Autorité de protection des données
Gegevensbeschermingsautoriteit

Autorisation (délivrée) n° 001/2025 du 18 juillet 2025

Objet: demande d'autorisation visée à l'article 21, § 4, de la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique : « Command-and-Control servers communicatiemetadata – waarschuwing » (AH-2025-0034)

Le Service d'Autorisation et d'Avis de l'Autorité de protection des données (ci-après, « l'Autorité »),

Vu la loi du 3 décembre 2017 *portant création de l'Autorité de protection des données,* (ci-après, la « LCA ») ;

Vu l'article 21, § 4, de la loi du 26 avril 2024 *établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique* (ci-après, la « Loi NIS2 ») ;

Vu la loi du 13 juin 2005 *relative aux communications électroniques* (ci-après, la « LCE ») ;

Vu le règlement (UE) 2016/679 *du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* (ci-après, le « RGPD »);

Vu la loi du 30 juillet 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* (ci-après, la « LTD »);

Vu les articles 44, 54 et 55 du Règlement d'Ordre Intérieur de l'Autorité de Protection des Données (ci-après, le « ROI ») ;

Vu la demande d'autorisation du Directeur Général du Centre pour la Cybersécurité Belgique, Monsieur Miguel De Bruycker (ci-après, « le demandeur »), reçue le 23 mai 2025 ;

Vu les demandes d'informations complémentaires adressées au Centre pour la Cybersécurité Belgique, le 28 mai 2025 et le 3 juin 2025 ;

Vu les documents et réponses communiquées par le Centre pour la Cybersécurité Belgique, le 20 juin 2025 ;

Vu la demande d'information complémentaire adressée au Centre pour la Cybersécurité Belgique, le 24 juin 2025 ;

Vu les documents et réponses communiqués par le Centre pour la Cybersécurité Belgique le 8 juillet 2025, y compris une liste adaptée d'adresses IP joint à laquelle est jointe une note technique complémentaire ;

Vu la demande d'information complémentaire adressée au Centre pour la Cybersécurité Belgique, le 11 juillet 2025, et la réponse communiquée le 14 juillet 2025 ;

Vu la confirmation de la complétude du dossier envoyée au demandeur le 16 juillet 2025 ;

Vu l'évocation du dossier en Comité de direction de l'Autorité et la discussion subséquente du 17 juillet 2025 ;

Prend, le 18 juillet 2025, la décision suivante :

I. Objet et contexte de la demande d'autorisation

1. Le demandeur a introduit auprès de l'Autorité une demande d'autorisation visée à l'article 21, § 4, de la Loi NIS2 (ci-après, « **la Demande** »). Cette disposition, à lire en combinaison avec l'article 23, § 3, de la LCA[1], prévoit une compétence spécifique dans le cadre de laquelle l'Autorité est amenée à

---

[1] « *§ 3. Dans le cadre de l'application de la loi du 13 juin 2005 relative aux communications électroniques et de lois particulières et sans préjudice des pouvoirs des autorités de contrôle visées aux titres 2 et 3 de la loi du 31 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et de ceux de la commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité créée par l'article 43/1 de la loi organique du 30 novembre 1998 des services de renseignement et de sécurité, le service d'autorisation et d'avis émet des autorisations d'accès aux métadonnées de communication relatives au trafic ou à la localisation pour les institutions compétentes, pour les finalités qui ne relèvent pas :*

- de l'exercice des missions de prévention, de recherche, de détection ou de poursuite d'un fait qui constitue une infraction pénale, ou ;

- de la recherche des personnes disparues, ou ;

- de la sécurité nationale.

Pour être complète, la demande d'autorisation contient les éléments suivants :

1° l'identification de l'institution demanderesse ;

2° la base légale permettant à cette institution de demander auprès des opérateurs des métadonnées de communication relatives au trafic ou à la localisation ;

autoriser (ou pas) l'accès du Centre pour la Cybersécurité Belgique (ci-après, « **le CCB** ») à des métadonnées de communications électroniques traitées par les opérateurs de télécommunications[2].

2. L'article 21, § 2, de la Loi NIS2, prévoit ce qui suit :

> « *Lorsque cela s'avère* ***strictement nécessaire*** *à la réalisation de ses tâches énumérées à* ***l'article 19, § 1er, 1° à 5°,*** *le* ***CSIRT national*** *peut obtenir d'un opérateur visé à l'article 2, 11°, de la loi du 13 juin 2005, des données d'identification visées à l'article 2, alinéa 1er, 5°, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges ou des métadonnées de communications électroniques au sens de l'article 2, 93°, de la loi précitée du 13 juin 2005 conservées par celui-ci.*
>
> *Sans porter atteinte aux, ou sans s'immiscer dans les compétences des personnes exerçant la police judiciaire ni des autorités judiciaires,* ***les finalités poursuivies par les tâches précitées sont*** *:*
>
> *1° sans finalité à caractère pénal, la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave;*
>
> *2° la prévention de menaces graves contre la sécurité publique;*
>
> *3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information.*
>
> *Le CSIRT national peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci* » (mis en gras par l'Autorité).

3. Le CCB agit notamment **en tant que CSIRT national**[3] et l'article 19, § 1er, 1° à 4° (le 5° n'étant pas pertinent dans le cadre de la présente demande) de la Loi NIS2, attribue les tâches suivantes au CSIRT national :

> « *1° surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes*

3° l'exercice de la mission, dont les finalités ne relèvent pas de l'une des matières énumérées à l'alinéa 1er, premier à troisième tirets, justifiant de la nécessité et du caractère proportionnel de la demande ;

4° le cas échéant, la motivation de l'urgence ou de l'extrême urgence ;

5° la signature de la personne apte à engager l'institution demanderesse.

Lorsque la demande d'autorisation est complète, la décision de l'Autorité de protection des données est rendue au plus tard dans les dix jours ouvrables compris comme tous les jours autres que le samedi, le dimanche et les jours fériés légaux. La décision de l'Autorité de protection de données est motivée ».

[2] Selon l'article 2, 11°, de la LCE, un opérateur est « *une personne ou entreprise qui fournit un réseau public de communications électroniques ou un service de communications électroniques accessible au public* ».

[3] Voir l'article 16, al. 2, de la Loi NIS2 et l'article 3, § 1er, de l'arrêté royal du 9 juin 2024 *exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.*

concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information ;

2° activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel ;

3° réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant ;

4° rassembler et analyser des données forensiques, et assurer une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité ;

5° réaliser, à la demande d'une entité essentielle ou importante, un scan proactif des réseaux et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important ».

4. La demande concerne un projet intitulé « *Command-and-Control servers communicatiemetadata – waarschuwing* » (ci-après, « **le Projet** »). L'objectif du CCB est de pouvoir collecter des métadonnées de communications électroniques relatives à de (potentielles) victimes des activités malveillantes de « *command-and-control servers* » (ci-après « **C2-servers** »)[4] préalablement identifiés sur la base de sources disponibles au CCB (déclaration d'incidents, signalements ou alertes transmis par des autorités homologues étrangères ou par des partenaires privés de confiance, etc.). Il s'agirait de mettre en place un cadre de coopération avec les opérateurs concernés afin de pouvoir identifier, sur la base du trafic vers et depuis ces C2-servers, quelles sont les victimes (potentielles) belges concernées, à charge pour le CCB ensuite, de prendre contact avec celles-ci, à la suite d'une demande d'identification auprès des opérateurs concernés[5]. Plus concrètement, une fois qu'il disposerait des adresses IP dédiées aux C2-servers, l'opérateur concerné serait chargé de collecter les métadonnées des communications électroniques transitant par son réseau vers et depuis ces adresses, et de les communiquer au CCB (CSIRT national). Sur la base de l'analyse de ces métadonnées, le CCB (CSIRT national) identifierait alors les adresses IP de victimes potentielles de ces C2-servers. A l'aide de ces adresses IP, le CCB (CSIRT national) adresserait alors des demandes d'identification (identité et données de contact) de leurs détenteurs aux opérateurs concernés, afin de pouvoir prendre contact avec eux. Enfin, il informerait ceux-ci afin qu'ils puissent se prémunir contre la menace concernée.

5. Le demandeur a notamment joint à sa demande une note explicative du Projet et de la procédure qui serait mise en place (ci-après, « **la Note** »). Outre cette Note, à la demande de l'Autorité, le demandeur a ultérieurement communiqué l'avis rendu par son DPO (ci-après, « **l'avis du DPO** »), l'analyse d'impact réalisée à propos du Projet (ci-après, « **l'AIPD** ») et une note complémentaire

[4] Voir notamment à ce sujet, la réponse communiquée par le demandeur reprise au considérant n° 26.

[5] La demande d'autorisation ne porte pas sur cette partie du processus envisagé par le demandeur.

concernant chaque adresse IP identifiée dans le cadre de la demande initialement introduite auprès de l'Autorité (ci-après, « la **Note complémentaire** »).

II. Examen

La présente décision est structurée comme suit et comporte une annexe :

II.1. Question préalable : publicité des autorisations délivrées par l'Autorité

6. L'Autorité rappelle que conformément à l'article 44 de son ROI, ses décisions sur demande d'autorisations **doivent être publiées sur son site internet**. Elles doivent en outre être motivées en fonction des faits concernés et des informations communiquées par le demandeur[6]. Par conséquent, ceux-ci sont ensuite accessibles au public via internet, dans la mesure où la décision de l'Autorité les cite.

7. La **finalité** de cette publication est **double** : elle a trait d'une part, aux **objectifs de la transparence administrative**, et d'autre part, à la **protection des personnes à l'égard du traitement de données à caractère personnel** elle-même. S'agissant de la transparence administrative, il s'agit : de permettre un contrôle externe effectif de l'action de l'Autorité, de veiller au respect de l'état de droit, de renforcer la confiance du citoyen en l'Autorité et de renforcer l'efficacité et la rationalité du fonctionnement de l'Autorité[7]. En matière de protection des données, l'objectif poursuivi est d'assurer la transparence au regard des traitements de données qui sont autorisés par l'Autorité, et, en relation avec la finalité de la transparence administrative, d'assurer la meilleure contestabilité des décisions d'autorisation (ou de refus d'autorisation) délivrées par l'Autorité[8].

[redacted]

9. A titre préliminaire, l'Autorité a interrogé le demandeur quant à la possibilité pour celle-ci de publier les informations communiquées[10]. Celui-ci a notamment répondu ce qui suit :

---

[6] Voir le considérant n° 21.

[7] C'est de cette manière que l'Autorité avait exprimé la finalité poursuivie par l'article 32 de la Constitution (voir l'avis n° 42/2023 du 9 février 2023 *concernant un avant-projet de loi modifiant la loi du 11 avril 1994 relative à la publicité de l'administration (CO-A-2022-311)*, considérant n° 15).

[8] Il convient de souligner le législateur n'a pas organisé de recours spécifique contre la décision d'autorisation ou de refus d'autorisation de l'Autorité. L'Autorité part dans ce contexte du principe qu'un recours peut être introduit en la matière devant le Conseil d'Etat.

[9] Voir https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage ;

https://en.wikipedia.org/wiki/Traffic_Light_Protocol ; https://ccb.belgium.be/fr/cert/le-traffic-light-protocol-tlp, dernièrement consultés le 26/05/2025.

[10] Plus précisément, elle a attiré l'attention du demandeur sur la nécessité pour celle-ci de publier les informations relatives au Projet envisagé dans le cadre de son analyse et de la motivation de celle-ci, et d'une part, l'a interrogé sur la portée légale de la catégorisation opérée, et sur la possibilité pour l'Autorité de publier dans sa décision sur demande d' autorisation, tout ou partie des éléments de cette note et des réponses communiquées par le demandeur aux questions qui lui sont posées (sur ce point, il appartient au demandeur d'identifier quelles informations communiquées par lui ne peuvent pas être publiées et sur quelle base légale).

« *Conformément à l'**article 26 § 3** de la* [...**loi NIS2**]*, les autorités compétentes dans le cadre de la loi NIS2 (dont le CCB - comme Autorité Nationale de Cybersécurité et CSIRT national)* ***sont tenues de limiter l'accès aux informations découlant de la loi NIS2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de cette même loi afin de sauvegarder les intérêts liés à la sécurité publique.***

[...]

[redacted]

[redacted]

11. Cela étant précisé, l'Autorité prend acte de l'explication fournie par le demandeur. **Il incombe à celui-ci, dans les 10 jours ouvrables à compter de la communication de la présente décision** (la date d'envoi du courrier électronique à l'attention du demandeur par l'Autorité faisant foi), **de lui indiquer clairement quels sont selon lui les passages de la décision de l'Autorité qui ne peuvent pas être publiés aux motifs avancés par lui et repris ci-avant**[12]. L'Autorité insiste sur le fait que cette exigence **constitue une condition de l'autorisation délivrée**, au même titre que ses autres préconisations.

II.2. Portées de la compétence d'autorisation de l'Autorité et de la demande

II.2.1. Principes concernant la compétence d'autorisation de l'Autorité

12. A titre introductif, l'Autorité rappelle les **réserves sérieuses** qu'elle a déjà émises **quant à l'attribution à celle-ci d'une compétence d'autorisation** dans le domaine du traitement des données de communications électroniques[13], et se réfère en particulier aux **considérants nos 58-72 de son avis n° 32/2022** du 16 février 2022 *concernant les articles 7, 25, 1° et 47 du projet de loi portant dispositions diverses en matière d'Economie (CO-A-2021-280, CO-A-2021-281 et CO-A-2021-283)*. Bien que le Projet soit assez différent de l'hypothèse visée par l'Autorité au considérant n° 67 de cet avis[14], l'Autorité attire l'attention du demandeur sur l'intérêt d'étudier plus en profondeur la question

---

[11] Certes, l'article 113, al. 2, de cet arrêté royal, est « *sans préjudice d'autres dispositions légales ou réglementaires spécifiques aux informations non classifiées* ».

[12] Le demandeur surlignera d'une couleur de son choix les passages concernés.

[13] Voir les considérants nos 68 et s. de l'avis n° 32/2022 du 16 février 2022 *concernant les articles 7, 25, 1° et 47 du projet de loi portant dispositions diverses en matière d'Economie (CO-A-2021-280, CO-A-2021-281 et CO-A-2021-283)*. Voir également les considérants nos 59 et s. de l'annexe à l'avis du Comité de direction de l'APD du 25 février 2022 *concernant un avant-projet de loi modifiant la loi du 3 décembre 2017 portant création de l'Autorité de protection des données (AH-2022-0020)*, disponible sur

https://www.autoriteprotectiondonnees.be/publications/avis-concernant-un-avant-projet-de-loi-modifiant-la-loi-du-3-decembre-2017-portant-creation-de-lautorite-de-protection-des-donnees.pdf, dernièrement consulté le 02/06/2025.

