Autorité de protection des données
Gegevensbeschermingsautoriteit

(Verleende) machtiging nr. 001/2025 van 18 juli 2025

Betreft: machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid: "Command-and-Control servers communicatiemetadata – waarschuwing" (AH-2025-0034)

De Autorisatie- en Adviesdienst van de Gegevensbeschermingsautoriteit (hierna "de Autoriteit");

Gelet op de wet van 3 december 2017 *tot oprichting van de Gegevensbeschermingsautoriteit* (hierna "de WOG");

Gelet op artikel 21, § 4, van de wet van 26 april 2024 *tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid* (hierna "de NIS2-wet");

Gelet op de wet van 13 juni 2005 *betreffende de elektronische communicatie* (hierna "de WEC");

Gelet op Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 *betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG* (hierna "de AVG");

Gelet op de wet van 30 juli 2018 *betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens* (hierna "de WVG");

Gelet op de artikelen 44, 54 en 55 van het Reglement van interne orde van de Gegevensbeschermingsautoriteit (hierna "het RIO");

Gelet op de machtigingsaanvraag van de directeur-generaal van het Centrum voor Cybersecurity België, de heer Miguel De Bruycker (hierna "de aanvrager"), ontvangen op 23 mei 2025;

Gelet op de verzoeken om aanvullende informatie die op 28 mei 2025 en 3 juni 2025 aan het Centrum voor Cybersecurity België zijn gericht;

Gelet op de documenten en antwoorden die op 20 juni 2025 door het Centrum voor Cybersecurity België zijn verstrekt;

Gelet op het verzoek om aanvullende informatie dat op 24 juni 2025 aan het Centrum voor Cybersecurity België is gericht;

Gelet op de documenten en antwoorden die op 8 juli 2025 door het Centrum voor Cybersecurity België zijn verstrekt, met inbegrip van een aangepaste lijst van IP-adressen waaraan een aanvullende technische nota is toegevoegd;

Gelet op het verzoek om aanvullende informatie dat op 11 juli 2025 aan het Centrum voor Cybersecurity België is gericht en het antwoord dat op 14 juli 2025 is verstrekt;

Gelet op de bevestiging van de volledigheid van het dossier die op 16 juli 2025 aan de aanvrager is verzonden;

Gelet op het feit dat het dossier in het Directiecomité van de Autoriteit aan de orde is gesteld en vervolgens is besproken op 17 juli 2025;

Neemt op 18 juli 2025 de volgende beslissing:

I. Voorwerp en context van de machtigingsaanvraag

1. De aanvrager heeft bij de Autoriteit een machtigingsaanvraag zoals bedoeld in artikel 21, § 4, van de NIS2-wet ingediend (hierna "**de aanvraag**"). Deze bepaling, die moet worden gelezen in samenhang met artikel 23, § 3, van de WOG[1], voorziet in een specifieke bevoegdheid in het kader waarvan de

[1] "*§ 3. In het kader van de toepassing van de wet van 13 juni 2005 betreffende de elektronische communicatie en van bijzondere wetgeving, en onverminderd de bevoegdheden van de toezichthoudende autoriteiten bedoeld in titel 2 en titel 3 van de wet van 31 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens en van de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten, opgericht bij artikel 43/1 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten verleent de autorisatie- en adviesdienst machtigingen voor toegang tot metadata betreffende communicatie met betrekking tot verkeer of locatie voor de bevoegde instellingen, voor doeleinden die niet vallen binnen het kader van:*

- de uitoefening van de taken van preventie, onderzoek, opsporing of vervolging van een feit dat een strafrechtelijke inbreuk vormt, of;

- het zoeken naar vermiste personen, of;

- de nationale veiligheid.

Om volledig te zijn bevat de machtigingsaanvraag de volgende elementen:

Autoriteit al dan niet een machtiging verleent aan het Centrum voor Cybersecurity België (hierna "**het CCB**") voor toegang tot metagegevens van elektronische communicatie die door de telecommunicatieoperatoren worden verwerkt[2].

2. Artikel 21, § 2, van de NIS2-wet bepaalt het volgende:

> "*Indien dat **strikt noodzakelijk** is voor de uitvoering van zijn taken opgesomd in **artikel 19, § 1, 1° tot 5°**, kan het **nationale CSIRT** identificatiegegevens bedoeld in artikel 2, eerste lid, 5°, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector of elektronische-communicatiemetagegevens bedoeld in artikel 2, 93°, van de wet van 13 juni 2005 verkrijgen van een operator in de zin van artikel 2, 11°, van de voormelde wet van 13 juni 2005, die deze gegevens bewaart.*
>
> *Zonder afbreuk te doen aan of zich in te mengen in de bevoegdheden van personen die de gerechtelijke politie uitoefenen en de gerechtelijke autoriteiten, **worden met voornoemde taken de volgende doeleinden nagestreefd**:*
>
> *1° zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten;*
>
> *2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid;*
>
> *3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen.*
>
> *Het nationale CSIRT kan bepalen binnen welke termijn de operator op zijn verzoek moet reageren, naargelang de dringendheid hiervan.*" (in vet aangeduid door de Autoriteit)

1° de identificatie van de verzoekende instelling;

2° de rechtsgrondslag die deze instelling toelaat om bij de operatoren metagegevens van communicatie op te vragen die verband houden met het verkeer of de locatie;

3° de uitoefening van de opdracht, waarvan de doeleinden niet behoren tot een van de aangelegenheden opgesomd in het eerste lid, eerste tot derde streepje, die de noodzakelijkheid; en de evenredigheid van het verzoek rechtvaardigt;

4° in voorkomend geval, de reden voor de dringende of uiterst dringende noodzaak;

5° de handtekening van de persoon die de verzoekende instelling kan verbinden.

Wanneer het verzoek om machtiging volledig is, wordt het besluit van de Gegevensbeschermingsautoriteit uiterlijk binnen tien werkdagen, te verstaan als alle andere dagen dan zaterdagen, zondagen en wettelijke feestdagen, meegedeeld. De beslissing van de Gegevensbeschermingsautoriteit wordt met redenen omkleed."

[2] Volgens artikel 2, 11°, van de WEC is een operator een "*persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst aanbiedt*".

3. Het CCB treedt met name op **als nationaal CSIRT**[3], en artikel 19, § 1, 1° tot en met 4° (5° is niet relevant in het kader van deze aanvraag), van de NIS2-wet wijst de volgende taken toe aan het nationale CSIRT:

> "*1° het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen;*
>
> *2° het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk;*
>
> *3° het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing;*
>
> *4° het verzamelen en analyseren van forensische gegevens en het zorgen voor dynamische risico- en incidentenanalyse en situationeel bewustzijn met betrekking tot cyberbeveiliging;*
>
> *5° op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen*".

4. De aanvraag heeft betrekking op een project met de titel "*Command-and-Control servers communicatiemetadata – waarschuwing*" (hierna "**het project**"). Het doel van het CCB bestaat erin metagegevens van elektronische communicatie te kunnen verzamelen die betrekking hebben op (potentiële) slachtoffers van kwaadaardige activiteiten van "*command-and-control servers*" (hierna "**C2-servers**")[4], die vooraf werden geïdentificeerd op basis van bronnen waarover het CCB beschikt (incidentmeldingen, meldingen of waarschuwingen van buitenlandse tegenhangers of van betrouwbare particuliere partners, enz.). Het gaat erom een samenwerkingskader op te zetten met de betrokken operatoren, zodat op basis van het verkeer van en naar deze C2-servers kan worden vastgesteld welke Belgische (potentiële) slachtoffers betrokken zijn, waarbij het vervolgens aan het CCB is om contact op te nemen met deze slachtoffers nadat bij de betrokken operatoren een verzoek tot identificatie is ingediend[5]. Meer concreet zou de betrokken operator, zodra hij over de IP-adressen beschikt die aan de C2-servers zijn toegewezen, belast worden met de verzameling van de metagegevens van de elektronische communicatie die via zijn netwerk van en naar deze adressen verloopt, en met de mededeling ervan aan het CCB (nationaal CSIRT). Op basis van de analyse van deze metagegevens

---

[3] Zie artikel 16, tweede lid, van de NIS2-wet en artikel 3, § 1, van het koninklijk besluit van 9 juni 2024 *tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*.

[4] Zie in dit verband met name het antwoord van de aanvrager in overweging nr. 26.

[5] De machtigingsaanvraag heeft geen betrekking op dit deel van het door de aanvrager beoogde proces.

zou het CCB (nationaal CSIRT) vervolgens de IP-adressen identificeren van potentiële slachtoffers van deze C2-servers. Aan de hand van deze IP-adressen zou het CCB (nationaal CSIRT) bij de betrokken operatoren verzoeken indienen tot identificatie van de houders ervan (identiteit en contactgegevens), teneinde met hen contact op te nemen. Tot slot zou het CCB deze personen informeren, zodat zij zich kunnen beschermen tegen de betrokken dreiging.

5. De aanvrager heeft bij zijn aanvraag met name een toelichtende nota bijgevoegd over het project en de procedure die zou worden ingevoerd (hierna "**de nota**"). Op verzoek van de Autoriteit heeft hij later ook het advies van zijn DPO (hierna "**het advies van de DPO**"), de effectbeoordeling van het project (hierna "**de GEB**") en een aanvullende nota over elk van de IP-adressen die in de oorspronkelijk bij de Autoriteit ingediende aanvraag waren vermeld (hierna "**de aanvullende nota**"), verstrekt.

II. Onderzoek

De onderhavige beslissing is als volgt opgebouwd en bevat een bijlage:

II.1 Voorafgaande kwestie: publicatie van door de Autoriteit verleende machtigingen

6. De Autoriteit herinnert eraan dat haar beslissingen over machtigingsaanvragen overeenkomstig artikel 44 van het RIO **op haar website moeten worden gepubliceerd**. Bovendien moeten zij worden gemotiveerd op basis van de betrokken feiten en de door de aanvrager verstrekte informatie[6]. Bijgevolg worden deze elementen via het internet toegankelijk voor het publiek, voor zover de beslissing van de Autoriteit ernaar verwijst.

