une utilisation efficace des moyens budgétaires, notamment à ce que les programmes retenus apportent une plus-value au Luxembourg et soient donc « à double usage idéalement ».
- Comme l'indiquent les Lignes directrices, « Un effort de défense cohérent et durable va de pair avec une anticipation stratégique s'étendant idéalement sur plusieurs décennies. En effet, le temps nécessaire pour bâtir des capacités militaires crédibles oblige à regarder loin. Or, il y a des limites objectives à tout effort de prospective. Afin d'être en mesure d'élaborer des recommandations concrètes et spécifiques, et aussi en temps utile, il importe d'harmoniser notre horizon stratégique avec celui de nos partenaires. ».
- L'accès aux technologies de pointe est un « réel défi auquel il s'agira de répondre en premier lieu par le développement, sinon le renforcement des partenariats existants. (…) Cet accès est d'autant plus important pour garantir l'interopérabilité et donc l'intégration des futures systèmes d'armes et de capacités de défense. ».
- La sécurité énergétique et des approvisionnements doit également être préservée.
- Parallèlement à la promotion de la coopération UE-OTAN, il importe de développer une autonomie européenne de défense.

Discussion

[25] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, pp. 57 et 58
[26] Warehouses Service Agency

❖ Constatant que les projets en cours depuis des années sont poursuivis, M. Jean-Marie Halsdorf (CSV) souhaiterait obtenir des précisions supplémentaires sur la médecine militaire.

Confirmant que certains projets, comme GovSat, existaient déjà, mais sans faire partie d'une stratégie globale, Monsieur le Ministre souligne que des projets nouveaux sont venus s'ajouter.

En ce qui concerne la médecine militaire, l'Armée et la Direction de la Défense dépendent du Ministère de la Santé. Pendant la crise de la COVID-19, le concept initial d'un hôpital militaire s'est avéré inapproprié aux besoins en cas de crise sanitaire. La Défense a alors cédé le lead à la Direction de la Santé pour élaborer un projet, à la condition que celui-ci réponde aux exigences de l'OTAN. En outre, il est difficile de trouver des médecins, surtout des spécialistes, d'autant plus qu'ils seront fonctionnaires touchant le traitement correspondant. Pour ces raisons, la médecine militaire n'est actuellement pas incluse dans l'effort de défense visé d'1%.

❖ - Le Luxembourg semblant coopérer principalement avec la Belgique, M. Claude Wiseler (CSV) voudrait apprendre plus sur la coopération avec ses autres voisins, la France et l'Allemagne.

Monsieur le Ministre rappelle que « Le « *NATO Defence Planning Process* » (NDPP) et le « *Capability Development Plan* » (CDP) de l'UE, demeurent les principales références pour orienter le développement capacitaire national. ».

Le LtCol Schons fait savoir que les systèmes antichar et les systèmes d'armement lourd font actuellement l'objet de négociations avec la France. Quant à l'Allemagne, l'Armée continue la bonne coopération avec ce partenaire dans le cadre du « Framework Nations Concept » (FNC) en matière de reconnaissance et pourrait le faire aussi avec ses drones tactiques et sa capacité de purification d'eau, les Lignes directrices indiquant que celle-ci et les drones pourront être rattachés à une unité d'un partenaire[27].

Dans le domaine Air, le programme MRTT avait été lancé en 2016 par les Pays-Bas et le Luxembourg, rejoints entretemps par l'Allemagne, la Norvège, la Belgique et la République tchèque. La capacité AFSC remplaçant les avions AWACS réunit quasiment tous les partenaires OTAN. Le programme AGS réunit une quinzaine de membres de l'OTAN.

Dans le domaine Espace, le Luxembourg coopère surtout avec les États-Unis d'Amérique. Concernant le satellite de reconnaissance NAOS[28], il a été construit par OHB Italia.

Dans le domaine Cyber, des discussions sont menées notamment avec l'Allemagne.
Les 25 et 26 avril 2023 a eu lieu la conférence « Luxembourg Autonomous Weapons Systems » (LAWS) avec la participation de nombreux États.

En réponse à la question de M. Wiseler relative au choix des systèmes d'armement, le LtCol Schons explique que le choix se fait en fonction de la digitalisation. Ces systèmes sont ou seront interopérables et le choix est dès lors limité. Ainsi, pour le bataillon de reconnaissance belgo-luxembourgeois, les véhicules en voie d'acquisition par la Belgique dans le cadre du partenariat stratégique franco-belge CaMo (Capacité Motorisée) sont étroitement liés au programme français SCORPION, de sorte que les nouveaux véhicules luxembourgeois

[27] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 47
[28] National Advanced Optical System

CLRV seront également équipés du système SCORPION. L'interopérabilité avec les Allemands se fera alors avec d'autres systèmes.

Le Gen Thull ajoute que les objectifs définis par le NDPP consistent à doter l'Alliance des capacités dont elle a besoin. Pour le Luxembourg, l'objectif retenu est l'augmentation des capacités de reconnaissance, celle-ci devant évoluer d'une reconnaissance légère à une reconnaissance de type médian. L'OTAN ne prescrit normalement pas le partenaire, mais a fait une exception ici en exigeant la création et l'exploitation commune d'un bataillon de reconnaissance belgo-luxembourgeois. Comme la Belgique, dont la taille ne permet pas non plus de satisfaire seule aux différentes exigences, a pris la décision de coopérer avec la France, le Luxembourg a choisi le même programme français.

Monsieur le Ministre fait remarquer que le choix des programmes et équipements ne se pose pas aux États-Unis d'Amérique comme aux partenaires européens, où les pays disposant d'une industrie d'armement et d'entreprises dans les domaines concernés se trouvent en situation de concurrence.

- Le même député voudrait également obtenir des explications plus détaillées sur le changement fondamental, en ce qui concerne la composante aérienne, par rapport aux Lignes directrices de la Défense luxembourgeoise à l'horizon 2025.

Monsieur le Ministre rappelle que les Lignes directrices précitées annonçaient ceci : « Actuellement, l'aéroport du Findel est déjà utilisé, de façon ponctuelle, à des fins militaires. La défense envisage l'implantation d'une zone gouvernementale dans l'enceinte de l'aéroport du Findel, qui pourrait prendre la forme d'un hangar permettant de stationner et d'assurer la maintenance des futurs aéronefs acquis par la défense, en coopération avec les partenaires nationaux. ». Or, il n'y a pas de place suffisante pour réaliser ce projet. Le Luxembourg met dès lors l'accent sur les partenariats et la mutualisation des ressources (« pooling & sharing »). Les nouvelles Lignes directrices indiquent que « Peu de pays ont la capacité de mener des opérations complexes d'envergure significative. Tenant compte de nos limitation structurelles, nos partenariats internationaux de référence – Belgique, Pays-Bas, France, Allemagne et les Etats-Unis ainsi que la NATO Support and Procurement Agency (NSPA), Agence européenne de défense (AED), Organisation Conjointe de Coopération en matière d'Armement (OCCAr), etc. – sont indispensables. Ces partenariats sont le garant de notre plus-value opérationnelle et mutuelle ainsi que de notre crédibilité.

Sans être exhaustif, il y a lieu de mentionner ici les participations du Luxembourg aux programmes multinationaux tels que A400M, « Multi-Role Tanker Transport » (MRTT), « Allied Ground Surveillance » (AGS), « Airborne Warning and Control System » (AWACS), etc. qui sont des réalités aujourd'hui et qui continuent à gagner en importance. Ils permettent notamment de répondre aux ambitions et exigences de l'OTAN ainsi que de l'UE. ».

❖ M. Marc Goergen (Piraten) souhaitant savoir comment l'augmentation des effectifs et l'acquisition du matériel nécessaires pour atteindre un effort de défense d'1% du PIB peuvent être réalisées dans les délais fixés, Monsieur le Ministre confirme que le recrutement de personnel s'avère le plus difficile. Comme le Luxembourg se spécialise dans certains domaines, il convient de recruter des spécialistes. Au niveau de la rémunération, le secteur privé représente une concurrence sérieuse pour le recrutement de spécialistes en informatique. La future loi sur l'organisation de l'Armée joue ici un rôle essentiel, notamment par la création des carrières A2 et B1.

L'expert informaticien de la Défense relate qu'il vient du secteur privé, où des salaires très élevés sont effectivement payés à partir d'un certain niveau de compétences. Or, la motivation revêt une grande importance surtout chez les jeunes informaticiens. La défense offre une sphère d'activité qu'on ne trouve pas dans le secteur privé. Cet argument a permis

de mettre en place une équipe solide au sein de la Défense. En outre, des efforts sont entrepris, avec le soutien du Luxembourg House of Cybersecurity, pour inciter à l'école plus de jeunes, aussi plus de filles, à choisir l'informatique. Il importe aussi de rendre attentif au traitement plus élevé dans la Fonction publique en début de carrière, ce qui constitue aussi une motivation qu'il convient de sauvegarder par la suite.

❖ - Mme Stéphanie Empain (déi gréng) voudrait être éclairée sur la BACA (cf. p. 6).

Le Gen Thull renvoie à l'OSCE qui a élaboré en matière de maîtrise des armements le Document de Vienne sur les mesures de confiance et de sécurité[29] prévoyant une série de mécanismes de contrôle. Ceux-ci étaient gérés par le Luxembourg par le GIVO – Groupement d'inspecteurs vérificateurs et observateurs. Le Luxembourg a ensuite emprunté la voie multinationale et a mis en place avec la Belgique et les Pays-Bas la BACA (Benelux Arms Control Agency) installée en Belgique. La BACA est chargée de la mise en œuvre des contrôles d'armements à l'étranger, incluant en particulier le Traité sur les Forces armées conventionnelles en Europe (FCE – CFE Treaty on Conventional Armed Forces in Europe). Le Luxembourg a un représentant auprès de la BACA qui en a assuré la présidence les deux dernières années.

- Selon la même députée, l'importance des Lignes directrices réside dans la cohérence des investissements et dans la prévisibilité pour l'Armée de l'évolution de la défense et donc de son propre développement. Se pose la question de la flexibilité des Lignes directrices pour s'adapter à des imprévus ou des changements d'orientation politique.

Monsieur le Ministre assure que les Lignes directrices sont suffisamment flexibles pour tenir compte de changements de la situation de sécurité. Cependant, le gros se base sur des éléments capacitaires auxquels sera attachée une importance de plus en plus grande. Ainsi, de gros investissements sont effectués dans le domaine Cyber, par exemple, lequel ne nécessite toutefois pas tant de main d'œuvre que d'autres domaines. Le gros des Lignes directrices devrait pouvoir s'exécuter sur toute la période prévue, donc jusqu'en 2035, la flexibilité nécessaire pour s'adapter à l'évolution de la situation de sécurité concernera en particulier l'Armée.

Le Gen Thull déclare que les premiers changements seront couverts par les Lignes directrices.

2. Projet de loi 8157

En réponse à une question de M. Marc Goergen concernant l'opérationnalité du programme, une représentante ministérielle fait savoir qu'en décembre dernier, deux des onze satellites de la constellation O3b mPower ont été lancés ; le prochain lancement est prévu pour le mois prochain. La constellation devrait être opérationnelle d'ici la fin de l'année.

La commission adopte le rapport en sa majorité (ADR : abstention) et propose comme temps de parole le modèle de base.

3. Projet de loi 8167

La commission désigne sa présidente rapportrice du projet de loi.

L'avis du Conseil d'État ne donne pas lieu à observation.

