Autorité de protection des données
Gegevensbeschermingsautoriteit

Autorisation (délivrée) n° 001/2026 du 16 février 2026

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 » (C2) - alertes – 2 (AH-2025-0072)

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 13 novembre 2025 ;

Vu l'Autorisation de l'Autorité n° 001/2025 du 18 juillet 2025 *concernant une 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)*, reprise en Annexe 2 ;

Vu la demande d'informations complémentaires adressée au Centre pour la Cybersécurité Belgique, le 24 novembre 2025 ;

Vu les informations complémentaires communiquées par le Centre pour la Cybersécurité Belgique, le 21 janvier 2026 ;

Vu la confirmation de la complétude du dossier envoyée au demandeur le 4 février 2026 ;

Prend, le 16 février 2026, 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 Demande est en relation directe avec l'Autorisation de l'Autorité n° 001/2025 du 18 juillet 2025 *concernant une 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)* (ci-après, « **l'Autorisation n° 001/2025** », reprise en Annexe 2) **dans le cadre de laquelle elle s'inscrit**. L'Autorité renvoie à l'Autorisation n° 001/2025 aux fins d'introduction et de contextualisation de la présente Demande. Est en cause un projet du Demandeur en vertu duquel celui-ci prend contact avec les victimes de serveurs C2 à la suite de l'analyse de métadonnées de communications électroniques collectées auprès de fournisseurs de réseaux de communications électroniques (opérateurs) belges (ci-après, « **le Projet** » du demandeur). **La présente Autorisation doit être lue avec l'Autorisation n° 001/2025.**

2. Le Demandeur a joint à sa Demande (catégorisée « SENSIBLE NON-CLASSIFIE (AR 20.12.2024) », « TLP :AMBER+STRICT ») les **quatre annexes** (ensemble, « **la Documentation** ») suivantes auxquelles il sera renvoyé comme indiqué ci-après :
   - [redacted] ci-après la « **Note de Projet** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT » ;
   - [redacted] ci-après la « **Procédure Interne** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT » ;

- [redacted] ci-après la « **Note de Méthode** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT » ;
- [redacted], ci-après « **la Liste des C2S** », catégorisée « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) - TLP :AMBER+STRICT ».

3. S'agissant de la **catégorisation des annexes**, le CCB indique dans la Note de Projet que « *Alle documenten die door het CCB in het kader van dit project worden geproduceerd, zijn geclassificeerd als "GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)" - TLP:AMBER+STRICT* ». L'Autorité en prend acte et **en tiendra compte pour autant que les documents concernés reprennent bien la mention pertinente**. Concernant la publication de la présente autorisation, 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 – l'Autorité insiste sur le respect de ce délai), les passages de sa décision qui selon lui, ne peuvent pas être publiés aux motifs avancés par lui (**considérants nos 6-11 de l'Autorisation n° 001/2025**)[1].

4. Via la Demande, sont en substance demandés : l'accès à de nouvelles métadonnées de communications électroniques et l'autorisation nécessaire à cet accès moyennant l'adaptation de certaines des conditions fixées dans l'Autorisation n° 001/2025 compte-tenu d'éléments et modalités complémentaires fixés dans le Projet (modifications du projet initial).

II. Examen

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

[1] Cet exercice n'est évidemment pas nécessaire pour l'Annexe 2.

II.1. Modifications de la demande initiale en relation avec le contexte de l'Autorisation n° 001/2025 et approche suivie dans le cadre de la présente autorisation

5. Si la Documentation relative au Projet communiquée par le Demandeur est adaptée, il n'est pas toujours évident d'identifier clairement les nuances de la Demande par rapport à ce qui a été autorisé par l'Autorité dans son Autorisation n° 001/2025. Le Demandeur ne vise pas non plus les considérants pertinents de l'Autorisation n° 001/2025 qui seraient, d'une manière ou d'une autre à l'aune de son Projet adapté, problématiques.

6. **La présente autorisation ne peut pas être lue comme une validation de la Documentation communiquée par le demandeur. Il appartient au demandeur d'identifier clairement et explicitement les considérants pertinents d'une Autorisation de l'Autorité qui**, d'une manière ou d'une autre, poseraient problèmes à l'aune de son Projet **et nécessiteraient selon lui une adaptation de l'approche suivie par l'Autorité**. Encore lui incombe-t-il d'**indiquer pour quels motifs une telle adaptation est nécessaire** en vue de la bonne poursuite de son Projet. A défaut, l'Autorité doit mener un exercice de lecture croisée des documents qui est source d'erreur, d'incompréhension et d'inefficacité. L'Autorité rappelle qu'en la matière, elle est tenue à un délai de décision particulièrement contraignant, certes suspendu pendant le cours de la mise en état du dossier.

7. Cela étant dit, **l'Autorité est favorable à la démarche suivie par le Demandeur consistant à lui soumettre une demande d'autorisation préalable compte-tenu des modifications de son Projet**, 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. Une telle approche garantit un travail plus efficace et plus sûr sur le plan juridique.

8. Sur la base de la Demande et de la Documentation communiquées, **l'Autorité observe que les aspects suivants du Projet modifié du Demandeur appellent une réaction et le cas échéant, une décision spécifique, au regard de l'Autorisation n° 001/2025** :

- L'extension de la Demande quant aux types de métadonnées concernées ;
- L'extension de la Demande à deux autres opérateurs (Proximus et Telenet) ;
- L'extension de la Demande à des métadonnées de communications électroniques qui ont eu lieu dans le passé (accès à des métadonnées de communications électroniques conservées par les opérateurs) ;
- La possible extension de la Demande quant à la finalité poursuivie et quant à des traitements ultérieurs de données ;
- La question du recours à des mesures alternatives afin d'agir contre les serveurs C2 (blocage, communication aux autorités judiciaires et via Threat Alerts) ;
- La modification de la régularité avec laquelle le CCB (CSIRT national) vérifie qu'une adresse IP demeure dédiée à l'activité d'un serveur C2 ;
- La limitation des informations contextuelles communiquées aux opérateurs ;
- Les droits des personnes concernées.

9. L'Autorité s'est également penchée plus en profondeur sur **certains aspects techniques** du Projet du Demandeur.

10. Tous ces sujets sont traités dans les développements suivants.

II.2. Extension de la Demande quant aux métadonnées concernées

II.2.1. Quant aux types de métadonnées concernées

11. Il ressort de la Documentation communiquée par le Demandeur que sont désormais visées « *Indien mogelijk, andere* ***beschikbare*** ***metagegevens,*** [redacted] (mis en gras et souligné par l'Autorité). L'Autorité a invité le demandeur à identifier précisément et exhaustivement ces autres métadonnées et à justifier de leur nécessité dans le cadre de son Projet. Celui-ci a répondu ce qui suit :

> « *Met deze passage uit de interne procedure wordt bedoeld dat aan de ISPs gevraagd zou worden om minstens een minimale set metadata te delen* [redacted] *Deze vraag zou, mits autorisatie door de GBA, afdwingbaar zijn.* ***Daarnaast echter, nodigen we ISPs immer uit om andere metadata te delen, indien mogelijk en beschikbaar, en daarom dus ook niet verplichtend of afdwingbaar, en ondergeschikt aan hun eventuele wettelijke beperkingen alsook technische mogelijkheden en beschikbare capaciteit****. Indien dit in de ogen van de GBA te ver gaat, kunnen we dit uit onze verzoeken aan de ISP's verwijderen.*

[redacted]

12. Cette réponse appelle les deux précisions suivantes. D'une part, l'Autorité rappelle que selon l'article 2, 93°, de la LCE, les « *métadonnées de communications électroniques* » *sont définies comme « les données* ***traitées*** *dans un réseau de communications électroniques* ***aux fins de la transmission, la distribution ou l'échange de contenu de communications électroniques****, y compris les données permettant de retracer une communication et d'en déterminer l'origine et la destination ainsi que les données relatives à la localisation de l'appareil produites dans le cadre de la fourniture de services de communications électroniques, et la date, l'heure, la durée et le type de communication* » (mis en gras par l'Autorité). Or sans pour autant que l'Autorité poursuive l'analyse à ce sujet, les données évoquées ci-avant ne semblent pas être nécessaires à la transmission des communications concernées mais plutôt être statistiques/agrégées supplémentaires relatives aux communications individuelles concernées.

13. D'autre part **plus fondamentalement**, l'Autorité partage la position du Demandeur selon laquelle l'hypothèse visée par l'article 21, § 2, de la Loi NIS2 concerne celle d'une **obligation** des opérateurs de communiquer les données concernées. Dans cette **première hypothèse** d'ailleurs, comme l'Autorité l'a déjà mis en évidence, chaque entité, l'opérateur d'une part, et le CCB (CSIRT National) d'autre part, sont des responsables du traitement distincts. Le premier est responsable d'une communication de données au CCB (CSIRT National) en vertu d'une obligation légale ancrée dans la Loi NIS2 s'imposant à lui, et le second est responsable d'un traitement de données nécessaire à la mise en œuvre de ses missions d'intérêt public consacrées dans la même loi.

