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

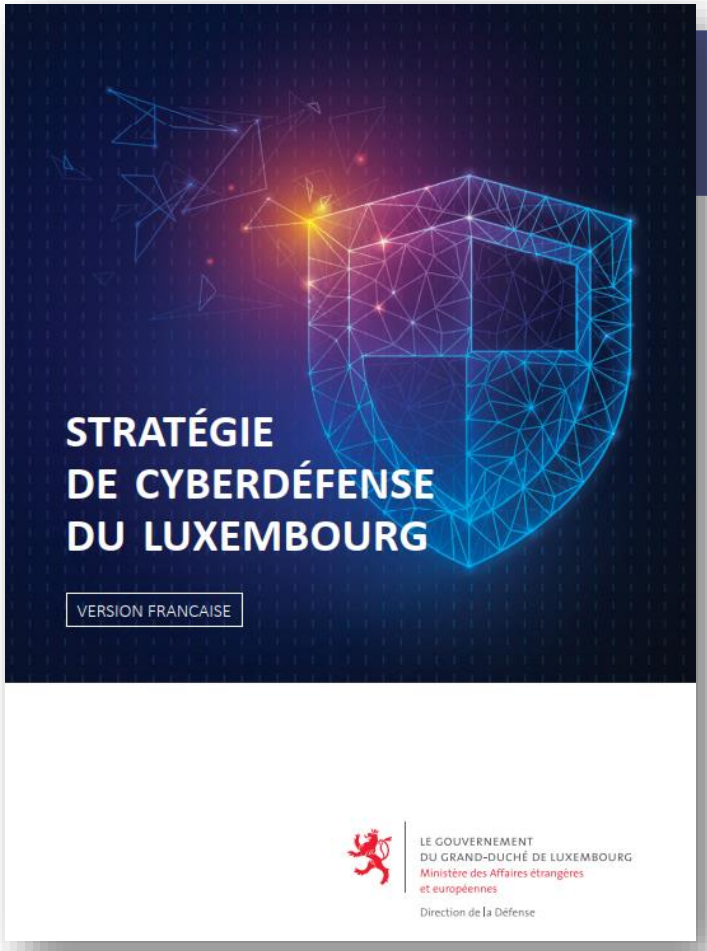
01 Contexte

02 Le projet: Luxembourg Cyber Defence Cloud

03 Questions - Réponses

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

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.

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

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.

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

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

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

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

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

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