[29] https://www.osce.org/fr/arms-control

Procès-verbal approuvé et certifié exact

Annexe : Présentation PowerPoint « Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 »

Lignes directrices de la Défense luxembourgeoise à l'horizon 2035

Commission de la Sécurité intérieure et de la Défense
Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

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

Direction de la défense

8167 - Dossier consolidé : 56

Agenda

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

1. Introduction
2. Nouvelles Lignes directrices
3. Questions & Réponses

1. Introduction

- Travail prévu par l'accord de coalition de 2018
- Actualisation nécessaire suite à :
  - Nouveaux objectifs capacitaires otaniens de 2021
  - Bouleversement profond de la stabilité politique et sécuritaire mondiale
  - Objectif du gouvernement d'atteindre un effort de défense de 1% vers 2028
  - Boussole stratégique de l'UE en matière de sécurité et de défense (2022)
  - Concept stratégique de l'OTAN de 2022
- Réalisée par la Direction de la défense et l'Etat-Major de l'Armée
- Versions française et anglaise

2. Lignes directrices 2035

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

1. Résumé exécutif
2. Pourquoi une actualisation
3. Evolution de la situation internationale et les implications
4. Finalités de la politique de défense du Luxembourg
5. Principes structurants de la politique de défense du Luxembourg
6. Objectifs à atteindre
7. Axes prioritaires du développement capacitaire
8. Efforts additionnels et complémentaires
9. Défis

Pourquoi une actualisation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Contexte, cadre et orientations de la politique de défense
- Références OTAN et UE de 2022 : concept stratégique et boussole stratégique
- Objectif national d'un effort équivalent à 1% du PIB à l'horizon 2028
- Projet de loi pour nouvelle loi-cadre de l'Armée en procédure

Evolution de la situation internationale et implications

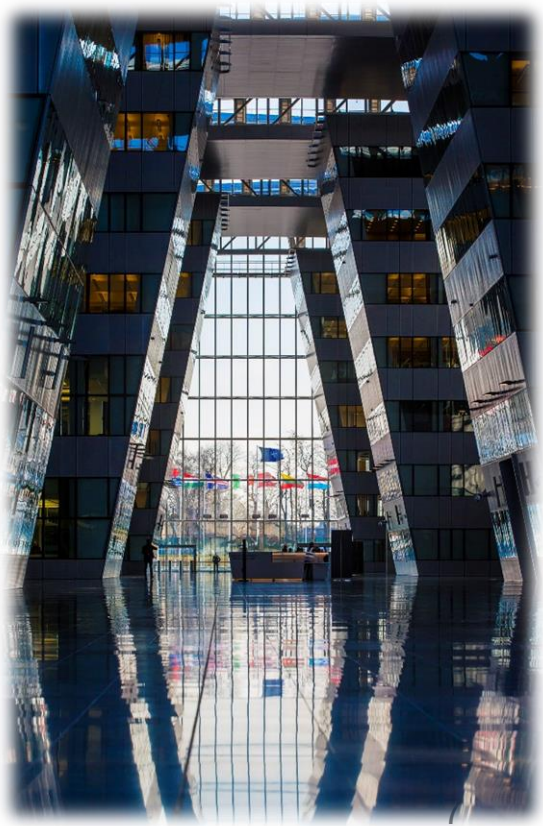
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Tendances sous-jacentes influençant la politique de défense
  - Contestation de l'ordre international fondé sur le règles et érosion des normes
  - Impact de la technologie
  - Risques sécuritaires liés aux changements environnementaux
- Menaces
  - Conventionnelles et nucléaires
  - Asymétriques et hybrides
  - Cyber
- Appréciation de l'environnement stratégique
  - Guerre d'agression russe contre l'Ukraine et politique chinoise assertive
  - Menaces conventionnelles = point focal
  - Nouvelles formes de menaces: Emerging Disruptive Technologies (EDT), Lethal Autonomous Weapons Systems (LAWS)
  - Impact de la crise climatique et environnementale
  - Besoin de transformations et d'objectifs stratégiques adaptés

Finalités de la politique de défense du Luxembourg

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Promotion de nos valeurs à l'échelle mondiale
- Préservation des intérêts essentiels de sécurité du Luxembourg à travers le système multilatéral basé sur le droit international
- A travers la Défense, dans son ensemble, le Luxembourg:
  - apporte sa part à la réponse globale de l'UE, l'OTAN, l'ONU et l'OSCE face aux défis de sécurité et de défense
  - contribue à la posture de dissuasion et de défense, essentielle pour préserver la paix, et au partage équitable du fardeau
  - soutient des mesures de confiance et de sécurité (OSCE)
  - contribue à une approche intégrée nationale



© NATO

Principes structurants de la politique de défense

- Solidarité
- Autonomie décisionnelle
- Partenariat transatlantique
- Adaptabilité et spécificité militaire
- Partenariats et mutualisation des ressources (« *pooling & sharing* »)
- Engagement pour la société luxembourgeoise
- Politique étrangère et de sécurité des « 3D » – diplomatie, défense, développement

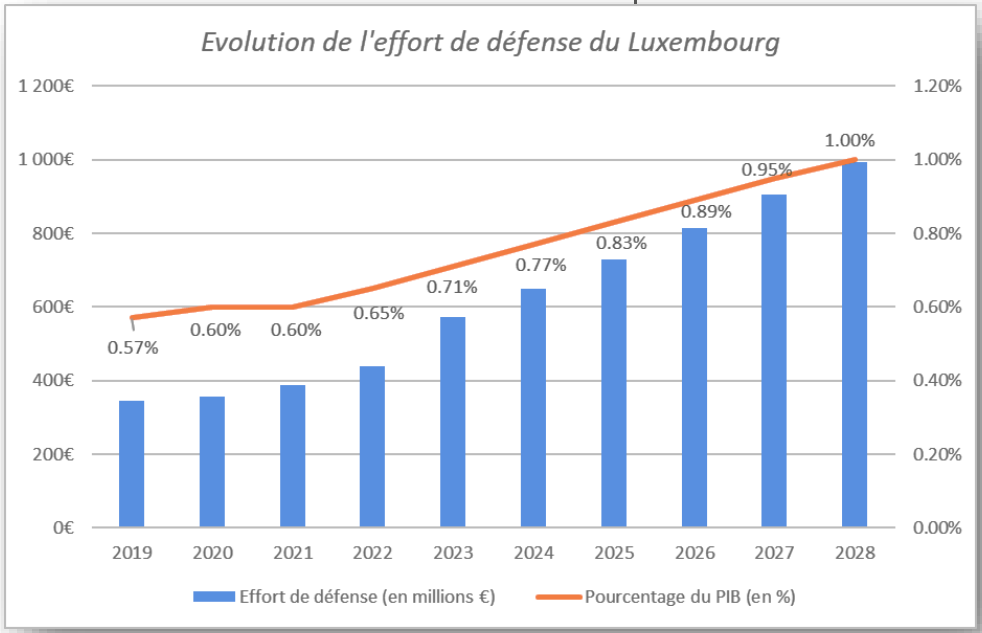
Objectifs à atteindre 1/2

- Développer des capacités, tout d'abord des forces
- Evolution possible des objectifs en fonction de l'environnement sécuritaire et des ressources humaines
- Sur le plan:
  - Organisationnel:
    - Augmentation des effectifs
    - Développement des capacités (communication, commandement, soutien, formation, entrainement et simulation)
  - Capacitaire:
    - Politique de développement capacitaire saine pour augmenter réactivité, puissance, résilience et opération en réseau
    - Double usage
  - Opérationnel:
    - Contribution aux opérations pour le maintien de la paix et aux missions de prévention ainsi que de gestion de crise
    - Contribution aux exercices et déploiements pour renforcer la posture de dissuasion et de défense sur territoire de l'Alliance
    - Contribution aux forces de réaction rapide
    - Assurer l'exécution des missions nationales et renforcement de la résilience
    - Contribuer à des engagements de prévention de conflits et de stabilisation
    - Contribuer à des opérations de secours et d'aide humanitaire

Objectifs à atteindre 2/2

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Effort de défense:
  - augmentation substantielle vers 1% du PIB au plus tôt à l'horizon 2028
  - 2% de l'effort de défense dédiés à la recherche et au développement dès cette année
- Prévention des risques sécuritaires liés aux changements environnementaux
  - Réduire d'au moins 45% les émissions de gaz à effet de serre vers 2030 et viser « net zero » vers 2050
  - Contribuer au « climate change and security action plan » de l'OTAN et mise en œuvre du Plan national intégré en matière d'énergie et de climat (PNEC)
- Approfondir la multinationalisation
- Soutenir la recherche et l'industrie
- Accroître le taux de féminisation



Axes prioritaires du développement capacitaire 1/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Terre:

- Développement des capacités de reconnaissance terrestres
- Accent sur mise en place et l'exploitation conjointe de l'objectif du bataillon binational de reconnaissance de combat médian, en coopération étroite avec FRA, et un renforcement d'une centaine de personnels pour l'Armée
- Réintégration des capacités antichar à moyenne portée
- Introduction de nouvelles capacités de reconnaissance
  - contrôleur aérien avancé
  - contre drones
  - protection contre les munitions rôdeuses
- Evolution et remplacement des drones tactiques et capacités de purification d'eau actuelles
- Capacité de déminage conformément aux exigences OTAN

8167 - Dossier consolidé : 66

Axes prioritaires du développement capacitaire 2/4

Air:

- Axe significatif pour croissance de l'effort de défense et de contributions opérationnelles à haute valeur ajoutée
- Capacités stratégiques A400M et MRTT
- Plates-formes plus légères à envisager dans cadre Benelux ou FNC
- Remplacement des AWACS par AFSC
- Maintien du soutien substantiel à AGS (drones stratégiques de l'OTAN), ainsi que des capacités ISR aériennes maritimes et d'évacuation médicales contractées
- Étude d'opportunités de:
  - Renforcement de la défense anti-aérienne (anti-access/area denial) dans cadre multinational
- Contribution aux capacités « Search and Rescue » sur base de la plate-forme H145M

© NATO

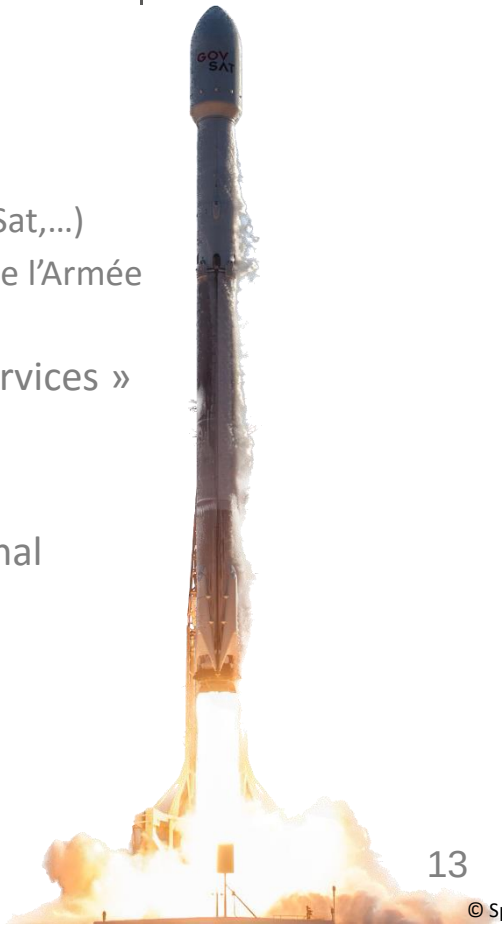
© Multinational MRTT Fleet

Axes prioritaires du développement capacitaire 3/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Espace:

- Mise en œuvre de la stratégie sectorielle de 2022
- Poursuite:
  - des activités de communications satellitaires sécurisées (WGS, GovSat,…)
  - du développement des capacités de communications déployables de l'Armée (p.ex missions EUTM Mozambique et MINUSMA)
- Développement du programme « Medium Earth Orbit Global Services » (MGS)
- Mise en œuvre et suivi du programme LUXEOSys
- Renforcer coopération en matière de capacités « Space Situational Awareness »



© SpaceX

Axes prioritaires du développement capacitaire 4/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Cyber:

- Mise en œuvre de la stratégie sectorielle de 2021, s'appuyant sur la stratégie nationale de cybersécurité
- Objectif à long terme : une des défenses les plus cybersécurisées
- Coopération avec NSPA pour le « Luxembourg Cyber Defence Cloud » (LCDC) et la « Cyber Range »
- Coopération Défense et Université du Luxembourg – Projet « National Competence Hub in Research in Cybersecurity and Cyber Defence »

LUXEMBOURG CYBERDEFENCECLOUD

CYBER RANGE LUXEMBOURG

Efforts additionnels et complémentaires

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Communication stratégique
- Etats-majors internationaux et organismes multinationaux
- Vérification et contrôle de l'exécution des traités multinationaux

- Médecine militaire
- Mobilité militaire
- Rénovation des infrastructures militaires nationales, NSPA et WSA

8167 - Dossier consolidé : 70

Défis

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Engagement politique sur le long terme,

horizon stratégique harmonisé avec partenaires, OTAN et UE

- Ressources humaines
- Autonomie décisionnelle
- Augmentation de l'effort de défense
- Processus d'anticipation stratégique
- Accès aux technologies de pointe
- Sécurité énergétique et des approvisionnements
- Autonomie européenne de défense et coopération UE-OTAN renforcée

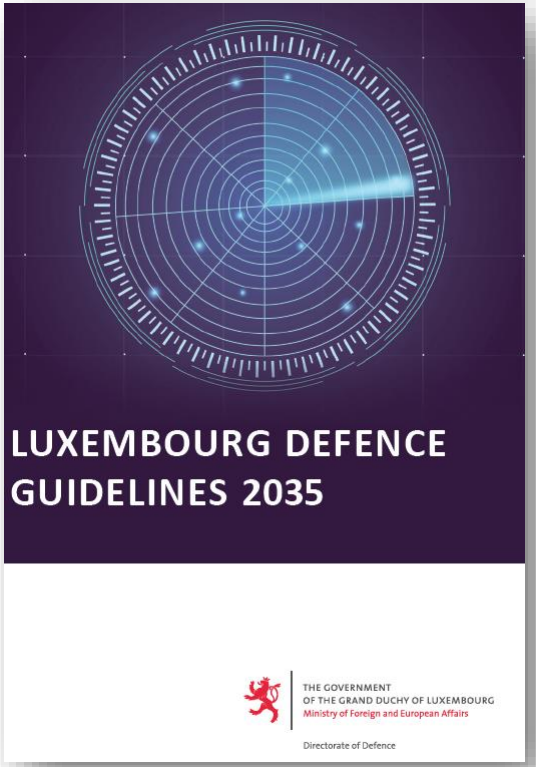
8167 - Dossier consolidé : 71

3. Questions et réponses

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

➢ Questions?


LIGNES DIRECTRICES DE LA DEFENSE LUXEMBOURGEOISE A L'HORIZON 2035
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères et européennes
Direction de la Défense


LUXEMBOURG DEFENCE GUIDELINES 2035
THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign and European Affairs
Directorate of Defence

33

CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session ordinaire 2022-2023

MW/PR

P.V. SID 25
P.V. AEECA 33

Commission de la Sécurité intérieure et de la Défense

Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

Procès-verbal de la réunion du 11 mai 2023

Ordre du jour :

1. Présentation des nouvelles Lignes directrices de la défense

2. Uniquement pour les membres de la Commission de la Sécurité intérieure et de la Défense

   8157 Projet de loi autorisant le Gouvernement à financer le programme « Medium Earth Orbit Global Services » (MGS)
   - Rapportrice : Madame Stéphanie Empain

   - Adoption d'un projet de rapport

3. 8167 Projet de loi autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

   - Désignation d'un rapporteur
   - Examen de l'avis du Conseil d'État

*

Présents : Mme Diane Adehm, M. André Bauler, M. François Benoy, Mme Stéphanie Empain, M. Léon Gloden, M. Marc Goergen, M. Max Hahn, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, Mme Lydia Mutsch, membres de la Commission de la Sécurité intérieure et de la Défense

Mme Nathalie Oberweis, observatrice déléguée

Mme Simone Beissel, Mme Djuna Bernard, M. Yves Cruchten, M. Emile Eicher, Mme Stéphanie Empain, M. Jean-Marie Halsdorf, M. Fernand Kartheiser, M. Laurent Mosar, Mme Lydia Mutsch, Mme Nathalie Oberweis, Mme Lydie Polfer, M. Claude Wiseler, membres de la Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

M. François Bausch, Ministre de la Défense

Mme Nina Garcia, Coordinatrice générale Défense, M. Tom Köller, Directeur, LtCol Tom Schons, Chef du Département Planification stratégique, M. Alain Charlier, M. Ben Fetler, M. Michael Schuster, Direction de la Défense, du Ministère des Affaires étrangères et européennes

Lëtzebuerger Arméi :

Gen Steve Thull, Chef d'État-Major

Mme Marianne Weycker, de l'Administration parlementaire

Excusés : Mme Nancy Arendt épouse Kemp, membre de la Commission de la Sécurité intérieure et de la Défense

M. Marc Spautz, membre de la Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

M. Jean Asselborn, Ministre des Affaires étrangères et européennes

*

Présidence : Mme Stéphanie Empain, Présidente de la Commission de la Sécurité intérieure et de la Défense

*

1. Présentation des nouvelles Lignes directrices de la défense

Après quelques mots introductifs de Madame la Présidente, Monsieur le Ministre présente les Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 (désignées ici par « les Lignes directrices »), document adopté par le Conseil de gouvernement le 28 avril 2023. L'élaboration a pris deux ans, certains éléments importants ayant nécessité du temps pour devenir réalité et visant aussi un horizon plus lointain. Suivant l'accord de coalition 2018-2023 :

« La continuité de la politique de défense nationale contribue à assurer la confiance légitime que le Luxembourg doit susciter auprès de ses partenaires européens. La poursuite de la mise en œuvre des « Lignes Directrices de la Défense à l'horizon 2025 et au-delà » constituera le fil rouge du développement de l'Armée luxembourgeoise. Cette stratégie ambitieuse consacre la continuité des missions de l'Armée, assure la participation du secteur privé, s'oriente sur les priorités des lacunes capacitaires européennes et prend en compte les capacités à double-usage civile et militaire. Elle sera mise à jour à mi-mandat afin de tenir compte de l'évolution des contextes national et international. ».

Les Lignes directrices revêtent également une importance particulière en raison de la situation de sécurité moins bonne par rapport à celle en 2017, où les « Lignes directrices de la défense luxembourgeoise à l'horizon 2025 et au-delà » ont été présentées. Par ailleurs, l'OTAN[1] a adopté en automne 2021 des objectifs capacitaires qui engendrent, entre autres, comme conséquence pour le Luxembourg la création du bataillon de reconnaissance belgo-luxembourgeois.

[1] Organisation du Traité de l'Atlantique Nord

La situation de sécurité est marquée principalement par la guerre en Ukraine. S'y ajoutent notamment les relations conflictuelles entre l'OTAN et la Chine, de même que le changement climatique qui génère des conflits pour l'accès à des ressources, telles l'eau ou des énergies fossiles.

La discussion sur l'effort de défense continue. En 2014, l'OTAN a recommandé dans sa déclaration du sommet du Pays de Galles un niveau minimum de dépenses de défense de 2% du PIB[2]. Les Alliés, dont la part du PIB est inférieure à ce niveau recommandé par la directive OTAN, « - cesseront toute diminution des dépenses de défense ; - chercheront à augmenter leurs dépenses de défense en termes réels à mesure que croîtra leur PIB ; - chercheront à se rapprocher dans les dix années à venir des 2% recommandés, en vue d'atteindre leurs objectifs capacitaires OTAN et de combler les insuffisances capacitaires de l'OTAN ». Aujourd'hui, 2% du PIB sont considérés plutôt comme minimum et certains pays sont d'avis que l'effort de défense devrait augmenter jusqu'à 2,5%, voire 3%. Monsieur le Ministre regrette que la discussion soit menée sans poser la question, en ce qui concerne certains pays, de l'objectif des dépenses et sans tenir compte de la situation spécifique de notre pays.

Les « Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 » sont d'abord le résultat d'une bonne coopération entre la Direction de la Défense et la Lëtzebuerger Armëi et ensuite aussi avec le Ministère des Affaires étrangères et européennes, la Représentation Permanente du Luxembourg auprès du Conseil de l'Atlantique Nord (OTAN) et le Haut-Commissariat à la Protection nationale (HCPN).

Monsieur le Ministre souligne que des Lignes directrices s'étendant sur 12 ans donnent à l'Armée une sécurité de planification. Le fait que le Luxembourg est le pays le plus riche de l'Union européenne (UE), en ce qui concerne le PIB et le revenu par habitant, lui confère une situation exceptionnelle. La croissance exceptionnelle au cours des dernières décennies n'était possible que grâce à l'intégration dans une architecture sécuritaire formée par des collectivités comme l'OTAN, les Nations unies, l'OSCE[3], l'UE, etc., dont le Luxembourg est membre. L'orateur met dès lors l'accent sur la solidarité du Luxembourg et la promotion de nos valeurs à l'échelle mondiale. De même, une autre finalité de la politique de défense luxembourgeoise est la préservation des intérêts essentiels de notre sécurité à travers le multilatéralisme basé sur le droit international. Dans ce contexte, le Luxembourg doit agir en tant que partenaire solidaire ; une politique crédible de défense et de dissuasion est essentielle pour préserver la paix. Tout aussi important est le soutien des mesures de confiance et de sécurité, celles-ci étant actuellement négligées (« Confidence and Security Building Measures »), alors qu'un rôle primordial revient à la prévention, puisque le but doit être l'empêchement de conflits.

Au cœur de la transformation de la défense luxembourgeoise se trouve la mise en place du bataillon binational mentionné ci-dessus. Ensuite, il y a trois domaines nouveaux, dans lesquels le Luxembourg se spécialise depuis quelques années : l'Espace, l'Air et le Cyber. Un autre chantier important constitue la future nouvelle loi-cadre sur l'Armée.

La défense se voit confrontée à de multiples défis qui risquent d'évoluer de plus en plus vite, ces défis ne provenant pas seulement du contexte géopolitique, mais aussi de la remise en cause, au moins en Europe, de l'ordre international fondé sur des règles.

Les menaces deviennent de plus en plus complexes : aux menaces conventionnelles et nucléaires s'ajoutent des menaces asymétriques et hybrides[4] et des menaces cyber. Les

[2] Produit intérieur brut
[3] Organisation pour la sécurité et la coopération en Europe
[4] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 20 : « Les actions hybrides sont un mélange d'activités coercitives et subversives, de méthodes traditionnelles (comme p.ex. diplomatiques, militaires, économiques) et non

changements environnementaux ont un double effet sur la sécurité : un effet sur le fonctionnement des armées, plus précisément sur leur manœuvrabilité, et sur les installations[5] et un effet d'aggravation des conflits pour l'accès aux ressources (cf. supra), engendrant aussi des afflux de réfugiés. En conséquence, il importe de procéder en matière de défense à des transformations et à une adaptation des objectifs stratégiques.

