Autorité de protection des données
Gegevensbeschermingsautoriteit

Contrôle ultérieur n° 004/2026 du 22 octobre 2026

Objet: Demande de contrôle ultérieur visé à l'article 21, § 4, al. 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 : « Command-and-Control » (C2) – alertes (AUT-2026-00178)

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, al. 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* (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 de contrôle ultérieur de la Directrice Générale adjointe du Centre pour la Cybersécurité Belgique, Madame Phédra Clouner (ci-après, « la Demanderesse »), reçue le 30 septembre 2026 ;

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)* (ci-après, « l'Autorisation n° 001/2025 ») ;

Vu l'Autorisation de l'Autorité n° 001/2026 du 16 février 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 » (C2) - alertes – 2 (AH-2025-0072)* (ci-après, « l'Autorisation n° 001/2026 ») ;

Vu l'Autorisation de l'Autorité n° 002/2026 du 25 juin 2026 *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 » (C2) - alertes – 3 (AUT-2026-00049)* (ci-après, « l'Autorisation n° 002/2026 ») ;

Vu l'Autorisation de l'Autorité n° 003/2026 du 5 octobre 2026 *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 » (C2) - alertes – 4(AUT-2026-00052)* (ci-après, « l'Autorisation n° 003/2026 ») ;

Vu la demande adressée au Centre pour la Cybersécurité Belgique de communiquer les demandes adressées aux opérateurs, le 29 septembre 2026 ;

Vu la communication de ces demandes par le Centre pour la Cybersécurité Belgique, le 1er octobre 2026 ;

Vu la demande d'informations complémentaires adressée au Centre pour la Cybersécurité Belgique, le 8 octobre 2026 ;

Vu les informations complémentaires communiquées par le Centre pour la Cybersécurité Belgique, le 13 octobre 2026 ;

Vu la confirmation de la complétude du dossier envoyée à la Demanderesse le 13 octobre 2026 ;

Prend, le 22 octobre 2026, la décision suivante :

I. Objet et contexte de la demande de contrôle ultérieur

1. Le CCB (CSIRT National) a introduit auprès de l'Autorité une Demande de contrôle ultérieur visée à l'article 21, § 4, al. 2, de la Loi NIS2 (ci-après, « **la Demande** »). Cette Demande s'inscrit dans le cadre **des Autorisations nos 001/2025, 001/2026, 002/2026 et 003/2026**[1] (ensemble, « **les Autorisations précédentes** »). L'Autorité renvoie par conséquent à ces Autorisations précédentes aux fins d'introduction et de contextualisation de la présente Demande. Elle s'y réfère également quant à la description du projet mis en œuvre dans ce contexte par le CCB (CSIRT National) (ci-après, « **le Projet** » du CCB (CSIRT National)). **La présente décision** sur contrôle ultérieur **doit être lue avec les Autorisations précédentes qui ensemble forment un tout**.

2. Le CCB (CSIRT National) a joint à sa Demande (catégorisée « SENSIBLE NON-CLASSIFIE (AR 20.12.2024) », « TLP :AMBER+STRICT ») les **deux annexes** (ensemble, « **la Documentation** ») suivantes, auxquelles il sera renvoyé comme indiqué ci-après :

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

3. A la demande de l'Autorité et conformément à l'article 21, § 4, al. 2, 2e phrase, de la Loi NIS2, le CCB (CSIRT National) a ensuite communiqué les demandes qui ont été adressées aux trois opérateurs concernés (Belnet, Proximus et Telenet), ci-après, les « **Demandes adressées aux opérateurs** », également catégorisées « GEVOELIG NIET-GECLASSIFICEERD (KB 20.12.2024) », « TLP :AMBER+STRICT. L'Autorité signale d'emblée que **ces demandes doivent systématiquement être jointes à toute demande de contrôle ultérieur**.

II. Examen

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

II.1. Analyse 4
II.1.1. Situation urgente 4
II.1.2. Evaluation des demandes adressées aux opérateurs 5

[1] Au moment de l'introduction de sa Demande, le CCB (CSIRT National) ne disposait toutefois pas encore de l'Autorisation n° 003/2026 de telle sorte que le cas échéant, il ne pourrait lui être tenu rigueur, dans le cadre de la présente Demande, de ne pas encore avoir pris en considération cette Autorisation.