7. Het **doel** van deze publicatie is **tweeledig**: enerzijds heeft het betrekking op de **doelstellingen van administratieve transparantie**, en anderzijds op de **bescherming van personen met betrekking tot de verwerking van persoonsgegevens**. Wat administratieve transparantie betreft, gaat het erom een doeltreffende externe controle op het optreden van de Autoriteit mogelijk te maken, de eerbiediging van de rechtsstaat te waarborgen, het vertrouwen van de burger in de Autoriteit te versterken en de efficiëntie en doeltreffendheid van de Autoriteit te versterken[7]. Wat gegevensbescherming betreft, is het doel om transparantie te waarborgen met betrekking tot de door de Autoriteit toegestane gegevensverwerkingen, en, in verband met het doel van administratieve transparantie, om de betwistbaarheid van de beslissingen van de Autoriteit tot verlening (of weigering) van een machtiging te waarborgen[8].

[redacted]

9. De Autoriteit heeft de aanvrager vooreerst gevraagd of zij de verstrekte informatie mag publiceren[9]. Hij antwoordde met name het volgende (vrije vertaling):

---

[6] Zie overweging nr. 21.

[7] Op deze manier heeft de Autoriteit het doel van artikel 32 van de Grondwet verwoord (zie advies nr. 42/2023 van 9 februari 2023 *met betrekking tot een voorontwerp van wet tot wijziging van de wet van 11 april 1994 betreffende de openbaarheid van bestuur (CO-A-2022-311)*, overweging nr. 15).

[8] Er dient te worden benadrukt dat de wetgever niet in een specifiek rechtsmiddel heeft voorzien tegen de beslissing van de Autoriteit tot verlening of weigering van een machtiging. De Autoriteit gaat er in dit verband van uit dat ter zake beroep kan worden ingesteld bij de Raad van State.

[9] Meer bepaald heeft zij de aandacht van de aanvrager gevestigd op de noodzaak voor haar om de informatie met betrekking tot het voorgenomen project te publiceren in het kader van haar analyse en de motivering daarvan, en heeft zij hem enerzijds ondervraagd over de wettelijke draagwijdte van de toegepaste indeling, en anderzijds over de mogelijkheid voor de Autoriteit om in haar beslissing over de machtigingsaanvraag alle of een deel van de elementen uit deze nota en uit de antwoorden die

"*Overeenkomstig* ***artikel 26, § 3****, van de* […**NIS2-wet**] *zijn de bevoegde autoriteiten in het kader van de NIS2-wet (waaronder het CCB – als nationale cyberbeveiligingsautoriteit en nationaal CSIRT)* ***verplicht om de toegang tot de informatie die voortvloeit uit de NIS2-wet te beperken tot de personen die ervan op de hoogte moeten zijn en er toegang toe moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van diezelfde wet, teneinde de belangen in verband met de openbare veiligheid te beschermen****.*

[…]

[redacted]

[redacted]

[redacted]

[redacted]

11. Dit gezegd zijnde, neemt de Autoriteit akte van de uitleg van de aanvrager. **Het is aan hem om <u>binnen 10 werkdagen</u> vanaf de kennisgeving van deze beslissing** (de datum van verzending van de e-mail van de Autoriteit aan de aanvrager geldt als bewijs) **duidelijk aan te geven welke passages van de beslissing van de Autoriteit volgens hem niet mogen worden gepubliceerd om de door hem aangevoerde en hierboven genoemde redenen[10]**. De Autoriteit benadrukt dat deze vereiste, net als haar andere aanbevelingen, **een voorwaarde vormt voor de verleende machtiging**.

<u>II.2. Reikwijdte van de machtigingsbevoegdheid van de Autoriteit en van de aanvraag</u>

<u>II.2.1. Beginselen betreffende de machtigingsbevoegdheid van de Autoriteit</u>

12. Bij wijze van inleiding herinnert de Autoriteit aan de **ernstige bedenkingen** die zij reeds heeft geuit **met betrekking tot de toekenning aan haar van een machtigingsbevoegdheid** op het gebied van de verwerking van metagegevens van elektronische communicatie[11]. Zij verwijst hierbij in het

door de aanvrager werden verstrekt op de aan hem gestelde vragen te publiceren (waarbij het aan de aanvrager staat om te bepalen welke door hem meegedeelde informatie niet mag worden gepubliceerd en op welke wettelijke basis dit steunt).

[10] De aanvrager zal de betrokken passages met een kleur naar keuze markeren.

[11] Zie overweging nr. 68 e.v. van het advies nr. 32/2022 van 16 februari 2022 *over de artikelen 7, 25, 1° en 47 van het ontwerp van wet houdende diverse bepalingen inzake Economie (CO-A-2021-280, CO-A-2021-281 en CO-A-2021-283)*. Zie ook overweging nr. 59 e.v. van de bijlage bij het advies van het Directiecomité van de GBA van 25 februari 2022 *inzake een*

bijzonder naar de **overwegingen nrs. 58-72 van haar advies nr. 32/2022** van 16 februari 2022 *over de artikelen 7, 25, 1° en 47 van het ontwerp van wet houdende diverse bepalingen inzake Economie (CO-A-2021-280, CO-A-2021-281 en CO-A-2021-283)*. Hoewel het project aanzienlijk verschilt van de hypothese waarop de Autoriteit doelde in overweging nr. 67 van dat advies[12], vestigt de Autoriteit de aandacht van de aanvrager op het belang om grondiger te onderzoeken of voor een project zoals het onderhavige geen normatief kader voor dit type gegevensverwerkingen door het CCB (nationaal CSIRT) zou kunnen worden ingevoerd via een aanpassing van de NIS2-wet (en een verdere uitwerking ervan in een koninklijk uitvoeringsbesluit). Dat kader zou met name in specifieke passende waarborgen kunnen voorzien, met name op het vlak van transparantie, en zou de voorafgaande controle door de Autoriteit overbodig maken (in het bijzonder wanneer het gaat om verkeer dat essentiële of belangrijke entiteiten betreft). De Autoriteit erkent echter dat dit laatste punt verdere reflectie vergt, wat niet kan worden gerealiseerd binnen het kader van deze aanvraag.

13. Bovendien wijst zij erop dat **haar niet-exhaustieve controle** uitsluitend gebaseerd is op de door de aanvrager verstrekte documenten en informatie. **Deze controle houdt <u>geen</u> beoordeling in van de overeenstemming van de beoogde gegevensverwerkingen met de AVG en de bepalingen van het Belgisch recht die van toepassing zijn op de verwerking van persoonsgegevens.** Met andere woorden, de afgifte van een machtiging kan niet worden geïnterpreteerd als een waarborg voor de naleving van al deze regels.

14. Anderzijds wijst de Autoriteit "*er* [met name] *op dat elke inmenging in het recht op bescherming van persoonsgegevens, vooral als het gaat om een ernstige inmenging zoals in deze, slechts toelaatbaar is* ***als ze wordt omkaderd door een voldoende duidelijke en nauwkeurige norm waarvan de toepassing voor de betrokken personen voorzienbaar is****. Elke norm die de verwerking van persoonsgegevens omkadert, in het bijzonder wanneer die verwerking een ernstige inmenging vormt in de rechten en vrijheden van de betrokken personen, moet voldoen aan* ***de eisen van voorzienbaarheid en nauwkeurigheid*** *zodat* ***de betrokken personen*** *bij het lezen van de norm*

voorontwerp van wet tot wijziging van de wet van 3 december 2017 tot oprichting van de Gegevensbeschermingsautoriteit (AH-2022-0020), beschikbaar op

https://www.gegevensbeschermingsautoriteit.be/publications/advies-inzake-een-voorontwerp-van-wet-tot-wijziging-van-de-wet-van-3-december-2017-tot-oprichting-van-de-gegevensbeschermingsautoriteit.pdf, laatst geraadpleegd op 02/06/2025.

[12] "*Voor de opdrachten van het BIPT en het CCB die geen dwangbesluit impliceren ten aanzien van betrokkenen en die geen massale verzameling van metagegevens van elektronische communicatie impliceren, komt het daarentegen toe aan de wetgever om deze toegang passend te regelen door die te beperken tot geanonimiseerde gegevens, of ook gepseudonimiseerde gegevens, en daarbij het gebruik van de pseudonimiseringssleutel te beveiligen en te voorzien in alle andere passende maatregelen, liever dan te voorzien in een systeem van voorafgaande toestemming.*" (vetgedrukte opmaak werd in dit advies niet behouden)

Zie ook, *Parl. St.*, Kamer van volksvertegenwoordigers, nr. 55-2572/001, pp. 171-172, en meer in het bijzonder nr. 55-2572/002, pp. 127-128, waarin de wetgever uiteenzet waarom hij de door de Autoriteit voorgestelde aanpak (namelijk afzien van een systeem van voorafgaande toestemming) niet volgt.

Het project daarentegen houdt regelmatige en voortdurende verzamelingen in van niet-gepseudonimiseerde of niet-geanonimiseerde metagegevens van elektronische communicatie, verbonden aan het verkeer dat via IP-adressen loopt die zijn toegewezen aan C2-servers en waarbij essentiële of belangrijke entiteiten betrokken zijn, onverminderd het debat over de verzameling van metagegevens van elektronische communicatie met betrekking tot verkeer naar andere potentiële slachtoffers (rechtspersonen of natuurlijke personen die niet onder de verplichtingen van de NIS2-wet vallen).

duidelijk zien aan welke verwerkingen hun gegevens worden onderworpen en in welke omstandigheden een gegevensverwerking is toegelaten*. In uitvoering van artikel 6.3 van de AVG, gecombineerd met de artikelen 22 van de Grondwet en 8 van het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden, moeten de* ***essentiële factoren van de verwerking*** *er* ***nauwkeurig*** *in worden* ***beschreven****. Het betreft in het bijzonder het of de precieze* ***doeleinde(n)*** *van de verwerking; de* ***identiteit van de verwerkingsverantwoordelijke(n)****; de* ***categorieën van verwerkte gegevens****, met dien verstande dat ze - in overeenstemming met artikel 5.1. van de AVG, "ter zake dienend, relevant en beperkt tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt" moeten zijn; de* ***categorieën van betrokken personen*** *(personen van wie de gegevens worden verwerkt); de* ***bewaringstermijn van de gegevens****; de ontvangers of* ***categorieën van ontvangers*** *waaraan hun gegevens worden meegedeeld en de* ***omstandigheden waarin en de redenen waarvoor ze worden meegedeeld*** *en* ***alle maatregelen om een rechtmatige en behoorlijke verwerking van deze persoonsgegevens te garanderen****."* (vetgedrukt in de originele tekst)[13]

15. In dit verband herinnert artikel 54, § 3, van het RIO[14] aan deze beginselen met betrekking tot de machtigingsbevoegdheid van de Autoriteit.