14. La **seconde hypothèse** dans laquelle l'opérateur **déciderait volontairement** d'échanger des données avec le CCB (CSIRT National) est juridiquement sensiblement différente et soulève des questions additionnelles (qu'en est-il du fondement légal et de la licéité de la communication des données par l'opérateur dans ce contexte ? ; qu'en est-il des responsabilités de l'opérateur et du CCB (CSIRT National) au regard de l'ensemble des traitements de données mis en œuvre – deviennent-ils plutôt responsables *conjoints* des traitements concernés ? ; etc.). **En tout état de cause, l'Autorité n'est pas compétente pour aborder ces questionnements dans le cadre de la présente Demande, ni *a fortiori*, pour se prononcer à propos de cette seconde hypothèse de**

traitement de données, dès lors que celle-ci selon elle, sort du champ d'application de l'article 21, § 2, de la Loi NIS2.

15. L'Autorité s'est par ailleurs interrogée sur ce que signifiait pour le Demandeur la référence, quant aux données communiquées par les opérateurs, à des **données brutes** (« *CCB ontvangt liefst ruwe gegevens als beschikbaar maar kan eventueel werken op geaggregeerde gegevens* »). Le Demandeur a répondu ce qui suit :

> « ***Ruwe data zoal Pcaps (of dus Full Packet Capture) – indien ze beschikbaar zijn en (zowel legaal als technisch) kunnen/mogen gedeeld worden –*** *kunnen immer meer informatie geven en analyses verrijken mbt het type en schaal van aanval. Geaggregeerde metadata is echter ook reeds voldoende om eerste analyses uit te voeren om te verifiëren dat het effectief gaat om kwaadaardig verkeer met Belgische slachtoffers en hen te waarschuwen. Verdere analyse op ruwere data kan vervolgens uitgevoerd worden in samenspraak met het slachtoffer* » (mis en gras par l'Autorité).

16. Au-delà des développements précédents concernant ce qui peut ou qui doit être communiqué par les opérateurs, l'Autorité confirme qu'il est **illégal dans le cadre du Projet et de la présente Autorisation de collecter auprès des opérateurs des données de PCAP (*packet capture*)** dès lors que telles données portent notamment sur (contiennent) le **contenu de communications électroniques**, ce qui va par définition et donc manifestement, au-delà du concept de métadonnées de communications électroniques rappelé au considérant n° 12.

II.2.2. Quant aux opérateurs concernés (Belnet, Telenet et Proximus)

17. La Demande concerne l'accès à des métadonnées de communications électroniques traitées par **Belnet, Telenet et Proximus**. Ces deux derniers opérateurs n'étaient pas concernés dans le contexte de l'Autorisation n° 001/2025. Notamment compte-tenu de l'exigence de non-discrimination consacrée dans l'article 21, § 1er, de la Loi NIS2, l'Autorité a interrogé le demandeur sur la raison pour laquelle sa Demande est étendue (et n'est étendue qu'à) Telenet et Proximus, l'Autorité étant dès le départ partie du principe que Belnet présentait une spécificité telle, liée aux types d'organisations constituant sa clientèle (services publics, hôpitaux, etc.), que son inclusion ne soulevait pas d'interrogation. Le Demandeur a répondu ce qui suit :

> « *Uniquement Proximus, Telenet et Belnet sont visés par la demande puisque nous avons déjà pu établir des contacts préliminaires avec ces trois opérateurs. Nous savons que ces opérateurs sont d'accord à collaborer avec le CCB dans le cadre du présent projet. Cela nous permet de concentrer, encore dans un second temps, l'exécution du projet sur des opérateurs*

qui souhaitent collaborer avec nous, ce qui facilite son lancement. Avec ces trois opérateurs, nous savons que la collaboration sera fructueuse et permettra d'éventuellement encore faire positivement évoluer le projet avant de l'étendre à d'autres opérateurs ».

18. L'Autorité prend acte de cette réponse. L'Autorité attire l'attention du CCB (CSIRT National), dès lors qu'il implique d'autres opérateurs que Belnet, sur l'importance, dans l'accomplissement de ses objectifs, de veiller au respect des principes d'objectivité et de non-discrimination conformément à **l'article 21, § 1er, de la Loi NIS2**. Compte-tenu de la finalité du Projet, qui entend viser des menaces graves et aider tous types d'entités à se prémunir contre celles-ci, **il appartient au CCB (CSIRT National) d'également veiller à ce que la couverture géographique du Projet et sa couverture en termes d'infrastructures de réseaux publics de communications électroniques en Belgique soient pertinentes et cohérentes**. L'Autorité insiste en outre, sur l'importance du **partage des informations à propos des serveurs C2** via les canaux usuels du CCB (CSIRT National), d'autant plus importante en l'occurrence concernant les opérateurs et entités qui n'entrent pas dans le champ d'application du Projet[2]. Une information à temps et de qualité à propos des serveurs C2 et des adresses IP qu'ils exploitent permet aussi, de limiter leurs victimes potentielles.

II.2.3. Quant aux communications électroniques concernées (communications du passé, articles 122 et 123 de la LEC)

19. « *La demande porte, d'une part sur les MDC conservées par l'opérateur concerné à partir de la date de la présente demande d'autorisation aussi longtemps que les adresses IP concernées sont dédiées aux C2-serveurs concernés, et d'autre part sur les MDC* ***conservées conformément aux délais visés aux articles 122 et 123 de la LCE par l'opérateur concerné antérieurement la date de la présente demande*** *d'autorisation* ***lorsque des éléments à disposition du CCB permettent d'établir une activité malveillante antérieure*** [redacted] (soulignement enlevé et mis en gras par l'Autorité)[3].

20. Le Demandeur entend ainsi accéder à des métadonnées de **communications électroniques qui se sont produites dans le passé.** Pour chaque adresse IP, la Documentation communiquée identifie une **date « *first seen* »** à compter de laquelle les métadonnées conservées par les opérateurs doivent être communiquées. De telle sorte que la Demande interagit avec les règles régissant la conservation des métadonnées par les opérateurs, y compris et en particulier la **législation applicable à la rétention obligatoire des métadonnées** de communications électroniques par ces entités[4]. Cette

---

[2] Voir notamment les considérants nos 45-47.

[3] Point n° 6 de la Demande.

[4] Conformément à l'article 127/1, § 5, al. 2, de la LCE, le ministre compétent « *fait publier au Moniteur belge une circulaire qui comprend une liste des autorités belges qui sont habilitées à obtenir d'un opérateur des données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 et 127* » et une telle circulaire a été publiée dans le *Moniteur Belge* du 1er mars 2024, p. 29298, également disponible sur https://www.ibpt.be/operateurs/publication/ciculaire-concernant-lacces-des-autorites-aux-

matière a donné lieu à plusieurs arrêts de la Cour de Justice de l'Union européenne[5] et dernièrement à **l'arrêt de la Cour constitutionnelle n° 97/2024** du 26 septembre 2024 par lequel notamment, la Cour pose des questions préjudicielles (toujours pendantes) à la Cour de Justice de l'Union Européenne.

21. Il se dégage de la demande du CCB (CSIRT National) que celui-ci entend accéder à des **données visées aux articles 122 et 123 de la LCE** :

- Les **§§ 2 et 3 de l'article 122** ***permettent*** aux opérateurs de traiter les « *données de trafic* » concernant les abonnés ou les utilisateurs finaux à certaines fins qui leurs sont propres, à savoir en substance : la facturation des abonnés, les paiements d'interconnexion, une certaine finalité de marketing et l'offre de services à données de trafic ou de localisation ;

- **L'article 122, § 4, de la LCE** vise une ***obligation*** de conservation de données à charge des opérateurs, afin d'établir la fraude ou l'utilisation malveillante du réseau ou du service ou d'identifier son auteur ou son origine ;

- **L'article 122, § 4/1, de la LCE** prévoit quant à lui que les opérateurs ***peuvent*** conserver certaines données afin d'assurer la sécurité et le bon fonctionnement de leurs réseaux et services de communications électroniques, et en particulier pour détecter et analyser une atteinte potentielle ou réelle à cette sécurité, en ce compris identifier l'origine de cette atteinte ;

- Enfin **l'article 123 de la LCE** prévoit que les opérateurs de réseaux mobiles peuvent conserver des données de localisation autres que les données relatives au trafic se rapportant à un abonné ou un utilisateur final dans une série de cas, notamment lorsque cela est nécessaire pour le bon fonctionnement et la sécurité du réseau ou du service **(§ 1er, 1°)**, ou lorsque cela est nécessaire pour détecter ou analyser les fraudes ou l'utilisation malveillante du réseau **(§ 1er, 2°)**.

---

donnees-conservees-par-les-operateurs, dernièrement consulté le 25/11/2025. L'IBPT a également publié une « Fiche pour le CCB » via son site internet, voir

https://www.ibpt.be/file/cc73d96153bbd5448a56f19d925d05b1379c7f21/5da03db1d36747df364858db70be696bbebad26e/10-fiche-pour-le-centre-pour-la-cybersecurite-belgique.pdf, dernièrement consulté le 25/11/2025. L'Autorité ne se prononce pas à propos du contenu de ces documents.

[5] C.J.U.E. (Gr. Ch.), arrêt du 20 septembre 2022, *Bundesrepublic Deutschland c/ SpaceNet AG, Telekom Deutschland GmbH*, affs jointes C-793/19 et C-794/19 ; C.J.U.E. (Gr. Ch.), arrêt du 5 avril 2022, *G.D. c/ Commissionner of An GardaSiochana et al.*, aff. C-140/20 ; C.J.U.E. (Gr. Ch.), arrêt du 6 octobre 2020, *La Quadrature du Net*, affs jointes C-511/18, C-512/18 et C-520/18 ; C.J.U.E. (Gr. Ch.), arrêt du 21 décembre 2016, *Tele2 Sverige*, affs jointes C-203/15 et C-698/15 ; C.J.U.E. (Gr. Ch.), arrêt du 8 avril 2014, *Digital Rights Ireland*, affs jointes C-293/12 et C-594/12.