II.1.1.1. Approche suivie dans la présente Demande de contrôle ultérieur 5
II.1.1.2. Considérations relatives à la Demande de contrôle ultérieur 6
II.1.1.3. Absence d'autre commentaire 16
II.2. Décision 16
Annexe 1 : liste d'adresses IP dédiées à des C2-servers 24

II.1. Analyse

II.1.1. Situation urgente

4. Pour rappel, l'article 21, § 4, al. 2, de la Loi NIS2, dispose que « *En cas de **situation urgente dûment justifiée**, le CSIRT national peut se passer du contrôle préalable visé à l'alinéa 1er et solliciter directement les données. Cette demande est envoyée sans délai à l'autorité visée à l'alinéa 1er pour permettre un contrôle ultérieur* » (mis en gras par l'Autorité). L'alinéa 3 de cette disposition précise encore que « *Lorsqu'à la suite du contrôle visé à l'alinéa 2, l'autorité de protection des données refuse de confirmer la validité de la demande de métadonnées de communications électroniques visée à l'alinéa 1er, le CSIRT national le notifie sans délai à l'opérateur concerné et supprime les métadonnées reçues* ». En l'absence d'une situation urgente dûment justifiée, l'Autorité devrait constater que les trois Demandes adressées aux opérateurs ne sont pas valides, à défaut de consultation préalable de l'Autorité en vue de l'obtention d'une autorisation.

5. Dans sa Demande, le CCB (CSIRT National) justifie de l'urgence comme suit :

> « *La situation urgente est dûment justifiée par un incident, **classé d'incident de niveau national sous le plan national d'urgence cybernétique*** [redacted] *Pour **s'assurer aussi rapidement que possible que les mêmes attaquants n'ont pas également infiltré d'autres réseaux et systèmes d'informations en Belgique, et le cas échéant prévenir ces autres victimes** (qui pourraient être des entités NIS2), le CCB a déterminé que l'urgence lui permettait d'effectuer directement une demande de MDCE auprès des opérateurs* » (mis en gras par l'Autorité).

6. **L'Autorité considère que la situation décrite par le CCB (CSIRT National)** dans sa Demande, à savoir des infractions pénales susceptibles de relever de la criminalité grave et constituant une

menace grave contre la sécurité publique qui sont **en train de se produire** (voir les considérants nos **12-16**), **constitue bien un cas de situation urgente dûment justifiée**. De telle sorte que le CCB (CSIRT National) était en droit d'adresser directement ses demandes aux opérateurs et de solliciter ensuite un contrôle ultérieur par l'Autorité.

7. Reste à déterminer si ces demandes adressées aux opérateurs pouvaient être autorisées par l'Autorité.

II.1.2. Evaluation des demandes adressées aux opérateurs

II.1.1.1. Approche suivie dans la présente Demande de contrôle ultérieur

8. Via les Demandes adressées aux opérateurs, l'accès à des métadonnées de communications électroniques relatives à [redacted] **nouvelles adresses IP** a été demandé. Ces Demandes et la Demande de contrôle ultérieur du CCB (CSIRT National) s'inscrivent strictement dans les limites juridiques et techniques des Autorisations précédentes de l'Autorité. Notamment, la Demande de contrôle ultérieur s'inscrit dans la même finalité et le même Projet, concerne les opérateurs Proximus, Telenet et Belnet et les mêmes métadonnées de communications électroniques. Le CCB (CSIRT National) réitère dans sa Demande que : « *Les modifications nécessaires ont été apportées aux procédures internes du CCB pour s'aligner entièrement aux éléments soulevés par l'APD dans son autorisation n° 002/2026* » (mis en gras par l'Autorité).

9. Autrement dit, **la Demande de contrôle ultérieur**, au-delà du fait qu'elle constitue une demande de contrôle ultérieur nécessitant d'apprécier l'urgence (considérants nos 4-7) et de déterminer l'approche à suivre par l'Autorité (considérant n° 10), **ne soulève aucun nouveau questionnement de nature juridique ou technique**, de telle sorte que l'Autorité se limite à renvoyer à ses Autorisations précédentes quant aux cadres normatif et technique du Projet, et en particulier, quant à la base légale permettant au CCB (CSIRT National) de demander auprès des opérateurs des métadonnées de communication relatives au trafic ou à la localisation, et quant à l'exercice de sa mission par celui-ci justifiant de la nécessité et du caractère proportionné de ces demandes.