16. Deze **standpunten en beginselen werden ook herhaald in het kader van de eerste machtiging die door de Autoriteit werd afgegeven**, namelijk (verleende) machtiging nr. 001/2024 van 6 november 2024 *betreffende een machtigingsaanvraag zoals bedoeld in artikel 15, § 2, tweede lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (AH-2024-0010)*[15].

17. Tot slot benadrukt de Autoriteit dat **artikel 21, § 1, van de NIS2-wet** het volgende bepaalt: "*In het kader van de uitoefening van zijn bevoegdheden neemt het nationale CSIRT alle passende maatregelen*

---

[13] Advies van de Autoriteit nr. 108/2021 van 28 juni 2021 *over een voorontwerp van wet betreffende het verzamelen en het bewaren van de identificatie-, verkeers- en locatiegegevens in de sector van de elektronische communicatie en de toegang daartoe voor de autoriteiten en over een ontwerp van koninklijk besluit tot wijziging van het koninklijk besluit van 19 september 2013 tot uitvoering van artikel 126 van de wet van 13 juni 2005 betreffende de elektronische communicatie (CO-A-2021-099)*, overweging nr. 27.

[14] Hierin staat het volgende:

"*In overeenstemming met de beginselen van voorspelbaarheid en rechtmatigheid die zijn vastgelegd in artikel 22 van de Grondwet, kan de GBA niet in de plaats treden van de wetgever en de essentiële elementen bepalen van de verwerking van persoonsgegevens waarvoor machtiging wordt gevraagd.*

In het kader van zijn bevoegdheid om machtiging te verlenen als bedoeld in de paragrafen 1 en 2, en op basis van de door de aanvrager verstrekte informatie, eventueel naar aanleiding van een verzoek om aanvullende informatie van de dienst, verifieert de dienst of de elementen van de gevraagde gegevensverwerking gebaseerd zijn op en voldoen aan de normatieve bepaling(en) van wettelijke rangorde waarin zij worden vastgesteld.

De dienst verifieert ook, voor zover mogelijk en op dezelfde basis, of de voorwaarden van het voor machtiging ingediende voorstel van gegevensverwerking voldoen aan de beginselen van noodzakelijkheid en evenredigheid ten aanzien van de bescherming van het recht op bescherming van de persoonlijke levenssfeer en het recht op bescherming van persoonsgegevens."

[15] Beschikbaar (in het Frans) op https://www.autoriteprotectiondonnees.be/publications/autorisation-n0-001-2024-du-6-novembre-2024.pdf, laatst geraadpleegd op 02/06/2025.

om de in de artikel en 19 en 20 bepaalde doelstellingen te verwezenlijken. Deze maatregelen moeten ***evenredig*** *zijn met die doelstellingen, en* ***in overeenstemming met de beginselen van objectiviteit, transparantie en non-discriminatie****.*" (in vet aangeduid door de Autoriteit)

II.2.2. Reikwijdte van de machtigingsaanvraag

18. In wezen verzoekt de aanvrager de Autoriteit om haar door de wetgever **toegekende machtigingsbevoegdheid** te **modaliseren** door een **algemene machtiging** af te geven met betrekking tot zijn project voor de **continue verwerking** van metagegevens van elektronische communicatie[16]. Door het project in het algemeen toe te staan, zou de Autoriteit in de praktijk de mogelijkheid behouden om in het kader van de uitvoering ervan per geval tussen te komen, na ontvangst van regelmatige updates van de lijst met aan C2-servers toegewezen IP-adressen die aan de operatoren worden meegedeeld. Zij zou aanvullende informatie kunnen opvragen bij het CCB (nationaal CSIRT) en, indien nodig, een of meer IP-adressen uit de betreffende update van deze lijst kunnen verwijderen. De operatoren zouden dan de betrokken metagegevens van elektronische communicatie die tot dan toe waren verzameld, moeten verwijderen[17]. Het CCB (nationaal CSIRT) zou op zijn beurt ook de gegevens moeten verwijderen die het inmiddels heeft ontvangen (afhankelijk van de reactiesnelheid van de Autoriteit kan het CCB (nationaal CSIRT) inmiddels al dan niet metagegevens hebben ontvangen die door de operator zijn verzameld).

19. De Autoriteit is van mening dat **deze benadering niet kan worden gevolgd**. **De wetgever heeft de Autoriteit** immers **niet de bevoegdheid gegeven om de** continue **mededeling** van metagegevens van elektronische communicatie door de operatoren op verzoek van het CCB (nationaal CSIRT) **te reglementeren** door middel van een **algemene machtiging** die met name de toepasselijke voorwaarden vaststelt en de mogelijkheden voor de Autoriteit bepaalt **om gericht en *a posteriori* in te grijpen** in deze gegevensstroom[18]. En als de wetgever een dergelijke bevoegdheid

[16] Uit de meegedeelde nota blijkt met name het volgende:

[redacted]

[18] De door de wetgever vastgestelde termijn voor het verlenen van de betrokken machtiging bevestigt deze benadering. Als de **uiterst korte machtigingstermijn** – rekening houdend met het feit dat deze per definitie niet gericht is op dringende gevallen (in geval van dringendheid kan de aanvrager de machtiging van de Autoriteit overslaan, waarna de Autoriteit achteraf een controle moet uitvoeren) –, **zoals vastgelegd door de wetgever** (tien dagen – exclusief zaterdagen, zondagen en feestdagen, te rekenen vanaf de volledigheid van het dossier), al moeilijk te verenigen is met de uitvoering van een effectieve voorafgaande controle door de Autoriteit van een concreet verzoek om toegang tot metagegevens van elektronische communicatie, **dan is die termijn des te minder geschikt voor een situatie waarin de Autoriteit een algemeen kader voor toegang tot metagegevens zou moeten uitwerken**.

Ter vergelijking: in het verleden beschikte de Autoriteit over een termijn van twee maanden om zich uit te spreken over normatieve teksten. Opmerking: tegenwoordig kunnen aanvragers van een advies verzoeken dat dit advies binnen een termijn van één maand na de volledigheid van het dossier wordt uitgebracht (dit gebeurt evenwel onverminderd het standpunt van de Autoriteit over de gepastheid van die termijn).

aan de Autoriteit had willen toekennen, had dit niet gekund zonder het risico het Belgisch grondwettelijk recht te schenden[19]. Overeenkomstig artikel 21, § 4, van de NIS2-wet en **artikel 23, § 3, van de WOG** moet het voorwerp van de voorafgaande machtiging door de Autoriteit dan ook "***een verzoek om*** *elektronische-communicatie****metagegevens***" zijn (in vet aangeduid en onderstreept door de Autoriteit) dat door het CCB (nationaal CSIRT) aan een operator zal worden gericht, en dit overeenkomstig de rechtspraak van het Hof van Justitie ter zake.

20. **De controle door de Autoriteit, zoals bedoeld in artikel 21, § 4, van de NIS2-wet en artikel 23, § 3, van de WOG**, is duidelijk en expliciet een **voorafgaande** controle, behalve in dringende gevallen. **De Autoriteit alleen toestaan te reageren op een verzoek om toegang dat reeds aan de operatoren is meegedeeld en dus op een reeds gestarte verwerking (de metagegevens worden verzameld door de operator en ook meegedeeld aan het CCB (nationaal CSIRT))**, zou neerkomen op het instellen van een **latere controle die in strijd is met de bovengenoemde bepalingen**. Zoals het Hof van Justitie reeds heeft verklaard: "[...] *de onafhankelijke toetsing die artikel 15, lid 1, van richtlijn 2002/58 vereist,* [moet] ***voorafgaand aan elke toegang tot de betrokken gegevens*** *plaatsvinden,* ***behalve in naar behoren gemotiveerde urgente gevallen****, waarin de toetsing op korte termijn dient plaats te vinden. Met een latere toetsing kan immers niet worden tegemoetgekomen aan het doel van een voorafgaande toetsing, dat erin bestaat te verhinderen dat tot de betrokken gegevens een toegang wordt verleend die verder gaat dan strikt noodzakelijk is.*"[20] (in vet aangeduid en onderstreept door de Autoriteit)

21. Bij wijze van conclusie **moet elk verzoek** tot mededeling van metagegevens van elektronische communicatie **vooraf ter goedkeuring worden voorgelegd aan de Autoriteit**, **voordat** het aan een operator kan worden gericht. Het is vervolgens aan de Autoriteit om een **met redenen omklede beslissing** te nemen[21].

22. Dit gezegd zijnde, is het ten eerste niet uitgesloten dat, wanneer de juridische en feitelijke context van daaropvolgende aanvragen identiek is aan die van een eerste aanvraag, **deze daaropvolgende aanvragen verwijzen naar de juridische en feitelijke context van de eerste aanvraag zoals uiteengezet in de bij die gelegenheid verleende machtiging**, voor zover deze daaropvolgende

---

[19] In dit verband verwijst de Autoriteit *mutatis mutandis* naar het standpunt dat zij met name op basis van de rechtspraak van het Grondwettelijk Hof en de adviespraktijk van de Raad van State heeft ingenomen met betrekking tot het Informatieveiligheidscomité in de overwegingen nrs. 19-23 van haar advies nr. 268/2022 van 21 december 2022 *over een voorontwerp van wet betreffende maatregelen van bestuurlijke politie inzake reisbeperkingen en het Passagier Lokalisatie Formulier en houdende wijzigingen van diverse wetsbepalingen betreffende het Informatieveiligheidscomité (CO-A-2022-299)*. Zie met name ook advies nr. 69.166/4 van de Raad van State van 10 juni 2021 *over een voorontwerp van wet 'houdende omzetting van het Europees wetboek voor elektronische communicatie en wijziging van diverse bepalingen inzake elektronische communicatie'*, in het bijzonder punt 2.3.1. Het Europees recht legt in dit geval duidelijk geen regelgevende tussenkomst op aan de Autoriteit.