[14] « *Par contre, pour les missions de l'IBPT et du CCB qui n'impliquent pas la prise de décision coercitive à l'égard des personnes concernées et qui n'impliquent pas de collecte massive de métadonnées de communications électroniques, en lieu et place de prévoir un système d'autorisation préalable, c'est au législateur qu'il revient d'encadrer adéquatement cet accès en le limitant à des données anonymisées, voire pseudonymisées tout en sécurisant l'utilisation de la clef de pseudonymisation et en prévoyant toute autre mesure adéquate* » (mise en gras omise dans le présent avis).

de savoir si pour un projet tel que le Projet, un encadrement normatif de ce type de traitements de données par le CCB (CSIRT national) ne pourrait pas être mis en place par une adaptation de la Loi NIS2 (et sa précision dans un arrêté royal d'exécution), qui prévoirait notamment des garanties appropriées spécifiques notamment en termes de transparence, et que le contrôle préalable de l'Autorité soit supprimé (en particulier s'agissant du trafic impliquant des entités essentielles ou importantes). L'Autorité concède néanmoins que ce dernier point nécessite une réflexion plus approfondie, qui ne peut être menée dans le contexte de la présente demande.

13. En outre, elle rappelle que **son contrôle non exhaustif** est exclusivement fondé sur les documents et informations communiqués par le demandeur. Il **ne consiste pas en une évaluation de la conformité des traitements de données envisagés au RGPD et aux dispositions de droit belge applicables au traitement de données à caractère personnel**. Autrement dit, la délivrance d'une autorisation ne peut être interprétée comme une garantie de conformité à l'ensemble de ces règles.

14. D'autre part, l'Autorité « *rappelle* [notamment] *que toute ingérence dans le droit au respect de la protection des données à caractère personnel, en particulier lorsque l'ingérence s'avère importante comme c'est le cas en l'espèce, n'est admissible que* ***si elle est encadrée par une norme suffisamment claire et précise et dont l'application est prévisible pour les personnes concernées.*** *Ainsi, toute norme encadrant des traitements de données à caractère personnel, en particulier lorsque ceux-ci constituent une ingérence importante dans les droits et libertés des personnes concernées, doit répondre* ***aux exigences de prévisibilité et de précision*** *de sorte qu'à sa lecture,* ***les personnes concernées, puissent entrevoir clairement les traitements qui sont faits de leurs données et les circonstances dans lesquelles un traitement de données est autorisé****. En exécution de l'article 6.3 du RGPD, lu en combinaison avec les articles 22 de la Constitution et 8 de la Convention européenne des droits de l'homme et des libertés fondamentales, les* ***éléments essentiels du traitement*** *doivent y être* ***décrits avec précision****. Il s'agit, en particulier, de la ou des* ***finalité(s)*** *précise(s) du traitement ; de* ***l'identité du (ou des) responsable(s) du traitement*** *; des* ***catégories de données traitées****, étant entendu que celles-ci doivent s'avérer – conformément à l'article 5.1. du RGPD, « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » ; des* ***catégories de personnes concernées*** *(personnes à propos desquelles des données seront traitées) ; de la* ***durée***

Voir également, *Doc. Parl.*, Ch. des Représentants, n° 55-2572/001, pp. 171-172, et plus particulièrement, n° 55-2572/002, pp. 127-128, où le législateur énonce les raisons pour lesquelles il ne suit pas l'approche (consistant à se passer d'un mécanisme d'autorisation préalable) proposée par l'Autorité.

Le Projet implique quant à lui des collectes régulières et continues de métadonnées de communications électroniques non pseudonymisées ou anonymisées, liées au trafic transitant par des adresses IP dédiées à des C2-servers et impliquant des entités essentielles ou importantes, sans préjudice du débat concernant la collecte de métadonnées de communications électroniques relatives au trafic vers d'autres victimes potentielles (personnes morales ou physiques non visées par les obligations de la Loi NIS2).

de conservation des données *; des destinataires ou* ***catégories de destinataires*** *auxquels leurs données sont communiquées et les* ***circonstances dans lesquelles et les raisons pour lesquelles elles seront communiquées*** *ainsi que* ***toutes mesures visant à assurer un traitement licite et loyal de ces données à caractère personnel*** » (mise en gras dans le texte original)[15].

15. A cet égard, l'article 54, § 3, du ROI[16] rappelle ces principes au regard de la compétence d'autorisation de l'Autorité.

16. Ces **positions et principes ont également été rappelés dans le contexte de la première autorisation délivrée par l'Autorité**à savoir l'Autorisation (délivrée) n° 001/2024 du 6 novembre 2024 *concernant une demande d'autorisation visée à l'article 15, § 2, al. 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (AH-2024-0010)*[17].

17. Enfin, l'Autorité souligne que **l'article 21, § 1er, de la Loi NIS2** dispose que « *dans le cadre de l'exercice de ses compétences, le CSIRT national prend toutes les mesures adéquates afin de réaliser les objectifs définis aux articles 19 et 20. Ces mesures doivent être* ***proportionnelles*** *à ces objectifs, et* ***respecter les principes d'objectivité, de transparence et de non-discrimination*** » (mis en gras par l'Autorité).

II.2.2. Portée de la demande d'autorisation

18. En substance, le demandeur demande à l'Autorité de **modaliser la compétence d'autorisation qui lui a été attribuée** par le législateur en délivrant une **autorisation générale** relative à son Projet encadrant le **traitement continu** de métadonnées de communications électroniques[18]. En autorisant

---

[15] Avis de l'Autorité n° 108/2021 du 28 juin 2021, *concernant un avant-projet de loi relatif à la collecte et à la conservation des données d'identification, de trafic et de localisation dans le secteur des communications électroniques et à leur accès par les autorités et un projet d'arrêté royal modifiant l'arrêté royal du 19 septembre 2013 portant exécution de l'article 126 de la loi du 13 juin 2005 relative aux communications électroniques (CO-A-2021-099)*, considérant n° 27.

[16] Selon lequel :

« *Conformément aux principes de prévisibilité et de légalité notamment consacrés dans l'article 22 de la Constitution, l'Autorité ne peut se substituer au législateur et déterminer les éléments essentiels des traitements de données à caractère personnel dont l'autorisation est sollicitée.*

Dans le cadre de sa compétence d'autorisation visée aux paragraphes 1er et 2, et sur base des informations communiquées par le demandeur, le cas échéant, à la suite d'une demande d'informations complémentaires du Service, le Service vérifie que les éléments du traitement de données sollicité reposent sur et sont conformes à la (ou aux) disposition(s) normatives de rang législatif qui les identifie(nt).

Le Service vérifie également, dans la mesure du possible et sur la même base, si les modalités du projet de traitement soumis à autorisation sont conformes aux principes de nécessité et de proportionnalité en matière de protection du droit au respect la vie privée et du droit à la protection des données à caractère personnel ».

[17] Disponible sur https://www.autoriteprotectiondonnees.be/publications/autorisation-n0-001-2024-du-6-novembre-2024.pdf, dernièrement consulté le 02/06/2025.

[18] Il se dégage notamment ce qui suit de la Note communiquée :

le Projet en général, l'Autorité conserverait ensuite, en pratique, la possibilité de réagir au cas par cas, dans le cadre de la mise en œuvre du Projet, à la suite de la réception de mises à jour régulières de la liste des adresses IP dédiées à des C2-servers communiquées aux opérateurs. Elle pourrait demander des informations complémentaires au CCB (CSIRT national) et le cas échéant, retirer l'une ou l'autre des adresses IP reprises dans la mise à jour concernée de cette liste. Les opérateurs devraient alors supprimer les métadonnées de communications électroniques concernées, collectées jusque-là[19]. Le CCB (CSIRT national) devrait également supprimer les données reçues entre-temps par lui, sur cette base (selon la réactivité de l'Autorité, le CCB (CSIRT national) aura en effet reçu ou pas, entre-temps, des métadonnées collectées par l'opérateur).

19. L'Autorité considère que **cette approche ne peut pas être suivie**. En effet, **le législateur n'a pas donné à l'Autorité la compétence de réglementer la communication** continue de métadonnées de communications électroniques par les opérateurs, à la demande du CCB (CSIRT national), moyennant une **autorisation générale** fixant notamment les conditions applicables et les possibilités pour l'Autorité **d'intervenir ponctuellement et *a posteriori***, dans ce flux de données[20]. Et si le législateur avait voulu attribuer une telle compétence à l'Autorité, il ne l'aurait pu sans risquer de contrarier le droit constitutionnel belge[21]. Ainsi, conformément à l'article 21, § 4, de la Loi NIS2 et à **l'article 23, § 3, de la LCA**, ce qui doit être l'objet de l'autorisation préalable de l'Autorité, c'est

[redacted]

[20] Le délai fixé par le législateur pour délivrer l'autorisation concernée confirme cette approche. Si le **délai d'autorisation excessivement court**, compte-tenu du fait qu'il ne vise par définition pas les situations d'urgence (en cas d'urgence, le demandeur peut passer outre l'autorisation de l'Autorité chargée en suite, de réaliser un contrôle ultérieur), **fixé par le législateur** (dix jours – samedis, dimanches et jours fériés exclus, à compter de la complétude du dossier), est déjà difficilement compatible avec la mise en œuvre d'un contrôle préalable effectif par l'Autorité à l'égard d'une demande concrète d'accès à des métadonnées de communications électroniques, **il est *a fortiori* inadapté pour une situation dans laquelle l'Autorité devrait penser l'encadrement général d'un accès à des métadonnées**.

Comparativement et historiquement, c'est d'un délai de deux mois dont l'Autorité jouissait pour s'exprimer à l'égard de textes normatifs. Remarque : désormais, les demandeurs d'avis peuvent demander que l'avis leur soit délivré dans un délai d'un mois à compter de la complétude du dossier (cela étant constaté sans préjudice de la position de l'Autorité quant à la pertinence de ce délai).

[21] A ce sujet, l'Autorité renvoie *mutatis mutandis*, à la position étayée à l'appui notamment, de la jurisprudence de la Cour constitutionnelle et de la légisprudence du Conseil d'Etat, qu'elle a exprimée à propos du Comité de Sécurité de l'Information, aux considérants nos 19-23 de son avis n° 268/2022 du 21 décembre 2022 *concernant un avant-projet de loi concernant des mesures de police administrative en matière de restrictions de voyage et de Formulaire de Localisation du Passager et modifiant diverses dispositions relatives au Comité de sécurité de l'information (CO-A-2022-299)*. Voir notamment et également l'avis du Conseil d'Etat n° 69.166/4 du 10 juin 2021, *sur un avant-projet de loi 'portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques'*, paragraphe 2.3.1., en particulier. Le droit européen n'impose clairement pas, en l'occurrence, une intervention de nature réglementaire de la part de l'Autorité.

« ***une demande de métadonnées*** *de communications* électroniques » (mis en gras et souligné par l'Autorité) qui sera adressée à un opérateur par le CCB (CSIRT national), et ce, conformément à la jurisprudence de la Cour de justice en la matière.

20. En particulier, **le contrôle de l'Autorité prévu dans les articles 21, § 4, de la Loi NIS2 et 23, § 3, de la LCA**, est clairement et explicitement un contrôle **préalable**, sauf hypothèse de cas urgent. **Ne permettre à l'Autorité que de réagir à une demande d'accès déjà communiquée aux opérateurs et par conséquent, à un traitement déjà initié (les métadonnées sont collectées par l'opérateur et sont également communiquées au CCB (CSIRT national))**, reviendrait à mettre en place un **contrôle ultérieur contraire aux dispositions précitées**. Comme la Cour de justice l'a déjà exprimé : « *le contrôle indépendant requis conformément à l'article 15, paragraphe 1, de la directive 2002/58 doit intervenir* ***préalablement à tout accès aux données concernées, sauf en cas d'urgence dûment justifiée****, auquel cas ledit contrôle doit intervenir dans de brefs délais. En effet, un contrôle ultérieur ne permettrait pas de répondre à l'objectif du contrôle préalable, qui consiste à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire* »[22] (mis en gras et souligné par l'Autorité).

21. En conclusion, **chaque demande** de communication de métadonnées de communications électroniques **doit être soumise pour autorisation préalable à l'Autorité, avant** de pouvoir être adressée à un opérateur. Il incombe ensuite à l'Autorité de prendre une **décision motivée**[23].

22. Cela étant précisé, premièrement, il n'est pour autant pas exclu que lorsque le contexte juridique et factuel de demandes subséquentes est identique à celui d'une première demande, **ces demandes subséquentes se réfèrent aux contextes juridique et factuel de la première demande et exposé dans l'autorisation délivrée à cette occasion**, pour autant que ces demandes subséquentes **restent motivées et circonstanciées en fonction de ce contexte et des éléments propres (notamment factuels) relatifs à ces demandes**[24].

23. Il en est **de même *mutatis mutandis* s'agissant de l'hypothèse d'une demande concernant un contrôle ultérieur** dans le cadre du Projet, dans le cas où en raison de **l'urgence**, le CCB (CSIRT national) aurait dû communiquer l'adresse IP d'un C2-server et collecter les métadonnées concernées directement auprès d'un opérateur, sans autorisation préalable de l'Autorité.

---

[22] C.J.U.E. (assemblée plénière), arrêt du 30 avril 2024 (QUADRATURE DU NET 2), aff. C-470/21, paragraphe n° 127.

[23] Article 23, § 3, dernier alinéa de la LCA.

[24] Dans un contexte juridique toutefois différent (demandes d'écoutes téléphonique dans le domaine du droit pénal), voir par exemple C.J.U.E. (troisième chambre), arrêt du 16 février 2023 (HYA, IP, DD, ZI, ET SS), aff. C-349/21, paragraphes nos 50 et s.

24. Deuxièmement, s'agissant d'une première demande dans le cadre du Projet particulier du demandeur, **l'Autorité est favorable à la démarche suivie par celui-ci** consistant à lui soumettre une demande d'autorisation préalable initiale, plutôt que, à supposer que l'urgence puisse être invoquée dans le cadre de cette demande (ce qui n'a pas été évalué par l'Autorité en l'occurrence), de placer l'Autorité devant le fait accompli, dans une situation de contrôle ultérieur.

II.3. Finalité des traitements de données et mission d'intérêt public du CCB (CSIRT national) fondant ces traitements

25. S'agissant de la **finalité concrète** poursuivie par le Projet et les traitements de données y liés, l'Autorité a invité le demandeur à confirmer clairement et précisément que la seule finalité poursuivie par le Projet est d'**informer les victimes potentielles des C2-servers afin que celles-ci prennent les mesures nécessaires éventuelles pour se protéger contre les activités menées via ces serveurs** (le cas échéant, en demandant une intervention du CSIRT national, et à charge pour les entités concernées, selon les cas d'espèce, de s'acquitter des obligations d'information leur incombant en exécution de la Loi NIS2 – alerte précoce, etc.)[25]. **L'AIPD précise que l'effet/le résultat recherché sur les personnes est** « *que les personnes concernées soient informées aussi vite que possible des cybermenaces émanant de serveurs C2 dont elles font l'objet et que ces personnes prennent les mesures nécessaires afin de se protéger, si possible avant que les menaces ne se concrétisent* ».