10. Dans le cadre de la présente Demande de contrôle ultérieur, **l'Autorité réalise *a posteriori*, le même contrôle que celui qu'elle réalise dans le cadre d'une demande d'autorisation**. En ce sens et en l'occurrence, elle **s'est limitée à vérifier si dans les faits, sur la base des informations communiquées par le CCB (CSIRT National)** (à ce sujet, voir les considérants nos 90-93 de l'Autorisation n° 001/2025 et les considérants nos 23-39 et 42 de l'Autorisation n° 002/2026), **les adresses IP concernées relevaient bien du champ d'application de son Projet** et pouvaient par conséquent donner lieu à la collecte de métadonnées de communications électroniques auprès des opérateurs concernés, y compris concernant des communications passées pour lesquelles les opérateurs ont légalement conservé ces métadonnées (voir à ce sujet les considérants nos 19-28 de l'Autorisation n° 001/2026 ; considérants nos 23-39 et 46-50 de l'Autorisation n° 002/2026). A

défaut, la collecte de métadonnées de communications électroniques auprès des opérateurs concernés serait contraire au RGPD (articles 5, 1., a), b) et c), et 6, 1., e)) et à la Loi NIS2 (article 21, § 2) et ne pourrait par conséquent pas être autorisée par l'Autorité.

11. Ces vérifications ont mené aux commentaires suivants.

II.1.1.2. Considérations relatives à la Demande de contrôle ultérieur

a) Menace grave contre la sécurité publique

12. Dans la Note contextuelle, le CCB (CSIRT National) indique ce qui suit :

> « [redacted] » (mis en gras par l'Autorité).

13. S'agissant de l'incident en tant que tel, [redacted]

> « [redacted]
>
> [redacted]
>
> [redacted]
>
> [redacted]
>
> [redacted]
>
> […]

[redacted]

14. S'agissant de la **menace grave contre la sécurité publique** concernée, l'Autorité considère en l'occurrence que le CCB (CSIRT National) ne peut se borner à renvoyer aux autorisations précédentes de l'Autorité et à la menace [redacted] en se limitant à indiquer que « [redacted] ». Il n'est effectivement **pas exclu que cette technique soit utilisée par des criminels poursuivant d'autres objectifs**.

15. Cela étant précisé, l'Autorité considère que les demandes adressées aux opérateurs par le CCB (CSIRT National) **peuvent bien être fondées sur l'objectif de prévenir une menace grave contre la sécurité publique** et ce, en raison de la nature de la cible des faits concernés ainsi qu'en raison de la nature de ces derniers :

    - **Quant à la nature de la cible** : [redacted]

    - **Quant à la nature des faits**, en relation avec les considérants nos 10-18 de l'Autorisation n° 002/2026, et nonobstant les réserves émises par l'Autorité concernant l'appréciation de la criminalité grave, les éléments communiqués par le CCB (CSIRT National) [redacted] portent bien à croire qu'est en cause de la **criminalité grave présentant une menace grave contre la sécurité publique**. L'incident à l'appui des demandes adressées aux opérateurs par le CCB (CSIRT National) implique en effet : [redacted]

[2] [redacted]

[3] [redacted]

[4] [redacted]

[redacted]

Enfin, le CCB (CSIRT National) indique que l'incident concerné est **classé comme « incident de niveau national sous le »** « Plan national de réaction aux crises cyber et incidents de cybersécurité » fixé par l'Arrêté Royal du 14 avril 2026 *portant fixation du plan national de réaction aux crises cyber et incidents de cybersécurité pour le territoire belge, la mer territoriale et la zone économique exclusive*, et repris en annexe (non publiée) de ce même arrêté.

16. **La documentation du CCB (CSIRT National) doit être adaptée afin de préciser la nature de la menace grave contre la sécurité publique concernée**, sur la base des développements précédents.

17. Compte-tenu des faits mis en avant dans la Demande de contrôle ultérieur, l'Autorité souhaite réattirer l'attention du CCB (CSIRT National) sur le **considérant n° 18 de son Autorisation n° 001/2026** selon lequel : « *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*[…]*. 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* ». Ceci est d'autant plus vrai dans le cadre d'une situation urgente telle que celle rencontrée dans le cadre de la présente Demande de contrôle ultérieur. L'Autorité observe qu'il est tout d'abord d'autant plus recommandé, dans une telle situation dans laquelle la Belgique est clairement et activement ciblée, d'assurer la meilleure couverture du territoire belge envisageable compte-tenu des moyens à disposition du CCB (CSIRT National), en envisageant une coopération avec des opérateurs supplémentaires à Proximus, Belnet et Telenet, tels que Orange Belgium (VOO) et même des opérateurs B2B.