[20] HvJ-EU (voltallige zitting), arrest van 30 april 2024 (QUADRATURE DU NET 2), zaak C-470/21, punt 127.

[21] Artikel 23, § 3, laatste lid, van de WOG.

aanvragen **gemotiveerd en gedetailleerd blijven in het licht van die context en de specifieke (met name feitelijke) elementen met betrekking tot deze aanvragen**[22].

23. **Hetzelfde geldt *mutatis mutandis* voor het geval van een aanvraag betreffende een latere controle** in het kader van het project, indien het CCB (nationaal CSIRT) wegens **dringendheid** het IP-adres van een C2-server moest meedelen en de betrokken metagegevens rechtstreeks bij een operator moest verzamelen, zonder voorafgaande machtiging van de Autoriteit.

24. Ten tweede **staat de Autoriteit**, aangezien het gaat om een eerste aanvraag in het kader van het specifieke project van de aanvrager, **positief tegenover de door hem gevolgde aanpak** om haar een voorafgaande machtiging te vragen, in plaats van – ervan uitgaande dat in het kader van deze aanvraag een beroep op dringendheid zou kunnen worden gedaan (wat de Autoriteit in dit geval niet heeft beoordeeld) – de Autoriteit voor een voldongen feit te plaatsen in een situatie van latere controle.

II.3. Doeleinde van de gegevensverwerkingen en taak van algemeen belang van het CCB (nationaal CSIRT) waarop deze verwerkingen gebaseerd zijn

25. Wat betreft het **concrete doeleinde** van het project en de daarmee verband houdende gegevensverwerkingen, heeft de Autoriteit de aanvrager verzocht om duidelijk en nauwkeurig te bevestigen dat het enige doeleinde van het project is om **potentiële slachtoffers van C2-servers te informeren, zodat zij eventueel de nodige maatregelen kunnen treffen om zich te beschermen tegen activiteiten die via deze servers worden uitgevoerd** (in voorkomend geval door een beroep te doen op het nationale CSIRT, en waarbij het aan de betrokken entiteiten is om, afhankelijk van het geval, te voldoen aan hun meldingsverplichtingen uit hoofde van de NIS2-wet – vroegtijdige waarschuwing, enz.)[23]. **De GEB preciseert dat het beoogde effect/resultaat voor de personen is** "*dat de betrokken personen zo snel mogelijk worden geïnformeerd over cyberdreigingen afkomstig van C2-servers waarvan zij het doelwit zijn, en dat deze personen de nodige maatregelen treffen om zich te beschermen, indien mogelijk voordat de dreigingen een concrete vorm aannemen*" (vrije vertaling).

26. De aanvrager antwoordde met name het volgende (vrije vertaling):

> "*Het doeleinde van het project* [...] *is* ***zowel het informeren van verantwoordelijken*** *voor informatiesystemen die het slachtoffer zijn van C2-servers (zodat zij de nodige*

[22] In een andere juridische context (verzoeken tot aftappen van telefoongesprekken op strafrechtelijk gebied), zie bijvoorbeeld HvJ-EU (Derde kamer), arrest van 16 februari 2023 (HYA, IP, DD, ZI, EN SS), zaak C-349/21, punt 50 e.v.

[23] De nota is hierover niet helemaal duidelijk (zij vermeldt met name, ook al heeft deze passage betrekking op het wettelijk kader, het volgende: "*2) Het CCB streeft bij de opvraging drie doestellingen na: a) het voorkomen, onderzoeken en opsporen van inbreuken online; b) het voorkomen van ernstige bedreigingen voor de openbare veiligheid; c) het onderzoeken van beveiligingsproblematieken. 3) Deze bevoegdheid van CCB dient uitgevoerd te worden zonder afbreuk te doen aan of zich te mengen in de bevoegdheden van de gerechtelijke autoriteiten en politie*").

maatregelen kunnen treffen om zich te beschermen) ***als*** ***het onderzoeken van beveiligingsproblemen bij*** *elektronische-communicatie****netwerken*** *of -diensten of informatiesystemen.*
Deze doeleinden sluiten aan bij elk van de ***drie*** ***doeleinden zoals bedoeld in artikel 21, § 2, tweede lid, van de NIS2-wet***

1° zonder strafrechtelijke finaliteit, het voorkomen, onderzoeken en opsporen van inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, met inbegrip van zware criminele feiten: een waarschuwing aan een NIS2-entiteit, een kritieke infrastructuur, een private organisatie, een overheidsinstantie of een burger maakt het mogelijk om inbreuken die online of via een elektronische-communicatienetwerk of -dienst worden gepleegd, ***te voorkomen en op te sporen*** […]*;*

2° het voorkomen van ernstige bedreigingen voor de openbare veiligheid: een waarschuwing aan een NIS2-entiteit, een kritieke infrastructuur of een overheidsinstantie maakt het mogelijk deze te beschermen tegen ernstige cyberdreigingen; Het door het CCB nagestreefde ***doeleinde*** *(het identificeren en informeren van slachtoffers van C2-servers zodat zij zich kunnen beschermen) is het* ***voorkomen van schade*** *die zou worden veroorzaakt door aanvallen via C2-servers. De schade die wordt veroorzaakt door cyberaanvallen waarbij gebruik wordt gemaakt van C2-servers, maakt dit type dreiging tot een ernstige bedreiging voor de openbare veiligheid;*

3° het onderzoeken van beveiligingsproblemen bij elektronische-communicatienetwerken of -diensten of informatiesystemen: door de metagegevens te analyseren kunnen geïnfecteerde of kwetsbare informatiesystemen worden opgespoord ***en kunnen deze problemen worden verholpen****.*

De dreigingen die voortvloeien uit de activiteiten van C2-servers en hun netwerk van "zombie"-computers (botnet) zijn welbekend. Deze servers worden met name gebruikt om:
• informatie op gecompromitteerde computers te stelen of te wijzigen (met latere doorverkoop van de informatie);
• andere computers te identificeren en te infecteren door het verspreiden van virussen en kwaadaardige programma's (malware);
• deel te nemen aan Distributed Denial of Service-aanvallen (DDoS);
• de rekenkracht van de computers te benutten of distributed computing uit te voeren, met name om wachtwoorden te kraken;
• gebruikerssessies te stelen (gebruikersaccount en wachtwoord);
• cryptomunten te minen;

• enz.;

C2-servers stellen een tegenstander in staat te communiceren met gecompromitteerde systemen om er controle over te krijgen. De term "command and control" verwijst naar de technieken die tegenstanders kunnen aanwenden om te communiceren met de systemen die zij binnen het netwerk van een slachtoffer controleren. Tegenstanders ***proberen doorgaans het normale en verwachte verkeer na te bootsen*** *om opsporing te voorkomen. Er bestaan tal van manieren waarop een tegenstander command and control kan instellen, met verschillende niveaus van zichtbaarheid, afhankelijk van de netwerkstructuur en de verdedigingsmechanismen van het slachtoffer. (Command and Control. Tactic TA00ll - Enterprise I MITRE ATT&CK®)*" (vetgedrukte opmaak aangepast door de Autoriteit, onderstreept door de Autoriteit)

"*Essentiële of belangrijke entiteiten in de zin van de NIS2-wet* ***moeten****, in voorkomend geval,* ***een NIS2-incidentmelding indienen*** *(als aan de criteria voor een significant incident is voldaan) en/of een melding van een inbreuk in verband met persoonsgegevens doen (als aan de criteria is voldaan). Zij moeten bovendien de nodige maatregelen nemen om incidenten te voorkomen en passende beveiligingsmaatregelen treffen (artikel 30 van de NIS2-wet).*

De geïdentificeerde C2-servers kunnen ook schade berokkenen aan organisaties of particulieren die ***geen NIS2-entiteit*** *zijn. Deze organisaties of particulieren* ***kunnen*** *steeds* ***vrijwillig*** *een incident* ***melden*** *aan het CCB (artikel 38 van de NIS2-wet).*

In dat geval moet het CCB deze meldingen op dezelfde manier verwerken als verplichte meldingen; er ***kan*** *evenwel* ***voorrang worden gegeven aan de verwerking van lopende verplichte meldingen****.*

Het behoort tot de taak van het CCB om meldingen te sturen naar organisaties of particulieren die het slachtoffer zijn van cyberdreigingen, en om cyberincidenten te voorkomen.

Daarnaast moeten de betrokken organisaties die onder de AVG vallen, de nodige maatregelen treffen om hun verwerkingen van persoonsgegevens te beveiligen, krachtens artikel 32 van de AVG." (in vet aangeduid door de Autoriteit)

27. De Autoriteit heeft de aanvrager ook bevraagd over het **verstrekken van "vroegtijdige waarschuwingen"** waarop de nota de nadruk legt en zoals bedoeld in artikel 19, § 1, 2°, van de NIS2-wet. De NIS2-wet is hierover niet helemaal duidelijk. **Het verstrekken van vroegtijdige waarschuwingen wordt** als zodanig namelijk **noch in de NIS2-wet, noch in Richtlijn (EU)**

2022/2555 van het Europees Parlement en de Raad van 14 december 2022 *betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn)* (hierna "**de NIS2-richtlijn**") **gedefinieerd**. Het concept van **vroegtijdige waarschuwingen bestaat echter wel in de context van de meldingen** waarnaar wordt verwezen in het kader van de rapportageverplichtingen van de betrokken entiteiten[24]. Artikel 19, § 1, 2°, van de NIS2-wet heeft naast het verstrekken van vroegtijdige waarschuwingen ook betrekking op het verstrekken van "*meldingen*". In verband hiermee is ook de vraag gerezen onder welke activiteit de "**Cyber Threat Alerts**"-service valt[25].