Afin d'atteindre les objectifs, la politique de défense suit les principes structurants suivants :

- la solidarité envers les partenaires ;
- l'autonomie décisionnelle, laquelle « porte d'abord sur la liberté des choix politiques stratégiques et ensuite sur le contrôle des activités opérationnelles et du cycle de vie des capacités » ;
- le partenariat transatlantique ;
- l'adaptabilité et la spécificité militaire ; il convient de rappeler que « L'adaptabilité et la spécificité du métier militaire impliquent que les forces armées ne peuvent pas être soumises en totalité aux mêmes règles et lois que celles applicables aux fonctionnaires et autres agents de l'État. Cela est dû à la nature unique de leurs missions, qui comprennent la maîtrise de situations d'urgence, l'engagement dans des opérations de maintien de la paix ainsi que la préparation au combat. Par conséquent, une législation spécifique est nécessaire pour réglementer les activités de l'Armée et garantir qu'elle puisse remplir ses obligations de manière efficace conformément aux normes éthiques et juridiques internationales applicables. Cette législation doit inclure des lois spécifiques sur le régime de travail, la discipline militaire, les procédures de conduite des opérations et les procédures de justice militaire. Il est important que cette législation soit révisée régulièrement pour qu'elle reste pertinente par rapport au milieu en constante mutation dans lequel l'Armée opère. » ;
- les partenariats et la mutualisation des ressources (« pooling and sharing »), ce qui se révèle aussi plus rentable et efficace ;
- l'engagement pour la société luxembourgeoise ;
- la politique étrangère et de sécurité des « 3D » : diplomatie, défense, développement.

L'objectif général est le développement des capacités, tout d'abord des forces, ensuite celles dans les domaines aérien, spatial et cyber. Les objectifs « pourront évoluer en fonction de la volatilité de l'environnement sécuritaire, que ce soit sur le plan international ou national, ceci dans la limite des contraintes légales – lois d'acquisitions – et budgétaires ».[6]

S'agissant en particulier de l'effort de défense, une augmentation substantielle est prévue pour atteindre 1% du PIB en 2028, ce qui fait une dépense d'1 milliard d'euros. Il ne s'agit pas d'une dépense unique, mais il importe de maintenir l'effort de défense à ce niveau. Dès l'année en cours, 2% de l'effort de défense sont consacrés à la recherche et au développement, spécialement dans le domaine des matériaux et des systèmes de propulsion.

Dans le cadre de la prévention des risques sécuritaires liés aux changements environnementaux, le niveau « net zero » d'ici 2050 est visé, tout en veillant à maintenir l'efficacité opérationnelle, militaire et économique.

---

conventionnelles (comme p.ex. utilisation abusive des réseaux sociaux, informations manipulées) utilisées de façon coordonnée par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs politiques, sans que le seuil d'une guerre officiellement déclarée ne soit atteint. La caractéristique de ces actions hybrides est que celles-ci sont difficilement attribuables à un acteur précis. En conséquence, le choix de réponse sera limité. Le fait que ces menaces ne peuvent être contrées dans leur totalité à tout moment, souligne l'importance de la résilience des outils étatiques, en particulier de la défense. »

[5] p. ex. inondation de la base aérienne d'Offutt (Nebraska) par la crue du Mississippi en 2019 ou encore dévastation de la base aérienne de Tyndall (Florida) par l'ouragan Michael en 2018

[6] Les objectifs sur le plan organisationnel, capacitaire et opérationnel sont détaillés aux pages 9 et 10 de l'annexe et aux pages 33 à 43 des Lignes directrices de la Défense luxembourgeoise à l'horizon 2035.

L'accroissement du taux de femmes dans l'Armée est un autre objectif. Les Lignes directrices indiquent que « La Défense appuie les programmes relatifs au développement du rôle des femmes dans la résolution des conflits. L'ONU[7] note que : « les femmes jouent un rôle déterminant dans la consolidation de la paix et notant que la participation pleine et concrète des femmes aux activités de prévention et de règlement des conflits et de reconstruction est intimement corrélée à l'utilité et à la viabilité à long terme de ces efforts, et soulignant à cet égard qu'il importe que les femmes participent sur un pied d'égalité avec les hommes à tout ce qui est entrepris pour maintenir et promouvoir la paix et la sécurité, et qu'il faut les associer davantage à la prise des décisions qui intéressent la prévention et le règlement des conflits et la consolidation de la paix, S/RES/2282 (2016) ». ».

Le « NATO Defence Planning Process » (NDPP) et le « Capability Development Plan » (CDP) de l'UE sont les principales références pour orienter le développement capacitaire national qui se compose de quatre axes prioritaires :

- Land (Terre) :
  - développement des capacités de reconnaissance terrestres
  - accent mis sur le bataillon binational (belgo-luxembourgeois) de reconnaissance de combat médian en coopération étroite avec la France

  Pour cela, l'Armée a besoin de renforts, dont du matériel plus lourd, en ce qui concerne les véhicules et l'armement → systèmes modernes antichar, remplacement des Dingos par les CLRV[8].
  - introduction de nouvelles capacités de reconnaissance, tels le contrôle aérien avancé (JTAC[9] - assure la coordination des systèmes d'armement dans l'espace aérien pour soutenir les troupes au sol (contrôle de l'appui aérien)) et les systèmes contre drone (protection des unités contre les attaques par drones)
  - remplacement des drones tactiques et des capacités de purification d'eau
  - mise en conformité de la capacité de déminage aux exigences OTAN

- Air :
  - axe en développement et significatif pour atteindre les objectifs de défense, dont la croissance de l'effort de défense et de contributions opérationnelles à haute plus-value
  - capacités stratégiques A400M[10] et MRTT[11]
  - remplacement des aéronefs AWACS[12] par la capacité AFSC (« Alliance Future Surveillance and Control »)[13]
  - maintien du soutien substantiel de la Défense au programme drone AGS[14]
  - études d'opportunités de renforcement de la défense anti-aérienne « Anti-Access/Area Denial » (A2/AD)
  - contribution aux missions « Search and Rescue » (SAR) - missions de recherche et de sauvetage d'aéronefs en détresse – avec les hélicoptères H-145M

- Space (Espace) :
  - mise en œuvre de la stratégie sectorielle décrite dans la première stratégie spatiale de défense de 2022 autour de quatre axes de développement :

  1. consolider les capacités spatiales actuelles, 2. soutenir une liberté d'action dans et à partir de l'espace, 3. favoriser la coopération nationale et internationale, 4. attirer et fidéliser une main d'œuvre qualifiée et motivée

[7] Organisation des Nations unies
[8] Véhicules de commandement, de liaison et de reconnaissance – cf. dossier parlementaire 7852
[9] Joint Terminal Attack Controller
[10] Avion de transport militaire polyvalent Airbus A400M Atlas – cf. dossier parlementaire 7979
[11] Multi-Role Tanker Transport – avion militaire de transport et de ravitaillement Airbus A330 – cf. dossier parlementaire 7513
[12] Airborne Warning and Control System – Système aéroporté de détection et de contrôle
[13] https://www.nato.int/cps/en/natohq/news_195803.htm
[14] Alliance Ground Surveillance – Capacité alliée de surveillance terrestre ; https://www.nato.int/cps/fr/natohq/topics_48892.htm

- poursuite des programmes existants, tels que WGS[15], GovSat[16] et LUXEOSys[17]
- développement du nouveau programme MGS[18], lequel sera réalisé avec les États-Unis d'Amérique avec, comme prestataire de services, la SES[19]

- Cyber :
  - mise en œuvre de la stratégie sectorielle de 2021, qui s'étend sur dix ans et se situe dans le cadre de la stratégie nationale de cybersécurité, visant notamment à renforcer la résilience de la Défense luxembourgeoise : « Dans cette perspective, la stratégie met l'accent sur l'amélioration des compétences du 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.

    L'objectif à long terme de la stratégie consiste à garantir que le Luxembourg dispose d'une des défenses les plus cybersécurisées grâce à la maximisation des capacités de cyberdéfense.

    La cyberdéfense est en train de forger sa place dans les forces armées ainsi qu'au sein du paysage de la cybersécurité du Grand-Duché. Les objectifs stratégiques suivants ont été retenus en matière de mise en œuvre : - attirer et fidéliser une main d'œuvre qualifiée et motivée ; - renforcer davantage la coopération nationale et internationale dans le domaine cyber ; - intégrer la cyberdéfense dans l'ensemble des activités, des actifs et de la culture de la Défense luxembourgeoise ; - cartographier un paysage « Cyber Futures », identification des priorités identifiées et programme de recherche enclenchés. » [20]
  - En étroite coopération avec la NSPA[21] a été lancé le projet « Luxembourg Cyber Defence Cloud » (LCDC)[22].
  - La Défense et l'Université du Luxembourg, avec d'autres collaborateurs publics et privés, ont lancé un projet de mise en place d'un Centre national de compétences en recherche sur la cybersécurité et la cyberdéfense (« National Competence Hub in Research in Cybersecurity and Cyber Defence »).

Des efforts additionnels et complémentaires sont nécessaires pour la réalisation des objectifs fixés dans le cadre des axes prioritaires du développement capacitaire :

- développement de la communication stratégique, laquelle « contribuera activement aux efforts de dissuasion en véhiculant le message d'une défense crédible »
- développement de la présence de cadres dans des États-majors internationaux et des organismes multinationaux : « L'insertion de cadres dans différentes structures de commandement et de contrôle, que ce soit au niveau de l'OTAN, de l'UE, de l'ONU ou d'autres organes, tels que le Corps européen, l'EATC[23], ou encore le Centre d'excellence Espace de l'OTAN, est une obligation découlant directement des missions de l'Armée sur le plan internationales telles qu'arrêtées par la loi. »[24]
- vérification et contrôle de l'exécution des traités multinationaux par l'Agence de contrôle des armements du Benelux (BACA)

[15] Wideband Global Satellite Communications System
[16] https://govsat.lu/
[17] Luxembourg Earth Observation System – dossier parlementaire 7542
[18] Medium Earth Global Services – dossier parlementaire 8157
[19] Société Européenne des Satellites - https://www.ses.com/fr/press-release/le-luxembourg-annonce-son-intention-dexploiter-le-systeme-o3b-mpower-de-ses-pour
[20] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, pp. 52 et 53
[21] NATO Support and Procurement Agency
[22] Dossier parlementaire 8167
[23] European Air Transport Command, https://eatc-mil.com/en
[24] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 55

- développement de la médecine militaire, d'une capacité « medical surgical team » (Med-ST) en réponse aux exigences de l'OTAN, en étroite collaboration avec la Belgique et la France
- mobilité militaire : « Outre la dimension du soutien logistique au profit du bataillon binational, la démarche de la création d'un hub militaire multimodal (M3H) s'inscrira dans le cadre du mécanisme de développement capacitaire de l'UE, où la mobilité militaire renforcée, tant à l'extérieur qu'au sein du territoire de l'UE, figure comme secteur prioritaire (focus area). Dans le sillage de cette logique, le Luxembourg s'engage dans le projet PESCO « Network of Logistic Hubs in Europe and Support to Operations». L'objectif central de ce projet est d'établir et d'exploiter un réseau de plate-formes logistiques (« Logistics Hubs » ou « LogHubs ») en Europe. Dans un contexte plus large encore, agencé par la refonte des mécanismes de dissuasion et de défense sur le continent européen, un M3H luxembourgeois se destine potentiellement comme maillon clé en termes d'appuis de la nation hôte ou de transit au sein du réseau de renforcement et de soutien établi au profit des forces de l'OTAN. Concrètement, cette capacité visera à faciliter l'activation, le renforcement et le maintien en puissance des forces de l'Alliance en cas de besoin. »[25]
- rénovation des infrastructures militaires nationales, de la WSA[26] et de la NSPA, dont le Luxembourg est le pays hôte.