18. Ensuite, bien que l'Autorité ait compris l'objectif du CCB (CSIRT National) de limiter au maximum la diffusion des adresses IP afin d'éviter que la menace concernée ne se déplace vers d'autres adresses et que son suivi soit tenu en échec, et sans remettre en cause le fait qu'il appartienne au CCB (CSIRT National) de décider de la manière d'agir dans ce contexte, elle réitère l'importance de communiquer à propos de la menace par les canaux appropriés, s'agissant également d'une manière d'atteindre l'objectif poursuivi par le Projet sans collecte de métadonnées de communications électroniques (voir les considérants nos 73-81 de l'Autorisation n° 001/2025).

19. Pour le surplus, l'Autorité prend acte de la classification de l'incident concerné en vertu du « Plan national de réaction aux crises cyber et incidents de cybersécurité » et des conséquences y liées dans le cadre de l'application de ce Plan.

b) Eléments et sources sur la base desquels les adresses IP sont retenues

20. Parmi les [redacted] adresses IP concernées, [redacted] la Note contextuelle indique ce qui suit :

> « [redacted] ».

21. L'Autorité a adressé au CCB (CSIRT National) une demande d'informations complémentaires[5] à la suite de laquelle celui-ci a précisé ce qui suit :

« [redacted]

[5] « [redacted] ».

[redacted] » (mis en gras par l'Autorité).

22. L'Autorité prend acte de ces informations qui nécessitent les commentaires suivants.

23. **Premièrement**, l'Autorité rappelle qu'il incombe au CCB (CSIRT National) d'indiquer les sources sur la base desquelles il retient des adresses IP dans le cadre de son Projet. En l'état, la Note contextuelle n'indique pas sur quelle base les [redacted] adresses IP [redacted] ont été sélectionnées. La Demande de contrôle ultérieur **aurait dû indiquer dès le départ que** [redacted] La Note contextuelle doit être adaptée en ce sens.

24. **Deuxièmement**, sur la base des informations complémentaires fournies par le CCB (CSIRT National), l'Autorité comprend que l'attaque concernée a consisté en [redacted]

    Lorsqu'une demande d'autorisation ou de contrôle ultérieur concerne des adresses IP identifiées dans le cadre d'une attaque informatique, **l'Autorité attend du CCB (CSIRT National) qu'il identifie précisément** (même si cela est succinct) **dans sa demande**, sur la base des informations dont il dispose à ce moment, **les étapes de cette attaque informatique**. Dans le cadre de la présente Demande de contrôle ultérieur, il aurait certainement été utile de communiquer à l'Autorité [redacted]

25. Ces précisions sont déterminantes pour l'Autorité à plusieurs égards. Avant tout, elles sont directement liées à la motivation sur la base de laquelle des adresses IP sont sélectionnées en vue d'une collecte de métadonnées de communications électroniques. Ensuite, elles contribuent à déterminer la gravité de la menace concernée (systèmes et technologies impactés, victimes potentielles, niveau de sophistication de l'acteur concerné). Enfin, elles permettent à l'Autorité de rechercher la qualification des faits concernés au regard du droit pénal, ce qui est le cas échéant nécessaire à l'évaluation du fondement légal sollicité par le CCB (CSIRT National).

c) Dates first seen

26. L'Autorité observe que dans les Demandes adressées aux opérateurs, le CCB (CSIRT National) utilise une autre terminologie s'agissant des dates first seen que celle utilisée dans le cadre de ses demandes adressées à l'Autorité. Les demandes aux opérateurs se réfèrent à une « 'Go back until' datum » définie en note de bas de page comme « *Gegevens die door de operators* ***gedurende 12 maanden*** *worden bewaard op grond van artikelen 122, § 4, 2° en § 4/1 ; en 126/1, § 1 en 2 van de WEC en die door het CCB worden opgevraagd krachtens artikel 127/1, § 2, 2°, 4° en 6°, en § 4 WEC* » (mis en gras par l'Autorité). La Liste de C2S communiquée indique quant à elle, au titre de la colonne dédiée aux dates first seen : « *Go back until date (= First seen date,* ***or max*** *1 year before DPA authorisation date ; whichever was latest)* » (mis en gras par l'Autorité). **L'Autorité considère que ces mentions sont ambigües** (*quid* des métadonnées qui seraient conservées pour des durées inférieures à 12 mois ? – celles-ci sont en principes visées dans les demandes d'autorisations ; « ou maximum » n'indique pas précisément le délai applicable ; il n'est pas non plus exclu que des métadonnées de communications électroniques plus anciennes que 12 mois à compter de l'autorisation délivrée par l'Autorité soient encore légalement conservées selon le droit belge, et celles-ci ne sont *a priori* pas exclues des demandes d'autorisation).