22. Dans le cadre du recours introduit devant la Cour constitutionnelle à l'encontre de la Loi du 20 juillet 2022 *relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*[6], la Cour constitutionnelle a posé à la Cour de justice des **questions préjudicielles** à propos notamment de l'article 5, 4° et 5°, de cette Loi, dispositions qui introduisent les actuels **paragraphes 4 et 4/1 de l'article 122 de la LCE**[7], et de son article 6, en ce qu'il prévoit l'actuel **§ 1er, 1° et 2°, de l'article 123 de la LCE**[8]. Autrement dit, **les dispositions visées aux trois derniers tirets du considérant n° 21 sont l'objet de questions préjudicielles en cours d'analyse par la Cour de justice**.

23. Dans ce contexte, l'Autorité a posé plusieurs questions au demandeur afin : de vérifier où en était l'affaire précitée auprès de la Cour de justice et si une évaluation de son impact sur son Projet avait été réalisée ; d'identifier pendant combien de temps les opérateurs concernés (Proximus, Telenet et Belnet) conservent les métadonnées de communications électroniques recherchées pour leurs propres finalités ; et de comprendre comment (selon quelle procédure et sur quelle base) sont fixées les dates « *first seen* »[9]. Enfin, la Note de Projet indiquant que « *Bij ernstige incidenten blijkt bovendien vaak dat de intrusie vele maanden soms jaren aanwezig was alvorens gedetecteerd te worden* », l'Autorité a interrogé le demandeur quant à la question de savoir s'il disposait de chiffres en la matière. Celui-ci a répondu ce qui suit :

[redacted]

[6] L'arrêt est cité au considérant n° 19.

[7] Voir B.23 et B.32.

[8] Voir B.33.1., B.35.3, B.39.2 et B.39.3.

[redacted]

« *Het CCB kan hierover geen details of structurele cijfers vrijgeven* [redacted]

24. L'Autorité prend par conséquent acte du fait que **la date « *first seen* » constitue la date la plus ancienne confirmée du lien entre l'activité concernée du serveur C2 visé et l'adresse IP concernée par la Demande.**

25. **Cependant,** il appartient au demandeur d'adapter sa documentation et plus précisément, la Note de Méthode, afin qu'à la date retenue comme « *first seen* » **corresponde un événement concret.** [redacted]

26. Quant à la durée de conservation des métadonnées pour les finalités propres des opérateurs et quant à l'état de **l'affaire pendante devant la Cour de Justice** et à l'évaluation de son impact sur le Projet, le demandeur a répondu ce qui suit :

« *Nous* ***n'avons pas connaissance de la durée de conservation des métadonnées auprès des opérateurs concernés pour les finalités qui leurs sont propres.*** *Notre*

projet ***se base uniquement sur les données que ses opérateurs sont légalement obligés de retenir dans le cadre de la LCE*** » (mis en gras par l'Autorité).

« ***L'affaire est actuellement toujours pendante devant la Cour de Justice (CJUE). L'opinion de l'avocat général n'a pas encore été rendu.*** *Les informations peuvent être retrouvées ici. Des observations écrites ont été émises par la Commission européenne, des États membres et les requérants. Le CCB a pu prendre connaissance et analyser l'arrêt de la Cour constitutionnelle n°97/2024 du 26 septembre 2024 lors de son adoption, et pris acte du fait que la Cour n'annule pas à ce stade la loi du 20 juillet 2022. Cela semblait déjà être un élément important comparé au traitement que la Cour constitutionnelle avait réservé à la précédente loi de 2016. Par ailleurs, le mécanisme d'accès aux catégories de données de communications électroniques (selon leur finalité de conservation) par les autorités compétentes ne fait pas partie des questions préjudicielles posées à la CJUE dans l'affaire C-661/24.*

Le potentiel impact porte essentiellement sur l'éventuelle rétention de données de communication électronique, par les opérateurs, pour des finalités de lutte contre la fraude et contre les utilisations malveillantes du réseau ou du service (en ce compris l'identification des auteurs et de l'origine). Si la CJUE venait à considérer le mécanisme de rétention pour les finalités ci-dessus tel qu'établit en droit belge comme contraire au droit de l'Union, cela pourrait mener à une rétention moindre de données pour lesquelles le CCB requiert l'accès.

Cela étant, ni l'arrêt de la Cour constitutionnelle n°97/2024 ni les questions préjudicielles posées à la CJUE ne remettent en cause les possibilités d'accès à des catégories de données de communications électroniques (selon leur finalité de conservation) dans le cadre des finalités visées à l'article 21, § 1er, et § 2, alinéa 2, 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 (loi NIS2). L'impact, bien que non négligeable du point des données auxquelles le CCB peut le cas échéant avoir accès, n'est pas de nature à remettre en cause fondamentalement l'action du CCB en matière d'accès à certaines données de communication électronique pour des finalités -toujours sans caractère pénal- de prévention, la recherche et la détection des infractions commises en ligne ou par le biais d'un réseau ou service de communications électroniques, de prévention de menaces graves contre la sécurité publique, et d'examen de défaillances de la sécurité des réseaux ou de services de communications électroniques ou des systèmes d'information » (mis en gras par l'Autorité).

27. Il appartient au demandeur de **mettre en place dans le cadre du Projet, un processus garantissant qu'il tire directement et dès que possible les conséquences dans le cadre de**

son Projet, de l'arrêt à venir de la Cour de Justice. L'Autorité souligne dans ce contexte l'importance de la question posée au demandeur concernant la durée de conservation des métadonnées de communications électroniques par les opérateurs **pour leurs propres finalités** (question à laquelle le Demandeur n'a pas pu apporter de réponse). En effet actuellement et juridiquement, l'accès aux métadonnées traitées par les opérateurs sur la base des **paragraphes 2 et 3 de l'article 122** ne pose pas de problème.

28. Dans ces conditions, les métadonnées relatives à des communications électroniques antérieures à la date de la présente décision **ne peuvent être collectées sur la base des dates « *first seen* » identifiées** par le CCB (CSIRT National) (se référer à la Note de Méthode et à l'Annexe 1) **que si les quatre conditions suivantes sont remplies** :

- Les métadonnées sont collectées sur la base de **fondements légaux précis** (article et selon, paragraphe, alinéa, littera et numéro) explicitement et clairement identifiés par le CCB (CSIRT National) à l'attention des opérateurs (le CCB CSIRT National ne peut se limiter sur ce point, à se référer de manière générale aux articles 122 et 123 de la LCE) ;

- Les métadonnées sont **conservées légalement par les opérateurs concernés**, conformément aux articles 122 et 123 de la LCE, en fonction du fondement légal de la demande ;

- Le Demandeur met en place un processus permettant la **prise en compte directe dans le cadre de son Projet, de l'arrêt attendu de la Cour de justice** : il doit réévaluer la licéité des traitements de métadonnées mis en œuvre dans le cadre du Projet sur la base de ce dernier, et en tirer les conséquences ;

- Chaque date « *first seen* » retenue est associée, dans la documentation conservée par le Demandeur, à un événement concret indiquant un **lien entre l'activité concernée du serveur C2 visé par la Demande et l'adresse IP concernée. Si cette date est trop ancienne** au regard des délais de conservation licite des métadonnées par les opérateurs, la date des métadonnées qui peuvent être collectées **devra être adaptée en conséquence dans la documentation du Demandeur**. L'Autorité **attire l'attention du Demandeur** à ce propos, en particulier concernant [redacted]

II.4. Extension de la Demande quant à la finalité poursuivie et quant aux traitements ultérieurs de données ?

29. S'agissant de la finalité poursuivie par le Demandeur, la demande indique ce qui suit : « *Le projet (voir fiche projet en annexe) porte sur l'identification et l'alerte des victimes (y compris les entités NIS2, les autorités publiques, tes entreprises, les citoyens, etc.) de serveurs C2 proportionnellement aux objectifs légaux (tels que la détection des infractions commises en ligne ou via un réseau ou un service de communication électronique (sans finalité pénale) - l'alerte des victimes potentielles et la prévention des menaces graves pour la sécurité publique)* ». La Note de Projet semble toutefois aller plus loin que ce qu'a autorisé l'Autorité à l'aune du projet initial dans les considérants nos 25 et 29 de l'Autorisation n° 001/2025 : « *Hel doel van het CCB-project en het daaropvolgende verzoek om toegang tot elektronischecommunicatiemetagegevens bij operators van elektronische communicatie is enerzijds het Informeren van de beheerders van Informattesystemen die het slachtoffer zijn van C2-servers, zodat zij de nodige maatregel kunnen nemen om zich te beschermen,* ***en anderzijds hel onderzoeken van tekortkomingen In de beveiliging van netwerken en Informatiesystemen*** » (mis en gras modifiée par l'Autorité). Cette Note poursuit néanmoins ultérieurement comme suit « *Deze doelstellingen vloeien voornamelijk voort uit de taak van het nationale CSIRT zoals vastgelogd in artikel 19, § 1, 2° van de NIS2-wet. Het gaat erom waarschuwingen en informatie over cyberdreigingen en kwetsbaarheden te verspreiden onder potentiële slachtoffers, indien mogelijk in bijna-realtime. Op die manier heeft het project een preventief effect op de uitvoering van dreigingen en schade bij de doelwitten van de C2-servers*[…]. ***Voor de uitvoering ervan*** *is het noodzakelijk om tekortkomingen in de beveiliging van elektronische communicatienetwerken en informatiesystemen te onderzoeken, d.w.z. het opsporen, observeren en analyseren van IT-beveiligingsproblemen die verband houden met de betrokken bedreigingen* » (mise en gras modifiée par l'Autorité).