Pour réussir les défis, les Lignes directrices soulignent l'importance « de montrer un engagement politique avec une vision claire sur le long terme et d'arbitrer en continu entre les objectifs et les ressources disponibles. (…) La Défense continuera à évoluer à travers différentes formes de coopération dans les grands ensembles multinationaux. » et harmonisera son horizon stratégique avec celui de ses partenaires. « La Défense continuera à s'appuyer sur les mécanismes de planification de l'OTAN et de l'UE. »

- Les efforts à faire nécessitent une augmentation du personnel et des qualifications de celui-ci en raison de la complexité croissante du métier militaire.
- Il importe de veiller à préserver une autonomie décisionnelle suffisante. L'objectif capacitaire primaire de l'Armée, le bataillon de reconnaissance belgo-luxembourgeois, répond au principe de solidarité, mais entraîne aussi une réduction de l'autonomie décisionnelle.
- L'augmentation significative de l'effort de défense exige une utilisation efficace des moyens budgétaires, notamment à ce que les programmes retenus apportent une plus-value au Luxembourg et soient donc « à double usage idéalement ».
- Comme l'indiquent les Lignes directrices, « Un effort de défense cohérent et durable va de pair avec une anticipation stratégique s'étendant idéalement sur plusieurs décennies. En effet, le temps nécessaire pour bâtir des capacités militaires crédibles oblige à regarder loin. Or, il y a des limites objectives à tout effort de prospective. Afin d'être en mesure d'élaborer des recommandations concrètes et spécifiques, et aussi en temps utile, il importe d'harmoniser notre horizon stratégique avec celui de nos partenaires. ».
- L'accès aux technologies de pointe est un « réel défi auquel il s'agira de répondre en premier lieu par le développement, sinon le renforcement des partenariats existants. (…) Cet accès est d'autant plus important pour garantir l'interopérabilité et donc l'intégration des futures systèmes d'armes et de capacités de défense. ».
- La sécurité énergétique et des approvisionnements doit également être préservée.
- Parallèlement à la promotion de la coopération UE-OTAN, il importe de développer une autonomie européenne de défense.

Discussion

[25] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, pp. 57 et 58
[26] Warehouses Service Agency

❖ Constatant que les projets en cours depuis des années sont poursuivis, M. Jean-Marie Halsdorf (CSV) souhaiterait obtenir des précisions supplémentaires sur la médecine militaire.

Confirmant que certains projets, comme GovSat, existaient déjà, mais sans faire partie d'une stratégie globale, Monsieur le Ministre souligne que des projets nouveaux sont venus s'ajouter.

En ce qui concerne la médecine militaire, l'Armée et la Direction de la Défense dépendent du Ministère de la Santé. Pendant la crise de la COVID-19, le concept initial d'un hôpital militaire s'est avéré inapproprié aux besoins en cas de crise sanitaire. La Défense a alors cédé le lead à la Direction de la Santé pour élaborer un projet, à la condition que celui-ci réponde aux exigences de l'OTAN. En outre, il est difficile de trouver des médecins, surtout des spécialistes, d'autant plus qu'ils seront fonctionnaires touchant le traitement correspondant. Pour ces raisons, la médecine militaire n'est actuellement pas incluse dans l'effort de défense visé d'1%.

❖ - Le Luxembourg semblant coopérer principalement avec la Belgique, M. Claude Wiseler (CSV) voudrait apprendre plus sur la coopération avec ses autres voisins, la France et l'Allemagne.

Monsieur le Ministre rappelle que « Le « *NATO Defence Planning Process* » (NDPP) et le « *Capability Development Plan* » (CDP) de l'UE, demeurent les principales références pour orienter le développement capacitaire national. ».

Le LtCol Schons fait savoir que les systèmes antichar et les systèmes d'armement lourd font actuellement l'objet de négociations avec la France. Quant à l'Allemagne, l'Armée continue la bonne coopération avec ce partenaire dans le cadre du « Framework Nations Concept » (FNC) en matière de reconnaissance et pourrait le faire aussi avec ses drones tactiques et sa capacité de purification d'eau, les Lignes directrices indiquant que celle-ci et les drones pourront être rattachés à une unité d'un partenaire[27].

Dans le domaine Air, le programme MRTT avait été lancé en 2016 par les Pays-Bas et le Luxembourg, rejoints entretemps par l'Allemagne, la Norvège, la Belgique et la République tchèque. La capacité AFSC remplaçant les avions AWACS réunit quasiment tous les partenaires OTAN. Le programme AGS réunit une quinzaine de membres de l'OTAN.

Dans le domaine Espace, le Luxembourg coopère surtout avec les États-Unis d'Amérique. Concernant le satellite de reconnaissance NAOS[28], il a été construit par OHB Italia.

Dans le domaine Cyber, des discussions sont menées notamment avec l'Allemagne.
Les 25 et 26 avril 2023 a eu lieu la conférence « Luxembourg Autonomous Weapons Systems » (LAWS) avec la participation de nombreux États.

En réponse à la question de M. Wiseler relative au choix des systèmes d'armement, le LtCol Schons explique que le choix se fait en fonction de la digitalisation. Ces systèmes sont ou seront interopérables et le choix est dès lors limité. Ainsi, pour le bataillon de reconnaissance belgo-luxembourgeois, les véhicules en voie d'acquisition par la Belgique dans le cadre du partenariat stratégique franco-belge CaMo (Capacité Motorisée) sont étroitement liés au programme français SCORPION, de sorte que les nouveaux véhicules luxembourgeois

[27] Lignes directrices de la Défense luxembourgeoise à l'horizon 2035, p. 47
[28] National Advanced Optical System

CLRV seront également équipés du système SCORPION. L'interopérabilité avec les Allemands se fera alors avec d'autres systèmes.

Le Gen Thull ajoute que les objectifs définis par le NDPP consistent à doter l'Alliance des capacités dont elle a besoin. Pour le Luxembourg, l'objectif retenu est l'augmentation des capacités de reconnaissance, celle-ci devant évoluer d'une reconnaissance légère à une reconnaissance de type médian. L'OTAN ne prescrit normalement pas le partenaire, mais a fait une exception ici en exigeant la création et l'exploitation commune d'un bataillon de reconnaissance belgo-luxembourgeois. Comme la Belgique, dont la taille ne permet pas non plus de satisfaire seule aux différentes exigences, a pris la décision de coopérer avec la France, le Luxembourg a choisi le même programme français.

Monsieur le Ministre fait remarquer que le choix des programmes et équipements ne se pose pas aux États-Unis d'Amérique comme aux partenaires européens, où les pays disposant d'une industrie d'armement et d'entreprises dans les domaines concernés se trouvent en situation de concurrence.

- Le même député voudrait également obtenir des explications plus détaillées sur le changement fondamental, en ce qui concerne la composante aérienne, par rapport aux Lignes directrices de la Défense luxembourgeoise à l'horizon 2025.

Monsieur le Ministre rappelle que les Lignes directrices précitées annonçaient ceci : « Actuellement, l'aéroport du Findel est déjà utilisé, de façon ponctuelle, à des fins militaires. La défense envisage l'implantation d'une zone gouvernementale dans l'enceinte de l'aéroport du Findel, qui pourrait prendre la forme d'un hangar permettant de stationner et d'assurer la maintenance des futurs aéronefs acquis par la défense, en coopération avec les partenaires nationaux. ». Or, il n'y a pas de place suffisante pour réaliser ce projet. Le Luxembourg met dès lors l'accent sur les partenariats et la mutualisation des ressources (« pooling & sharing »). Les nouvelles Lignes directrices indiquent que « Peu de pays ont la capacité de mener des opérations complexes d'envergure significative. Tenant compte de nos limitation structurelles, nos partenariats internationaux de référence – Belgique, Pays-Bas, France, Allemagne et les Etats-Unis ainsi que la NATO Support and Procurement Agency (NSPA), Agence européenne de défense (AED), Organisation Conjointe de Coopération en matière d'Armement (OCCAr), etc. – sont indispensables. Ces partenariats sont le garant de notre plus-value opérationnelle et mutuelle ainsi que de notre crédibilité.

Sans être exhaustif, il y a lieu de mentionner ici les participations du Luxembourg aux programmes multinationaux tels que A400M, « Multi-Role Tanker Transport » (MRTT), « Allied Ground Surveillance » (AGS), « Airborne Warning and Control System » (AWACS), etc. qui sont des réalités aujourd'hui et qui continuent à gagner en importance. Ils permettent notamment de répondre aux ambitions et exigences de l'OTAN ainsi que de l'UE. ».

❖ M. Marc Goergen (Piraten) souhaitant savoir comment l'augmentation des effectifs et l'acquisition du matériel nécessaires pour atteindre un effort de défense d'1% du PIB peuvent être réalisées dans les délais fixés, Monsieur le Ministre confirme que le recrutement de personnel s'avère le plus difficile. Comme le Luxembourg se spécialise dans certains domaines, il convient de recruter des spécialistes. Au niveau de la rémunération, le secteur privé représente une concurrence sérieuse pour le recrutement de spécialistes en informatique. La future loi sur l'organisation de l'Armée joue ici un rôle essentiel, notamment par la création des carrières A2 et B1.

L'expert informaticien de la Défense relate qu'il vient du secteur privé, où des salaires très élevés sont effectivement payés à partir d'un certain niveau de compétences. Or, la motivation revêt une grande importance surtout chez les jeunes informaticiens. La défense offre une sphère d'activité qu'on ne trouve pas dans le secteur privé. Cet argument a permis

de mettre en place une équipe solide au sein de la Défense. En outre, des efforts sont entrepris, avec le soutien du Luxembourg House of Cybersecurity, pour inciter à l'école plus de jeunes, aussi plus de filles, à choisir l'informatique. Il importe aussi de rendre attentif au traitement plus élevé dans la Fonction publique en début de carrière, ce qui constitue aussi une motivation qu'il convient de sauvegarder par la suite.

❖ - Mme Stéphanie Empain (déi gréng) voudrait être éclairée sur la BACA (cf. p. 6).

Le Gen Thull renvoie à l'OSCE qui a élaboré en matière de maîtrise des armements le Document de Vienne sur les mesures de confiance et de sécurité[29] prévoyant une série de mécanismes de contrôle. Ceux-ci étaient gérés par le Luxembourg par le GIVO – Groupement d'inspecteurs vérificateurs et observateurs. Le Luxembourg a ensuite emprunté la voie multinationale et a mis en place avec la Belgique et les Pays-Bas la BACA (Benelux Arms Control Agency) installée en Belgique. La BACA est chargée de la mise en œuvre des contrôles d'armements à l'étranger, incluant en particulier le Traité sur les Forces armées conventionnelles en Europe (FCE – CFE Treaty on Conventional Armed Forces in Europe). Le Luxembourg a un représentant auprès de la BACA qui en a assuré la présidence les deux dernières années.

- Selon la même députée, l'importance des Lignes directrices réside dans la cohérence des investissements et dans la prévisibilité pour l'Armée de l'évolution de la défense et donc de son propre développement. Se pose la question de la flexibilité des Lignes directrices pour s'adapter à des imprévus ou des changements d'orientation politique.

Monsieur le Ministre assure que les Lignes directrices sont suffisamment flexibles pour tenir compte de changements de la situation de sécurité. Cependant, le gros se base sur des éléments capacitaires auxquels sera attachée une importance de plus en plus grande. Ainsi, de gros investissements sont effectués dans le domaine Cyber, par exemple, lequel ne nécessite toutefois pas tant de main d'œuvre que d'autres domaines. Le gros des Lignes directrices devrait pouvoir s'exécuter sur toute la période prévue, donc jusqu'en 2035, la flexibilité nécessaire pour s'adapter à l'évolution de la situation de sécurité concernera en particulier l'Armée.