26. Le demandeur a notamment répondu ce qui suit :

> « *L'objectif du projet* [...] *vise* ***à la fois l'information des responsables*** *des systèmes d'information victimes de serveurs C2 (afin que ceux-ci puissent prendre les mesures nécessaires pour se protéger)* ***<u>et</u> l'examen de défaillances de la sécurité des réseaux*** *ou de services de communications électroniques ou des systèmes d'information.*
> *Ces objectifs rejoignent chacune des* ***<u>trois</u> finalités visées à l'article 21, § 2, alinéa 2, de la loi NIS2***
>
> *1° sans finalité à caractère pénal. la prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, en ce compris des faits qui relèvent de la criminalité grave : un avertissement fourni à une entité NIS2, à une infrastructure critique, à une organisation privée, à une administration publique*

[25] La Note n'est pas totalement claire à ce sujet (elle indique notamment, même si ce passage est lié au cadre légal, « *2) Het CCB streeft bij de opvraging drie doestellingen na: a) het voorkomen, onderzoeken en opsporen van inbreuken online; b) het voorkomen van ernstige bedreigingen voor de openbare veiligheid; c) het onderzoeken van beveiligingsproblematieken. 3) Deze bevoegdheid van CCB dient uitgevoerd te worden zonder afbreuk te doen aan of zich te mengen in de bevoegdheden van de gerechtelijke autoriteiten en politie* »).

*ou à un citoyen permet **de prévenir et détecter** des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques* [...] ;

*2° la prévention de menaces graves contre la sécurité publique : un avertissement fourni à une entité NIS2, à une infrastructure critique ou à une administration publique permet de protéger celles-ci contre des cybermenaces graves ; **La finalité** poursuivie par le CCB (l'identification et l'information de victimes des serveurs C2 afin que celles-ci puissent se protéger) consiste à **prévenir des dommages** que provoqueraient les attaques menées au travers de serveurs C2. Les dommages causés par les cyberattaques menées grâce à ces serveurs C2 qualifient effectivement ce type de menace de menace grave contre la sécurité publique ;*

*3° l'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information : l'analyse des métadonnées permet de détecter des systèmes d'information infectés ou vulnérables **et de remédier à ces défaillances**.*

Les menaces découlant des activités de serveurs C2 et leur réseau de machines « zombies » (botnet) sont bien connues. Ces serveurs servent notamment à :
• dérober ou modifier de l'information sur les machines compromises (avec revente ultérieure des informations) ;
• identifier et infecter d'autres machines par diffusion de virus et de programmes malveillants (malwares) ;
• participer à des attaques groupées de déni de service (DDoS) ;
• exploiter la puissance de calcul des machines ou effectuer des opérations de calcul distribué notamment à casser des mots de passe ;
• voler des sessions utilisateurs (compte utilisateur et mot de passe) ;
• miner des cryptomonnaies ;
• etc;

*Les serveurs C2 permettent à un adversaire de communiquer avec les systèmes compromis afin de les contrôler. La commande et le contrôle (« commander and control ») désignent les techniques que les adversaires peuvent utiliser pour communiquer avec les systèmes qu'ils contrôlent au sein du réseau d'une victime. Les adversaires **tentent généralement d'imiter le trafic normal et attendu** afin d'éviter toute détection. Il existe de nombreuses façons pour un adversaire d'établir une commande et un contrôle avec différents niveaux de furtivité, en fonction de la structure du réseau et défenses de la victime. (Command and Control. Tactic TA00ll - Enterprise I MITRE ATT&CK®)* » (mise en gras modifiée par l'Autorité, souligné par l'Autorité).

« Les entités essentielles ou importantes au sens de la loi NIS2 ***devront,*** *le cas échéant,* ***procéder à une notification d'incident NIS2*** *(si les critères d'un incident signification sont réunis) et/ou à une notification de violation de données à caractère personnel (si les critères sont réunis). Elles devront également prendre les mesures nécessaires pour prévenir la survenance d'un incident et mettre en oeuvre les mesures de sécurité appropriées (art. 30 de la loi NIS2).*

Les serveurs C2 identifiés sont susceptibles également d'entrainer des dommages pour des organisations ou des particuliers qui ne sont ***pas des entités NIS2****. Ces organisations ou particuliers ont toujours la* ***possibilité de notifier volontairement*** *un incident au CCB (art. 38 de la loi NIS2).*

Dans ce cas, le CCB doit traiter ces notifications de la même manière que les notifications obligatoires, avec la ***possibilité de traiter les notifications obligatoires en cours de manière prioritaire****.*

Il relève de la mission du CCB d'adresser des messages d'alerte aux organisations ou particuliers victimes de cybermenaces et de prévenir la survenance de cyberincident.

Par ailleurs, les organisations concernées qui sont soumises au RGPD devraient prendre des mesures nécessaires pour sécuriser leurs traitements de données à caractère personnel, en vertu de l'article 32 du RGPD » (mis en gras par l'Autorité).

27. L'Autorité a également interrogé le demandeur quant au **mécanisme « d'alerte précoce »** sur lequel la Note met l'accent, visé à l'article 19, § 1er, 2°, de la Loi NIS2. La Loi NIS2 n'est toutefois pas totalement claire à son sujet. En effet, en tant que tel, **le mécanisme d'alerte précoce n'est défini ni par la Loi NIS2, ni par la Directive (UE) 2022/2555** du Parlement européen et du Conseil du 14 décembre 2022 *concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2)* (ci-après, « **la Directive NIS2** »). Le concept **d'alerte précoce existe néanmoins dans le contexte des notifications** visées dans le cadre des obligations d'information des entités concernées[26]. Et l'article 19, § 1er, 2°, de la Loi NIS2 vise quant à lui, outre le mécanisme d'alerte précoce, la « *diffusion de messages d'alerte* ». En relation avec ce questionnement, s'est aussi posée la question de savoir de quelle activité relève le service « **Cyber Threat Alerts** »[27].

---

[26] Voir art. 23, 4., a), de la Directive NIS2 et art. 35, § 1er, 1°, de la Loi NIS2.

[27] Voir https://atwork.safeonweb.be/fr/protect-my-organisation/cyber-threat-alerts, dernièrement consulté le 02/06/2025.

28. Interrogé à propos de ce contexte, le demandeur a notamment répondu ce qui suit :

> « *L'obtention de métadonnées de communications électroniques et l'avertissement des victimes relève* ***notamment de la mission visée à l'article 19, § 1er, alinéa 1er, 2°, de la loi NIS2*** *- à savoir l'activation du mécanisme d'alerte précoce, de la diffusion de messages d'alerte, d'annonces et de diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents. Ce projet* ***concourt également aux tâches de surveillance et d'analyse des cybermenaces, des vulnérabilités et les incidents - notamment l'analyse dynamique des risques et de données forensiques*** *(19, § 1er, alinéa 1er, 1 ° et 40).*
>
> [...].
>
> *Le législateur a donc prévu explicitement cette nouvelle compétence de l' APD (contrôle de l'accès à des métadonnées de communications électroniques) au profit notamment du CCB.*
>
> *Pour rappel,* ***les tâches du CCB ne sont pas exercées pour des finalités à caractère pénal****, même si les actions entreprises participent à la prévention d'incident et d'infractions en matière de cybercriminalité. L'article 21 NI52 précise explicitement que les missions du CCB sont exercées « sans porter atteinte aux, ou sans s'immiscer dans les compétences des personnes exerçant la police judiciaire ni des autorités judiciaires ».*
>
> [...] » (mis en gras par l'Autorité, soulignement modifié par l'Autorité).
>
> « *Le «* ***mécanisme d'alerte précoce » du CCB visé à l'article 19, § 1er, alinéa 1er, 2°, de la loi NIS2 doit être clairement distingué de la notification « alerte précoce »*** *d'un incident significatif (dans les 24 heures) visé à l'article 35, § 1er, 1 °.*
>
> *L'article 19, § 1er, alinéa 1er, 2°, de la loi NIS2 concerne les missions et obligations légales du CCB (comme CSIRT national), notamment d'activer « le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents » auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel ».* ***Il s'agit pour le CCB de développer des projets visant à informer au maximum les entités NIS2, d'autres autorités publiques, les organisations privées ou les citoyens (« autres parties prenantes concernées ») sur les cybermenaces, les vulnérabilités et les incidents (si possible en temps quasi réel)****. Le présent projet* ***vise à remplir cette mission légale***

dans le prolongement des projets existants (Cyber Threat Alerts, Early Warning System, Spear Warning). Les mécanismes d' « alerte « précoce » et « de diffusion de message » d'alerte visé à l'article précité sont effectués par le CCB, afin de prévenir le plus vite possible *une ou plusieurs entité (personne morale ou physique) d'une menace de cybersécurité, si possible avant que cette menace se concrétise ou conduise à un incident.*

L'article 35, § 1er, 1 ° de la loi NIS2 concerne lui les obligations d'information à charge des entités essentielles ou importantes NIS2 [...] » (mis en gras et souligné par l'Autorité).

29. A l'aune de ces réponses, l'Autorité considère que **le Projet est fondé sur <u>l'article 19, § 1er, 2°, de la Loi NIS2</u>**. Il s'agit de diffuser des messages d'alerte et des informations sur les cybermenaces et les vulnérabilités, auprès des victimes potentielles, si possible en temps réel. Ce faisant, le Projet a effectivement et en conséquence un effet préventif quant à la réalisation des menaces et dommages auprès des cibles des C2-servers (article 21, § 2, 1° et 2°, de la Loi NIS2)[28]. Et il nécessite dans sa mise en œuvre l'examen de défaillances de la sécurité des réseaux de communications électroniques et des systèmes d'information (article 21, § 2, 3°, de la Loi NIS2), soit la détection, l'observation et l'analyse des problèmes de sécurité informatique liés aux menaces concernées (article 19, § 1er, 10), de la Loi NIS2).

30. L'Autorité a interrogé le demandeur quant à la question de savoir s'il avait connaissance **de l'existence d'une initiative similaire à celle du Projet dans un autre Etat Membre**[29]. Celui-ci a notamment indiqué ne pas être informé d'une telle initiative dans un autre Etat Membre de l'Union.

<u>II.4. Entités victimes potentielles concernées et métadonnées collectées</u>

31. Les traitements de données impliqués dans le cadre du Projet, et en particulier l'identification concrète des métadonnées qui seront collectées et communiquées au CCB dépend des C2-servers qui seront sélectionnés et identifiés par le CCB (CSIRT national) ainsi que des victimes (potentielles) qui seront identifiées. **Les méthodes et critères de sélection des C2-servers et des victimes concernés ont en outre un impact décisif dans l'applicabilité des règles de protection des données**. C'est à l'aune de ceux-ci que peuvent notamment être appréciés le respect du principe de finalité, du principe de proportionnalité (impliquant ceux de minimisation et d'exactitude des données) et le

---

[28] L'AIPD précise clairement que l'effet/résultat recherché sur les personnes est « *que les personnes concernées soient informées aussi vite que possible des cybermenaces émanant de serveurs C2 dont elles font l'objet et que ces personnes prennent les mesures nécessaires afin de se protéger, si possible avant que les menaces ne se concrétisent* ».

[29] Dans un premier temps, il a répondu ce qui suit :

« *L'équivalent du CCB en France (ANSSI) dispose de compétences en vertu de L2321-2-1 du Code de la défense français lui permettant le recueil de ce type de données sur le réseau d'un opérateur de communications électroniques (copie de serveurs) avec un contrôle de l'ARCEP (l'Autorité de régulation des communications électroniques)* ».

caractère objectif et non-discriminatoire du Projet entrepris, dans l'exercice de sa mission pertinente par le CCB (CSIRT national).

32. **Au-delà** de la question de la licéité des traitements de données à caractère personnel, la qualité de ces méthodes et critères **contribue à prévenir la réalisation du risque principal causé par le Projet**, à savoir la collecte de métadonnées relatives à des communications électroniques (et l'identification ultérieure des parties à ces communications) qui ne concernent pas des C2-servers et leurs victimes, et les conséquences y liées (interception et conservation illicite de métadonnées de communications électroniques ; possibilité de détournement du système mis en place par une source ; impact sur les employés ou visiteurs de l'entité concernée qui sont susceptibles d'être impliqués dans le trafic entre le serveur concerné et le système d'information de l'entité[30] ; démarche(s) entreprise(s) par la victime supposée concernée à l'encontre de l'adresse IP identifiée et de son titulaire).

II.4.1. Métadonnées traitées

33. Le Projet prévoit la collecte des métadonnées de communications électroniques qui ont eu lieu vers et depuis les adresses IP des C2-servers listés et ce, jusqu'à ce que la liste de ces adresses IP soit mise à jour par le CCB (CSIRT national). **Ces métadonnées sont les suivantes : « *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes* »**. Elles n'appellent en tant que telles, pas de commentaire de la part de l'Autorité.

34. A la demande de l'Autorité, le demandeur a confirmé que **les métadonnées collectées ne porteront que sur les communications électroniques postérieures au moment où la demande de communication de métadonnées est adressée à l'opérateur concerné**. L'Autorité attire l'attention du demandeur sur le fait qu'à l'avenir, dans le cadre du Projet, il pourrait également demander l'autorisation de traiter les métadonnées relatives aux communications électroniques émises à partir **de la date d'introduction de sa demande** d'autorisation auprès de l'Autorité, **pour autant que les** opérateurs concernés aient conservé ces données dans le cadre de leurs activités de fourniture de services de communications électroniques (et non en vertu de quelque obligation légale de conserver ces données[31]).

35. Interrogé quant aux **opérateurs concernés**, le demandeur a répondu que « *La demande de métadonnées peut être adressée à tous les opérateurs de communications électroniques actifs en Belgique. Conformément aux dispositions de la loi du 13 juin 2005 relative aux communications électroniques, tout opérateur, entendus comme une personne ou entreprise qui fournit un réseau*

---

[30] Voir le considérant n° 101.

[31] Un tel questionnement posant la question de la légalité des obligations de rétention de métadonnées de communications électroniques imposées aux opérateurs, ce qui dépasse le contexte de la demande.

public de communications électroniques ou un service de communications électroniques accessible au public en Belgique, est susceptible de se voir adresser une demande. ***Dans une première phase, Belnet serait contacté en priorité*** » (mis en gras par l'Autorité).

36. L'Autorité attire l'attention du demandeur sur le fait que **sa demande d'autorisation doit identifier les opérateurs concernés**. En l'occurrence, l'Autorité note que la demande porte sur des métadonnées **traitées par l'opérateur Belnet**.

II.4.2. Entités victimes concernées

Entités relevant du champ d'application de la Loi NIS2 et autres entités

37. L'Autorité a observé sur la base de la Note communiquée que le Projet semblait aller au-delà de l'identification de victimes constituant des entités soumises aux obligations consacrées dans la Loi NIS2 (c.-à-d., des entités essentielles ou importantes) : sont visées les victimes « *inclusief NIS-2-entiteiten, overheidstinstanties, ondernemingen, burgers, enz.* ». En ce qu'il déborderait **du champ d'application *ratione personae* des obligations consacrées dans la Loi NIS2**, le fondement juridique du Projet pourrait poser question.