30. Dans ces conditions, l'Autorité a invité le demandeur à confirmer que les considérants nos 25 et 29 de l'Autorisation n° 001/2025 restaient d'actualité dans le cadre de son Projet et dans la négative, ce qui serait concrètement envisagé de nouveau. Le demandeur a répondu ce qui suit :

> « ***Les considérants 25 et 29 de l'autorisation restent tout à fait d'actualité.*** *Ce passage du projet concernant l'objectif du projet souligne surtout les considérations de l'Autorité au point 29, à savoir :*
>
> 1. *« 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. » ; et*
> 2. *« Et il nécessite dans sa mise en oeuvre 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 ».*
>
> *Nous avons repris les considérations de l'Autorité directement dans la nouvelle version de notre projet* » (mis en gras par l'Autorité).

31. L'Autorité prend acte de cette réponse et souligne qu'il n'y a bien **qu'une seule finalité** poursuivie par le Projet, à savoir diffuser des messages d'alerte et des informations sur les cybermenaces et les vulnérabilités, auprès des victimes potentielles, si possible en temps réel. L'examen des défaillance nécessaires dans ce cadre (« *En anderzijds hel onderzoeken van...* ») ne constitue pas une finalité distincte du traitement des métadonnées de communications électroniques mais s'intègre bien à la finalité précitée. Effectivement, les opérations de traitement y liées sont nécessaires pour que le Demandeur puisse accomplir la finalité du Projet.

32. Ces questionnements peuvent être mis en relation avec le sujet du **traitement ultérieur des données** collectées dans le cadre de la Demande. Deux passages de la Note de Projet sont susceptibles de poser question en la matière : « *Zo mogen de analyses op basis van de verzamelde metagegevens niet worden doorgegeven voor toezicht, incidentrespons of strafrechtelijke vervolging,* ***tenzij wettelijk anders bepaald*** » (mise en gras par l'Autorité) – quelles sont ces autres hypothèses ? ; « *Gegevens die ouder zijn dan een jaar worden door een geautomatiseerd systeem vernietigd,* ***onverminderd de resultaten van het onderzoek en de rapporten*** *die door het CCB zijn opgesteld in het kader van het* ***onderzoek*** *naar de C2-servers dat is gestart nadat communicatie tussen deze servers en slachtoffers was vastgesteld* » (mis en gras par l'Autorité) – Ces résultats et rapports contiennent-ils par conséquent des métadonnées de communications électroniques et leur finalité d'utilisation est-elle bien limitée à justifier la prise de contact avec les victimes concernées ? Dans la négative, qu'en est-il ? Interrogé à ce sujet, le Demandeur a répondu ce qui suit :

> « *Ce passage du projet vise en effet à exclure tout traitement ultérieur des données, sauf si cela est requis par une disposition légale applicable.* ***Nous visons ici en particulier l'article 29 du Code d'instruction criminel,*** *qui pourrait nous imposer le traitement ultérieur des données reçues dans le cadre de notre obligation légale de notifier des infractions pénales aux autorités judiciaires.*
> *Ce passage a été inclus dans notre projet pour répondre aux considérations que l'Autorité avait émise au point 105 de son autorisation, à savoir « [...] 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) [...]* » (mis en gras par l'Autorité).
>
> « *Met rapporten wordt ten eerste bedoeld: de waarschuwings- en adviesrapporten die aan de slachtoffers zouden worden gestuurd. Deze zullen de nodige elementen bevatten om elk slachtoffer apart correct te informeren over de aanval die we bij hen vaststelden en hoe deze kan gemitigeerd worden. Bijvoorbeeld: het CCB stelde tussen moment X en Y malware Z vast*

op poorten A en B van een aan jullie behorend IP-adres C. Dit zullen nooit de ruwe metadata-gegevens zijn.

Anderzijds zullen ook rapporten opgesteld worden ***ter informeren van de andere veiligheidsdiensten, waarin informatie op geaggregeerde wijze zal verwerkt worden om trends vast te stellen, volgens onze samenwerkingsverplichtingen bepaald in artikel 25, § 2, van de NIS2-wet en in artikel 20, § 1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten.***

Tot slot zullen er ook rapporten aan de bevoegde procureur des Konings overgemaakt worden volgens de wettelijke verplichtingen waarin vastgestelde inbreuken worden gemeld, met alle informatie die relevant is voor het onderzoek (zie ook vraag 5.2.1) » (mis en gras par l'Autorité).

33. L'Autorité réitère tout d'abord à l'attention du Demandeur le considérant n° 105 de son Autorisation n° 001/2025 : « *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*[10] » (mise en gras et soulignement modifié par l'Autorité dans le cadre de la présente Autorisation). Par la phrase mise en gras, l'Autorité visait avant tout les règles qui régissent le Projet lui-même, telles que les règles de protection des données qui s'y appliquent dont la mise en œuvre pourrait nécessiter un traitement ultérieur des métadonnées de communications électroniques (par exemple pour démontrer la licéité ou l'illicéité d'un traitement de données).

34. Dans le cadre du Projet, l'Autorité observe que l'application de **l'article 29 du Code d'instruction criminelle**[11] peut dans une certaine mesure, paraître contradictoire avec la finalité du Projet lui-même et avec les intentions du Demandeur. Sur ce dernier point, l'approche suivie par le Demandeur consiste à [redacted]

---

[10] « *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* ».

[11] L'article 29, § 1er, du Code d'instruction criminelle est rédigé comme suit :

« *Toute autorité constituée, tout fonctionnaire ou officier public et, pour le secteur des prestations familiales, toute institution coopérante au sens de la loi du 11 avril 1995 visant à instituer "la charte" de l'assuré social qui, dans l'exercice de ses fonctions acquerra la connaissance d'un crime ou d'un délit, sera tenu de donner avis sur-le-champ au procureur du Roi près le tribunal dans le ressort duquel ce crime ou ce délit aura été commis ou dans lequel l'inculpé pourrait être trouvé, et de transmettre à ce magistrat tous les renseignements, procès-verbaux et actes qui y sont relatifs* ».

[redacted] L'objectif initial ne peut pas être ici de recueillir des preuves en vue d'alimenter des procédures pénales. Cette potentielle contradiction est d'autant plus observable si ce Projet est mis en perspective avec le monitoring des réseaux qui est envisagé dans la stratégie nationale en matière de cybersécurité[13], le fait que les fonctionnaires du CCB (CSIRT National) ne paraissent pas soumis au secret professionnel[14] et la possibilité à terme, d'étendre le Projet à des serveurs C2 « belges »[15]. Cette contradiction se retrouve dans le libellé même de l'article 21, § 2, al. 3, de la Loi NIS2 qui (*lex posterior* par rapport à l'article 29 du Code d'instruction criminelle) vise « ***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* » (mis en gras par l'Autorité). Une application systématique de l'article 29 du Code d'instruction criminelle dans un tel contexte (normatif, du Projet et de la stratégie nationale en matière de cybersécurité) pourrait dans les faits réduire sensiblement la portée de cette restriction (« *sans finalité à caractère pénal* ») contrairement à l'intention exprimée par le législateur dans la Loi NIS2 elle-même.

35. Cela étant précisé, **l'Autorité n'est pas compétente pour se prononcer sur l'application de l'article 29 du Code d'instruction criminelle dans le cadre du Projet au stade de sa saisine en vue de la délivrance d'une autorisation**. L'application de cette disposition entraînera le cas échéant un traitement de données à caractère personnel distinct et ultérieur fondé sur une obligation de droit belge, à évaluer notamment sur la base de l'article 6, 4., du RGPD (traitement fondé sur le droit belge), en dehors de la compétence d'autorisation de l'Autorité.

36. S'agissant de **l'échange d'informations avec les services de renseignements et de sécurité** visés par les articles **25, § 2, de la Loi NIS2**[16] et l'article **20, § 1er, de la Loi du 30 novembre**

[redacted]

[13] Voir sur ce point l'Avis de l'Autorité n° 69/2025 *concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (CO-A-2025-108)*, considérants nos 11-15.

[14] Le secret professionnel fait obstacle à l'application de l'article 29 du Code d'instruction criminelle, voir notamment en ce sens Cour Const., Arrêt n° 44/2019 du 14 mars 2019, B.5.4.

[15] Voir la réponse communiquée par le Demandeur et citée au considérant n° 55 de l'Autorisation n° 001/2025 :

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

[16] Cette disposition est rédigée comme suit :

« *En fonction des besoins nécessaires à l'exécution de la présente loi, les autorités visées au paragraphe 1er coopèrent également, au niveau national, 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* ».