27. Comme l'Autorité l'a souligné dans le considérant n° 47 de son Autorisation n° 002/2026, les délais de conservation des métadonnées dans le cadre des articles 126/1 et 126/3 de la LCE, comptés à partir de la date des communications, varient entre 6 mois, 9 mois, 12 mois et aussi longtemps qu'un certain niveau de menace est fixé par l'Organe de coordination pour l'analyse de la menace, selon des zones géographiques concernées. Un arrêté ministériel – dont ne dispose pas l'Autorité et qui n'est publié que « *par mention* » – consacre en tout état de cause la liste des zones géographiques soumises à l'obligation de conservation des données ainsi que leur durée de conservation, conformément à l'article 126/3, § 6, de la LCE. S'agissant des données visées à l'article 122, § 4, 2°, une durée de conservation de 12 mois est bien prévue, tandis que s'agissant du § 4/1 de ce même article, la durée de conservation prévue est indéterminée et dépend de la pratique des opérateurs (l'Autorité rappelle néanmoins que ces dispositions font actuellement l'objet d'une affaire devant la Cour de justice[6]).

28. Dans ce contexte, l'Autorité réitère les trois points suivants :

    - Dans le considérant n° 48 de son Autorisation n° 002/2026, elle a indiqué ce qui suit : « *Il* ***incombe au CCB (CSIRT National) de veiller à ce que les dates first seen*** *identifiées dans la Note contextuelle communiquée par le CCB (CSIRT National)* ***entrent bien dans les périodes couvertes par l'obligation de conservation des métadonnées précitées, à compter de la date de la présente décision****.* ***A défaut, il conviendra de retenir une date ultérieure (tout en conservant bien entendu également la date first seen***

[6] Voir les considérants nos 21 et s. de l'Autorisation n° 001/2026 et plus récemment, voir Aff. C-661/24, Conclusions de l'Avocat Général M. Szpunar, 3 septembre 2026.

initialement retenue) » (mise en gras et soulignement modifiés dans la présente décision) ;

- En outre, c'est au CCB (CSIRT National) qu'il revient d'identifier les **fondements légaux pertinents** selon les finalités et cas concernés, compte-tenu des dates first seen identifiées. Dès son Autorisation n° 001/2026 (Point n° 6, 1er tiret, du dispositif), l'Autorité a souligné que les métadonnées doivent être « *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)* » (mise en gras dans la présente décision) ;

- Enfin, au considérant n° 50 de son Autorisation n° 002/2026 l'Autorité avait souligné que « *conformément au* ***principe d'accountability*** *(articles 5, 2., et 24 du RGPD), le CCB (CSIRT National) doit être capable de justifier du fondement légal sur la base duquel les métadonnées communiquées effectivement par un opérateur étaient conservées par celui-ci (cette obligation incombe également à l'opérateur concerné qui est responsable du traitement de conservation des métadonnées) – articles 122 et 123, ou articles 126/1 et 127/1 de la LCE* ». Chaque responsable du traitement doit être en mesure de justifier la légalité des traitements de données mis en œuvre sous sa responsabilité : l'un ne peut requérir que des métadonnées licitement conservées, et ce dans certaines hypothèses légalement définies, et l'autre ne peut conserver des métadonnées que dans certains cas légalement définis et n'est obligé de les communiquer que dans ces hypothèses.