28. Toen hem hierover vragen werden gesteld, antwoordde de aanvrager met name het volgende (vrije vertaling):

> "*Het verkrijgen van metagegevens van elektronische communicatie en het waarschuwen van slachtoffers maakt* ***met name*** *deel uit van* ***de taak zoals bedoeld in artikel 19, § 1, eerste lid, 2°, van de NIS2-wet*** *– namelijk het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie over cyberdreigingen, kwetsbaarheden en incidenten. Dit project* ***draagt ook bij aan de taken van monitoring en analyse van cyberdreigingen, kwetsbaarheden en incidenten*** *–* ***met name de dynamische analyse van risico's en forensische gegevens*** *(19, § 1, eerste lid, 1° en 4°).*
>
> […].
>
> *De wetgever heeft dus expliciet voorzien in deze nieuwe bevoegdheid van de GBA (controle van de toegang tot metagegevens van elektronische communicatie), met name ten behoeve van het CCB.*
>
> *Ter herinnering:* ***de taken van het CCB worden niet uitgevoerd voor strafrechtelijke doeleinden****, ook al dragen de ondernomen acties bij tot het voorkomen van incidenten en inbreuken op het gebied van cybercriminaliteit. Artikel 21 van de NIS2-wet bepaalt uitdrukkelijk dat de taken van het CCB worden uitgevoerd "zonder afbreuk te doen aan of zich in te mengen in de bevoegdheden van personen die de gerechtelijke politie uitoefenen en de gerechtelijke autoriteiten".*
>
> […]." (in vet aangeduid door de Autoriteit, onderlijnde opmaak gewijzigd door de Autoriteit)

[24] Zie artikel 23, 4., a), van de NIS2-richtlijn en artikel 35, § 1, 1°, van de NIS2-wet.

[25] Zie https://atwork.safeonweb.be/nl/protect-my-organisation/cyber-threat-alerts, laatst geraadpleegd op 02/06/2025.

"*Het* ***"verstrekken van vroegtijdige waarschuwingen" van het CCB zoals bedoeld in artikel 19, § 1, eerste lid, 2°, van de NIS2-wet moet duidelijk worden onderscheiden van het bezorgen van een "vroegtijdige waarschuwing"*** *van een significant incident (binnen 24 uur) zoals bedoeld in artikel 35, § 1, 1°.*

Artikel 19, § 1, eerste lid, 2°, van de NIS2-wet heeft betrekking op de wettelijke taken en verplichtingen van het CCB (als nationaal CSIRT), met name "het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten en aan de bevoegde autoriteiten en andere relevante belanghebbenden over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk". ***Het CCB moet projecten ontwikkelen om NIS2-entiteiten, andere overheidsinstanties, private organisaties of burgers ("andere relevante belanghebbenden") zo goed mogelijk te informeren over cyberdreigingen, kwetsbaarheden en incidenten (in bijna-realtime indien mogelijk).*** *Dit project* ***heeft tot doel deze wettelijke taak te vervullen in het verlengde van bestaande projecten (Cyber Threat Alerts, Early Warning System, Spear Warning). "Het verstrekken van vroegtijdige waarschuwingen" en "het verstrekken van meldingen" zoals bedoeld in het bovengenoemde artikel worden door het CCB uitgevoerd om*** *een of meer entiteiten (rechtspersonen of natuurlijke personen)* ***zo snel mogelijk te waarschuwen*** *voor een cyberdreiging, indien mogelijk voordat deze dreiging een concrete vorm aanneemt of tot een incident leidt.*

Artikel 35, § 1, 1°, van de NIS2-wet heeft betrekking op de rapportageverplichtingen van essentiële of belangrijke NIS2-entiteiten […]." (in vet aangeduid en onderstreept door de Autoriteit).

29. Op basis van deze antwoorden is de Autoriteit van mening dat **het project steunt op artikel 19, § 1, 2°, van de NIS2-wet**. Het betreft het verspreiden van meldingen en informatie over cyberdreigingen en kwetsbaarheden onder potentiële slachtoffers, indien mogelijk in real time. Hierdoor heeft het project daadwerkelijk een preventief effect op de verwezenlijking van dreigingen en schade bij doelwitten van C2-servers (artikel 21, § 2, 1° en 2°, van de NIS2-wet)[26]. Voor de uitvoering ervan is het noodzakelijk beveiligingsproblemen bij elektronische-communicatienetwerken en informatiesystemen te onderzoeken (artikel 21, § 2, 3°, van de NIS2-wet). Dit omvat het opsporen,

[26] De GEB preciseert duidelijk dat het beoogde effect/resultaat voor de personen is "*dat de betrokken personen zo snel mogelijk worden geïnformeerd over cyberdreigingen afkomstig van C2-servers waarvan zij het doelwit zijn, en dat deze personen de nodige maatregelen treffen om zich te beschermen, indien mogelijk voordat de dreigingen een concrete vorm aannemen*" (vrije vertaling).

observeren en analyseren van computerbeveiligingsproblemen die verband houden met de betrokken dreigingen (artikel 19, § 1, 10°, van de NIS2-wet).

30. De Autoriteit heeft de aanvrager gevraagd of hij op de hoogte was **van het bestaan van een soortgelijk initiatief als het project in een andere lidstaat**[27]. Hij heeft met name aangegeven dat hij niet bekend was met een dergelijk initiatief in een andere lidstaat van de Unie.

II.4. Betrokken mogelijk benadeelde entiteiten en verzamelde metagegevens

31. De gegevensverwerking in het kader van het project, en in het bijzonder de concrete identificatie van de metagegevens die zullen worden verzameld en aan het CCB zullen worden meegedeeld, is afhankelijk van de C2-servers die door het CCB (nationaal CSIRT) zullen worden geselecteerd en geïdentificeerd, alsook van de (potentiële) slachtoffers die zullen worden geïdentificeerd. **De methoden en criteria voor de selectie van C2-servers en slachtoffers hebben bovendien een doorslaggevende invloed op de toepasselijkheid van de regels inzake gegevensbescherming.** Aan de hand daarvan kan met name worden beoordeeld of het doelbindingsbeginsel, het evenredigheidsbeginsel (waaronder het beginsel van minimale gegevensverwerking en het beginsel van de juistheid van de gegevens) en het objectieve en niet-discriminerende karakter van het project worden nageleefd bij de uitvoering van de relevante taak door het CCB (nationaal CSIRT).

32. **Los** van de vraag of de verwerking van persoonsgegevens rechtmatig is, **draagt** de kwaliteit van deze methoden en criteria **bij tot het voorkomen van het belangrijkste risico van het project**, namelijk de verzameling van metagegevens van elektronische communicatie (en de daaropvolgende identificatie van de partijen bij deze communicatie) die geen betrekking hebben op C2-servers en hun slachtoffers, en de daarmee samenhangende gevolgen (onrechtmatige onderschepping en bewaring van metagegevens van elektronische communicatie; mogelijk misbruik van het opgezette systeem door een bron; gevolgen voor werknemers of bezoekers van de betrokken entiteit die mogelijk betrokken zijn bij het verkeer tussen de betrokken server en het informatiesysteem van de entiteit[28]; maatregelen die door het vermeende slachtoffer worden getroffen tegen het geïdentificeerde IP-adres en de houder daarvan).

II.4.1. Verwerkte metagegevens

[27] In eerste instantie antwoordde hij het volgende (vrije vertaling):

"*De Franse tegenhanger van het CCB (ANSSI) beschikt, op grond van artikel L2321-2-1 van de Franse Code de la défense, over bevoegdheden om dit soort gegevens op het netwerk van een elektronische-communicatieoperator te verzamelen (kopie van servers), onder toezicht van de ARCEP (Autorité de régulation des communications électroniques).*"

[28] Zie overweging nr. 101.

33. Het project voorziet in de verzameling van metagegevens van elektronische communicatie die heeft plaatsgevonden van en naar de IP-adressen van de vermelde C2-servers, totdat de lijst met deze IP-adressen wordt bijgewerkt door het CCB (nationaal CSIRT). **Het gaat om de volgende metagegevens: "*Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*"**. Als zodanig geven zij geen aanleiding tot opmerkingen van de Autoriteit.

34. Op verzoek van de Autoriteit heeft de aanvrager bevestigd dat **de verzamelde metagegevens alleen betrekking zullen hebben op elektronische communicatie die plaatsvindt na het moment waarop het verzoek tot mededeling van metagegevens aan de betrokken operator wordt gericht**. De Autoriteit wijst de aanvrager erop dat hij in het kader van het project in de toekomst ook toestemming zou kunnen vragen om metagegevens te verwerken met betrekking tot elektronische communicatie die is verzonden **vanaf de datum van indiening van zijn** machtigings**aanvraag** bij de Autoriteit, **op voorwaarde dat** de betrokken operatoren deze gegevens hebben bewaard in het kader van hun activiteiten voor het aanbieden van elektronische-communicatiediensten (en niet op grond van een wettelijke verplichting om deze gegevens te bewaren[29]).

35. Op de vraag naar de **betrokken operatoren** antwoordde de aanvrager het volgende (vrije vertaling): "*Het verzoek om metagegevens kan worden gericht aan alle elektronische-communicatieoperatoren die in België actief zijn. Overeenkomstig de bepalingen van de wet van 13 juni 2005 betreffende de elektronische communicatie kan elke operator, zijnde een persoon of onderneming die een openbaar elektronische-communicatienetwerk of een voor het publiek beschikbare elektronische-communicatiedienst in België aanbiedt, een verzoek ontvangen.* ***In een eerste fase zou in de eerste plaats contact worden opgenomen met Belnet.***" (in vet aangeduid door de Autoriteit)

36. De Autoriteit wijst de aanvrager erop dat **zijn machtigingsaanvraag de betrokken operatoren moet identificeren**. In dit geval merkt de Autoriteit op dat de aanvraag betrekking heeft op metagegevens die **door de operator Belnet worden verwerkt**.

II.4.2. Betrokken benadeelde entiteiten

Entiteiten die onder het toepassingsgebied van de NIS2-wet vallen en andere entiteiten

37. De Autoriteit heeft op basis van de meegedeelde nota opgemerkt dat het project verder lijkt te gaan dan de identificatie van benadeelde entiteiten die onderworpen zijn aan de verplichtingen van de NIS2-

[29] Een dergelijke vraag heeft betrekking op de rechtmatigheid van de verplichtingen inzake de bewaring van metagegevens van elektronische communicatie die aan de operatoren worden opgelegd, wat buiten de context van de aanvraag valt.

wet (dat wil zeggen essentiële of belangrijke entiteiten). Het project heeft immers betrekking op slachtoffers "*inclusief NIS-2-entiteiten, overheidstinstanties, ondernemingen, burgers, enz.*". Aangezien het project daarmee buiten **het toepassingsgebied *ratione personae* van de in de NIS2-wet neergelegde verplichtingen** zou treden, kan de rechtsgrond van het project vragen oproepen.