Le Gen Thull déclare que les premiers changements seront couverts par les Lignes directrices.

2. Projet de loi 8157

En réponse à une question de M. Marc Goergen concernant l'opérationnalité du programme, une représentante ministérielle fait savoir qu'en décembre dernier, deux des onze satellites de la constellation O3b mPower ont été lancés ; le prochain lancement est prévu pour le mois prochain. La constellation devrait être opérationnelle d'ici la fin de l'année.

La commission adopte le rapport en sa majorité (ADR : abstention) et propose comme temps de parole le modèle de base.

3. Projet de loi 8167

La commission désigne sa présidente rapportrice du projet de loi.

L'avis du Conseil d'État ne donne pas lieu à observation.

[29] https://www.osce.org/fr/arms-control

Procès-verbal approuvé et certifié exact

Annexe : Présentation PowerPoint « Lignes directrices de la Défense luxembourgeoise à l'horizon 2035 »

Lignes directrices de la Défense luxembourgeoise à l'horizon 2035

Commission de la Sécurité intérieure et de la Défense
Commission des Affaires étrangères et européennes, de la Coopération, de l'Immigration et de l'Asile

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

Direction de la défense

8167 - Dossier consolidé : 86

Agenda

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

1. Introduction
2. Nouvelles Lignes directrices
3. Questions & Réponses

8167 - Dossier consolidé : 87

1. Introduction

- Travail prévu par l'accord de coalition de 2018
- Actualisation nécessaire suite à :
  - Nouveaux objectifs capacitaires otaniens de 2021
  - Bouleversement profond de la stabilité politique et sécuritaire mondiale
  - Objectif du gouvernement d'atteindre un effort de défense de 1% vers 2028
  - Boussole stratégique de l'UE en matière de sécurité et de défense (2022)
  - Concept stratégique de l'OTAN de 2022
- Réalisée par la Direction de la défense et l'Etat-Major de l'Armée
- Versions française et anglaise

2. Lignes directrices 2035

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

1. Résumé exécutif
2. Pourquoi une actualisation
3. Evolution de la situation internationale et les implications
4. Finalités de la politique de défense du Luxembourg
5. Principes structurants de la politique de défense du Luxembourg
6. Objectifs à atteindre
7. Axes prioritaires du développement capacitaire
8. Efforts additionnels et complémentaires
9. Défis

Pourquoi une actualisation

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Contexte, cadre et orientations de la politique de défense
- Références OTAN et UE de 2022 : concept stratégique et boussole stratégique
- Objectif national d'un effort équivalent à 1% du PIB à l'horizon 2028
- Projet de loi pour nouvelle loi-cadre de l'Armée en procédure

Evolution de la situation internationale et implications

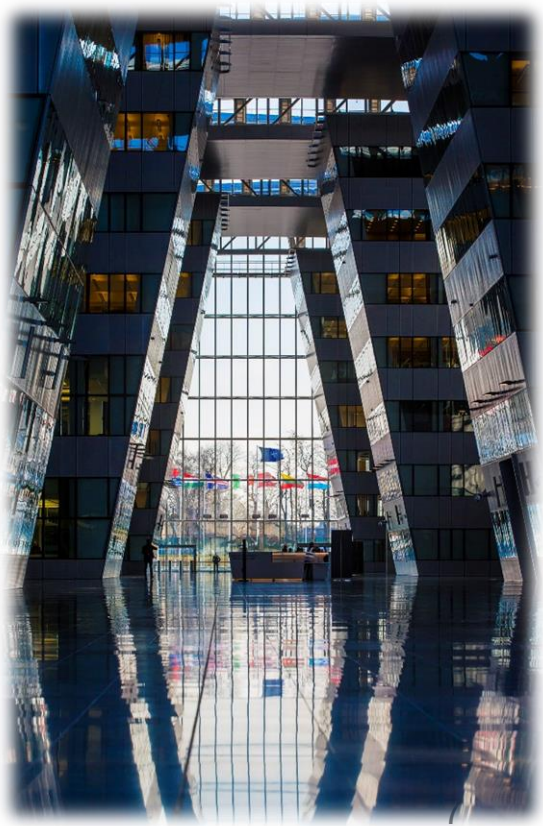
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Tendances sous-jacentes influençant la politique de défense
  - Contestation de l'ordre international fondé sur le règles et érosion des normes
  - Impact de la technologie
  - Risques sécuritaires liés aux changements environnementaux
- Menaces
  - Conventionnelles et nucléaires
  - Asymétriques et hybrides
  - Cyber
- Appréciation de l'environnement stratégique
  - Guerre d'agression russe contre l'Ukraine et politique chinoise assertive
  - Menaces conventionnelles = point focal
  - Nouvelles formes de menaces: Emerging Disruptive Technologies (EDT), Lethal Autonomous Weapons Systems (LAWS)
  - Impact de la crise climatique et environnementale
  - Besoin de transformations et d'objectifs stratégiques adaptés

Finalités de la politique de défense du Luxembourg

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Promotion de nos valeurs à l'échelle mondiale
- Préservation des intérêts essentiels de sécurité du Luxembourg à travers le système multilatéral basé sur le droit international
- A travers la Défense, dans son ensemble, le Luxembourg:
  - apporte sa part à la réponse globale de l'UE, l'OTAN, l'ONU et l'OSCE face aux défis de sécurité et de défense
  - contribue à la posture de dissuasion et de défense, essentielle pour préserver la paix, et au partage équitable du fardeau
  - soutient des mesures de confiance et de sécurité (OSCE)
  - contribue à une approche intégrée nationale



© NATO

Principes structurants de la politique de défense

- Solidarité
- Autonomie décisionnelle
- Partenariat transatlantique
- Adaptabilité et spécificité militaire
- Partenariats et mutualisation des ressources (« *pooling & sharing* »)
- Engagement pour la société luxembourgeoise
- Politique étrangère et de sécurité des « 3D » – diplomatie, défense, développement

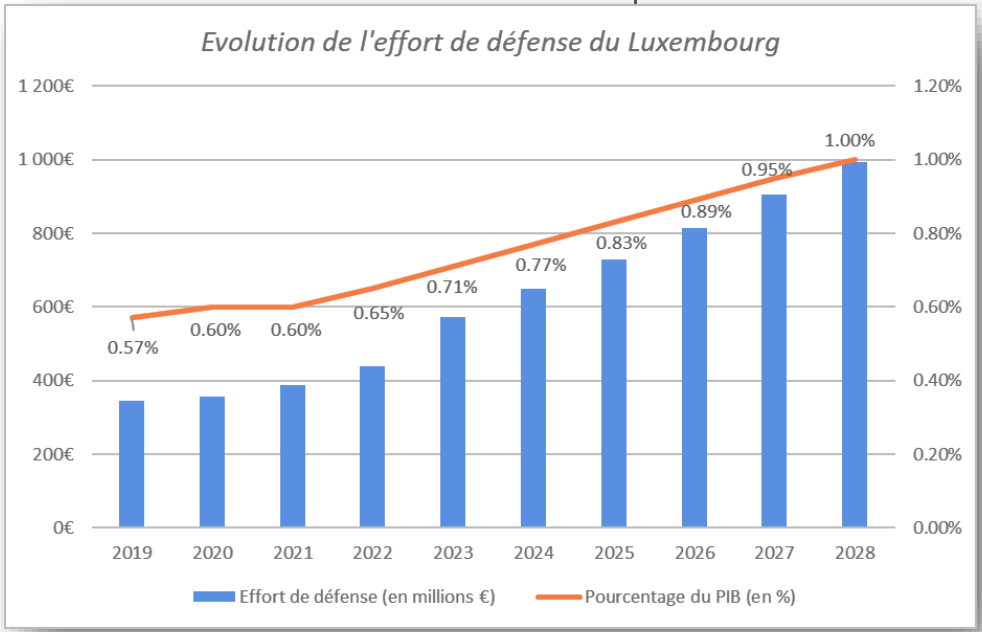
Objectifs à atteindre 1/2

- Développer des capacités, tout d'abord des forces
- Evolution possible des objectifs en fonction de l'environnement sécuritaire et des ressources humaines
- Sur le plan:
  - Organisationnel:
    - Augmentation des effectifs
    - Développement des capacités (communication, commandement, soutien, formation, entrainement et simulation)
  - Capacitaire:
    - Politique de développement capacitaire saine pour augmenter réactivité, puissance, résilience et opération en réseau
    - Double usage
  - Opérationnel:
    - Contribution aux opérations pour le maintien de la paix et aux missions de prévention ainsi que de gestion de crise
    - Contribution aux exercices et déploiements pour renforcer la posture de dissuasion et de défense sur territoire de l'Alliance
    - Contribution aux forces de réaction rapide
    - Assurer l'exécution des missions nationales et renforcement de la résilience
    - Contribuer à des engagements de prévention de conflits et de stabilisation
    - Contribuer à des opérations de secours et d'aide humanitaire

Objectifs à atteindre 2/2

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Effort de défense:
  - augmentation substantielle vers 1% du PIB au plus tôt à l'horizon 2028
  - 2% de l'effort de défense dédiés à la recherche et au développement dès cette année
- Prévention des risques sécuritaires liés aux changements environnementaux
  - Réduire d'au moins 45% les émissions de gaz à effet de serre vers 2030 et viser « net zero » vers 2050
  - Contribuer au « climate change and security action plan » de l'OTAN et mise en œuvre du Plan national intégré en matière d'énergie et de climat (PNEC)
- Approfondir la multinationalisation
- Soutenir la recherche et l'industrie
- Accroître le taux de féminisation



Axes prioritaires du développement capacitaire 1/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Terre:

- Développement des capacités de reconnaissance terrestres
- Accent sur mise en place et l'exploitation conjointe de l'objectif du bataillon binational de reconnaissance de combat médian, en coopération étroite avec FRA, et un renforcement d'une centaine de personnels pour l'Armée
- Réintégration des capacités antichar à moyenne portée
- Introduction de nouvelles capacités de reconnaissance
  - contrôleur aérien avancé
  - contre drones
  - protection contre les munitions rôdeuses
- Evolution et remplacement des drones tactiques et capacités de purification d'eau actuelles
- Capacité de déminage conformément aux exigences OTAN

8167 - Dossier consolidé : 96

Axes prioritaires du développement capacitaire 2/4

Air:

- Axe significatif pour croissance de l'effort de défense et de contributions opérationnelles à haute valeur ajoutée
- Capacités stratégiques A400M et MRTT
- Plates-formes plus légères à envisager dans cadre Benelux ou FNC
- Remplacement des AWACS par AFSC
- Maintien du soutien substantiel à AGS (drones stratégiques de l'OTAN), ainsi que des capacités ISR aériennes maritimes et d'évacuation médicales contractées
- Étude d'opportunités de:
  - Renforcement de la défense anti-aérienne (anti-access/area denial) dans cadre multinational
- Contribution aux capacités « Search and Rescue » sur base de la plate-forme H145M