29. Autrement dit, **en principe et de manière générale, par adresse IP concernée** :

- Le CCB (CSIRT National) doit clairement déterminer la date de début de la période rétrospective pendant laquelle les communications électroniques échangées sont pertinentes (et dont les métadonnées sont par conséquent requises) dans le cadre du Projet – **la date first seen**. Cette période rétrospective de trafic s'étend de la date first seen à la date d'autorisation délivrée par l'Autorité (ou à la date d'introduction de la demande effectuée directement auprès des opérateurs dans les situations telles que celles en cause dans le cadre du présent contrôle ultérieur) ;

- **Selon les fondements légaux sollicités** (les fondements légaux portent tant sur l'accès revendiqué par le CCB (CSIRT National) que sur la conservation des métadonnées par les opérateurs), le CCB (CSIRT National) doit ensuite vérifier si cette période rétrospective se recoupe intégralement avec la (les) période(s) légale(s) de conservation par les opérateurs des métadonnées demandées. Si tel n'est pas le cas, il doit ajuster la (ou les) période(s)

rétrospective(s) et retenir une (ou plusieurs) date(s) de début plus récente(s), en fonction du fondement légal de la conservation des métadonnées par les opérateurs – **une (ou plusieurs) date(s) ultérieure(s)** à la date first seen.

Pour ce qui concerne les délais de conservation des métadonnées qui sont fixés par les opérateurs eux-mêmes (articles 123 et 122, § 4/1, de la LCE), il appartient au CCB (CSIRT National) de consulter les opérateurs afin d'établir leur pratique. D'ailleurs dès son Autorisation n° 001/2026 (considérant n° 23), l'Autorité avait interrogé le CCB (CSIRT National) à ce sujet. L'Autorité observe encore que les Demandes d'autorisation adressées aux opérateurs contiennent la mention suivante : « *Wij verzoeken u tevens ons (indien dit nog niet is gebeurd) via dezelfde hierboven genoemde kanalen mee te delen op welke wettelijke basis u zich, na een interne juridische beoordeling, baseert om de opslag van elektronische-communicatiemetagegevens te rechtvaardigen, en voor welke periode dit geldt* ».

- La (les) **date(s) retenue(s) et les fondements légaux concernés doivent être clairement communiqués aux opérateurs**. S'agissant de la date par exemple, si au moment « t » de la décision de l'Autorité (ou de la demande adressée aux opérateurs dans le cas d'une situation urgente), les métadonnées requises sont des métadonnées qui ne peuvent et/ou doivent être conservées que pour une durée de 9 mois par les opérateurs en raison du fondement légal de leur conservation, et que la date first seen est « t - 10 mois », la date retenue à l'attention des opérateurs aux fins de la collecte des métadonnées (« 'Go back until' datum » pour reprendre la terminologie du CCB (CSIRT National)) ne pourra pas être plus ancienne que « t - 9 mois ». Car les métadonnées relatives à des communications électroniques ayant eu lieu au-delà de cette date dans le passé ne peuvent plus être conservées au moment « t ». Ce qui en théorie, n'exclut pas que conservées à un autre titre, c'est-à-dire sur la base d'un autre fondement légal de conservation, tout ou partie de celles-ci resteraient disponibles par ailleurs.

30. L'Autorité invite le CCB (CSIRT National) s'il le souhaite, à lui faire part des éventuelles difficultés qu'il rencontrerait le cas échéant en pratique, à cet égard. Ceci notamment compte-tenu du fait que **l'Autorité n'a aucune vue sur la manière concrète, sur les plans technique et organisationnel**, **avec laquelle les opérateurs exécutent leurs obligations** ni sur les possibilités de conserver les métadonnées de communications électroniques.

31. Ainsi **alternativement à ce qui est expliqué au considérant n° 29, dernier tiret**, l'Autorité ne peut pas non plus automatiquement exclure que les opérateurs soient **par exemple** techniquement tout à fait capables d'exécuter correctement leur obligation légale à l'égard du CCB (CSIRT National),

lorsque ce dernier requiert de ceux-ci : qu'ils communiquent en un exemplaire unique[7], l'ensemble des métadonnées requises et visées aux articles 122, § 4, 2°, et § 4/1, et 126/1, §§ 1 et 2, générées par le trafic réalisé à compter de la date first seen communiquée **ou**, selon les communications concernées, à défaut de conservation de métadonnées pour un trafic d'une telle ancienneté[8], qu'ils communiquent les métadonnées générées par le trafic le plus ancien[9] dont la conservation est encore licite à la date de la décision de l'Autorité, et que dans toutes les hypothèses, ils indiquent systématiquement le fondement légal de la conservation des métadonnées communiquées.