38. Interrogé à ce sujet, le demandeur a répondu ce qui suit :

> « *La loi NIS2* ***contient à la fois des dispositions applicables aux seules entités NIS2*** *(l'enregistrement, la gestion des risques en matière de cybersécurité, la notification obligatoire des incidents significatifs, la supervision, etc) - champ d'application ratione personae « entités NIS2 »* ***mais aussi d'autres dispositions à destination de toutes organisations ou personnes situées en Belgique*** *-ratione personae « toute entité/citoyen » (et donc non limitées aux seules entités NIS2).*
>
> ***Parmi les dispositions à portée plus large*** *(non limitées aux seules entités NIS2), on peut citer, par exemple, les tâches du CCB* ***comme autorité nationale de cybersécurité, autorité de gestion des crises cyber et CSIRT national (art. 17, 18, 19, 20 et 21), le signalement des vulnérabilités et protection des hackeurs éthiques (art. 22 et 23), les dispositions en matière de coopération au niveau national (art. 25), la stratégie nationale en matière de cybersécurité (art. 28), les notifications volontaires (art. 38) ou sur le traitement des données à caractère personnel (titre 6)****.*
>
> *L'article 19, § 1er, alinéa 1er, 2°, de la loi NIS2 dispose qu'une des tâches du CCB est d'activer « le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités*

essentielles et importantes concernées ***ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées****, si possible en temps quasi réel » (nous soulignons). Il ressort de la disposition précitée que* ***la tâche d'alerte précoce du CCB n'est pas limitée aux entités essentielles et importantes NIS2 mais est bien étendue aux autres entités établies en Belgique, qu'ils s'agissent d'entités publiques, privées, ou de personnes physiques*** » (mis en gras par l'Autorité).

39. L'Autorité prend acte de cette explication. Toutefois, elle attire l'attention du demandeur sur les points suivants.

40. L'Autorité souligne qu'au regard des **principes de prévisibilité et de légalité** rappelés précédemment[32], la possibilité du Projet ne se dégage pas si clairement de la Loi NIS2. Que le CCB (CSIRT national) ait la possibilité en vertu de la législation, d'informer à propos des menaces conformément à l'article 19, § 1er, 2°, de la Loi NIS2 (et de détecter et analyser celles-ci)[33] si possible en temps réel, et de collecter des métadonnées de communications électroniques à certaines fins lorsque cela est nécessaire à l'exercice de ses missions, n'implique pas nécessairement que le CCB (CSIRT national) puisse collecter en temps réel les métadonnées **de toutes les communications électroniques** provenant ou à destination d'adresses IP dédiées à des C2-servers (les menaces) qu'il identifie/détermine, concernant des victimes potentielles et ce, **quelles que soient ces victimes,** afin d'envoyer des messages d'avertissement. Cela d'autant moins que le mécanisme « d'alerte précoce » auquel se réfère le CCB n'est pas défini par le droit applicable.

41. En l'occurrence, dès lors que la Loi NIS2 a pour objectif clair et explicite de par son intitulé même et du dispositif qu'elle prévoit, d'établir un cadre « *pour la cybersécurité des réseaux et des systèmes d'information* ***d'intérêt général pour la sécurité publique*** » (mis en gras par l'Autorité), il est **moins prévisible qu'en exécution de la Loi NIS2, le Projet puisse porter également sur les métadonnées de communications électroniques** (et l'identification ultérieure) **de personnes** (morales et physiques) **qui ne sont pas soumises au champ d'application *ratione personae* des obligations de la Loi NIS2,** en ce qu'elles ne seraient ni des entités essentielles, ni des entités importantes. Certes, les entités autres que les entités essentielles ou importantes peuvent effectivement adresser des notifications au CCB (CSIRT national). Ces notifications sont cependant **volontaires** et les notifications obligatoires peuvent être traitées prioritairement[34]. Les **tâches d'assistance du CCB (CSIRT national),** conformément à la Loi NIS2, semblent aussi, dans la logique de la finalité de la Loi NIS2, **tournées vers les entités essentielles ou importantes**[35]. Et

---

[32] Voir les considérants nos 14-15.

[33] Voir plus précisément, le considérant n° 29.

[34] Voir l'article 38 de la Loi NIS2.

[35] Selon l'article 19, § 1er, de la Loi NIS2, le CCB (CSIRT national) a pour tâche de « *surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national et, sur demande, apporter une assistance aux entités essentielles et importantes*

la Loi NIS2 facilite directement les possibilités de repérage du trafic des entités essentielles ou importantes par le CCB (CSIRT national) dès lors que celui-ci **doit recevoir les plages IP utilisées par ces entités** (y compris leurs mises à jour) ainsi que leurs données de contact[36]. Inversement d'ailleurs, ces éléments renforcent le caractère prévisible du Projet par rapport au dispositif de la Loi NIS2, en ce qui concerne les entités essentielles ou importantes.

42. Or dans le contexte normatif applicable au Projet, l'accès aux métadonnées de communications électroniques doit être limité à ce qui est **strictement nécessaire**[37]. Il existe d'ailleurs, en outre, **d'autres manières d'informer les autres « parties prenantes »**[38] (et les entités essentielles ou importantes d'ailleurs) qui ne nécessitent pas de traiter des métadonnées de communications électroniques[39].

43. **Cela étant précisé, compte-tenu de la finalité limitée du Projet telle que reprise dans la présente décision[40], de l'impact des menaces concernées et de l'intérêt du Projet pour la cybersécurité en Belgique de manière générale**, force est de constater que ces autres manières d'informer atteindraient moins efficacement l'objectif d'intérêt public poursuivi par la Loi NIS2 (soit la sécurité des systèmes d'information d'intérêt général pour la sécurité publique) et que le Projet s'inscrit bien dans l'esprit de cette loi, sans préjudice des commentaires ultérieurs[41].

44. En conclusion, **l'Autorité considère que le Projet peut concerner à la fois les métadonnées de communications électroniques entre les C2-servers et les entités essentielles ou importantes visées par la Loi NIS2, et les métadonnées de communications électroniques entre ces mêmes C2-servers ainsi que d'autres entités** non soumises aux obligations de la Loi NIS2.

45. **Cependant s'agissant de ces autres entités,** l'Autorité considère que cette interprétation de la Loi NIS2 **devrait être confirmée à brève échéance par le législateur**, soit par une loi interprétative, soit via une modification de la Loi NIS2[42], afin de garantir notamment la sécurité juridique des traitements de données mis en œuvre. Il appartient au CCB d'entreprendre des démarches en ce sens

---

concernées pour surveiller en temps réel ou quasi réel leurs réseaux et systèmes d'information »; « *réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées, le cas échéant* », « *réaliser, à la demande d'une entité essentielle ou importante, un scan proactif des réseaux et des systèmes d'information de l'entité concernée afin de détecter les vulnérabilités susceptibles d'avoir un impact important* ».

[36] Voir les articles 13 et 14 de la Loi NIS2.

[37] Voir notamment l'article 21, § 2, de la Loi NIS2.

[38] A supposer que les « *parties prenantes* » puissent bien être toute victime potentielle, la Loi NIS2 ne définissant pas qui sont ces parties prenantes (en l'occurrence, elles seraient, dans le cadre du Projet, des catégories de personnes concernées).

[39] Voir les considérants nos 79 et s.

[40] Voir le considérant n° 39.

[41] Voir les considérants nos 73 et s.

[42] Si le législateur entendait modifier la Loi NIS2 sur la base du Projet, voir également le considérant n° 12.

et l'Autorité prêtera attention à ce point dans le cadre des demandes d'autorisation (ou de contrôle ultérieur) futures.

Critère sur la base duquel une entité NIS2 est considérée comme une victime potentielle

46. La Note communiquée par le demandeur indique que « *Belgische gebruikers worden enkel geïdentificeerd als er* ***sterke aanwijzingen zijn dat*** *de gebruiker* ***contact heeft gehad*** *met een kwaadaardig buitenlands IP-adres* » (mis en gras par l'Autorité). A cet égard, l'Autorité a interrogé le demandeur quant à la question de savoir quels critères et données sont utilisés pour déterminer qu'il y a de tels « *sterke aanwijzingen* » ; elle l'a invité à confirmer que l'objectif était de prendre contact avec toute victime potentielle concernée et dans la négative, lui a demandé de communiquer les critères utilisés pour identifier les victimes à contacter.

47. Le demandeur a précisé ce qui suit :

> « ***Les communications électroniques en provenance et à destination*** *de serveurs vérifiés par le CCB comme command-and-control (C2)* ***doivent être considérées avec des indices sérieux comme liées à une activité malveillante. L'analyse des métadonnées par le CB pourra confirmer*** *la nature malveillante de ces activités, et éventuellement fournir plus de contexte et le niveau d'urgence de l'attaque* » (mis en gras par l'Autorité).
>
> « *L'objectif est bien d'analyser toutes les métadonnées et de pouvoir prendre contact avec toute victime concernée (personne morale ou personne physique)* ».

48. En outre, dès lors **qu'aucune donnée relative au contenu** des communications électroniques n'est collectée, l'Autorité a invité le demandeur à préciser sur la base de quelle **méthode** et de quels **critères** il est considéré que les métadonnées collectées (à savoir, « *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes* ») **indiquent qu'une entité est potentiellement une victime/cible du C2-server concerné**. En relation avec ce questionnement, le tableau communiqué dans la Note indique aux points nos 5.1 et 5.2., ce qui suit : « *5.1 CCB slaat de ontvangen data beveiligd op voor maximaal 1 jaar, dit* ***om grondige analyses te kunnen maken over meerdere gegevens****. 5.2 CyTRIS analyseert de data,* ***onderscheidt de malicious communicatie van de normale*** » (mis en gras par l'Autorité). L'Autorité a demandé au demandeur de confirmer la finalité de ces « *grondige analyses* »[43], l'a interrogé sur le temps nécessaire à l'identification d'une victime, sur les critères utilisés pour distinguer les communications malveillantes

[43] A ce sujet, voir les considérants nos 111 et s.

des communications normales et enfin, l'a invité à clarifier si un C2-server peut, en pratique, être utilisé à des fins à la fois licites et illicites.

49. Le demandeur a renvoyé vers la réponse citée au considérant n° 47 et a en outre répondu ce qui suit :

[redacted]

« *Les analyses approfondies reprises au point 5.1 peuvent permettre de* ***faire des liens dans le temps entre les activités de différents serveurs C2*** *et de* ***suivre efficacement les actions malveillantes*** *des auteurs et des menaces* » (mis en gras par l'Autorité).

« *Le temps d'analyse par le CCB des données reçus* ***dépendra de la quantité de ces données, mais peut s'actualiser assez vite (quelques heures/jours)****. Lorsque l'on constate l'existence d'un système victime, le CCB effectue la demande auprès l'ISP concerné pour identifier de l'organisation ou la personne avec l'adresse IP concernée. Le délai d'identification dépend de l'urgence de la requête envoyée à l'opérateur (le CCB peut déterminer le délai endéans lequel l'opérateur répond à sa demande, en fonction de l'urgence de celle-ci, conformément à l'article 21, § 2, alinéa 3). Il est nécessaire d'agir dans les plus brefs délais pour avertir utilement les responsables des systèmes victimes* » (mis en gras par l'Autorité).

« *Les* ***communications électroniques échangées entre un serveur command-and-control (C2) - (vérifié par le CCB) et une autre adresse IP doivent être considérées avec des indices sérieux comme liées à une activité malveillante*** *(tentative de fraude, vol d'informations, espionnage, DDoS, etc). Voir aussi les réponses sur Q11*[44].

---

[44] Considérant n° 47.

[redacted]

[redacted]

[redacted]

[redacted]

II.4.3. C2-servers concernés

52. Selon l'AIPD, « ***Un serveur C2 peut être défini comme*** *un serveur utilisé par un attaquant ou un malware pour communiquer avec et contrôler des machines infectées ou compromises (appelées "bots" ou "zombies"). Ces serveurs C2 sont utilisés pour lancer des cyberattaques et pour récupérer les données volées. Un serveur C2 peut également être défini plus précisément comme un réseau ou système d'information utilisé à des fins d'identification, d'accès ou d'utilisation illicite ou non autorisée de réseaux et systèmes d'information tiers ou de données se trouvant sur, étant traitées par, ou transitant à travers un réseau et système d'information tiers (définition inspirée du U.S. Code § 650-Definitions (16) Malicious cyber command and contrai)* » (mis en gras par l'Autorité). L'identification de ces serveurs résultera **des sources d'informations disponibles au CCB (CSIRT national)**, [redacted]

[redacted]

53. Ces sources d'information découlent effectivement clairement de l'application de la Loi NIS2 et en particulier, des articles 17, 18, 19, 25, 27, 34-38, 44 et 48 de cette loi.

54. Selon la Note communiquée, le Projet est limité aux **C2-servers étrangers** (« *buitenlandse C2-servers* » ; « *externe C2 servers* ») ou plus exactement, aux **adresses IP étrangères** (« *buitenlands IP-adressen* »). Car les C2-servers « situés » en Belgique font l'objet d'un autre projet (« *Het betreft enkel communicatie met externe C2 servers. Detectie van C2 servers binnen de netwerken van de BE ISPs maken deel uit van een andere procedure, buiten de scope van dit project* »). L'Autorité a notamment interrogé le demandeur quant à la question de savoir de quelle manière dans cette hypothèse de C2-servers « belges », les victimes de ces C2-servers sont alors informées. Celui-ci a répondu ce qui suit :

> « *Le projet est volontaire limité à ce stade aux serveurs* ***C2 situés à l'étranger*** *afin* ***d'éviter d'éventuelles interactions préjudiciables sur des enquêtes pénales en cours ou des enquêtes des services de renseignement.*** *Tant que l'on ne dispose pas de données d'identification et de lien avec des entités situées en Belgique, il n'est pas possible pour les services précités d'entamer une enquête. La majorité des C2 serveurs actifs en Belgique sont* ***situés à l'étranger*** » (mis en gras par l'Autorité).

55. L'Autorité a réinterrogé le demandeur à ce sujet et quant à la manière dont sont considérés des C2-servers comme étant situés à l'étranger[45]. Celui-ci a répondu ce qui suit :

> « *Les* ***ranges IP*** *sont attribués par pays.* [redacted]

[45] Plus précisément, eu égard à la compétence territoriale des juridictions en matière pénale, l'Autorité doute que la localisation d'un C2-server en Belgique soit nécessaire pour que celles-ci soient compétentes (en effet, dans les hypothèses de cybermenaces visées par le Projet il y a clairement des éléments constitutifs des infractions concernées qui sont localisés sur le territoire belge).

- Autrement dit, comment est-il décidé qu'un C2-server est situé en Belgique (et partant, exclu du Projet) ? ;
- Comment les entités concernées étaient informées lorsqu'elles sont victimes de C2-servers situés en Belgique ? ;
- Enfin à l'aune de la réponse fournie, en quoi informer une victime en vue de la prévention d'un dommage à son niveau peut-il porter atteinte à une enquête pénale ou de renseignement ? (Il est à noter que ces services réalisent certainement également des enquêtes relatives à des C2-servers dont la localisation est à l'étranger).