38. Op vragen hierover antwoordde de aanvrager het volgende (vrije vertaling):

> "*De NIS2-wet* ***bevat zowel bepalingen die alleen van toepassing zijn op NIS2-entiteiten*** *(registratie, beheer van cyberbeveiligingsrisico's, verplichte melding van significante incidenten, toezicht, enz.) – toepassingsgebied ratione personae "NIS2-entiteiten" –* ***als andere bepalingen die gelden voor alle organisaties of personen in België*** *– ratione personae "alle entiteiten/burgers" (en dus niet beperkt tot NIS2-entiteiten).*
>
> ***Tot de bepalingen met een bredere reikwijdte*** *(niet beperkt tot NIS2-entiteiten) behoren bijvoorbeeld de taken van het CCB* ***als nationale cyberbeveiligingsautoriteit, autoriteit voor cybercrisisbeheer en nationaal CSIRT (artikelen 17, 18, 19, 20 en 21), de melding van kwetsbaarheden en de bescherming van ethische hackers (artikelen 22 en 23), de bepalingen inzake samenwerking op nationaal niveau (artikel 25), de nationale cyberbeveiligingsstrategie (artikel 28), de vrijwillige meldingen (artikel 38) of de verwerking van persoonsgegevens (titel 6)****.*
>
> *Artikel 19, § 1, eerste lid, 2°, van de NIS2-wet bepaalt dat het CCB onder meer het volgende tot taak heeft: "het verstrekken van vroegtijdige waarschuwingen, meldingen en aankondigingen en het verspreiden van informatie onder de betrokken essentiële en belangrijke entiteiten* ***en aan de bevoegde autoriteiten en andere relevante belanghebbenden*** *over cyberdreigingen, kwetsbaarheden en incidenten, in bijna-realtime indien mogelijk" (wij onderstrepen). Uit bovengenoemde bepaling blijkt dat* ***de taak met betrekking tot vroegtijdige waarschuwingen van het CCB niet beperkt is tot essentiële en belangrijke NIS2-entiteiten, maar ook geldt voor andere in België gevestigde entiteiten, of het nu gaat om publieke of private entiteiten of natuurlijke personen****."* (in vet aangeduid door de Autoriteit)

39. De Autoriteit neemt akte van deze uitleg. Zij vestigt echter de aandacht van de aanvrager op de volgende punten.

40. De Autoriteit benadrukt dat, gelet op de eerder genoemde **beginselen van voorspelbaarheid en rechtmatigheid**[30], de mogelijkheid van het project niet zo duidelijk uit de NIS2-wet blijkt. Dat het CCB (nationaal CSIRT) op grond van de wetgeving de mogelijkheid heeft om overeenkomstig artikel 19, § 1, 2°, van de NIS2-wet informatie te verstrekken over dreigingen (en deze op te sporen en te analyseren)[31] indien mogelijk in real time, en om metagegevens van elektronische communicatie te verzamelen voor bepaalde doeleinden wanneer dat nodig is voor de uitvoering van zijn taken, betekent niet noodzakelijk dat het CCB (nationaal CSIRT) in real time de metagegevens mag verzamelen **van alle elektronische communicatie** van of naar IP-adressen die zijn toegewezen aan C2-servers (de dreigingen) die het identificeert/vaststelt, met betrekking tot potentiële slachtoffers, **wie deze slachtoffers ook mogen zijn**, met het oog op het versturen van waarschuwingen. Dit geldt des te meer omdat het verstrekken van "vroegtijdige waarschuwingen" waarnaar het CCB verwijst, niet is gedefinieerd in het toepasselijke recht.

41. Aangezien de NIS2-wet, zoals blijkt uit de titel en het dispositief ervan, duidelijk en expliciet tot doel heeft een kader te creëren "*voor de cyberbeveiliging van netwerk- en informatiesystemen **van algemeen belang voor de openbare veiligheid***" (in vet aangeduid door de Autoriteit), is het in dit geval **minder voorspelbaar dat het project in het kader van de uitvoering van de NIS2-wet ook betrekking kan hebben op de metagegevens van elektronische communicatie** (en de latere identificatie) **van personen** (rechtspersonen en natuurlijke personen) **die niet onder het toepassingsgebied *ratione personae* van de verplichtingen van de NIS2-wet vallen**, omdat zij geen essentiële of belangrijke entiteiten zijn. Entiteiten die geen essentiële of belangrijke entiteiten zijn, kunnen weliswaar meldingen doen aan het CCB (nationaal CSIRT). Deze meldingen zijn echter **vrijwillig** en verplichte meldingen kunnen met voorrang worden verwerkt[32]. De **ondersteunende taken van het CCB (nationaal CSIRT)**, overeenkomstig de NIS2-wet, lijken, in de logica van het doeleinde van de NIS2-wet, ook **gericht** te zijn **op essentiële of belangrijke entiteiten**[33]. Daarnaast vergemakkelijkt de NIS2-wet rechtstreeks de mogelijkheden voor het CCB (nationaal CSIRT) om het verkeer van essentiële of belangrijke entiteiten op te sporen, aangezien het CCB **de door deze entiteiten gebruikte IP-bereiken** (inclusief updates daarvan) en hun contactgegevens **moet ontvangen**[34]. Omgekeerd versterken deze elementen het voorspelbare karakter van het project in het licht van het dispositief van de NIS2-wet voor wat betreft essentiële of belangrijke entiteiten.

---

[30] Zie de overwegingen nrs. 14-15.

[31] Zie meer bepaald overweging nr. 29.

[32] Zie artikel 38 van de NIS2-wet.

[33] Volgens artikel 19, § 1, van de NIS2-wet heeft het CCB (nationaal CSIRT) de volgende taken: "*het monitoren en analyseren van cyberdreigingen, kwetsbaarheden en incidenten op nationaal niveau, en, op verzoek, het verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten met betrekking tot het realtime of bijna-realtime monitoren van hun netwerk- en informatiesystemen*"; "*het reageren op incidenten en verlenen van bijstand aan de betrokken essentiële en belangrijke entiteiten, indien van toepassing*"; "*op verzoek van een essentiële of belangrijke entiteit: het proactief scannen van de netwerk- en informatiesystemen van de betrokken entiteit om kwetsbaarheden met mogelijk significante gevolgen op te sporen*".

[34] Zie de artikelen 13 en 14 van de NIS2-wet.

42. In de normatieve context die van toepassing is op het project, moet de toegang tot metagegevens van elektronische communicatie echter beperkt blijven tot wat **strikt noodzakelijk** is[35]. Bovendien bestaan er **andere manieren om andere "belanghebbenden"**[36] (en essentiële of belangrijke entiteiten) **te informeren** zonder dat daarvoor metagegevens van elektronische communicatie hoeven te worden verwerkt[37].

43. **Dit gezegd zijnde, gelet op het beperkte doeleinde van het project zoals opgenomen in deze beslissing[38], de impact van de betrokken dreigingen en het belang van het project voor de cyberveiligheid in België in het algemeen**, moet worden vastgesteld dat deze andere manieren van informeren minder doeltreffend zouden zijn om het door de NIS2-wet nagestreefde doel van algemeen belang te bereiken (namelijk de beveiliging van informatiesystemen van algemeen belang voor de openbare veiligheid) en dat het project wel degelijk in de geest van deze wet past, onverminderd latere opmerkingen[39].

44. Tot slot **is de Autoriteit van mening dat het project zowel betrekking kan hebben op de metagegevens van elektronische communicatie tussen de C2-servers en de essentiële of belangrijke entiteiten waarop de NIS2-wet van toepassing is, als op de metagegevens van elektronische communicatie tussen diezelfde C2-servers en andere entiteiten** die niet onder de verplichtingen van de NIS2-wet vallen.

45. **Wat deze andere entiteiten betreft**, is de Autoriteit echter van mening dat deze interpretatie van de NIS2-wet **op korte termijn door de wetgever moet worden bevestigd**, hetzij door een interpretatieve wet, hetzij door een wijziging van de NIS2-wet[40], om met name de rechtszekerheid van de uitgevoerde gegevensverwerkingen te waarborgen. Het komt het CCB toe om in dit verband de nodige stappen te ondernemen, en de Autoriteit zal hierop letten in het kader van toekomstige verzoeken om machtiging (of latere controle).

Criterium op basis waarvan een NIS2-entiteit als potentieel slachtoffer wordt beschouwd

46. In de door de aanvrager verstrekte nota staat het volgende: "*Belgische gebruikers worden enkel geïdentificeerd als er* ***sterke aanwijzingen zijn dat*** *de gebruiker* ***contact heeft gehad*** *met een*

[35] Zie met name artikel 21, § 2, van de NIS2-wet.

[36] Ervan uitgaande dat de "*belanghebbenden*" wel degelijk alle potentiële slachtoffers kunnen zijn, aangezien de NIS2-wet niet definieert wie deze belanghebbenden zijn (in dit geval zouden zij, in het kader van het project, categorieën van betrokkenen zijn).

[37] Zie overweging nr. 79 e.v.

[38] Zie overweging nr. 39.

[39] Zie overweging nr. 73 e.v.

[40] Indien de wetgever voornemens was de NIS2-wet op basis van het project te wijzigen, zie ook overweging nr. 12.

kwaadaardig buitenlands IP-adres." (in vet aangeduid door de Autoriteit) In dit verband heeft de Autoriteit de aanvrager gevraagd welke criteria en gegevens worden gebruikt om te bepalen of er sprake is van dergelijke "*sterke aanwijzingen*"; zij heeft hem verzocht te bevestigen dat het de bedoeling is om contact op te nemen met alle betrokken potentiële slachtoffers en, indien dat niet zo is, de criteria mee te delen die worden gebruikt om de slachtoffers te identificeren die moeten worden gecontacteerd.