1998 *organique des services de renseignement et de sécurité*[17], les considérations développées au sujet de l'article 29 du Code d'instruction criminelle valent *mutatis mutandis*. L'Autorité comprend néanmoins de la réponse du demandeur que des métadonnées brutes de communications électroniques ne seront pas échangées ; il s'agit de : « *informatie op geaggregeerde wijze zal verwerkt worden om trends vast te stellen* ». Elle relève au passage que sur la base de la pratique d'avis de l'Autorité, les deux dispositions précitées ne peuvent pas *à elles seules*, conformément aux principes de prévisibilité et de légalité consacrés dans les articles 8 CEDH et 22 de la Constitution, fonder un traitement de données à caractère personnel. Elle attire encore l'attention du demandeur sur le fait que si des données ne sont pas à caractère personnel de son point de vue, leur communication à un destinataire pour lesquelles ces données pourraient être des données à caractère personnel constitue bien quant à elle, un traitement de données à caractère personnel[18]. Et notamment, quant aux éléments à prendre en considération pour déterminer si des données peuvent être à caractère personnel pour un destinataire, il convient également de prendre en compte les voies légales dont celui-ci dispose pour obtenir des informations complémentaires auprès de tiers[19].

37. Cela étant précisé, de nouveau, **<u>au stade de sa saisine en vue de la délivrance d'une autorisation</u>**, **<u>l'Autorité n'est pas compétente</u> pour se prononcer sur l'application d'éventuelles obligations légales du CCB (CSIRT National) de communiquer des données liées au Projet aux services de renseignements et de sécurité**. Le cas échéant, ce traitement de données à caractère personnel distinct et ultérieur fondé sur une obligation de droit belge, à évaluer notamment sur la base de l'article 6, 4., du RGPD (traitement fondé sur le droit belge), serait en dehors de la compétence d'autorisation de l'Autorité.

---

[17] Cette disposition est rédigée comme suit :

« *Les services de renseignement et de sécurité, les services de police, les autorités administratives et judiciaires veillent à assurer entre eux une coopération mutuelle aussi efficace que possible. Les services de renseignement et de sécurité veillent également à assurer une coopération avec les services de renseignement et de sécurité étrangers* ».

[18] Voir dans ce sens C.J.U.E., arrêt du 9 novembre 2023, *Gesamtverband Autoteile-Handel eV c/ Scania CV AB*, aff. C-319/22, paragraphes nos 48-49 :

« *Dans ces conditions, le VIN constitue une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, de la personne physique mentionnée dans le même certificat, dans la mesure où celui qui y a accès pourrait disposer de moyens lui permettant de l'utiliser pour identifier le propriétaire du véhicule auquel il se rapporte ou la personne pouvant disposer de ce véhicule à un titre juridique autre que celui de propriétaire.*

Ainsi que M. l'avocat général l'a fait observer aux points 34 et 41 de ses conclusions, lorsque les opérateurs indépendants peuvent raisonnablement disposer des moyens leur permettant de rattacher un VIN à une personne physique identifiée ou identifiable, ce qu'il appartient à la juridiction de renvoi de vérifier, ce VIN constitue pour eux une donnée à caractère personnel, au sens de l'article 4, point 1, du RGPD, ***ainsi que, indirectement, pour les constructeurs automobiles qui le mettent à disposition, même si le VIN n'est pas, en soi, pour ces derniers une donnée à caractère personnel*** *et ne l'est pas, en particulier, lorsque le véhicule auquel ce VIN a été attribué n'appartient pas à une personne physique* » (mis en gras par l'Autorité).

Plus récemment repris dans C.J.U.E. (1re Ch.), arrêt du 4 septembre 2025, *CEPD c/ CRU* (ou « SRB »), aff. C-413/23, paragraphe n° 84.

[19] C.J.U.E. (2e Ch.), arrêt du 19 octobre 2016, *Breyer*, aff. C-582/14, paragraphes 43-48 ; C.J.U.E. (4e Ch.), arrêt du 7 mars 2024, *IAB Europe c/ Gegevensbeschermingsautoriteit*, aff. C-604/22, paragraphe n° 48.

II.5. Recours à des mesures alternatives afin d'agir contre les serveurs C2

38. Le Demandeur motive dans la Note de Projet les raisons pour lesquelles les alternatives à la collecte de métadonnées évoquées par l'Autorité dans son Autorisation n° 001/2025 ne sont pas retenues. Ces considérations sont à mettre en relation avec les considérants nos 74-78 de l'Autorisation n° 001/2025.

39. Tout d'abord et en substance, le Demandeur réitère les **limites des compétences du CCB (CSIRT National)** et souligne qu'il n'a pas de contrôle sur les **suites judiciaires** réservées à des communications sur la base de l'article 29 du Code d'instruction criminelle[20]. S'il est effectivement clair qu'il appartient à l'autorité judiciaire de définir la politique qu'elle entend suivre en la matière, comme l'Autorité l'indique au considérant n° 76 de son Autorisation n° 001/2025, « *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* ».

40. Ensuite, concernant le **filtrage volontaire par les opérateurs**, le Demandeur indique que [redacted] (mise en gras omise par l'Autorité). Ceci appelle les deux commentaires suivants.

41. Premièrement, sans approfondir ici ce que les opérateurs prévoiraient le cas échéant dans les conditions contractuelles de leurs services, l'Autorité rappelle que ceux-ci ont bien également des **obligations légales quant à la sécurité de leurs services**. Notamment, ils ont une obligation d'agir en cas de « *cybermenace importante* » et l'IBPT est susceptible de pouvoir lui-même donner des instructions contraignantes aux fournisseurs d'infrastructures numériques dans ce cadre[21]. Or le Projet est clairement dirigé à l'encontre de menaces graves. En outre, l'article 121/8, § 1er, de la LCE dispose que « *Sans prendre connaissance du contenu des communications, les opérateurs prennent les*

---

[20] Plus précisément :

[redacted]

Krachtens artikel 29 van het Strafwetboek is elke ambtenaar die bij de uitoefening van zijn functie kennis krijgt van een misdrijf of een overtreding, verplicht om de procureur des Konings hiervan onmiddellijk op de hoogte te brengen en hem de desbetreffende informatie door te geven. We kunnen echter geen uitspraak doen over wat er gebeurt met dergelijke aangiften bij het openbaar ministerie (dat volledig onafhankelijk en volgens zijn eigen prioriteiten handelt), laat staan over de beslissing om IP-adressen al dan niet te blokkeren/filteren of de gerechtelijke autoriteiten in te schakelen om IP-adressen van C2-servers te filteren/blokkeren (bijv. art. 39bis, § 1, Strafwetboek) » (mise en gras omise par l'Autorité).

[21] Voir les articles 107/2 à 107/5 de la LCE.

mesures appropriées, proportionnées, préventives et curatives, compte tenu des possibilités techniques les plus récentes, de manière à détecter les fraudes et utilisations malveillantes sur leurs réseaux et services et éviter que les utilisateurs finaux ne subissent un préjudice ou ne soient importunés ».

42. Deuxièmement, il ne peut être exclu en principe qu'un blocage d'une adresse IP par un opérateur ne pourra jamais être mise en œuvre et ne sera jamais efficace en vue de la protection de ses clients. Autrement dit, **il n'est pas exclu que l'approche du Projet puisse se combiner, à un certain moment et/ou dans certaines hypothèses, avec une action de filtrage/blocage des opérateurs.** [redacted]

43. Enfin, et c'est là **le point décisif soulevé par le Demandeur** qui a conduit l'Autorité **à autoriser la demande d'accès introduite dans le cadre de son Projet plutôt que d'imposer le recours à des voies alternatives n'impliquant pas le traitement de métadonnées de communications électroniques**, le Demandeur précise que [redacted] (mise en gras modifiée par l'Autorité).

44. C'est donc bien au CCB (CSIRT National) *in fine* et *in concreto*, qu'il appartient d'apprécier, dans l'exercice de sa mission légale et en utilisant la marge de manœuvre dont il jouit à cette fin, si et quand une mesure alternative de blocage/filtrage par un tiers pourrait être utile, afin de garantir le meilleur niveau de sécurité compte-tenu de la politique qu'il mène en la matière. **Ce que l'Autorité demande est qu'il <u>envisage</u> cette possibilité** et que celle-ci ne soit pas systématiquement pour toute

hypothèse, écartée d'office. Etant entendu dans ce contexte, que l'Autorité a bien pris acte du fait qu'il n'était pas juridiquement compétent pour *imposer* une telle mesure.

45. **Ces considérations en revanche, ne remettent pas en cause l'intérêt de recourir à Threat Alerts tel que visé aux considérants nos à 79-81 de l'Autorisation n° 001/2025.** Dans sa Note de Projet, le Demandeur précise ce qui suit :

> « *De dienst Cyber Threat Alerts biedt algemene of gerichte informatie aan organisaties (NIS2 entiteiten of niet)* ***die zich hebben geregistreerd op het SafeOnWeb@Work platform van het CCB en die deze dienst hebben geactiveerd.***
>
> [redacted] *Het doel is om deze slachtoffers in staat te stellen zich te beschermen tegen kwaadwillige activiteiten die via deze C2-servers worden uitgevoerd.* ***Het doel van het CCB is vervolgens om uitsluitend de slachtoffers van een C2-server specifiek te informeren. Dit is vaak niet mogelijk via Cyber Threat Alerts,*** [redacted]
>
> ***De dienst Cyber Threat Alerts alleen volstaat dus niet om de slachtoffers van deze C2-servers te identificeren en te informeren.***
>
> [redacted] (mis en gras par l'Autorité).