[redacted]

« *La majorité des C2 serveurs actifs en Belgique sont situés à l'étranger. Seuls* ***quelques cas isolés pourraient impliquer les activités d'un serveur C2 situé en Belgique. Dans un tel cas****, le CCB dénoncera les faits aux autorités judiciaires qui pourront entamer des poursuites et informer les potentielles victimes (sans requête d'accès aux métadonnées de ces serveurs à adresser aux opérateurs télécom)* » (mis en gras par l'Autorité) ;

« *Il est exact que la compétence territoriale des juridictions belges en matière pénale n'est pas limitée aux seuls serveurs situés en Belgique (le lieu de survenance en Belgique des dommages ou des systèmes infectés est également un critère de compétence territoriale).* [redacted]

Toutefois, il serait ***possible de réévaluer cet élément dans une seconde phase du projet*** *et d'inclure aussi les serveurs situés en Belgique.*

Par ailleurs, il faut rappeler que ce projet a pour but ***de prévenir le plus rapidement possible les victimes de serveurs C2. Or, dans le cadre de serveurs C2 situés à l'étranger mais actifs en Belgique, l'action des autorités judiciaires est dans les faits ralenties par les procédures internationales*** *(commissions rogatoires). En pratique, certains services de pays tiers répondent très lentement, voire pas du tout, aux demandes de renseignements émanant de la Belgique. Le CCB souhaite utiliser ce projet pour* ***accroître considérablement la vitesse d'avertissement des victimes et leur permettre de se protéger contre les cyberattaques lancées par ces serveurs C2****, sans préjudice des enquêtes pénales potentiellement lancées par le Ministère Public* ».

56. S'agissant de la **nature des activités malveillantes** concernées (**la menace en cours**), la Note communiquée indique que « *De selectie van* ***kwaadaardige servers*** *gebeurt enkel in functie van* ***bedreigingen voor de openbare veiligheid****. Dit initiatief draagt bij aan het opsporen van beveiligingsproblemen met* ***significante gevolgen voor de nationale ICT-infrastructuur*** » (mis

en gras par l'Autorité). [redacted] La Note indique encore que le CCB (CSIRT national) dispose de diverses sources. Dans ce contexte, l'Autorité a interrogé le demandeur quant à la manière dont le CCB vérifie la qualité de l'information d'identification des C2-servers communiquée par des tiers (« *vertrouwde private partners* », autorité d'un Etat tiers, etc.), quant aux garanties mises en œuvre pour assurer la qualité de l'information communiquée et quant aux critères et données sur la base desquels la sélection des C2-servers est réalisée.

[redacted]

58. L'Autorité a réinterrogé plus précisément le demandeur à ce sujet[47] et celui-ci a communiqué les informations suivantes :

[redacted]

> « *Le projet porte en effet potentiellement sur tous les serveurs C2 portés à notre connaissance, mais* ***seuls les serveurs C2 <u>validés</u> par le CCB*** *et repris dans la liste concernée feront l'objet d'une demande d'accès aux métadonnées de communications électroniques auprès des opérateurs télécom. Seuls ces derniers seront concernés par ce projet.*

[46] Voir les considérants nos 47 et 49.

[redacted]

Comme indiqué, le CCB ***procède lui-même à une vérification des informations portées à sa connaissance (de différentes sources) et de la menace potentielle pour la Belgique****. Voir ici également le document C2 List, annexe 4.*

[redacted]

[redacted]Une Note complémentaire communiquée par le demandeur **identifie concrètement, à l'égard de chaque adresse IP communiquée, les démarches de vérification technique entreprises**[redacted]

[redacted]

[redacted]

61. A l'aune de ces développements, l'Autorité estime que la **collecte des sources d'identification des adresses IP listées par le demandeur** dans le cadre du Projet **doit être conforme à la Loi NIS2**. En outre, le Projet nécessite la mise en place d'un **processus efficace de vérification de la qualité des informations relatives aux C2-servers communiquées par l'ensemble de ces sources, et partant, du fait que les adresses IP concernées sont effectivement dédiées au trafic de C2-servers sélectionnés sur la base de la gravité de l'impact de leurs activités**. Ce processus doit comprendre **les combinaisons pertinentes de mesures techniques prévues dans la Note complémentaire** communiquée par le demandeur**, ainsi que le cas échéant, toute autre mesure supplémentaire qu'exigerait l'état de la technique en la matière**. Enfin, le demandeur doit **évaluer et indiquer le niveau de fiabilité des sources d'informations, services et prestataires de services** auxquels il recourt dans le cadre de la mise en œuvre du Projet. Ces processus et leur mise en œuvre doivent être **documentés** conformément au principe d'*accountability*[48].

62. Dès lors que les adresses IP sont susceptibles d'être réallouées au cours du temps (et peuvent d'ailleurs être attribuées de manière dynamique), l'Autorité a interrogé le demandeur quant à la **mise à jour** des adresses des C2-servers communiquées aux opérateurs. Une même adresse IP peut notamment ne plus être associable à l'activité malveillante en cause (et concerner du trafic licite). La Note indique que « *Het CCB zal regelmatige controle uitoefenen op de (blijvende) relevantie van de C2's die op de C2 lijst staan* ». Concrètement, l'Autorité a invité le demandeur à indiquer selon quelle méthode et à quelle fréquence l'activité ayant lieu via les adresses IP des C2-servers concernés est **réévaluée** (notamment compte-tenu du fait que l'information de base d'identification d'un C2-server est susceptible de provenir d'une source tierce au CCB).

[redacted]

[redacted]

[48] Articles 5, 2., et 24 du RGPD.

[49] Considérant n° 57.

[redacted]

65. Les points nos 4.1 et 4.2 (au sein du point « *Versturen metagegevens* ») du processus interne détaillé dans la note initialement communiquée par le demandeur prévoient que : « *de ISP Stuurt de metagegevens van eventueel gevonden communicaties van en naar de opgevraagde IP adressen zo snel als mogelijk terug naar het CCB* » ; « ***de ISP stuurt minstens dagelijks*** *een update, tenzij deze leeg is* » (mis en gras et souligné par l'Autorité). L'Autorité comprend par conséquent de la réponse communiquée par le demandeur que les vérifications du caractère à jour de la liste d'adresses IP ont lieu **au moins quotidiennement**.

66. Le Projet nécessite la mise en place d'un **processus efficace de contrôle au moins quotidien** (le cas échéant, plus fréquent si l'état de la technique le permettait et le nécessitait) **du caractère à jour des adresses IP des C2-servers concernés, basé sur les mesures de vérification visées aux considérants nos 59 et 61**. Ce processus et sa mise en œuvre doivent être **documentés** conformément au principe d'*accountability*.

67. L'Autorité a également interrogé le demandeur quant à l'éventuelle **procédure** mise en place dans le cas où une **erreur** serait découverte dans l'identification des adresses IP des C2-servers. Celui-ci a précisé ce qui suit : « *Retrait de la liste des adresses IP serveurs C2 et effacement des données. La procédure du projet prévoit l'envoi d'une nouvelle version de la liste à intervalles réguliers : en cas d'erreur,* ***une mise à jour sera adressée immédiatement aux ISP*** » (mis en gras et souligné par l'Autorité).

68. Le Projet nécessite que dès que le CCB (CSIRT national) constate qu'une adresse IP n'est plus liée au C2-server concerné, **l'opérateur concerné en soit immédiatement notifié via un canal adapté**

et cesse dès ce moment, la collecte des métadonnées relatives au trafic depuis et vers l'adresse concernée.

69. Le Projet doit **également prévoir un processus efficace de notification à l'attention du CCB (CSIRT national) cette fois, lorsque l'opérateur concerné dispose d'éléments objectifs** de nature à questionner l'exactitude des données concernées.

70. L'Autorité **doit être informée des mises à jour opérées** à la liste de C2-servers dans ce contexte, à l'occasion de la prochaine demande d'autorisation (ou de contrôle ultérieur) qui lui serait adressée dans le cadre du Projet.

71. Enfin, l'Autorité a invité le demandeur **à estimer** (donner un ordre de grandeur) le nombre d'adresses IP dédiées à des C2-servers qui seraient concernés par demande adressée à l'APD dans le cadre du Projet et la fréquence estimée des demandes d'autorisation qui seront communiquées à l'Autoritéau. Celui-ci a répondu ce qui suit :

> « *La demande du CCB sollicite une autorisation sur les demandes d'accès à des métadonnées qui découlent de l'exécution du présent projet (en ce compris les traitements et accès nécessaires dans le futur).* [redacted] *A défaut d'une autorisation pour la réalisation de ce projet spécifique, le CCB devrait introduire pour chaque nouvelle adresse IP ou chaque nouvelle liste ou mise à jour de la liste existante une nouvelle autorisation pour les mêmes finalités, avec les mêmes traitements et selon la même procédure). La fréquence estimée* ***pourrait être chaque semaine ou deux semaines, en tenant compte de délais de traitement courts nécessaires pour avertir utilement les responsables des systèmes victimes*** » (mis en gras et souligné par l'Autorité).

72. L'Autorité en prend acte.

II.5. Proportionnalité des traitements de données

II.5.1. Evaluation des alternatives aux traitements de donnés envisagés

73. La demande et la Note communiquée par le demandeur ne précisent rien quant aux alternatives au Projet qui auraient pu être envisagées afin d'avertir les victimes potentielles de C2-servers ou de prévenir leur dommage, sans que ne soient collectées des métadonnées de communications électroniques. Elle se limite en substance à souligner que la collecte des métadonnées et

l'avertissement des victimes sur cette base est nécessaire afin d'augmenter la visibilité des menaces concernées. De telle sorte que l'Autorité a interrogé le demandeur plus en détail à ce sujet.

Blocage/filtrage des adresses IP dédiées aux C2-servers

74. Premièrement, il convient de se demander si plutôt que de chercher à informer les victimes potentielles via la collecte de métadonnées de communications électroniques, le CCB ne dispose pas de moyens légaux permettant **de faire bloquer/filtrer, par les opérateurs concernés, le trafic depuis et vers les adresses IP dédiés aux C2-servers concernés**. Dans l'affirmative, il importe d'identifier la raison pour laquelle le recours à ce type d'intervention n'est pas privilégié (le C2-server étant bloqué, il ne pourrait plus causer de nouvelles victimes et il ne serait pas nécessaire de collecter des métadonnées de communications électroniques).

75. Le demandeur a répondu dans un premier temps ce qui suit : « *Le CCB **ne dispose pas du pouvoir de donner des injonctions aux ISPs** afin qu'ils bloquent le trafic entrant et/ou sortant de serveurs C2 ou encore du pouvoir de faire saisir de tels serveurs. **La seule possibilité d'action pour le CCB est donc, dans les plus brefs délais, de collecter des métadonnées, de les analyser d'identifier des responsables des systèmes d'information concernés et de les informer*** ». L'Autorité a réinterrogé le CCB (CSIRT national) plus en détails à ce propos afin d'obtenir la confirmation que celui-ci ne disposait pas de moyens légaux[50] en vue de faire bloquer les adresses IP concernées par les ISP. Celui-ci a précisé ce qui suit :

> « *Comme indiqué, le CCB ne dispose pas du pouvoir de donner des injonctions aux ISPs afin qu'ils bloquent le trafic entrant et/ou sortant de serveurs C2 ou encore du pouvoir de faire saisir de tels serveurs (d'autant plus lorsque ceux-ci sont situés à l'étranger). La seule possibilité d'action pour le CCB est donc, dans les plus brefs délais, de collecter des métadonnées, de les analyser, d'identifier des responsables des systèmes d'information concernés et de les informer.*

---

[50] A ce propos :

- *Quid* d'un filtrage/blocage réalisé sur base volontaire par l'ISP, une fois que le CCB (CSIRT National) lui notifie l'IP d'un C2-Server ? ;
- *Quid* de la saisine des autorités judiciaires en vue du filtrage/blocage des adresses IP des C2-Servers (ex., art. 39*bis*, § 1er, du Code d'instruction criminelle) ? ;
- *Quid* de la communication des listes de C2-Servers au SGRS dans le cadre de la compétence dont il dispose en vertu de l'article 11, § 1er, 2°/1, de la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité* ? ;

Autrement dit, à l'aune de la finalité poursuivie par le Projet (prévention du dommage et des infractions concernées) certaines de ces démarches sont-elles envisagées et quand dans le cadre du Projet ?

Et à terme, *quid* d'une évolution législative du type des articles XVII.34/1 et s. du CDE, adaptées mutatis mutandis au contexte du CCB (voir aussi l'article 9 du Règlement UE 2022/2065)?

Un filtrage/blocage réalisé volontairement par un ISP dépendrait de la bonne volonté de chaque opérateur, des moyens à sa disposition et de la compatibilité d'une telle mesure dans ses obligations légales/contractuelles. ***Un tel blocage/filtrage pourrait éviter certes de nouvelles victimes, mais n'impliquerait pas nécessairement l'alerte des victimes potentielles existantes****, c'est-à-dire les entités/personnes physiques ayant déjà interagis avec le serveur concerné. Compte tenu de ce qui précède, le projet proposé demeure la seule mesure efficace et proportionnée pour informer les Victimes* » ;

« *En vertu de l'article 29 du CIC, tout fonctionnaire qui, dans l'exercice de ses fonctions, a connaissance d'un crime ou d'un délit est tenu d'en informer immédiatement le procureur du Roi et de lui transmettre les informations s'y rapportant.* ***Nous ne pouvons toutefois pas nous prononcer sur ce qu'il advient de telles dénonciations effectuées auprès du Ministère public (qui agit en toute indépendance et selon ses propres priorités de poursuite), et encore moins sur la décision de bloquer/filtrer ou non des adresses IP ou la saisine des autorités judiciaires en vue de filtrage/blocage des adresses IP de C2 servers*** *(ex., art. 39bis, § 1er, CIC)* » ;

[redacted]

« *Dans le cas d'une communication d'informations,* ***les finalités des éventuels traitements de données effectués par le SGRS sont différentes*** *(et les possibilités de partage d'information ne sont pas identiques à celles du CCB)* » ;

« *Voir ci-dessus. Dans tous les cas, l'article 29 du CIC reste applicable au CCB. L'avertissement de la victime par le CCB n'empêche pas l'application de cet article* » ;

« *Compte tenu du contexte et des activités hautement dynamiques et rapides des serveurs C2,* ***ces procédures judiciaires semblent difficilement transposables à la situation envisagée par le projet*** » (mis en gras par l'Autorité).