© NATO

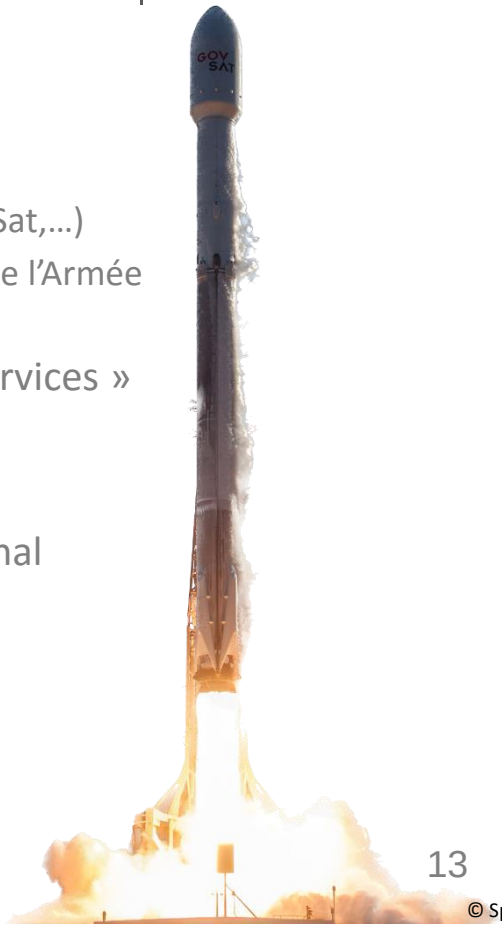
© Multinational MRTT Fleet

Axes prioritaires du développement capacitaire 3/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Espace:

- Mise en œuvre de la stratégie sectorielle de 2022
- Poursuite:
  - des activités de communications satellitaires sécurisées (WGS, GovSat,…)
  - du développement des capacités de communications déployables de l'Armée (p.ex missions EUTM Mozambique et MINUSMA)
- Développement du programme « Medium Earth Orbit Global Services » (MGS)
- Mise en œuvre et suivi du programme LUXEOSys
- Renforcer coopération en matière de capacités « Space Situational Awareness »



© SpaceX

Axes prioritaires du développement capacitaire 4/4

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

➢ Cyber:

- Mise en œuvre de la stratégie sectorielle de 2021, s'appuyant sur la stratégie nationale de cybersécurité
- Objectif à long terme : une des défenses les plus cybersécurisées
- Coopération avec NSPA pour le « Luxembourg Cyber Defence Cloud » (LCDC) et la « Cyber Range »
- Coopération Défense et Université du Luxembourg – Projet « National Competence Hub in Research in Cybersecurity and Cyber Defence »

LUXEMBOURG CYBERDEFENCECLOUD

CYBER RANGE LUXEMBOURG

Efforts additionnels et complémentaires

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

- Communication stratégique
- Etats-majors internationaux et organismes multinationaux
- Vérification et contrôle de l'exécution des traités multinationaux

8167 - Dossier consolidé : 100

- Médecine militaire
- Mobilité militaire
- Rénovation des infrastructures militaires nationales, NSPA et WSA

Défis

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Engagement politique sur le long terme,

horizon stratégique harmonisé avec partenaires, OTAN et UE

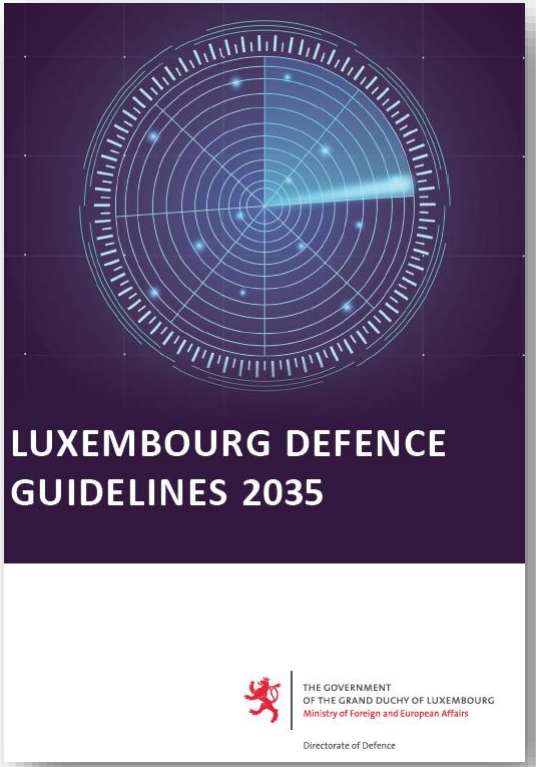
- Ressources humaines
- Autonomie décisionnelle
- Augmentation de l'effort de défense
- Processus d'anticipation stratégique
- Accès aux technologies de pointe
- Sécurité énergétique et des approvisionnements
- Autonomie européenne de défense et coopération UE-OTAN renforcée

3. Questions et réponses

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

➢ Questions?


LIGNES DIRECTRICES DE LA DEFENSE LUXEMBOURGEOISE A L'HORIZON 2035
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère des Affaires étrangères et européennes
Direction de la Défense


LUXEMBOURG DEFENCE GUIDELINES 2035
THE GOVERNMENT
OF THE GRAND DUCHY OF LUXEMBOURG
Ministry of Foreign and European Affairs
Directorate of Defence

8167/02

N° 8167²

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

* * *

RAPPORT DE LA COMMISSION DE LA SECURITE INTERIEURE ET DE LA DEFENSE

(22.6.2023)

La Commission se compose de : Mme Stéphanie EMPAIN, Présidente-Rapportrice ; Mmes Diane ADEHM, Semiray AHMEDOVA, Nancy ARENDT ép. KEMP, MM. André BAULER, François BENOY, Dan BIANCALANA, Léon GLODEN, Marc GOERGEN, Gusty GRAAS, Jean-Marie HALSDORF, Fernand KARTHEISER, Georges MISCHO, Mme Lydia MUTSCH, Membres.

*

I. ANTECEDENTS

Le projet de loi a été déposé à la Chambre des Députés le 2 mars 2023 par le Ministre de la Défense. Le texte du projet était accompagné d'un exposé des motifs, d'un commentaire des articles, d'une fiche financière et d'une fiche d'évaluation d'impact.

Le projet de loi a été présenté à la commission le 6 mars 2023.

Le Conseil d'État a émis son avis le 31 mars 2023.

La commission a examiné l'avis du Conseil d'État dans la réunion du 11 mai 2023, où elle a désigné sa présidente rapportrice du projet de loi.

Le présent rapport a été adopté le 22 juin 2023.

*

II. OBJET DU PROJET DE LOI

Le projet de loi n°8167 a comme objet d'autoriser le Gouvernement à financer l'acquisition et l'exploitation du projet « Luxembourg Cyber Defence Cloud », constitué par des environnements « cloud computing » spécialisés, ainsi que de composantes et services connexes. Y sont inclus les coûts d'exploitation, de maintenance, d'opération et de gestion.

Contexte et motifs du projet de financement du projet « Luxembourg Cyber Defence Cloud » (LCDC)

Le projet de loi vise à autoriser le Gouvernement à financer les coûts d'exploitation, de maintenance, d'opération et de gestion du projet LCDC, constitué d'environnements « cloud » ségrégés, ainsi que de composantes et services connexes. Ce projet fait partie de la stratégie de cyberdéfense du Luxembourg et a pour objectif de développer une infrastructure informatique évolutive, fiable, performante et sécurisée en termes de confidentialité, d'intégrité et de disponibilité. Une fois mise en place, la capacité

LCDC pourra aussi être mise à disposition des pays membres de l'OTAN et de l'Union européenne dans le cadre de la coopération multilatérale en matière de cyberdéfense. Ainsi, cette infrastructure informatique contribuera à la mise en place de mesures de sécurité et de services nécessaires pour assurer un niveau de cybersécurité élevé pour permettre l'hébergement et le traitement de données sensibles et/ou classifiées.

Le coût total du projet ne doit pas dépasser 250 360 323 euros, hors TVA, sur une période de douze ans, frais de gestion opérationnelle et marge inclus. Les dépenses associées seront prises en charge par le Fonds d'équipement militaire.

*

III. AVIS DU CONSEIL D'ETAT

Dans son avis du 31 mars 2023, le Conseil d'État ne fait aucune observation sur le fond du texte et se déclare d'accord avec le projet de loi.

*

IV. COMMENTAIRE DES ARTICLES

Article 1er

L'article 1er a pour objet d'autoriser le Gouvernement à acquérir le « Luxembourg Cyber Defence Cloud » (LCDC) et à en financer l'exploitation, la maintenance, l'opération et la gestion.

Le présent projet est, après la plateforme « Cyber Range » déjà opérationnelle, le deuxième grand projet de la stratégie de cyberdéfense du Luxembourg, dont les objectifs à long terme sont de disposer d'une défense les plus cyber-sécurisées de l'OTAN[1] et de l'UE[2] et de développer une expertise et des capacités qui pourront aussi être offertes aux Alliés et aux partenaires. Tandis qu'une « Cyber Range » est une plateforme de simulation qui donne aux responsables de sécurité informatique le moyen de s'entraîner contre les cyberattaques, un « cloud » permet de stocker et de traiter des données, ainsi que d'héberger des services informatiques. Comme l'indique l'exposé des motifs du projet de loi, l'informatique en nuage ou « cloud computing » est la fourniture de ressources et services informatiques à la demande via un réseau de serveurs distants, ce qui a l'avantage de pouvoir traiter les demandes des utilisateurs de manière efficace, sécurisée et flexible.

La stratégie de cyberdéfense nécessite une infrastructure informatique évolutive, fiable, performante et sécurisée. Outre les objectifs à long terme de cette stratégie, le Luxembourg doit pouvoir répondre à ses engagements au niveau international (OTAN, UE). Le présent projet est proactif, puisque le Luxembourg devance les exigences d'aujourd'hui de l'OTAN et, les exigences futures s'annonçant considérables, notre pays créera le cadre qui permettra aussi à ses Alliés et partenaires d'y avoir recours pour satisfaire celles-ci.

À côté de ses engagements au niveau international, le Luxembourg doit aussi pouvoir répondre de façon adéquate, comme le décrit l'exposé des motifs, aux défis de la transformation digitale croissante au niveau des Défenses des États membres de l'OTAN et de l'UE, ainsi que des agences OTAN et UE, et auprès des acteurs étatiques nationaux. Cette digitalisation fait augmenter les besoins de ressources informatiques qui doivent en plus satisfaire en matière de défense à des conditions spécifiques de sécurité.

Le LCDC se traduira par des environnements cloud privés et hautement sécurisés de la Défense luxembourgeoise qui permettent le stockage et le traitement de données. Le LCDC pourra stocker des données classifiées (OTAN, UE et éventuellement aussi des données nationales) et non-classifiées. Le stockage se fait dans des centres de données sécurisés, dont le standard de protection répond aux standards internationaux les plus hauts et conçus pour assurer une haute disponibilité.

Le LCDC hébergera principalement des projets qui contribuent

– à la résilience du Luxembourg face aux menaces cyber,

1 Organisation du Traité de l'Atlantique Nord (NATO – North Atlantic Treaty Organization)

2 Union européenne

– à l'effort de défense luxembourgeois au niveau de l'OTAN, de l'UE ou de partenaires ou Alliés,
– aux objectifs stratégiques de la Défense luxembourgeoise.

La commission note que le projet aura des retombées économiques pour le Luxembourg et renforcera l'image de notre pays, dont le côté fort peut consister justement dans de tels projets qui ne nécessitent pas la mise à disposition d'importants effectifs militaires, mais une équipe de spécialistes.

Article 2

La somme totale qui sera dépensée pour le LCDC est limitée à 250 360 323 euros.

La durée du projet s'étend de 2024 à 2035 : les deux premières années sont destinées à l'acquisition de l'infrastructure et à la mise en opération progressive jusqu'au niveau de capacité 1. Ensuite, après cinq ans d'opération, les équipements informatiques sont à remplacer, la durée de vie de ces équipements étant de cinq ans. En cas de succès, la capacité sera en outre augmentée de 50% au maximum.