46. Consciente que Threat Alerts ne suffit pas à atteindre l'objectif poursuivi par le Demandeur, l'Autorité a néanmoins interrogé ce dernier afin de savoir si ce canal est également utilisé pour communiquer à propos des serveurs C2 identifiés. Celui-ci a répondu ce qui suit :

> [redacted]

[redacted]

47. L'Autorité comprend de cette réponse que Threat Alerts n'est par conséquent **pas** actuellement utilisé pour diffuser de manière généralisée des informations à propos de serveurs C2. De nouveau, l'Autorité considère qu'il appartient au CCB (CSIRT National) **d'envisager la possibilité de recourir également à ce canal d'information** afin de diffuser une information appropriée (mesures préventives à prendre ou ne pas prendre, etc.) au sujet des serveurs C2 et adresses IP concernés. [redacted]

II.6. Vérification du fait qu'une adresse IP est et demeure dédiée à l'activité d'un serveur C2

II.6.1. Vérifications mises en œuvre

48. Dans le cadre de la Demande, l'Autorité a réinterrogé le Demandeur concernant les mesures de vérification mises en œuvre afin d'établir que les adresses IP concernées sont et demeurent dédiées au trafic de serveurs C2.

[redacted]

[redacted]

50. L'Autorité prend acte des mesures entreprises par le CCB (CSIRT National) [redacted] Ces mesures, qui sont appropriées, n'appellent pas de commentaire additionnel de la part de l'Autorité. Cela étant précisé, si l'Autorité comprend qu'effectivement, [redacted] entraîne une charge administrative de nature à ralentir celle-ci et par conséquent, préjudicier la mise en œuvre efficace du Projet, **il appartient néanmoins au CCB (CSIRT National) d'en conserver une trace minimale sous la forme de son choix, au titre de son obligation d'*accountability*** [redacted]

51. Par ailleurs, l'Autorité a également interrogé le demandeur quant à la manière dont il identifie [redacted] Celui-ci a répondu ce qui suit :

[redacted]

[redacted]

52. L'Autorité prend acte de ces précisions et de la méthode appropriée suivie par le CCB (CSIRT National) qui n'appelle pas de commentaire additionnel de la part de l'Autorité. Il conviendra **d'indiquer à quelles sources il est recouru** lorsque le CCB (CSIRT National) fonde son analyse de cette manière.

II.6.2. Modification de la fréquence de vérification des adresses IP

53. Dans sa Note de Projet, le CCB (CSIRT National) adapte la fréquence du contrôle des adresses IP listées afin de garantir que celles-ci demeurent bien dédiées au trafic d'un serveur C2. Pour rappel, **était envisagé un contrôle quotidien** de ces adresses (considérants nos 64-65 de l'Autorisation n° 001/2025). Cette Note explique **désormais ce qui suit :**

> « *De lijsten met C2-servers die aan de ISP's worden doorgegeven, moeten regelmatig worden bijgewerkt. Elk IP-adres op de lijst mag alleen op de lijst blijven staan als het nog steeds een C2-server betreft.*

[redacted]

[redacted] (mise en gras modifiée et soulignement ajouté par l'Autorité).

54. Dans ces conditions il convient d'adapter l'approche retenue dans le cadre de l'Autorisation n° 001/2025. Le Projet nécessite la mise en place d'un **processus efficace de contrôle au moins hebdomadaire et plus fréquent si cela se justifie, de l'actualité de la pertinence de chaque adresse IP concernée** au regard du Projet (vérification que l'adresse reste dédiée aux activités d'un serveur C2), **basé sur les mesures de vérification visées aux considérants nos 57 et 59 de l'Autorisation n° 001/2025** (voir également les considérants nos 49-51 de la présente Autorisation), **à charge pour le CCB de conserver une trace**, au titre de son obligation d'*accountability*, **de la justification de la périodicité retenue** [redacted]

II.7. Limitation des informations contextuelles communiquées aux opérateurs

55. S'agissant de la communication d'informations contextuelles aux opérateurs, afin que ceux-ci puissent s'acquitter de leurs propres obligations en matière de protection des données, le Demandeur précise ce qui suit dans sa Note de Projet :

> « *Wat betreft de informatie die het CCB aan de elektronische-communicatie-operator moet verstrekken bij een toegangsverzoek, dient te worden opgemerkt dat* ***artikel 127/1, § 6 van de WEC***[22] ***niet vereist dat de operator de precieze contextuele informatie met betrekking tot het verzoek wordt verstrekt,*** [redacted]

[22] Cette disposition est rédigée comme suit :

« *Les demandes que les autorités adressent aux opérateurs afin d'obtenir certaines données conservées en vertu des articles 122, 123, 126, 126/1, 126/3 ou 127 comprennent les mentions minimales suivantes:*

1° l'identité de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de cette autorité, l'identité de ce service;

2° la fonction de la personne de contact auprès de l'autorité demanderesse, ou, lorsque la demande est envoyée à l'opérateur par un service central pour le compte de l'autorité, la fonction de la personne de contact auprès de ce service central;

3° la base juridique sur laquelle se fonde la demande, sauf lorsque la demande est envoyée à l'opérateur par le biais d'un service central pour le compte d'une autre autorité;

4° le délai de réponse souhaité ».

[redacted]

Bovendien ***moet het CCB, overeenkomstig artikel 26, § 3 van de NIS2-wet, de toegang tot informatie, met name dergelijke gevoelige informatie, strikt beperken tot personen die deze informatie nodig hebben en er toegang toe moeten hebben voor de uitoefening van hun taken of hun opdracht in verband met de uitvoering van deze wet.*** [redacted]

Alle documenten die door het CCB in het kader van dit project worden geproduceerd, zijn geclassificeerd als "GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024)" - TLP:AMBER+STRICT » (mis en gras et souligné par l'Autorité).

56. Il est exact que l'article 127/1 de la LEC ne vise pas explicitement la communication par le CCB (CSIRT National) aux opérateurs de l'ensemble des informations contextuelles visées par l'Autorité dans son Autorisation n° 001/2025 et que l'article 26, § 3, de la Loi NIS2 impose au CCB de limiter l'accès aux informations dans le cadre de cette loi 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 son exécution.

57. Cependant, premièrement, le Demandeur **n'identifie pas** (et l'Autorité ne perçoit pas) **en quoi la communication d'informations contextuelles aux opérateurs** qui sont chargés de collecter et transmettre les métadonnées de communications électroniques **serait dommageable** pour le Projet du Demandeur et/ou les entités NIS2. Il convient d'ailleurs de rappeler et d'ajouter à ce sujet, que **le Projet du Demandeur ne porte pas que sur les entités NIS2** (toute victime potentielle étant concernée).

58. En tout état de cause deuxièmement, **l'opérateur a bien besoin de connaître** certaines informations dès lors que sa coopération est imposée. Et à ce sujet, le **cadre normatif** applicable à la sollicitation des opérateurs en vue d'obtenir des métadonnées de communications électroniques **prévoit notamment la mise en place de mesures techniques et organisationnelles**

spécifiques[23]. Et certaines données contextuelles concernées peuvent même être **publiques** (il en est ainsi du **pays d'origine de l'adresse IP**[24]).

59. Troisièmement, tant le CCB (CSIRT national) que l'opérateur sollicité sont des responsables du traitement et doivent, en vertu des **articles 5, 2, et 24 du RGPD,** être en mesure de démontrer que les traitements relevant de leurs responsabilités respectives sont conformes au RGPD (principe d'*accountability*). Il s'agit pour l'opérateur de veiller à ce que les métadonnées qu'il communique s'inscrivent bien dans la finalité du Projet du Demandeur.

60. Enfin quatrièmement, l'article 127/1, § 6, de la LCE prévoit les mentions « **minimales** » qui doivent se trouver dans la demande de métadonnées. Cette disposition permet ainsi de tenir compte d'une part, du fait que la LCE doive être combinée avec des législations spécifiques fondant l'accès aux métadonnées (telles qu'en l'occurrence, la Loi NIS2) qui pourraient le cas échéant, prévoir d'autres mentions complémentaires, et d'autre part, de l'avis de l'Autorité, de la mise en œuvre d'autres obligations légales telles que le principe d'*accountability* juste rappelé.

61. Il s'ensuit que le Demandeur doit à tout le moins indiquer dans les demandes adressées aux opérateurs, **par adresse IP** : le **pays d'origine** de l'adresse IP concernée ainsi que **la menace/l'activité malveillante concrète** (ransomware, espionnage, etc.) **concernée pour la Belgique** (se référer sur ce point aux considérants nos 56 et 58 de l'Autorisation n° 001/2025).

II.8. Durée de conservation des données

62. L'Autorité a réinterrogé le Demandeur sur la justification d'un délai de conservation des métadonnées collectées de 1 an, dès lors qu'une fois que les victimes potentielles contactées ont pu disposer d'un délai raisonnable pour s'interroger au sujet du traitement de données (et le cas échéant, solliciter le responsable du traitement), la nécessité de la conservation des données pour cette durée n'est pas si évidente. En particulier, l'Autorité s'est interrogée sur la finalité suivante évoquée dans la Documentation « *zodat de* ***informatie tussen de activiteiten van de verschillende C2-servers*** *(analyse van de dreiging en ontwikkeling ervan in de tijd)* ***op zinvolle wijze kan worden gekoppeld*** » (mis en gras par l'Autorité). De quels couplages serait-il question et de quelle manière ceux-ci

---

[23] Voir le considérant n° 89 de l'Autorisation n° 001/2025 et dans un domaine plus sensible, le considérant n° 68 de l'Avis n° 118/2025 du 12 novembre 2025 *concernant un projet d'arrêté royal fixant les règles de destruction des données obtenues illégalement visées à l'article 44/4 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et fixant les règles de coopération visées à l'article 44/5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO-A-2025-104).*

[24] Le Demandeur lui-même a rappelé que « *Les* ***ranges IP*** *sont attribués par pays.* [redacted]

s'intègrent-ils à la finalité poursuivie par le Projet du Demandeur ; ceux-ci ne pourraient-ils pas être réalisés sur la base de données agrégées ou anonymisées ? Le Demandeur a répondu ce qui suit :

[redacted] ***Dit kan inderdaad gebeuren op basis van geaggregeerde en geanonymiseerde gegevens***. [redacted] (mis en gras et souligné par l'Autorité).