76. L'Autorité prend acte de ces explications, qui appellent les commentaires suivants de la part de l'Autorité. Premièrement, la communication des activités illicites des C2-servers constatées dans le cadre du Projet aux autorités judiciaires demeure en tout état de cause pertinente et la politique criminelle en la matière est pour le reste susceptible d'évoluer. Deuxièmement, s'il est vrai que le SGRS et, plus largement, les services de renseignement et de sécurité poursuivent des finalités différentes, il n'en demeure pas moins que certaines des menaces identifiées dans la Note complémentaire peuvent

aussi relever de la compétence de ces services. Troisièmement enfin, à l'égard d'une éventuelle évolution législative qui serait inspirée, *mutatis mutandis*, des articles XVII.34/1 et s. du CDE, dans le contexte normatif du CCB (CSIRT national), l'Autorité attire l'attention du demandeur sur le fait qu'une action en référé sur requête unilatérale peut potentiellement produire un résultat dans les quelques jours. Il n'est donc pas évident qu'une procédure judiciaire de ce type soit d'office difficilement transposable à la situation visée par le Projet. Toutes ces voies d'action peuvent conduire à une interruption de la réalisation de la menace qui, sans collecte de métadonnées de communications électroniques, peuvent atteindre la finalité poursuivie par le Projet.

77. Cela étant précisé et sur la base des réponses communiquées par le demandeur, l'Autorité partage sa vision selon laquelle **le Projet en tant que tel, a une réelle plus-value, indépendamment de ces voies d'actions**.

78. Ce qui n'exclut pas que compte-tenu de sa finalité[51], au regard des principes de finalité et de proportionnalité (qui impose notamment la minimisation des données), **le Projet nécessite,** une fois que le CCB (CSIRT national) dispose d'informations fiables et vérifiées par lui dans le cadre du Projet, concernant des C2-servers, **d'envisager la mise en œuvre simultanée** par le CCB (CSIRT national), **des moyens dont il dispose qui donneraient la possibilité à d'autres autorités de faire bloquer/filtrer par les opérateurs concernés, les adresses IP des C2-servers concernés**, de manière à prévenir la réalisation des menaces concernées. Les actions entreprises en ce sens sont de nature à réduire la collecte de métadonnées et surtout, d'atteindre efficacement la finalité poursuivie par le Projet (soit prévenir la réalisation de dommage auprès de victimes potentielles), d'autant plus si les moyens concernés peuvent aboutir avant ou peu de temps après l'identification des victimes concernées[52].

Information via Cyber Threat Alerts

79. Deuxièmement, plutôt que de chercher à informer les victimes potentielles via la collecte de métadonnées de communications électroniques, l'Autorité a demandé au demandeur la raison pour laquelle **les adresses IP des C2-servers ne pourraient pas être communiquées via « Cyber Threat Alerts »[53]**, avec les informations pertinentes pour se prémunir des risques y liés. Auquel cas, toutes les entités concernées pourraient recevoir d'office les informations pertinentes et prendre des mesures de protection et le cas échéant, d'investigation. Une telle communication pourrait le cas échéant être adressée au groupe cible des menaces concernées.

---

[51] Voir les considérants nos 25 et 29.

[52] Cette solution n'implique en outre aucun partage d'informations relatives aux entités essentielles ou importantes (voir la réponse communiquée par le demandeur et citée au considérant n° 83, *in fine*).

[53] Voir plus haut, la note de bas de page n° 27.

80. Le demandeur a répondu ce qui suit :

> « *Le service Cyber Threat Alerts offre des informations générales ou ciblées* ***aux entités (NIS2 ou non) qui se sont enregistrées sur la plateforme du CCB*** *SafeOnWeb@Work et qui ont souscrit à ce service. Toutefois, ce service ne peut fonctionner sans informations pertinentes (notifications d'incident, de cybermenace significative, de vulnérabilités, etc) et individualisées (liste d'adresses IP infectées, type de système d'information impactés, etc).*
>
> ***Pour identifier les systèmes d'information « victimes »*** *d'activités malveillantes de serveurs C2 (reconnus comme telles par le CCB avec des indices sérieux)* ***et informer les responsables de ces systèmes d'information*** *(via le service Cyber Threat Alerts ou une autre forme de notification),* ***le CCB doit obtenir auprès des ISP des métadonnées de communications électroniques entre ces serveurs C2 et d'autres systèmes d'information. L'objectif est de permettre à ces victimes de se protéger*** *contre les activités malveillantes menées via ces serveurs C2.*
>
> *Le service Cyber Threat Alerts* ***ne permet donc pas à lui seul de connaître et d'informer les victimes*** *de ces serveurs C2* » (mis en gras et souligné par l'Autorité).

81. L'Autorité prend acte de cette réponse et de l'intention **d'informer spécialement et directement les victimes concernées**. Cela étant précisé, compte-tenu de sa finalité et en application des principes de finalité et de proportionnalité (y compris la minimisation des données), **le Projet nécessite d'envisager la mise en œuvre simultanée**, dans la mesure du possible (selon les informations à disposition du CCB (CSIRT National) et compte-tenu des risques pour la cybersécurité), **d'une information générale (pas seulement à l'attention des victimes concernées),** le cas échéant à l'attention uniquement des groupes cibles des menaces concernées, **à propos des C2-servers et adresses IP concernés via « Cyber Threat Alerts »**. Il s'agit effectivement **d'un moyen moins attentatoire** (ne nécessitant pas la collecte de métadonnées de communications électroniques) d'informer à propos des menaces concernées et ce, dès que le CCB (CSIRT national) dispose d'une information fiable et validée par lui, concernant des C2-servers ainsi que leurs adresses IP. Une entité qui traiterait sérieusement l'information communiquée par un tel canal pourrait d'ailleurs adopter des mesures internes de prévention plus rapidement (une notification individuelle arrivera par définition plus tard, dès lors qu'elle nécessite une autorisation préalable de l'Autorité, sauf en cas d'urgence)[54]. Dans ce contexte, l'Autorité comprend que la publication pure et simple des listes d'adresses IP dédiées aux C2-servers concernés peut conduire les auteurs des activités illicites

[54] Cette solution n'implique en outre aucun partage d'informations relatives aux entités essentielles ou importantes (voir la réponse communiquée par le demandeur et citée au considérant n° 83, *in fine*).

concernées à plus facilement contourner les mesures mises en place dans la lutte contre leurs activités (en recourant dès que possible à d'autres adresses IP). Elle conçoit que le CCB (CSIRT national) **doit conserver une marge d'appréciation dans la mise en œuvre du Projet afin d'assurer l'équilibre le plus approprié entre la diffusion plus large d'informations au sujet des IP dédiées aux C2-servers concernés et les communications spécifiques à l'attention des victimes potentielles concrètes**, et partant, de décider de l'équilibre optimal à atteindre sur le plan de la cybersécurité, dans la mise en œuvre de ses missions dans le cadre de la Loi NIS2.

II.5.2. Minimisation des données

82. Le CCB (CSIRT national) doit recevoir les **plages IP utilisées par les entités soumises à la Loi NIS2 (y compris leurs mises à jour) ainsi que leurs données de contact**[55]. Autrement dit, il n'est en principe pas nécessaire de consulter les opérateurs pour procéder ensuite à l'identification de ces entités. L'Autorité a invité le demandeur à lui préciser s'il en serait ainsi dans le cadre du Projet. Elle lui a encore demandé plus fondamentalement pour quelle raison il n'était pas envisagé que le CCB (CSIRT national) communique d'emblée à l'opérateur concerné, dans le cadre de sa demande de métadonnées de communications électroniques, ces plages d'IP afin que l'opérateur puisse directement filtrer les métadonnées de communications électroniques les plus pertinentes au regard du champ d'application de la Loi NIS2.

83. Le demandeur a répondu ce qui suit :

> « *Le CCB pourra **effectivement** vérifier avec les métadonnées reçues d'un ISP si les informations ne correspondent, le cas échéant, pas aux informations en sa disposition (plages IP des les entités NIS2), **sans** nécessairement **solliciter une identification ultérieure par un ISP**. Par contre, l'identification auprès des opérateurs de communication électronique sera indispensable pour les autres adresses IP* ».
>
> « *Comme expliqué précédemment, la mission visée à l'article 19, § 1er, alinéa 1er, 2°, de la loi NIS2 n'est pas limitée aux entités NIS2, elle s'étend également aux autorités compétentes et aux autres parties prenantes concernées. Il ressort de la disposition précitée que la tâche d'alerte précoce du CCB n'est pas limitée aux entités soumises aux obligations en matière de cybersécurité mais est bien étendue aux autres entités belges, qu'ils s'agissent d'entités publiques, privées, ou de personnes physiques.*
>
> *Communiquer uniquement les plages IP des entités NIS2 ne permet pas de remplir pleinement la mission dévolue au CCB en matière d'alerte précoce. En outre, il convient de limiter au strict*

[55] Voir les articles 13 et 14 de la Loi NIS2.

nécessaire le partage d'informations relatives aux entités NIS2 dans le respect de l'article 26 § 3 de la loi NIS2 » (mis en gras par l'Autorité).

84. L'Autorité prend acte de cette réponse.

II.6. Responsables du traitement, *accountability* et droits des personnes concernées

II.6.1. Liste de C2-servers avec données contextuelles

85. Le CCB, **en tant que CSIRT national**, est responsable du traitement de données à caractère personnel nécessité par le Projet. Cela étant précisé, **l'ISP concerné est également un responsable du traitement** à part entière relativement aux traitements de données qu'il réalise (mise en œuvre d'une obligation légale lui incombant en vertu de l'article 21 de la Loi NIS2). En tant que responsable du traitement, **il doit par conséquent également veiller à la licéité du traitement de données dont il est responsable**.

86. La Note indique que « *De*[...] *CCB C2-list wordt* ***zonder context*** *gedeeld met Belgische ISP's samen met een officiële aanvraag tot het delen aan het CCB van meta-data over de communicatie van en naar deze IP-adressen. Enkel de IP-adressen van deze lijst worden door het CCB gedeeld met de ISP's (zonder context),* ***dit bijvoorbeeld om te vermijden dat een ISP direct op hoogte is dat een bepaalde klant slachtoffer is van een specifieke dreigingsactor*** » (mis en gras par l'Autorité).

[redacted]

87. Dans un premier temps, l'Autorité considérant que **l'omission de ces informations quant au contexte à l'attention des opérateurs** les empêche de pouvoir vérifier si la demande qui leur est adressée est conforme au cadre normatif applicable, elle a interrogé le demandeur sur l'objectif poursuivi par cette limitation. D'autant plus que les opérateurs sont susceptibles de s'informer eux-mêmes quant aux menaces afin de protéger leur propre infrastructure, peut-être même via des sources privées identiques à celles du CCB (CSIRT national).

88. Le demandeur a répondu ce qui suit :

> « *Dans le projet, il est précisé que la liste de serveurs C2 et toutes les mises à jour sont mises à la disposition de l'APD, avec le contexte, dans le cadre de contrôle de l'article 21, §§2 et 4, de la loi NIS2, afin de permettre un contrôle par l'APD. La liste des serveurs C2 est effectivement mise à la disposition des ISPs sans contexte. Le but de ce projet est pour le CCB d'analyser des métadonnées de communications électroniques* ***pour détecter les communications suspectes*** *et identifier des victimes.* ***Vu qu'il s'agit d'information relatives à des victimes, le CCB souhaite minimiser le partage d'informations à ce qui est strictement nécessaire afin de permettre à l'opérateur de répondre à sa requête****. Après l'analyse de ces métadonnées, il est demandé à l'ISP de vérifier l'identité de la victime en question afin de l'alerter. Il est important pour le CCB d'avoir une procédure d'information structurée envers les victimes.*
>
> *Par ailleurs, le CCB a* ***l'obligation de limiter l'accès aux informations dans le cadre de la loi NIS2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la loi NIS2*** *(l'article 26 § 3 de la loi NIS2). En conséquence, certaines informations ne peuvent pas être librement partagées avec toutes les parties. Or,* ***il n'apparaît pas que les opérateurs de communication électronique aient besoin de l'entièreté des informations pour exécuter leurs obligations*** » (mis en gras par l'Autorité).

89. Avant tout, l'Autorité réitère d'une part, que **la sollicitation de la collaboration des opérateurs au Projet implique par définition un échange d'informations avec ceux-ci**. En tant que responsables du traitement, ils sont également tenus de veiller à la licéité des traitements de données qu'ils mettent en œuvre en vertu de l'obligation légale qui leur incombe. D'autre part, les opérateurs sont également tenus de coopérer avec d'autres entités telles que les autorités judiciaires et même les services de renseignement et de sécurité[56], de telle sorte que la manipulation de données le cas échéant particulièrement sensibles ne leur est pas étrangère, et qu'ils doivent mettre en œuvre des mesures techniques et organisationnelles nécessaires dans ce contexte[57]. L'Autorité considère par conséquent que **les données contextuelles du type de celles communiquées dans le cadre de la présente demande (première liste de C2-servers communiquée par le demandeur) doivent à tout le moins être communiquées également aux opérateurs**. Il en va **de même et *a fortiori* dans les cas d'urgence** lorsqu'une demande d'autorisation préalable n'est pas adressée

---

[56] Voir les articles 16/2, 18/7, 18/8 et 18/17 de la loi organique du 30 novembre 1998 *des services de renseignement et de sécurité*.

[57] Voir en particulier l'article 127/3 de la LCE prévoyant la constitution auprès de chaque opérateur d'une Cellule de coordination chargée de fournir aux autorités légalement habilitées, à leur demande, des données de communications électroniques, et spécialement son paragraphe 2.

à l'Autorité, et que la demande de collecte des métadonnées est directement adressée à l'opérateur concerné.

90. Cela étant précisé, l'Autorité souligne que ces **informations contextuelles telles qu'initialement communiquées à l'Autorité** dans le cadre de la présente demande sont **insuffisantes pour vérifier que la demande relève bien du champ d'application du Projet**. En effet, ces informations sont **essentiellement stéréotypées** et ne permettent pas de comprendre sur quelle base les adresses IP listées sont bien relatives à une menace visée par le Projet. Partant, **elles ne permettent pas la réalisation d'un contrôle par l'Autorité dans le cadre du processus d'autorisation**.

[redacted]

92. Le demandeur a, dans un premier temps, indiqué que les documents complémentaires seraient ultérieurement communiqués[60]. Dans un deuxième temps, il a communiqué une **Note complémentaire précisant notamment plus en détails le contexte relatif aux adresses IP listées**. Il a enfin illustré plus concrètement encore [redacted] les informations communiquées par ses sources, concernant trois des catégories de ces sources [redacted]

[58] A ce sujet, voir les considérants nos 54 et s.

[redacted]

93. L'Autorité considère que **chaque demande d'autorisation dans le cadre du Projet, ainsi que chaque demande de contrôle ultérieur en cas d'urgence, doit comporter les documents probants (du type de la Note complémentaire** ; sans préjudice de la possibilité pour l'Autorité de demander à l'appui des demandes ultérieures la communication des documents sur la base desquels le CCB (CSIRT national) identifie les adresses IP concernées) **sur la base desquels les adresses IP dédiées aux C2-servers sont identifiées comme étant pertinents dans le cadre du Projet**. Ces documents doivent **également indiquer les pays étrangers** desquels émanent les adresses concernées (le Projet étant limité à celles-ci).