47. De aanvrager preciseerde het volgende (vrije vertaling):

> "***Elektronische communicatie van en naar*** *servers die door het CCB zijn geverifieerd als command-and-control servers (C2),* ***moet worden beschouwd als een sterke aanwijzing voor kwaadaardige activiteiten****.* ***De analyse van de metagegevens door het CB kan*** *de kwaadaardige aard van deze activiteiten* ***bevestigen*** *en eventueel meer context en de graad van urgentie van de aanval verschaffen.*" (in vet aangeduid door de Autoriteit)
>
> "*Het doel is inderdaad om alle metagegevens te analyseren en contact op te nemen met alle betrokken slachtoffers (rechtspersonen of natuurlijke personen).*"

48. Aangezien er **geen gegevens over de inhoud** van de elektronische communicatie worden verzameld, heeft de Autoriteit de aanvrager bovendien verzocht te preciseren op basis van welke **methode** en welke **criteria** wordt aangenomen dat de verzamelde metagegevens (namelijk "*Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*") **aangeven dat een entiteit mogelijk een slachtoffer/doelwit is van de betrokken C2-server**. In verband met deze vraag wordt in de tabel in de nota onder de punten 5.1 en 5.2 het volgende vermeld: "*5.1 CCB slaat de ontvangen data beveiligd op voor maximaal 1 jaar, dit* ***om grondige analyses te kunnen maken over meerdere gegevens****. 5.2 CyTRIS analyseert de data,* ***onderscheidt de malicious communicatie van de normale****.*" (in vet aangeduid door de Autoriteit) De Autoriteit heeft de aanvrager gevraagd om het doeleinde van deze "*grondige analyses*"[41] te bevestigen, heeft hem gevraagd hoeveel tijd er nodig is om een slachtoffer te identificeren, heeft hem gevraagd welke criteria worden gebruikt om kwaadaardige communicatie te onderscheiden van normale communicatie, en heeft hem ten slotte verzocht te verduidelijken of een C2-server in de praktijk zowel voor geoorloofde als voor ongeoorloofde doeleinden kan worden gebruikt.

49. De aanvrager verwees naar het antwoord in overweging nr. 47 en antwoordde bovendien het volgende (vrije vertaling):

[41] Zie in dit verband overweging nr. 111 e.v.

[redacted]

"*De grondige analyses in punt 5.1 kunnen het mogelijk maken om* ***verbanden in de tijd te leggen tussen de activiteiten van verschillende C2-servers*** *en om* ***de kwaadaardige acties*** *van de daders en de dreigingen* ***doeltreffend te volgen***." (in vet aangeduid door de Autoriteit)

"*De tijd die het CCB nodig heeft om de ontvangen gegevens te analyseren,* ***hangt af van de hoeveelheid gegevens, maar de analyse kan vrij snel plaatsvinden (enkele uren/dagen)****. Wanneer wordt vastgesteld dat een systeem slachtoffer is, dient het CCB een verzoek in bij de betrokken ISP om de organisatie of de betrokkene achter het betreffende IP-adres te identificeren. De termijn voor de identificatie hangt af van de dringendheid van het verzoek dat aan de operator wordt gestuurd (het CCB kan de termijn bepalen waarbinnen de operator op zijn verzoek moet reageren, naargelang de dringendheid ervan, overeenkomstig artikel 21, § 2, derde lid). Het is noodzakelijk zo snel mogelijk te handelen om de verantwoordelijken van de getroffen systemen een zinvolle waarschuwing te geven.*" (in vet aangeduid door de Autoriteit)

"***Elektronische communicatie tussen een command-and-control server (C2) – (geverifieerd door het CCB) en een ander IP-adres moet worden beschouwd als een sterke aanwijzing voor kwaadaardige activiteiten*** *(poging tot fraude, diefstal van informatie, spionage, DDoS, enz.). Zie ook de antwoorden op V11*[42]*.*

[redacted]

[redacted]

[redacted]

II.4.3. Betrokken C2-servers

52. In de GEB staat het volgende (vrije vertaling): "***Een C2-server kan worden gedefinieerd*** *als een server die door een aanvaller of malware wordt gebruikt om te communiceren met en controle uit te oefenen over geïnfecteerde of gecompromitteerde computers (ook wel "bots" of "zombies" genoemd). Deze C2-servers worden gebruikt om cyberaanvallen uit te voeren en gestolen gegevens op te halen. Een C2-server kan ook worden gedefinieerd als een netwerk- of informatiesysteem dat wordt gebruikt voor onrechtmatig(e) of ongeoorloofd(e) identificatie van, toegang tot of gebruik van netwerk- en*

[42] Overweging nr. 47.

informatiesystemen van derden of gegevens die zich bevinden op, worden verwerkt door of worden doorgegeven via een netwerk- en informatiesysteem van derden (definitie geïnspireerd op de U.S. Code § 650- Definitions (16) Malicious cyber command and contrai)." (in vet aangeduid door de Autoriteit) De identificatie van deze servers zal gebeuren op basis van **de informatiebronnen waarover het CCB (nationaal CSIRT) beschikt**, [redacted]

[redacted]

53. Deze informatiebronnen vloeien duidelijk voort uit de toepassing van de NIS2-wet en in het bijzonder uit de artikelen 17, 18, 19, 25, 27, 34-38, 44 en 48 van deze wet.

54. Volgens de verstrekte nota is het project beperkt tot **buitenlandse C2-servers** ("*buitenlandse C2-servers*"; "*externe C2 servers*") of, om precies te zijn, tot **buitenlandse IP-adressen** ("*buitenlands IP-adressen*"). C2-servers die in België "gevestigd" zijn, vallen namelijk onder een ander project ("*Het betreft enkel communicatie met externe C2 servers. Detectie van C2 servers binnen de netwerken van de BE ISPs maken deel uit van een andere procedure, buiten de scope van dit project.*"). De Autoriteit heeft de aanvrager met name bevraagd over de manier waarop – in het geval van "Belgische" C2-servers – de slachtoffers van deze C2-servers worden geïnformeerd. Hij antwoordde het volgende (vrije vertaling):

> "*Het project is in dit stadium bewust beperkt tot **C2-servers die in het buitenland gevestigd zijn**, om **mogelijke nadelige interacties met lopende strafrechtelijke onderzoeken of onderzoeken van inlichtingendiensten te voorkomen**. Zolang er geen identificatiegegevens en verbanden met in België gevestigde entiteiten beschikbaar zijn, is het voor bovengenoemde diensten niet mogelijk om een onderzoek te starten. Het merendeel van de in België actieve C2-servers **is gevestigd in het buitenland**.*" (in vet aangeduid door de Autoriteit)

55. De Autoriteit heeft de aanvrager hierover opnieuw bevraagd, evenals over de manier waarop C2-servers worden beschouwd als zijnde in het buitenland gevestigd[43]. Hij antwoordde het volgende (vrije vertaling):

[43] Meer bepaald betwijfelt de Autoriteit, gelet op de territoriale bevoegdheid van de rechtbanken in strafzaken, dat de lokalisatie van een C2-server in België noodzakelijk is om deze rechtbanken bevoegd te maken (in de door het project beoogde gevallen van cyberdreigingen zijn er duidelijk elementen die tot de betrokken strafbare feiten behoren en die zich op Belgisch grondgebied bevinden).

- Met andere woorden: hoe wordt bepaald dat een C2-server in België gevestigd is (en dus van het project wordt uitgesloten)?;

"*De **IP-bereiken** worden per land toegekend.* [redacted]

"*Het merendeel van de in België actieve C2-servers is gevestigd in het buitenland. Slechts **enkele geïsoleerde gevallen zouden betrekking kunnen hebben op de activiteiten van een C2-server die in België gevestigd is**. **In een dergelijk geval** zal het CCB de feiten melden aan de gerechtelijke autoriteiten, die een vervolging kunnen instellen en de potentiële slachtoffers kunnen informeren (zonder dat een verzoek om toegang tot de metagegevens van deze servers bij de telecomoperatoren moet worden ingediend).*" (in vet aangeduid door de Autoriteit);

"*Het klopt dat de territoriale bevoegdheid van de Belgische rechtbanken in strafzaken niet beperkt is tot servers die in België gevestigd zijn (de plaats in België waar de schade optreedt of waar de systemen geïnfecteerd zijn, vormt eveneens een criterium voor territoriale bevoegdheid).*
[redacted]

*Het zou echter **mogelijk** zijn **om dit element in een tweede fase van het project opnieuw te evalueren** en ook servers die in België gevestigd zijn, op te nemen.*

*Bovendien moet worden opgemerkt dat dit project tot doel heeft **om slachtoffers van C2-servers zo snel mogelijk te waarschuwen**. **In het geval van C2-servers die in het buitenland gevestigd zijn maar in België actief zijn, wordt het optreden van de gerechtelijke autoriteiten in de praktijk echter vertraagd door internationale procedures** (rogatoire commissies). In de praktijk reageren sommige diensten van derde landen zeer traag of zelfs helemaal niet op verzoeken om inlichtingen van België. Het CCB wil dit project gebruiken om **de snelheid waarmee slachtoffers worden gewaarschuwd aanzienlijk te verhogen en hen in staat te stellen zich te beschermen tegen cyberaanvallen van deze C2-servers**, zonder afbreuk te doen aan eventuele strafrechtelijke onderzoeken die door het Openbaar Ministerie worden ingesteld.*"

56. Wat betreft de **aard van de kwaadaardige activiteiten** in kwestie (**bestaand gevaar**), vermeldt de meegedeelde nota het volgende: "*De selectie van **kwaadaardige servers** gebeurt enkel in functie*

- Hoe worden de betrokken entiteiten geïnformeerd wanneer zij het slachtoffer zijn van C2-servers die in België gevestigd zijn?;
- Tot slot, op basis van het gegeven antwoord: hoe kan het informeren van een slachtoffer met het oog op het voorkomen van schade op zijn niveau afbreuk doen aan een strafrechtelijk of inlichtingenonderzoek? (Er zij op gewezen dat deze diensten zeker ook onderzoeken uitvoeren met betrekking tot C2-servers die zich in het buitenland bevinden).