63. L'Autorité considère que le traitement d'analyse de données identifié dans la réponse communiquée par le Demandeur afin d'identifier des [redacted] **constitue un traitement ultérieur de données compatible avec la finalité initiale du Projet qui justifie que les métadonnées collectées soient conservées pour une durée d'un an à compter de leur collecte, malgré le fait qu'une telle conservation de données ne soit pas nécessaire afin d'avertir les victimes des serveurs C2.** En effet, si les analyses concernées ne sont pas en tant que telles nécessaires pour identifier les victimes potentielles et les informer, elles sont néanmoins **nécessaires pour perfectionner et adapter les méthodes utilisées par le CCB (CSIRT National)** afin d'identifier les serveurs C2, leurs victimes potentielles et les démarches à entreprendre par celles-ci et même de manière générale, à l'encontre des serveurs C2 concernés.

64. Cela étant précisé, **conformément au principe de minimisation des données**, ces analyses **doivent être réalisées sur la base de données anonymisées et à défaut, si cela s'avérait impossible en pratique** (ce qui devrait être documenté conformément au principe d'*accountability*), **sur la base de données agrégées.**

II.9. Droits des personnes concernées

65. Dans le contexte de l'Autorisation n° 001/2025 (considérants nos 99-102), le Demandeur avait indiqué que les droits des personnes concernées **n'étaient pas limités** dans le cadre de son Projet. La **Documentation confirme que les droits des personnes concernées sont applicables dans le cadre du Projet.**

66. Toutefois dans celle-ci, l'extrait suivant pose question : « *Het CCB is verplicht om, voor zover mogelijk, de betrokken natuurlijke personen te informeren over de toegang tot hun elektronische communicatiegegevens* ***wanneer dit het goede verloop van zijn taken of een lopend onderzoek niet meer in gevaar brengt*** *en wanneer deze personen kunnen worden geïdentificeerd* » (mis en gras par l'Autorité). L'Autorité a invité le demandeur à indiquer quelles hypothèses sont visées et quel en est le fondement légal. Celui-ci a répondu ce qui suit :

[redacted]

Cette limitation a pour fondement l'article 21, § 6, de la loi NIS2, selon lequel « Le CSIRT national informe, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement de ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées » (nous soulignons). Par « ses tâches », il faut entendre les tâches auxquelles le paragraphe 2 du même article 21 fait référence, à savoir celles énumérées à l'article 19, § 1er, [alinéa 1er,] 1° à 5°, de la même loi, dont fait partie la tâche « [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 ».

67. L'article 21, § 6, de la Loi NIS2 modalise effectivement une obligation d'informer les personnes concernées[25] mais ne prévoit pas de dérogation au droit d'accès des personnes concernées. En tout

[25] Cet « *alinéa impose au CSIRT de prévenir, dans la mesure du possible, les personnes physiques concernées de l'accès à leurs données de communications électroniques lorsque cela n'est plus susceptible de compromettre le bon déroulement des ses tâches ou d'une enquête en cours et lorsque ces personnes peuvent être identifiées. Cette disposition entend mettre en œuvre*

état de cause, soit la personne concernée est elle-même une victime potentielle du serveur C2 concerné. Auquel cas elle recevra une notification du CCB (CSIRT National) et sera donc nécessairement informée de la collecte préalable de données et sur les démarches à entreprendre (ou pas), conformément au Projet. Soit les analyses sont en cours, le statut de la personne concernée n'est donc pas encore déterminé et elle n'est pas encore identifiée et ne peut pas encore être informée. Le CCB (CSIRT National) ne sait donc pas encore l'informer et dans le cas où elle exercerait son droit d'accès, l'article 11 du RGPD serait d'application. Il en serait de même si l'adresse IP de la personne concernée n'est pas considérée comme étant celle d'une victime potentielle. Si néanmoins la personne concernée démontrait sur la base de documents probants la ou les adresses IP qui lui ont été attribuées pendant une ou des périodes déterminées, sa demande au titre du droit d'accès serait néanmoins recevable.

68. Cela étant précisé, **au stade de sa saisine en vue de la délivrance d'une autorisation, l'Autorité n'est pas compétente pour se prononcer sur l'application des droits des personnes concernées dans le cadre du Projet.**

II.10. Fondement légal du traitement et adaptation du cadre normatif existant

69. Dans son Autorisation n° 001/2025, l'Autorité attirait l'attention du demandeur sur l'intérêt que le législateur confirme la portée que l'Autorité a accepté de reconnaître à la Loi NIS2 dans cette même Autorisation (prise en compte du trafic d'entités qui ne sont pas NIS2, y compris des personnes physiques). Dans le contexte de la présente Demande, le Demandeur a renvoyé l'Autorité vers un Amendement n° 12 à un Projet de loi *relatif à la résilience des entités critiques*[26] complétant l'article 5 de la Loi NIS2 par un paragraphe 7 rédigé comme suit : « *Les articles 8 et 38 ainsi que les dispositions du titre 2 sont applicables à toute personne physique ou morale présente ou établie en Belgique* ». Dans le cadre de la mise en état du présent dossier d'Autorisation, l'Autorité a interrogé le demandeur et celui-ci a précisé qu'une disposition interprétative avait été proposée (à la suite de l'avis du Conseil d'Etat), et que celle-ci « *a été adoptée avec l'ensemble du projet de loi CER le 18 décembre 2025 par la Chambre des représentants. Nous sommes dans l'attente de la publication et de l'entrée en vigueur de cette loi. Selon les informations à notre disposition, la loi CER sera prochainement publiée sous la date de la loi du 19 décembre 2025* ».

70. L'Autorité **n'analyse pas la disposition adoptée entre-temps et se limite, en relation avec la Demande, au commentaire suivant.**

---

le principe de transparence et d'information vis-à-vis des personnes concernées, pour autant que cela ne préjudicie pas aux actions en cours », *Doc. Parl.*, Ch. des Représentants, n° 55-2572/001, p. 173.

[26] *Doc. Parl.*, Ch. des Représentants, n° 56-1002/002, p. 16.

71. De manière générale, l'Autorité n'a jamais remis en question que la Loi NIS2 dans toute une série d'hypothèses pouvait bien s'appliquer à des personnes physiques et impliquer le traitement de données à caractère personnel relatives à ces personnes, y compris des données de communications électroniques. D'ailleurs *in fine*, en matière de communications électroniques, même quand l'abonné au service de communications électroniques concerné est une personne morale (par exemple, une entité NIS2), les participants concrets aux communications électroniques sont susceptibles d'être des personnes physiques[27], de surcroît aisément identifiables par la personne morale concernée qui notamment, conservera en principe un *logging* de l'utilisation de son réseau privé[28]. Autrement dit dès le départ, il n'était clairement pas exclu qu'une application du Projet du Demandeur, même limitée au trafic des seules entités NIS2, puisse impliquer *in concreto* des personnes physiques et le traitement de données à caractère personnel relatives à celles-ci[29].

72. La préoccupation exprimée par l'Autorité était plus spécifique. Elle portait sur le fait que le Projet puisse impliquer un certain monitoring en temps réel au niveau des opérateurs, du trafic IP d'entités qui ne sont pas des entités NIS2, à savoir et entre autres, des entités (y compris des personnes physiques) qui ne sont pas la première et principale cible, compte-tenu de leurs finalités, des dispositifs normatifs européen et belge NIS2. C'est un questionnement qui est d'ailleurs à mettre en perspective avec le monitoring des réseaux qui est envisagé dans la stratégie nationale en matière de cybersécurité[30]. Sans entrer dans les finesses de ce sujet, il peut suffire de relever ce qui suit. Collecter des données à caractère personnel dans le cadre d'une intervention concrète à l'égard d'un incident de sécurité subi par une personne et le monitoring proactif et en temps réel du trafic IP au niveau des opérateurs, sont des traitements de données et approches (réactive ou proactive) différents ne présentant pas le même niveau d'ingérence dans les droits et libertés des personnes. Ils peuvent par conséquent nécessiter des cadres normatifs moins ou plus précis et détaillés conformément aux articles 22 de la Constitution, 8 de la CEDH et 7, 8 et 52 de la Charte européenne des droits fondamentaux. Et dans ce contexte, l'Autorité a pu rappeler les limites de son intervention dans le cadre d'une autorisation et la nécessité que le législateur détermine lui-même les éléments essentiels des traitements de données dont il prévoit la réalisation[31].

73. Cela étant rappelé, l'Autorité prend acte des démarches qui ont été entreprises en la matière.

---

[27] Soit les personnes physiques qui utilisent effectivement le service concerné.

[28] Voir d'ailleurs les considérants nos 31 et 101 de l'Autorisation n° 001/2025.