94. De la même manière, **en principe**, ces pièces **devraient aussi être communiquées à l'opérateur, à sa demande, dans le cas particulier où il** disposerait d'éléments objectifs de nature à questionner l'exactitude des adresses IP et données contextuelles communiquées, **et ce *a fortiori* également, lorsque dans ce même cas, en raison de l'urgence**, une demande d'autorisation préalable n'est pas adressée à l'Autorité, et que la demande de collecte des métadonnées est directement adressée aux opérateurs.

95. **Cependant**, il ne peut être exclu que la **communication de ces documents à l'opérateur soit limitée en raison du droit applicable** (article 26, § 3, de la Loi NIS2 ; obligation de confidentialité contractuelle inévitable ; autre). Dans ce cas, le CCB (CSIRT national) **peut ne pas communiquer ces documents et se limiter à indiquer aux opérateurs le motif** pour lequel ils ne sont pas communiqués.

II.6.4. Relations entre l'opérateur et l'entité victime concernée

96. La Note communiquée par le demandeur indique que « *Het CCB zal de ISP op de hoogte stellen wanneer het contact opneemt met/of waarschuwing stuurt naar een klant,* ***zodat de ISP een complementaire rol kan spelen in de communicatie en ondersteuning van de klant.*** *Dit zorgt ervoor dat de respons op cyberdreigingen gecoördineerd en effectief is, en voorkomt verwarring of tegenstrijdige informatie tussen de betrokken partijen.* ***De ISP contacteert zijn klant over de vaststelling enkel in overleg met het CCB.*** [...] *Wanneer CCB en ISPs (potentiële) slachtoffers waarschuwen is het belangrijk hierbij zorgvuldig te werk gaan en via goede informering* ***te voorkomen dat klanten overhaast zaken gaan verwijderen of blokkeren, wat zou kunnen leiden tot het verdwijnen van de kwaadaardige infrastructuur (C2) voordat het CCB het incident volledig heeft kunnen onderzoeken*** ».

97. Dans ce contexte, l'Autorité a interrogé le demandeur quant à la question de savoir sur quelle base légale le CCB (CSIRT national) peut régler la manière dont l'opérateur communique avec l'entité

concernée. En outre, elle l'a invité à confirmer que l'incident en question était bien celui qui a affecté l'entité concernée (à supposer que l'entité victime réclame l'intervention du CCB). Le demandeur a répondu ce qui suit :

> « ***Il ne s'agit pas ici de créer une obligation*** *à charge de l'ISP (de communiquer ou d'offrir une assistance à ses clients après le message d'alerte du CCB) mais plutôt* ***d'assurer, sur une base volontaire, une coordination efficace*** *entre l'ISP et le CCB dans les communications en lien avec les messages d'alerte envisagés (ou dans le cadre d'une assistance éventuelle fournie par l'ISP aux victimes afin de remédier aux menaces identifiées par le CCB)* » (mis en gras par l'Autorité).
>
> « *Le passage utilise la notion d'incident tel que défini à l'article 8, 5°, de la loi NIS2 : un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles. Le passage* ***porte sur un éventuel incident subi par la victime*** *(entité NIS2 ou non) et causé au travers d'un serveur C2. Dans un tel cas, le responsable du système victime* ***peut ou non solliciter l'assistance du CCB*** » (mis en gras par l'Autorité).

98. L'Autorité prend acte de cette réponse et relève que **la documentation relative au Projet devra être adaptée en fonction de la réponse communiquée par le demandeur** (coordination avec l'opérateur sur base volontaire).

II.6.3. Droits des personnes concernées

99. L'Autorité a invité le demandeur à lui indiquer, sur la base des dispositions normatives applicables au CCB (CSIRT national), si et dans quelle mesure selon lui, une personne concernée (au sens du RGPD) pourra exercer les droits dont elle jouit en vertu des articles 15 (accès), 16 (rectification), 17 (effacement) et 18 (limitation) du RGPD, dans le cadre du Projet[61]. Celui-ci a répondu que « *Les personnes concernées pourront exercer leurs droits dans le cadre du Projet. La loi NIS2 ne limite, le cas échéant, l'application des droits des personnes concernées que dans le cadre de la supervision des entités soumises aux obligations en matière de cybersécurité, ce qui n'est pas le cas en l'espèce* ».

[61] Tel que présenté à l'Autorité, c'est-à-dire lorsque les métadonnées collectées peuvent concerner d'autres personnes que les entités essentielles ou importantes.

100. Bien que tel ne semble *a priori* pas être le cas[62], l'Autorité a interrogé le demandeur quant à la question de savoir si des personnes concernées sont susceptibles de faire l'objet d'une décision fondée exclusivement sur un traitement automatisé de données visées à l'article 22 du RGPD. Le demandeur a répondu ce qui suit : « *Le projet ne prévoit pas de décision fondée exclusivement sur un traitement automatisé de données. Les données seront analysées et validées par des experts du CCB* ».

101. Les réponses fournies à ces questions demeurent pertinentes même lorsque les métadonnées concernent les communications électroniques d'un abonné personne morale. Par exemple, une fois qu'un incident sera porté à la connaissance de l'entité concernée, celle-ci[63] pourra identifier au sein de son réseau privé quels systèmes d'informations sont concernés et pourraient être en cause des communications impliquant ses employés ou visiteurs[64] qui seront le cas échéant amenés à rendre des comptes et justifier leurs actions.

102. S'agissant du droit d'opposition au traitement de données à caractère personnel, le demandeur a notamment confirmé qu'un droit d'opposition serait possible auprès du CCB et que la Loi NIS2 ne limitait pas l'application des droits des personnes concernées dans le contexte du Projet.

II.7. Traitement ultérieur de données

103. L'Autorité a interrogé le demandeur afin que celui-ci identifie les obligations légales de communication de données (d'initiative ou à la demande) en sa possession auxquelles le CCB (CSIRT national) est soumis[65], et qu'il lui explique comment il envisage l'application de ces obligations à l'égard des données (métadonnées de communications électroniques et données de contact et d'identification collectées par après) collectées dans le cadre du Projet.

104. Celui-ci a notamment répondu ce qui suit :

> « *Le CCB* ***n'envisage pas d'autres traitements que ceux mentionnés dans la fiche de projet****. A l'instar d'autres autorités publiques,* ***le CCB est néanmoins soumis à certaines dispositions légales, qui peuvent, le cas échéant, mener au partage d'informations avec d'autres autorités*** *(art 29, §1er du Code d'instruction, art. 14, al. 2, de la loi du 30*

[62] La Loi NIS2 s'applique en principe à des personnes morales. Néanmoins, une notification du CCB (CSIRT national) aura en principe un impact interne direct dans l'entité concernée qui cherchera certainement à identifier les terminaux (et leurs utilisateurs) avec lesquels le C2-server aurait communiqué.

[63] Ou le CCB (CSIRT national) si son assistance est requise ; ou toute entité qui procèderait à une enquête à propos de l'incident, au sein du système concerné.

[64] Par exemple, des employés qui ont cliqué sur un mail de phishing, le terminal d'un employé à partir duquel sont frauduleusement extraites des données, l'employé dont le login d'accès est utilisé pour se connecter à un système, etc.

[65] Par exemple, article 29, § 1er, du Code d'instruction criminelle ; article 14, al. 2, de la loi du 30 novembre 1998 *organique des services de renseignement et de sécurité* ; saisie par les autorités judiciaires, etc.

novembre 1998 organique des services de renseignement et de sécurité, saisie par les autorités judiciaires, etc.).

L'article 25 de la loi NIS2 établit une coopération au niveau national qui inclut un échange adéquat d'informations concernant la sécurité des systèmes et réseaux d'informations. Il s'agit de la coopération avec le NCCN, les services administratifs de l'Etat, les autorités administratives, en ce compris les autorités nationales en vertu des règlements (CE) n° 300/2008 et n° 2018/1139, les organes de contrôle au titre du règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE, la Banque Nationale de Belgique, l'Autorité des services et marchés financiers, l'Institut, les autorités compétentes en vertu de la loi du 1er juillet 2011, les autorités judiciaires, les services de renseignement et de sécurité visés par la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, les services de police visés par la loi du 7 décembre 1998 organisant un service de police intégré, structuré à deux niveaux et avec les autorités de protection des données. Le CCB a créé une plateforme de coordination et d'évaluation afin que les autorités compétentes (art. 15 de la loi NIS2) et le NCCN échangent de l'information et se coordonnent dans le cadre de l'exécution de la loi NIS2.

Par ailleurs, le CCB a l'obligation de limiter l'accès aux informations dans le cadre de la loi NIS2 aux personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec l'exécution de la loi NIS2. En conséquence, certaines informations ne peuvent pas être librement partagées avec tous les parties » (mis en gras et souligné par l'Autorité).

[...] ».

105. L'Autorité rappelle avant tout que les dispositions normatives encadrant la demande d'autorisation introduite auprès de l'Autorité, soit en particulier les articles 21, § 4, de la Loi NIS2 et 23, § 3, de la LCA, constituent un **dispositif normatif spécifique** (une *lex specialis* et en outre, une *lex posterior*) **régissant l'accès aux métadonnées de communications électroniques traitées par les opérateurs**. Autrement dit, les métadonnées collectées dans le cadre du Projet **ne peuvent pas être traitées ultérieurement à une autre fin que celle visée par le Projet** (y compris bien entendu, les traitements liés à la mise en œuvre des règles de droit régissant le Projet lui-même), sauf à

méconnaître le dispositif législatif belge régissant l'accès aux métadonnées de communications électroniques traitées par les opérateurs dans le cadre de leurs activités[66].

106. Ensuite, en droit belge, le CCB est l'autorité nationale visée à l'article 16 de la Loi NIS2[67], et il assure, en vertu de cette disposition « *les tâches d'autorité compétente pour les entités essentielles et importantes, de CSIRT national, de point de contact national unique pour l'exécution de la présente loi et de représentation de la Belgique au sein du groupe de coopération, du réseau des CSIRT et du réseau européen pour la préparation et la gestion des crises cyber (EU-CyCLONe) visé à l'article 16 de la directive NIS2* ». Le considérant n° 41 de la Directive NIS2 prévoit que « *Afin d'améliorer la relation de confiance entre les entités et les CSIRT, dans les cas où un CSIRT fait partie de l'autorité compétente, les États membres devraient pouvoir envisager de mettre en place une* ***séparation fonctionnelle entre d'une part les tâches opérationnelles assurées par les CSIRT****, notamment en lien avec le partage d'informations et l'assistance aux entités,* ***et d'autre part les activités de supervision des autorités compétentes*** » (mis en gras par l'Autorité). L'Autorité a interrogé le demandeur quant aux mesures mises en place à cet égard au sein du CCB.

107. Celui-ci a communiqué une réponse insistant principalement sur l'indépendance du service d'inspection du CCB[68].

108. S'agissant d'éventuels **traitements ultérieurs de données par le CCB lui-même**, l'Autorité a interrogé le demandeur afin d'identifier si le CCB envisageait, sur la base des compétences dont il jouirait par ailleurs en vertu de la Loi NIS2, une intervention contraignante auprès de la victime potentielle concernée. Plus clairement, l'Autorité l'a invité à confirmer qu'aucun traitement ultérieur

---

[66] Dans le même sens, voir Autorisation (délivrée) n° 001/2024 du 6 novembre 2024 *demande d'autorisation visée à l'article 15, § 2, al. 2, de la loi du 17 janvier 2003 relative au statut du régulateur des secteurs des postes et des télécommunications belges (AH-2024-0010)*, considérant n° 76.

[67] Voir l'article 16, al. 2, de la Loi NIS2 et l'article 3, § 1er, de l'arrêté royal du 9 juin 2024 *exécutant la loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.*

[68] « *Le CCB fait l'objet d'une séparation fonctionnelle entre le service d'inspection du CCB (NCCA) et les autres services (notamment CERT et CyTRIS qui assurent principalement les tâches de CSIRT national). En effet, dans le cadre de l'exécution de la loi du 20 juillet 2022 relative à la certification de cybersécurité des technologies de l'information et des communications et portant désignation d'une autorité nationale de certification de cybersécurité (loi CSA), le CCB a été doté d'un service d'inspection propre (NCCA). Ce même service d'inspection est chargé de la supervision de la loi NIS2. Différentes dispositions légales garantissent l'indépendance de ce service dans le cadre de ses missions d'inspection.*

Conformément à l'article 58, § 4, du Règlement UE 2019/881, à l'article 13, de la loi du 20 juillet 2022 précitée, et à l'article 3ter, §§ 2 et 3, de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, le service d'inspection accomplit ses missions en toute indépendance vis-à-vis des autres services du CCB et d'autres entités publiques ou privées. Il est doté pour ce faire d'un directeur propre.

En vertu de l'article 47, § 2 de la loi NIS2, les membres du service d'inspection de l'autorité nationale de cybersécurité et de l'éventuelle autorité sectorielle ou de l'éventuel service d'inspection sectoriel compétent et les experts appelés à participer à l'inspection ne peuvent avoir un intérêt quelconque, direct ou indirect, dans les entreprises ou institutions qu'ils sont chargés de contrôler, susceptible de compromettre leur objectivité.

Conformément à l'article 64 de la loi NIS2, le service d'inspection de l'autorité nationale de cybersécurité ou, le cas échéant, le service d'inspection sectoriel désigné par le Roi pour le secteur de l'administration publique exerce ses tâches de supervision en jouissant d'une indépendance opérationnelle vis-à-vis des entités de l'administration publique supervisées ».

des métadonnées et données d'identification collectées dans le cadre du Projet n'était envisagé par le CCB, quelle que soit sa fonction. Le demandeur a répondu ce qui suit :

> « *Le CCB n'a le pouvoir d'imposer une intervention contraignante auprès de la victime concernée que lorsque celle-ci est une entité essentielle ou importante NIS2 (dans le cadre de ses missions d'inspection)* ».
>
> « *Seuls les traitements mentionnés ci-avant (information des responsables des systèmes victimes et examen des défaillances des systèmes d'information) réalisés par le CCB sont prévus dans le cadre de ce projet* ».

109. Réinterrogé quant aux sujets justes évoqués[69], le CCB (CSIRT national) a notamment répondu ce qui suit :

> « [...] *Dans le cadre de la procédure envisagée,* ***les membres du service d'inspection ne font pas parties des membres du personnel pouvant avoir accès aux métadonnées de communication et aux données d'identification reçus des ISPs*** *(ils ne disposeront ainsi pas des droits d'accès à ces fichiers et aux systèmes d'information dédiés)* » (mis en gras par l'Autorité) ;
>
> « *Les traitements envisagés dans le cadre du projet ne portent pas sur des finalités de contrôle ou de sanctions des éventuelles entités NIS2 concernées, mais plutôt* ***pour les aider à identifier des menaces dans leurs réseaux et à mitiger/éviter des incidents plus vite****. Le service d'inspection du CCB n'aura pas accès, par défaut, à ces données (voir la réponse ci-dessus).*
>
> ***Toutefois,*** ***les services CERT ou CyTRIS du CCB pourraient, en cas d'absence de réponse d'une entité NIS2 dans un délai raisonnable (suite à la réception d'un message d'alerte) décider de transmettre certaines informations limitées au service d'inspection*** *(nom de l'entité, secteur concerné, la menace identifiée, date du message d'alerte – sans autre éléments ou données).* ***Celui-ci pourrait dès lors contacter***

---

[69] Plus précisément, l'Autorité a posé les deux questions complémentaires suivantes :

S'il est bien fait état de l'indépendance complète du service d'inspection, *quid* du CSIRT (national) ? Le service d'inspection peut-il collecter les données traitées par le CSIRT dans le cadre du Projet aux fins qui lui sont propres ? Ou existe-t-il un *chinese wall* entre le CSIRT national et le NCCA dans le cadre du Projet ?

