

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. 1^{er}. 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

I. Texte du projet de loi	2
II. Exposé des motifs	2
A. Contexte	2
B. Présentation du projet « <i>Luxembourg Cyber Defence Cloud</i> »	3
C. Evaluation des besoins pour la mise en place d'un service du type « <i>cloud computing</i> » dans le domaine de la sécurité et de la défense	4
D. Financement du projet	6
E. Procédure d'acquisition	6

III. Commentaire des articles	7
IV. Fiche financière	8
V. Fiche d'évaluation d'impact	11

*

TEXTE DU PROJET DE LOI

Art. 1^{er}. 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 conséquent, 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 Défense 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 Défense 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 nuage 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 ségrégués (« *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* privés¹ en offrant des services comme le stockage, la mise en réseau, ou le déploiement de machines virtuelles².

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 ségrégués 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 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 entre 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'entraînement 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 entre 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 croître.

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 : Il 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 fournis 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 accréditées 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'échelonnent 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 soutien⁴ MACCE⁵ (matériels MIDS⁶-ACCS⁷-CCE⁸) 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 1^{er}.

L'article 1^{er} 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 1^{er} 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 Défence 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 administrative¹⁰ 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 administratif¹¹ 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 personnel¹² ? 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 évaluation¹³ ? 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 transfrontaliers¹⁴ ? 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)