[29] Le serveur C2 également, d'une manière ou d'une autre, impliquera une ou plusieurs personnes physiques (par exemple, un criminel ou un agent d'un service d'un Etat hostile). Il n'est d'ailleurs pas exclu en théorie que l'adresse IP concernée soit à l'étranger, directement attribuable à une personne physique. Ceci n'impactait aucunement la licéité ou l'encadrement normatif d'un projet du demandeur qui n'aurait été limité qu'au monitoring du trafic des entités NIS2.

[30] Voir sur ce point l'Avis de l'Autorité n° 69/2025 *concernant la « Nationale Cybersecurity Strategie 3.0, 2026-2030 » (CO-A-2025-108)*, considérants nos 11-15.

[31] Voir les considérants nos 14 et 15 de l'Autorisation n° 001/2025.

II.11. Décision

L'Autorité décide, dans les limites rappelées aux considérants nos 12-17 de l'Autorisation n° 001/2025 et aux considérants nos 6-9, 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 de l'Autorisation n° 001/2025 ; considérants nos 2-4**) ;

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 ainsi qu'à l'Autorisation n° 001/2025, pour autant qu'elles restent motivées de manière circonstanciée pour le surplus.

L'Autorité est favorable à la démarche suivie par le Demandeur consistant à lui soumettre une demande d'autorisation préalable compte-tenu des modifications de son Projet, 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. Une telle approche garantit un travail plus efficace et plus sûr sur le plan juridique. Elle attend du Demandeur à l'avenir qu'il identifie clairement les considérants de ses décisions qui nécessiteraient des adaptations en raison de la modification du Projet (**considérants nos 18-24 de l'Autorisation n° 001/2025 ; considérants nos 6-7**) ;

3. L'Autorité n'est pas compétente pour aborder les questionnements liés à l'échange volontaire de données entre l'opérateur et le CCB (CSIRT National) dans le cadre de la demande d'autorisation faisant l'objet de la présente décision, ni *a fortiori*, pour se prononcer à propos d'une telle hypothèse de traitement de données dès lors que celle-ci sort du champ d'application de l'article 21, § 2, de la Loi NIS2 (**considérants nos 11-14**) ;

4. 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 de l'Autorisation n° 001/2025**) (**considérants nos 29-31**) ;

5. Toute demande d'autorisation préalable doit indiquer le ou les opérateurs concernés par la demande d'autorisation (**considérants nos 33-36 de l'Autorisation n° 001/2025**). L'accès aux métadonnées visées ci-après est autorisé auprès de Belnet, Proximus et Telenet (**considérants nos 17-18**) ;

6. Les métadonnées relatives à des communications électroniques antérieures à la date de la présente décision ne peuvent être collectées sur la base des dates « *first seen* » identifiées par le CCB (CSIRT National) (se référer à la Note de Méthode et à l'Annexe 1) que si les quatre conditions suivantes sont remplies (**considérants nos 19-28**) :

- Les métadonnées sont collectées sur la base de fondements légaux précis (article et selon, paragraphe, alinéa, littera et numéro) explicitement et clairement identifiés par le CCB (CSIRT National) à l'attention des opérateurs (le CCB CSIRT National ne peut se limiter sur ce point, à se référer de manière générale aux articles 122 et 123 de la LCE) ;

- Les métadonnées sont conservées légalement par les opérateurs concernés, conformément aux articles 122 et 123 de la LCE, en fonction du fondement légal de la demande ;

- Le Demandeur met en place un processus permettant la prise en compte directe dans le cadre de son Projet, de l'arrêt attendu de la Cour de justice : il doit réévaluer la licéité des traitements de métadonnées mis en œuvre dans le cadre du Projet sur la base de ce dernier, et en tirer les conséquences ;

- Chaque date « *first seen* » retenue est associée, dans la documentation conservée par le Demandeur, à un événement concret indiquant un lien entre l'activité concernée du serveur C2 visé par la Demande et l'adresse IP concernée. Si cette date est trop ancienne au regard des délais de conservation licite des métadonnées par les opérateurs, la date des métadonnées qui peuvent être collectées devra être adaptée en conséquence dans la documentation du Demandeur.

7. 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, y compris des personnes physiques (**considérants nos 37-44 de l'Autorisation n° 001/2025**). L'Autorité prend acte des démarches qui ont été entreprises par le Demandeur ainsi que du fait qu'une disposition interprétative ait été adoptée concernant la Loi NIS2. La préoccupation exprimée par l'Autorité dans son Autorisation n° 001/2025 portait sur le fait

que le Projet puisse impliquer un certain monitoring en temps réel au niveau des opérateurs, du trafic IP d'entités qui ne sont pas des entités NIS2, à savoir et entre autres, des entités (y compris des personnes physiques) qui ne sont pas la première et principale cible, compte-tenu de leurs finalités, des dispositifs normatifs européen et belge NIS2 (**considérants nos 69-73**) ;

8. L'identification d'une victime se fait sur la base de plusieurs éléments : [redacted] (**considérants nos 46-50 de l'Autorisation n° 001/2025**) ;

9. 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 communiquées par le Demandeur dans le cadre de l'Autorisation n° 001/2025 et de la présente autorisation (**considérants nos 48-52**), 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 de l'Autorisation n° 001/2025**).

10. Le Projet nécessite la mise en place d'un processus efficace de contrôle au moins hebdomadaire et plus fréquent si cela se justifie, de l'actualité de la pertinence de chaque adresse IP concernée au regard du Projet (vérification que l'adresse reste dédiée aux activités d'un serveur C2), basé sur les mesures de vérification visées aux considérants nos 57 et 59 de l'Autorisation n° 001/2025 (voir également les considérants nos 49-51 de la présente Autorisation), à charge pour le CCB de conserver une trace, au titre de son obligation d'*accountability*, de la justification de la périodicité retenue à l'aune de la dynamique des activités du serveur C2 concerné, de l'état de la technique et des bonnes pratiques pertinentes (**considérants nos 53-54**) ;

11. 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 de l'Autorisation n° 001/2025**) ;

12. Le CCB, dans les limites de ses possibilités et compétences, doit envisager la possible mise en œuvre simultanée par des tiers, de techniques de blocage/filtrage par les opérateurs concernés des adresses IP dédiées aux C2-servers concernés, de manière à prévenir la réalisation des menaces concernées. Etant entendu que c'est bien au CCB (CSIRT National) *in fine* et *in concreto*, qu'il appartient d'apprécier, dans l'exercice de sa mission légale et en utilisant la marge de manœuvre dont il jouit à cette fin, si et quand une mesure alternative de blocage/filtrage par un tiers pourrait être utile, afin de garantir le meilleur niveau de sécurité compte-tenu de la politique qu'il mène en la matière (**considérants nos 38-44**) ;

13. 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 de l'Autorisation n° 001/2025** ; **considérants nos 45-47**) ;

14. Le CCB (CSIRT National) doit à tout le moins indiquer dans les demandes adressées aux opérateurs, par adresse IP : le pays d'origine de l'adresse IP concernée ainsi que la menace/l'activité malveillante concrète (ransomware, espionnage, etc.) concernée pour la Belgique (se référer sur ce point aux considérants nos 56 et 58 de l'Autorisation n° 001/2025) (**considérants nos 55-61**) ;

15. 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 de Méthode (**considérant n° 2**) ; 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 dédiées aux C2-servers comme étant pertinentes dans le cadre du Projet (**considérants nos 90-93 de l'Autorisation n° 001/2025**) ;

16. L'Autorité n'est pas compétente, au stade de sa saisine en vue de la délivrance d'une autorisation, pour se prononcer à propos de l'exercice par les personnes concernées, de leurs droits tels que prévus aux articles 12 à 21 du RGPD. Les considérations développées à ce sujet dans la présente autorisation sont communiquées à titre purement indicatif (**considérants nos 65-68**) ;

17. 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 de l'Autorisation n° 001/2025**).

L'Autorité n'est toutefois pas compétente, au stade de sa saisine en vue de la délivrance d'une autorisation, pour se prononcer à propos des traitements ultérieurs de données fondés sur des obligations légales s'imposant au CCB (CSIRT National). Les considérations développées à ce sujet dans la présente autorisation sont communiquées à titre purement indicatif (**considérants nos 32-37**).

18. 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 à des fins d'*accountability*. Elles peuvent également être conservées pendant cette durée afin de permettre la réalisation du traitement d'analyse de données identifié dans la réponse communiquée par le Demandeur afin d'identifier des [redacted] Cela étant précisé, conformément au principe de minimisation des données, ces analyses doivent être réalisées sur la base de données anonymisées et à défaut, si cela s'avérait impossible en pratique (ce qui devrait être documenté conformément au principe d'*accountability*), sur la base de données agrégées (**considérants nos 111-114 de l'Autorisation n° 001/2025** ; **considérants nos 62-64**) ;

19. Dans les conditions et limites visées ci-avant et dans la présente décision, en particulier dans le point n° 6 concernant les dates « *first seen* », le CCB agissant en tant que CSIRT national, est autorisé à collecter auprès des opérateurs Belnet, Proximus et Telenet, 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 15 adresses IP dédiées à des C2-

servers contextualisées dans la Note de Méthode et reprise en Annexe 1, à partir des dates « *first seen* » le cas échéant adaptées, et ce, aussi longtemps que les adresses IP concernées sont dédiées aux C2-servers concernés ;

20. 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