Le demandeur a été invité à confirmer que les données collectées dans le cadre du Projet et de ses suites ne seront pas traitées par le CCB à des fins de contrôle ou sanction des entités concernées. Par exemple, le CCB (service d'inspection ou autre) ne vérifiera pas que les entités informées dans le cadre du Projet ont ou pas, le cas échéant, introduit une notification auprès du CCB.

l'entité en vue de l'encourager à entreprendre les mesures de protection nécessaires de ses systèmes d'information *(éventuellement de manière contraignante).*

Il convient néanmoins de signaler que le fait d'être victime d'un serveur C2 ne signifie pas nécessairement qu'un manquement aux obligations de cybersécurité ou de notification d'incident significatif découlant de la loi NIS2 ait été commis » (mis en gras par l'Autorité).

110. L'Autorité prend acte de cette réponse et souligne cependant qu'elle ne perçoit pas la raison pour laquelle le service d'inspection devrait intervenir dans le cadre du Projet. **Il est à noter que la Loi NIS2 ne prévoit pas d'obligation particulière à charge de celui** (victime ou autre) **qui reçoit un message d'alerte** (et le Projet non plus d'ailleurs), **de répondre à la communication qui lui est envoyée**. Certes, comme cela a déjà été évoqué précédemment (considérant n° 26), **il est possible** selon les cas, qu'à la suite de la communication reçue par le CCB (CSIRT national), **l'entité essentielle ou importante concernée soit obligée, conformément à la Loi NIS2, de procéder à une notification d'incident**. Mais il s'agit d'une autre hypothèse que celle qui consisterait à devoir communiquer une « réponse » à un message d'alerte reçu dans le cadre du Projet. **En tout état de cause, l'Autorité ne perçoit pas pourquoi, compte-tenu de la finalité du Projet** (qui ne constitue pas une finalité de contrôle), **le CCB en tant que CSIRT national** ne pourrait pas veiller à adapter la communication envoyée aux victimes concernées, afin d'encourager celles-ci à mettre en œuvre les mesures nécessaires (et le cas échéant, à recourir à son assistance), quitte à prendre plusieurs fois contact avec elles.

II.8. Durée de conservation des données

111. La Note communiquée précise que « *CCB slaat de ontvangen data beveiligd op voor maximaal 1 jaar, dit om* ***grondige analyses*** *te kunnen maken over meerdere gegevens* » (mis en gras par l'Autorité). L'AIPD indique que les données seront stockées « *jusqu'à la fin de l'investigation et de l'avertissement des victimes* ***et*** *jusqu'à maximum un an à partir de la collecte* » (mis en gras par l'Autorité). Ne percevant pas la nécessité de conserver les métadonnées de communications électroniques au-delà du temps nécessaire à l'investigation et l'avertissement des victimes, pour une durée allant jusqu'à 1 an[70], l'Autorité a invité le demandeur à concrétiser les premières réponses communiquées afin de clarifier la nécessité à laquelle répond la conservation envisagée.

112. Le demandeur a répondu ce qui suit :

[70] Et ce, d'autant moins que les métadonnées devraient être communiquées par les opérateurs concernés aussi longtemps que le C2-server concerné est actif.

« *Il est envisagé que les données soient stockées pour la durée du traitement nécessaire (information et analyse), c'est-à-dire jusqu'à la fin de l'investigation et de l'avertissement des victimes, et jusqu'à* ***maximum*** *un an à partir de la collecte initiale.* ***Elles seront supprimées au plus tard à l'expiration de ce délai, sans préjudice des résultats d'enquête et des rapports qui auront été établi par le CCB dans le cadre des enquêtes sur les serveurs C2 lancées après la constatation de communications entre ces serveurs et des victimes****.*

Ce délai doit permettre au CCB, durant un délai raisonnable, de croiser utilement les informations entre les activités des différents serveurs C2 (analyse de la menace et son évolution dans le temps). Ce délai permet également au CCB, le cas échéant, de pouvoir démontrer et justifier les traitements effectués (accountability RGPD et règles de responsabilité de droit commun) » (mise en gras modifiée par l'Autorité et souligné par l'Autorité).

113. A l'aune de cette explication, l'Autorité considère que les métadonnées collectées peuvent être **conservées jusqu'à la fin de l'investigation et de l'avertissement des victimes, et jusqu'à maximum un an à partir de la collecte initiale, afin de croiser utilement les informations entre les activités des différents serveurs C2 (analyse de la menace et son évolution dans le temps) et à des fins d'*accountability***.

114. Cette durée de conservation **ne pourra par conséquent pas être** « *sans préjudice des résultats d'enquête et des rapports qui auront été établi par le CCB dans le cadre des enquêtes sur les serveurs C2 lancées après la constatation de communications entre ces serveurs et des victimes* ». En effet premièrement, l'Autorité ne perçoit pas l'hypothèse concrète (ni la finalité) qui est visée par ce traitement de données qui n'apparaissait pas dans la demande initiale adressée à l'Autorité et la Note qui y était jointe. Deuxièmement, l'Autorité rappelle que la finalité du Projet est l'avertissement des victimes afin de prévenir la réalisation de la menace concernée (y compris la réalisation des analyses nécessaires à cette fin), et souligne en toute hypothèse, que tant la Loi NIS2 que la LCA limitent la compétence d'autorisation de l'Autorité à des fins non pénales.

II.9. Décision

Par ces motifs,
L'Autorité décide, dans les limites rappelées aux considérants nos 12-17, que

1. Le demandeur doit indiquer clairement à l'Autorité, dans les 10 jours ouvrables à compter de la communication de la présente décision (la date d'envoi du courrier électronique à

l'attention du demandeur, par l'Autorité, faisant foi), les passages de sa décision qui selon lui, ne peuvent pas être publiés aux motifs évoqués avancés par lui (**considérants nos 6-11**) ;

2. Chaque demande concrète d'autorisation d'accès à des métadonnées de communications électroniques auprès d'un opérateur doit être soumise pour autorisation préalable à l'Autorité. Ce qui n'exclut pas que les demandes d'autorisations subséquentes, ou de contrôle ultérieur en cas d'urgence, puissent se référer à la présente décision, pour autant qu'elles restent motivées de manière circonstanciée pour le surplus.

S'agissant d'une première demande dans le cadre du Projet particulier du demandeur, l'Autorité est favorable à la démarche suivie par celui-ci consistant à lui soumettre une demande d'autorisation préalable initiale, plutôt que, à supposer que l'urgence puisse être invoquée dans le cadre de sa demande, de placer l'Autorité devant le fait accompli, dans une situation de contrôle ultérieur (**considérants nos 18-24**) ;

3. Le Projet est fondé sur l'article 19, § 1er, 2°, de la Loi NIS2. Il s'agit de diffuser des messages d'alerte et des informations sur les cybermenaces et les vulnérabilités auprès des entités et personnes potentiellement victimes concernées, après avoir réalisé les actes d'analyse et de détection nécessaires à cette fin (**considérants nos 25-29**) ;

4. Toute demande d'autorisation préalable doit indiquer le ou les opérateurs concernés par la demande d'autorisation (**considérants nos 33-36**) ;

5. Le Projet peut concerner les métadonnées de communications électroniques entre les C2-servers et les entités essentielles ou importantes visées par la Loi NIS2, ainsi que les métadonnées de communications électroniques entre ces C2-servers et d'autres entités (**considérants nos 37-44**).

Cependant s'agissant de ces autres entités, l'Autorité considère que cette interprétation de la Loi NIS2 devrait être confirmée à brève échéance par le législateur, soit par une loi interprétative, soit via une modification de la Loi NIS2, afin de garantir notamment la sécurité juridique des traitements de données mis en œuvre. Il appartient au CCB d'entreprendre des démarches en ce sens et l'Autorité prêtera attention à ce point dans le cadre des demandes d'autorisation (ou de contrôle ultérieur) futures (**considérant n° 45**) ;

6. Conformément aux informations communiquées par le demandeur, l'identification d'une victime se fait sur la base de plusieurs éléments : [redacted]

[redacted]

(**considérants nos 46-50**) ;

7. La collecte des sources d'identification des adresses IP listées par le demandeur dans le cadre du Projet doit être conforme à la Loi NIS2. En outre, le Projet nécessite la mise en place d'un processus efficace de vérification de la qualité des informations relatives aux C2-servers communiquées par l'ensemble de ces sources et partant, du fait que les adresses IP concernées sont effectivement dédiées au trafic de C2-servers sélectionnés sur la base de la gravité de l'impact de leurs activités. Ce processus doit comprendre les combinaisons pertinentes de mesures techniques prévues dans la Note complémentaire communiquée par le demandeur, ainsi que le cas échéant, toute autre mesure supplémentaire qu'exigerait l'état de la technique en la matière. Enfin, le demandeur doit évaluer et indiquer le niveau de fiabilité des sources d'informations, services et prestataires de services auxquels il recourt dans le cadre de la mise en œuvre du Projet. Ces processus et leur mise en œuvre doivent être documentés au titre de l'accountability (**considérants nos 52-61**) ;

8. Le Projet nécessite la mise en place d'un processus efficace de contrôle au moins quotidien du caractère à jour des adresses IP des C2-servers concernés (le cas échéant, plus fréquent si l'état de la technique le permettait et le nécessitait), basé sur les mesures de vérification visées aux considérants nos 57 et 59. Ce processus et sa mise en œuvre doivent être documentés conformément au principe d'accountability (**considérants nos 62-66**) ;

9. Le Projet nécessite que, dès que le CCB (CSIRT national) constate qu'une adresse IP n'est plus liée au C2-server concerné, l'opérateur concerné en soit immédiatement notifié via un canal adapté et cesse dès ce moment la collecte des métadonnées relatives au trafic depuis et vers l'adresse concernée. Le Projet doit également prévoir un processus aussi efficace de notification à l'attention du CCB (CSIRT national) cette fois, lorsque l'opérateur concerné dispose d'éléments objectifs de nature à questionner l'exactitude des données concernées. L'Autorité doit être informée des mises à jour opérées à l'égard de la liste de C2-servers dans ce contexte, à l'occasion de la prochaine demande d'autorisation (ou de contrôle ultérieur) qui lui est adressée dans le cadre du Projet (**considérants nos 67-70**) ;

10. Nonobstant la réelle plus-value du Projet, celui-ci nécessite d'envisager la mise en œuvre simultanée par le CCB (CSIRT national) des moyens dont il dispose qui donneraient la possibilité à d'autres autorités, de faire bloquer/filtrer par les opérateurs concernés les

adresses IP dédiées aux C2-servers concernés, de manière à prévenir la réalisation des menaces concernées (**considérants nos 73-77**) ;

11. Compte-tenu de sa finalité, à l'aune des principes de finalité et de proportionnalité (y compris la minimisation des données), le Projet nécessite d'envisager la mise en œuvre simultanée, dans la mesure du possible (sur la base des informations à disposition du CCB (CSIRT National) et des risques pour la cybersécurité), d'une information générale (pas seulement à l'attention des victimes concernées) à propos des C2-servers et adresses IP concernés via « Cyber Threat Alerts » (**considérants nos 79-81**) ;

12. Les données contextuelles du type de celles communiquées dans le cadre de la présente demande (première liste de C2-servers communiquée par le demandeur) doivent à tout le moins être communiquées également aux opérateurs. Il en va de même et *a fortiori* dans les cas d'urgence, lorsqu'une demande d'autorisation préalable n'est pas adressée à l'Autorité, et que la demande de collecte des métadonnées est directement adressée aux opérateurs (**considérants nos 85-89**) ;

13. Chaque demande d'autorisation dans le cadre du Projet, ainsi que chaque demande de contrôle ultérieur en cas d'urgence, doit comporter les documents probants (du type de la Note complémentaire ; sans préjudice de la possibilité pour l'Autorité de demander à l'appui des demandes ultérieures la communication des documents sur la base desquels le CCB (CSIRT national) identifie les adresses IP concernées) sur la base desquels les adresses IP dédiées aux C2-servers sont identifiées comme étant pertinents dans le cadre du Projet. De la même manière, en principe, ces pièces devraient aussi être communiquées à l'opérateur, dans le cas particulier où il disposerait d'éléments objectifs de nature à questionner l'exactitude des adresses IP et données contextuelles communiquées, et ce *a fortiori* également, lorsque dans ce même cas, en raison de l'urgence, une demande d'autorisation préalable n'est pas adressée à l'Autorité, et que la demande de collecte des métadonnées est directement adressée aux opérateurs. A moins que la communication de ces documents à l'opérateur soit limitée en raison du droit applicable, ce qui doit être documenté (**considérants nos 90-95**) ;

14. La documentation relative au Projet doit être adaptée de manière à refléter que la coopération de l'opérateur dans la communication aux victimes potentielles se fait sur base volontaire (**considérants nos 96-98**) ;

15. Dans le cadre de la mise en œuvre du Projet, conformément aux réponses communiquées par le demandeur, aucune dérogation aux droits des personnes concernées n'est envisagée (**considérants nos 99-102**) ;

16. Les métadonnées de communications électroniques collectées par le CCB (CSIRT national) ne peuvent pas être traitées ultérieurement en vue de l'accomplissement d'une autre finalité que celle visée par le Projet (**considérants nos 103-110**) ;

17. Les métadonnées collectées peuvent être conservées jusqu'à la fin de l'investigation et de l'avertissement des victimes, et jusqu'à maximum un an à partir de leur collecte initiale, afin de croiser utilement les informations entre les activités des différents serveurs C2 (analyse de la menace et son évolution dans le temps) et à des fins d'*accountability* (**considérants nos 111-114**) ;

18. Dans les conditions et limites visées ci-avant et dans la présente décision, le CCB agissant en tant que CSIRT national, est autorisé à collecter auprès de l'opérateur Belnet, les métadonnées de communications électroniques suivantes, *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*, relatives aux communications électroniques émises vers et depuis les 14 adresses IP dédiées à des C2-servers contextualisées dans la Note complémentaire communiquée et reprises dans la liste communiquée par le demandeur le 8 juillet 2025 et dans l'Annexe ci-après, à partir de la date à laquelle la demande de communication de ces métadonnées sera adressée à Belnet et ce, aussi longtemps que les adresses IP concernées sont dédiées aux C2-servers concernés ;

19. La présente décision peut faire l'objet d'un recours devant le Conseil d'Etat.

Pour le Service d'Autorisation et d'Avis,
(sé.) Alexandra Jaspar, Directrice

[redacted]