La Défense luxembourgeoise sera le propriétaire du LCDC ; pour l'acquisition de l'infrastructure IT, elle collabore étroitement avec la NSPA[3]. La somme totale inclut le financement d'un environnement cloud pour la NSPA qui s'élève à 58 476 203 euros, ce qui représente une importante contribution à l'effort de défense au niveau de l'OTAN, le Luxembourg étant par ailleurs la « host nation » de la NSPA. Déjà aujourd'hui, le Luxembourg finance en partie l'infrastructure IT et les centres de données IT de la NSPA.

Le financement autorisé par le présent projet de loi exclut

– les coûts de gestion des environnements mis à disposition aux bénéficiaires,
– les cas d'utilisation des bénéficiaires,
– l'interconnexion vers les sites des bénéficiaires et la connexion internet des bénéficiaires.

Ces coûts sont à charge des bénéficiaires et déterminés dans l'accord technique conclu avec chaque bénéficiaire.

Le budget se répartit comme suit :

– coûts de l'infrastructure (serveurs, réseaux, configuration) : 127 095 671 euros ;
– projets déjà identifiés à héberger dans le LCDC : 42 768 064 euros ;
– services connexes (mesures spécifiques de sécurité, services IT de fournisseurs externes (monitoring de la performance du LCDC)) : 22 020 385 euros ;
– financement d'un environnement cloud pour la NSPA : 58 476 203 euros.

Article 3

Cet article, qui dispose que les dépenses sont liquidées à charge du Fonds d'équipement militaire, ne donne pas lieu à observation.

*

Compte tenu des observations qui précèdent, la Commission de la Sécurité intérieure et de la Défense propose en sa majorité à la Chambre des Députés d'adopter le projet de loi dans la teneur suivante :

*

3 NATO Support and Procurement Agency

8167

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

Art. 1er. Le Gouvernement est autorisé à acquérir le « Luxembourg Cyber Defence Cloud », constituée par des environnements cloud spécialisés, ainsi que de composantes et services connexes et à financer ses coûts d'exploitation, de maintenance, d'opération et de gestion.

Art. 2. Les dépenses occasionnées par la présente loi ne peuvent dépasser le montant de 250 360 323 euros, y inclus les frais liés à l'acquisition, l'exploitation, la maintenance, l'opération, la gestion du système et des composantes et services connexes du « Luxembourg Cyber Defence Cloud » à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale. Ce montant ne comprend pas la taxe sur la valeur ajoutée.

Art. 3. Les dépenses occasionnées par l'acquisition, l'exploitation, la maintenance, l'opération et la gestion du « Luxembourg Cyber Defence Cloud » sont liquidées à la charge du Fonds d'équipement militaire.

Luxembourg, le 22 juin 2023

La Présidente-Rapportrice,
Stéphanie EMPAIN

Impression: CTIE – Division Imprimés et Fournitures de bureau

Texte voté - projet de loi N°8167

CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

N° 8167

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

*

Art. 1er. Le Gouvernement est autorisé à acquérir le « Luxembourg Cyber Defence Cloud », constituée par des environnements cloud spécialisés, ainsi que de composantes et services connexes et à financer ses coûts d'exploitation, de maintenance, d'opération et de gestion.

Art. 2. Les dépenses occasionnées par la présente loi ne peuvent dépasser le montant de 250 360 323 euros, y inclus les frais liés à l'acquisition, l'exploitation, la maintenance, l'opération, la gestion du système et des composantes et services connexes du « Luxembourg Cyber Defence Cloud » à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale. Ce montant ne comprend pas la taxe sur la valeur ajoutée.

Art. 3. Les dépenses occasionnées par l'acquisition, l'exploitation, la maintenance, l'opération et la gestion du « Luxembourg Cyber Defence Cloud » sont liquidées à la charge du Fonds d'équipement militaire.

Projet de loi adopté par la Chambre des Députés
en sa séance publique du 27 juin 2023

Le Secrétaire général, Le Président,

s. Laurent Scheeck s. Fernand Etgen

Bulletin de vote n°6 - Projet de loi N°8167

Bulletin de Vote (Vote Public)

Date: 27/06/2023 16:37:50
Scrutin: 6
Vote: PL 8167 - Luxembourg Cyber Defense
Description: Projet de loi N°8167

Président: M. Etgen Fernand
Secrétaire Général: M. Scheeck Laurent

	Oui	Abst	Non	Total
Présents:	54	0	2	56
Procurations:	3	0	0	3
Total:	57	0	2	59

Nom du député	Vote	(Procuration)	Nom du député	Vote	(Procuration)
DP					
Agostino Barbara	Oui		Arendt Guy	Oui	
Bauler André	Oui		Baum Gilles	Oui	
Beissel Simone	Oui		Colabianchi Frank	Oui	
Etgen Fernand	Oui		Graas Gusty	Oui	
Hartmann Carole	Oui		Knaff Pim	Oui	
Lamberty Claude	Oui		Polfer Lydie	Oui	(Colabianchi Frank)
LSAP					
Asselborn-Bintz Simone	Oui		Biancalana Dan	Oui	
Burton Tess	Oui		Closener Francine	Oui	
Cruchten Yves	Oui		Di Bartolomeo Mars	Oui	
Hemmen Cécile	Oui		Kersch Dan	Oui	
Mutsch Lydia	Oui		Weber Carlo	Oui	
déi gréng					
Ahmedova Semiray	Oui		Benoy François	Oui	
Bernard Djuna	Oui		Empain Stéphanie	Oui	
Gary Chantal	Oui		Hansen Marc	Oui	
Lorsché Josée	Oui		Margue Charles	Oui	
Thill Jessie	Oui				
CSV					
Adehm Diane	Oui		Arendt épouse Kemp Nancy	Oui	
Eicher Emile	Oui		Eischen Félix	Oui	
Galles Paul	Oui		Gloden Léon	Oui	
Halsdorf Jean-Marie	Oui		Hansen Martine	Oui	
Hengel Max	Oui		Kaes Aly	Oui	
Lies Marc	Oui		Margue Elisabeth	Oui	
Mischo Georges	Oui		Modert Octavie	Oui	
Mosar Laurent	Oui		Roth Gilles	Oui	(Modert Octavie)
Schaaf Jean-Paul	Oui		Spautz Marc	Oui	
Wiseler Claude	Oui		Wolter Michel	Oui	
ADR					
Engelen Jeff	Oui		Kartheiser Fernand	Oui	
Keup Fred	Oui		Reding Roy	Oui	(Engelen Jeff)
DÉI LÉNK					
Cecchetti Myriam	Non		Oberweis Nathalie	Non	

Bulletin de Vote (Vote Public)

Date: 27/06/2023 16:37:50
Scrutin: 6
Vote: PL 8167 - Luxembourg Cyber Defense
Description: Projet de loi N°8167

Président: M. Etgen Fernand
Secrétaire Général: M. Scheeck Laurent

	Oui	Abst	Non	Total
Présents:	54	0	2	56
Procurations:	3	0	0	3
Total:	57	0	2	59

Nom du député	Vote (Procuration)	Nom du député	Vote (Procuration)
Piraten			
Clement Sven	Oui	Goergen Marc	Oui

n'ont pas participé au vote:

Nom du député	Nom du député
CSV	
Wilmes Serge	

Le Président:

Le Secrétaire Général:

8167/03

N° 8167[3]

CHAMBRE DES DEPUTES

Session ordinaire 2022-2023

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

* * *

DISPENSE DU SECOND VOTE CONSTITUTIONNEL PAR LE CONSEIL D'ETAT

(4.7.2023)

Le Conseil d'État,

appelé par dépêche du Président de la Chambre des députés du 27 juin 2023 à délibérer sur la question de dispense du second vote constitutionnel du

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

qui a été adopté par la Chambre des députés dans sa séance du 27 juin 2023 et dispensé du second vote constitutionnel ;

Vu ledit projet de loi et l'avis émis par le Conseil d'État en sa séance du 31 mars 2023 ;

se déclare d'accord

avec la Chambre des députés pour dispenser le projet de loi en question du second vote prévu par l'article 78, paragraphe 4, de la Constitution.

Ainsi décidé en séance publique à l'unanimité des 21 votants, le 4 juillet 2023.

Le Secrétaire général,
Marc BESCH

Le Président,
Christophe SCHILTZ

Impression: CTIE – Division Imprimés et Fournitures de bureau

Mémorial A N° 427 de 2023

JOURNAL OFFICIEL

DU GRAND-DUCHÉ DE LUXEMBOURG

MÉMORIAL A

N° 427 du 20 juillet 2023

Loi du 14 juillet 2023 autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes.

Nous Henri, Grand-Duc de Luxembourg, Duc de Nassau,

Le Conseil d'État entendu ;

Vu l'adoption par la Chambre des Députés ;

Vu la décision de la Chambre des Députés du 27 juin 2023 et celle du Conseil d'État du 4 juillet 2023 portant qu'il n'y a pas lieu à second vote ;

Avons ordonné et ordonnons :

Art. 1er.

Le Gouvernement est autorisé à acquérir le « Luxembourg Cyber Defence Cloud », constituée par des environnements cloud spécialisés, ainsi que de composantes et services connexes et à financer ses coûts d'exploitation, de maintenance, d'opération et de gestion.

Art. 2.

Les dépenses occasionnées par la présente loi ne peuvent dépasser le montant de 250 360 323 euros, y inclus les frais liés à l'acquisition, l'exploitation, la maintenance, l'opération, la gestion du système et des composantes et services connexes du « Luxembourg Cyber Defence Cloud » à prix constants aux conditions économiques de 2023 sans préjudice d'une adaptation des paiements annuels en fonction de l'évolution des conditions économiques telle que déterminée par l'évolution de l'indice des prix à la consommation nationale. Ce montant ne comprend pas la taxe sur la valeur ajoutée.

Art. 3.

Les dépenses occasionnées par l'acquisition, l'exploitation, la maintenance, l'opération et la gestion du « Luxembourg Cyber Defence Cloud » sont liquidées à la charge du Fonds d'équipement militaire.

Mandons et ordonnons que la présente loi soit insérée au Journal officiel du Grand-Duché de Luxembourg pour être exécutée et observée par tous ceux que la chose concerne.

Le Ministre de la Défense,
François Bausch

Cabasson, le 14 juillet 2023.
Henri

Doc. parl. 8167 ; sess. ord. 2022-2023.

Résumé

8167

PROJET DE LOI

autorisant le Gouvernement à financer l'acquisition, l'opération et la maintenance d'environnements cloud spécialisés, dénommés « Luxembourg Cyber Defence Cloud », ainsi que ses composantes et services connexes

Le projet de loi a pour objet d'autoriser le Gouvernement à acquérir le « Luxembourg Cyber Defence Cloud » (LCDC) et à en financer l'exploitation, la maintenance, l'opération et la gestion.

L'informatique en nuage ou « cloud computing » est la fourniture de ressources et services informatiques à la demande via un réseau de serveurs distants. La stratégie de cyberdéfense nécessite une infrastructure informatique évolutive, fiable, performante et sécurisée. Outre les objectifs à long terme de cette stratégie, le Luxembourg doit pouvoir répondre à ses engagements au niveau international (OTAN, UE) et doit aussi pouvoir répondre de façon adéquate aux défis de la transformation digitale croissante au niveau des Défenses des États membres de l'OTAN et de l'UE, ainsi que des agences OTAN et UE, et auprès des acteurs étatiques nationaux. Cette digitalisation fait augmenter les besoins de ressources informatiques qui doivent en plus satisfaire en matière de défense à des conditions spécifiques de sécurité.

Le LCDC se traduira par des environnements cloud privés et hautement sécurisés de la Défense luxembourgeoise qui permettent le stockage et le traitement de données.