II.1.1.3. Absence d'autre commentaire

32. Les vérifications menées par l'Autorité n'appellent pas d'autre commentaire.

II.2. Décision

L'Autorité, dans les limites rappelées aux considérants nos 12-17 de l'Autorisation n° 001/2025 et aux considérants nos 6-7 de l'Autorisation n° 001/2026, en prenant acte que les modifications nécessaires ont été apportées aux procédures internes du CCB (CSIRT National) pour s'aligner entièrement sur les éléments soulevés dans l'Autorisation n° 001/2026 (considérant n° 4 de l'Autorisation n° 002/2026) et sur les éléments soulevés dans l'Autorisation n° 002/2026 (considérant n° 3 de l'Autorisation n° 003/2026), décide que

1. Le CCB (CSIRT National) 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 CCB (CSIRT National), par l'Autorité, faisant foi), 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 ; considérants nos 2-4 de l'Autorisation n° 001/2026) ;

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'aux Autorisations nos 001/2025, 001/2026, 002/2026 et 03/2026, pour autant qu'elles restent motivées de manière circonstanciée pour le surplus.

---

[7] C'est-à-dire que les métadonnées relatives à une même communication électronique ne sont communiquées qu'en un seul exemplaire.

[8] Ce qui implique qu'entre-temps, les métadonnées alors conservées par les opérateurs ont dû être supprimées et ne sont plus disponibles au moment de la décision de l'Autorité.

[9] Mais plus récent par rapport à la date first seen.

L'Autorité est favorable à la démarche suivie par le CCB (CSIRT National) consistant à lui soumettre, dans la mesure du possible, 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 CCB (CSIRT National) à l'avenir qu'il identifie clairement les considérants de ses décisions d'autorisation (ou de contrôle ultérieur) 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 de l'Autorisation n° 001/2026).

Doivent être jointes à toute demande de contrôle ultérieur les demandes qui ont été adressées aux opérateurs concernés (**considérant n° 3**).

Dans le cadre de la présente demande de contrôle ultérieur, la situation décrite par le CCB (CSIRT National) constitue bien un cas de situation urgente dûment justifiée, de telle sorte que le CCB (CSIRT National) était en droit d'adresser directement ses demandes aux opérateurs et de solliciter ensuite un contrôle ultérieur par l'Autorité (**considérants nos 4-6**).

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 de l'Autorisation n° 001/2025 ; considérants nos 29-31 de l'Autorisation n° 001/2026) ;

4. 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) ;

5. 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 contextuelle et à la Liste de C2S) que si les quatre conditions suivantes sont remplies (considérants nos 19-28 de l'Autorisation n° 001/2026 ; considérants nos 23-39 et 46-50 de l'Autorisation n° 002/2026) :

- 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 (**considérants nos 26-31**) ;

- Les métadonnées sont conservées légalement par les opérateurs concernés, conformément aux articles 122 et 123 ou 126/1 de la LCE, en fonction du fondement légal de la demande ;

- Le CCB (CSIRT National) 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 CCB (CSIRT National), 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 CCB (CSIRT National).

- Lorsque sont concernées des données conservées conformément à l'article 126/1 de la LCE, pour chaque adresse IP concernée, le CCB (CSIRT National) doit indiquer dans sa demande, selon le fondement légal sollicité, la menace grave pour la sécurité publique qui est concernée (articles 126/1, § 1er, al. 3, et 127/1, 2°, de la LCE, et article 21, § 2, 2°, de la Loi NIS2) ou le fait relevant de la criminalité grave concerné (articles 126/1, § 1er, al. 3, et 127/1, 6°, de la LCE, et article 21, § 2, 1°, de la Loi NIS2), et la relation entre ceux-ci et l'adresse IP concernée. Dans ce contexte, une attention particulière doit être réservée à la description de l'acteur (ou du moyen) de la cybermenace concernée ;

  Dans le cadre de la présente Demande, les ▮ adresses IP concernées sont liées à une menace grave pour la sécurité publique, les articles 126/1, § 1er, al. 3, et 127/1, 2°, de la LCE, et article 21, § 2, 2°, de la Loi NIS2 sont applicables, et l'indication de cette menace doit être adaptée dans la Note contextuelle (**considérants nos 12-16**).

6. 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 CCB (CSIRT National) 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 de l'Autorisation n° 001/2026) ;

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

8. La collecte auprès de sources d'identification des adresses IP listées par le CCB (CSIRT National) 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 CCB (CSIRT National) dans le cadre de l'Autorisation n° 001/2025 et de l'Autorisation n° 001/2026 (considérants nos 48-52 de l'Autorisation n° 001/2026), ainsi que le cas échéant, toute autre mesure supplémentaire qu'exigerait l'état de la technique en la matière. Enfin, le CCB (CSIRT National) 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).

L'Autorité prend acte de la bonne pratique mise en œuvre par le CCB (CSIRT National) consistant à faire analyser et vérifier par au moins deux analyses les informations communiquées par ses partenaires externes. Elle prend également acte du fait que [redacted] (considérant n° 40 de l'Autorisation n° 002/2026).

En l'occurrence, la Demande de contrôle ultérieur devait indiquer que le [redacted] La Note contextuelle doit être adaptée en ce sens (**considérants nos 21-23**) ;

9. 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 40-42 de l'Autorisation n° 002/2026), 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 de l'Autorisation n° 001/2026) ;

10. 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) ;

11. 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 de l'Autorisation n° 001/2026 ; voir également les **considérants nos 17-19**) ;

12. 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 de l'Autorisation n° 001/2026 ; voir également les **considérants nos 17-19**) ;

13. 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. ; soit, selon le fondement légal de sa demande, la menace grave pour la sécurité publique concernée ou le fait relevant de la criminalité grave concerné) 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 de l'Autorisation n° 001/2026) ;

14. Chaque demande d'autorisation dans le cadre du Projet, ainsi que chaque demande de contrôle ultérieur en cas d'urgence, doit continuer d'être accompagnée d'une note contextuelle détaillée selon les adresses IP concernées et les acteurs/moyens de la menace concernés, structurée de la même manière que la Note contextuelle communiquée dans le cadre de la Demande adressée à l'Autorité dans le contexte de l'Autorisation n° 002/2026, le cas échéant précisée à l'aune des considérations développées dans les considérants nos 23-39 de l'Autorisation n° 002/2026. Une telle note doit également indiquer [redacted] ; 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 ; considérant n° 42 de l'Autorisation n° 002/2026).

L'Autorité accueille très favorablement les améliorations et le renforcement apportés par le CCB (CSIRT National) à la Note contextuelle communiquée avec la Demande, bien que certains points doivent encore retenir l'attention du CCB (CSIRT National) (considérants n° 8 et 11-12 de l'Autorisation n° 003/2026). L'Autorité souligne que plus l'information contextuelle pertinente est détaillée, moins il y a de chance que celle-ci s'interroge sur les éléments ayant conduit à la sélection de l'une ou l'autre adresse IP.

Lorsqu'une demande d'autorisation ou de contrôle ultérieur concerne des adresses IP identifiées dans le cadre d'une attaque informatique, l'Autorité attend du CCB (CSIRT National) qu'il identifie précisément (même si cela est succinct) dans sa demande, sur la base des informations dont il dispose à ce moment, les étapes de cette attaque informatique (**considérants nos 24-25**) ;

15. 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 l'Autorisation n° 001/2026 sont communiquées à titre purement indicatif (considérants nos 65-68 de l'Autorisation n° 001/2026) ;

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 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 l'Autorisation n° 001/2026 sont communiquées à titre purement indicatif (considérants nos 32-37 de l'Autorisation n° 001/2026) ;

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 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 CCB (CSIRT National) (dans le cadre de l'Autorisation n° 001/2026) afin d'identifier des « [redacted] », « [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 de l'Autorisation n° 001/2026) ;

18. Dans les conditions et limites visées ci-avant et dans la présente décision, conformément aux articles 122, 123, 127/1, § 2, 2°, et 126/1, § 1er, al. 3 de la LCE, et, et 21, §§ 2, 2°, et 4, de la Loi NIS2, l'Autorité confirme la validité des demandes adressées à Belnet, Proximus et Telenet, par le CCB agissant en tant que CSIRT National et de solliciter ensuite un contrôle ultérieur par l'Autorité. Ce dernier était en droit de collecter 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 [redacted] adresses IP dédiées à des C2-servers contextualisées dans la Note contextuelle et reprises dans l'Annexe 1 ci-après, 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 ;

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

SENSIBLE NON CLASSIFIE (AR 20.12.2024)

Annexe 1 : liste d'adresses IP dédiées à des C2-servers