*van **bedreigingen voor de openbare veiligheid**. Dit initiatief draagt bij aan het opsporen van beveiligingsproblemen met **significante gevolgen voor de nationale ICT-infrastructuur**.*" (in vet aangeduid door de Autoriteit) [redacted] In de nota wordt verder vermeld dat het CCB (nationaal CSIRT) over verschillende bronnen beschikt. In dit verband heeft de Autoriteit de aanvrager gevraagd hoe het CCB de kwaliteit van de door derden ("*vertrouwde private partners*", autoriteiten van derde landen, enz.) verstrekte informatie over de identificatie van C2-servers verifieert, welke waarborgen worden toegepast om de kwaliteit van de verstrekte informatie te garanderen en op basis van welke criteria en gegevens C2-servers worden geselecteerd.

[redacted]

58. De Autoriteit heeft de aanvrager hierover nader bevraagd[44] en deze heeft de volgende informatie verstrekt (vrije vertaling):

[redacted]

"*Het project heeft inderdaad potentieel betrekking op alle C2-servers waarvan wij in kennis worden gesteld, maar **enkel de C2-servers die door het CCB gevalideerd zijn** en opgenomen zijn in de betrokken lijst zullen het voorwerp uitmaken van een verzoek om toegang tot de metagegevens van elektronische communicatie bij de telecomoperatoren. Alleen deze laatste vallen onder het project.*

*Zoals aangegeven, **voert** het CCB **zelf een controle uit van de informatie die het ter kennis wordt gebracht (uit verschillende bronnen) en van de potentiële dreiging voor België**. Zie hier ook het document C2 List, bijlage 4.*

[redacted]

[redacted]Een aanvullende nota van de aanvrager **geeft voor elk doorgegeven IP-adres concreet aan welke technische controlemaatregelen zijn getroffen**[redacted]

[redacted]

[redacted]

[redacted]

61. In het licht van het bovenstaande is de Autoriteit van mening dat de **verzameling van bronnen voor de identificatie van IP-adressen die door de aanvrager worden vermeld** in het kader van het project, **in overeenstemming moet zijn met de NIS2-wet**. Bovendien vereist het project de invoering van een **doeltreffend proces voor de controle van de kwaliteit van de informatie over C2-servers die door al deze bronnen wordt verstrekt, en dus ook van het feit dat de betrokken IP-adressen daadwerkelijk bestemd zijn voor het verkeer van C2-servers die zijn geselecteerd op basis van de ernst van de impact van hun activiteiten**. Dit proces moet **de relevante combinaties van technische maatregelen** omvatten **die zijn opgenomen in de aanvullende nota** van de aanvrager, **alsmede, indien van toepassing, alle andere extra maatregelen die volgens de stand van de techniek op dit gebied vereist zijn**. Ten slotte moet de aanvrager **het betrouwbaarheidsniveau van de informatiebronnen, diensten en dienstverleners** waarop hij in het kader van de uitvoering van het project een beroep doet, **beoordelen en aangeven**. Deze processen en de uitvoering ervan moeten worden **gedocumenteerd** overeenkomstig het beginsel van *accountability*[45].

62. Aangezien IP-adressen in de loop van de tijd opnieuw kunnen worden toegewezen (en bovendien op dynamische wijze kunnen worden toegekend), heeft de Autoriteit de aanvrager vragen gesteld over de **bijwerking** van de adressen van de C2-servers die aan de operatoren worden meegedeeld. Eenzelfde IP-adres kan namelijk niet langer gekoppeld zijn aan de betrokken kwaadaardige activiteit (en betrekking hebben op geoorloofd verkeer). In de nota staat het volgende: "*Het CCB zal regelmatige controle uitoefenen op de (blijvende) relevantie van de C2's die op de C2 lijst staan*." Concreet heeft de Autoriteit de aanvrager verzocht aan te geven volgens welke methode en met welke frequentie de activiteit die via de IP-adressen van de betrokken C2-servers plaatsvindt, **opnieuw** wordt **beoordeeld** (met name gelet op het feit dat de basisinformatie voor de identificatie van een C2-server afkomstig kan zijn van een bron buiten het CCB).

[redacted]

[45] Artikelen 5.2 en 24 van de AVG.

65. De punten 4.1 en 4.2 (onder het punt "*Versturen metagegevens*") van het gedetailleerde interne proces dat in de oorspronkelijk door de aanvrager meegedeelde nota wordt beschreven, bepalen het volgende: "*de ISP Stuurt de metagegevens van eventueel gevonden communicaties van en naar de opgevraagde IP adressen zo snel als mogelijk terug naar het CCB*"; "***de ISP stuurt minstens dagelijks** een update, tenzij deze leeg is*" (in vet aangeduid en onderstreept door de Autoriteit). De Autoriteit begrijpt uit het antwoord van de aanvrager dat **minstens dagelijks** wordt gecontroleerd of de lijst met IP-adressen actueel is.

66. Het project vereist de invoering van een **doeltreffend proces dat ten minste dagelijks plaatsvindt** (indien nodig vaker, indien de stand van de techniek dit toelaat en vereist) **om te controleren of de IP-adressen van de betrokken C2-servers actueel zijn, op basis van de in de overwegingen 59 en 61 bedoelde controlemaatregelen**. Dit proces en de uitvoering ervan moeten worden **gedocumenteerd** overeenkomstig het beginsel van *accountability*.

67. De Autoriteit heeft de aanvrager ook gevraagd naar de eventuele **procedure** die wordt gevolgd wanneer een **fout** wordt ontdekt in de identificatie van de IP-adressen van de C2-servers. Hij antwoordde het volgende (vrije vertaling): "*Verwijdering van de lijst met IP-adressen van C2-servers en verwijdering van de gegevens. De procedure van het project voorziet in het regelmatig versturen van een nieuwe versie van de lijst: in geval van een fout **zal onmiddellijk een update naar de ISP's worden gestuurd**.*" (in vet aangeduid en onderstreept door de Autoriteit).

68. Het project vereist dat zodra het CCB (nationaal CSIRT) de vaststelling maakt dat een IP-adres niet langer gekoppeld is aan de betrokken C2-server, **de betrokken operator hiervan onmiddellijk in kennis wordt gesteld via een passend kanaal en vanaf dat moment stopt met het verzamelen van metagegevens met betrekking tot het verkeer van en naar het betrokken adres**.

69. Het project moet **ook voorzien in een doeltreffende kennisgevingsprocedure ter attentie van het CCB (nationaal CSIRT) wanneer de betrokken operator over objectieve elementen beschikt** die de juistheid van de betrokken gegevens in twijfel trekken.

70. De Autoriteit **moet op de hoogte worden gebracht van de updates die** in dit verband aan de lijst van C2-servers **worden aangebracht**, bij het volgende verzoek om machtiging (of latere controle) dat haar in het kader van het project wordt voorgelegd.

71. Ten slotte heeft de Autoriteit de aanvrager verzocht om **een inschatting te geven** (een orde van grootte) van het aantal IP-adressen die aan C2-servers zijn toegewezen en die in het kader van het project onder een aanvraag aan de GBA zouden vallen, evenals van de geraamde frequentie van de

machtigingsaanvragen die aan de Autoriteit zullen worden gericht. Hij antwoordde het volgende (vrije vertaling):

> "*Met de aanvraag van het CCB wordt een machtiging gevraagd voor de verzoeken om toegang tot metagegevens die voortvloeien uit de uitvoering van dit project (met inbegrip van de verwerkingen en de toegang die in de toekomst nodig zullen zijn).* [redacted] *Bij gebrek aan een machtiging voor de uitvoering van dit specifieke project zou het CCB voor elk nieuw IP-adres of elke nieuwe lijst of update van de bestaande lijst een nieuwe machtiging moeten aanvragen voor dezelfde doeleinden, met dezelfde verwerkingen en volgens dezelfde procedure). De geschatte frequentie* ***zou wekelijks of tweewekelijks kunnen zijn, rekening houdend met de korte verwerkingstermijnen die nodig zijn om de verantwoordelijken van de getroffen systemen een zinvolle waarschuwing te geven***." (in vet aangeduid en onderstreept door de Autoriteit)

72. De Autoriteit neemt hier akte van.

II.5. Evenredigheid van de gegevensverwerkingen

II.5.1. Beoordeling van alternatieven voor de beoogde gegevensverwerkingen

73. In de aanvraag en de nota van de aanvrager wordt niet ingegaan op alternatieven voor het project die hadden kunnen worden overwogen om potentiële slachtoffers van C2-servers te waarschuwen of schade te voorkomen, zonder dat metagegevens van elektronische communicatie worden verzameld. In essentie wordt alleen benadrukt dat het verzamelen van metagegevens en het waarschuwen van slachtoffers op basis daarvan noodzakelijk is om een beter zicht te krijgen op de betrokken dreigingen. De Autoriteit heeft de aanvrager hierover dan ook nader bevraagd.

Blokkeren/filteren van IP-adressen die aan C2-servers zijn toegewezen

74. Ten eerste moet worden nagegaan of het CCB, in plaats van te proberen potentiële slachtoffers te informeren via de verzameling van metagegevens van elektronische communicatie, niet over wettelijke middelen beschikt om **de betrokken operatoren te laten overgaan tot het blokkeren/filteren van het verkeer van en naar de IP-adressen die aan de betrokken C2-servers zijn toegewezen**. Zo ja, dan moet worden aangegeven waarom dergelijke maatregelen niet de voorkeur krijgen (wanneer de C2-server wordt geblokkeerd, kan deze immers geen nieuwe slachtoffers meer maken en zou de verzameling van metagegevens van elektronische communicatie niet nodig zijn).

75. De aanvrager antwoordde in eerste instantie het volgende (vrije vertaling): "*Het CCB* ***beschikt niet over de bevoegdheid om ISP's te gelasten*** *het inkomende en/of uitgaande verkeer van C2-servers*

te blokkeren, noch om dergelijke servers in beslag te laten nemen. ***De enige mogelijkheid voor het CCB is dus om zo snel mogelijk metagegevens te verzamelen, deze te analyseren, de verantwoordelijken voor de betrokken informatiesystemen te identificeren en hen te informeren.***" De Autoriteit heeft het CCB (nationaal CSIRT) hierover opnieuw meer in detail bevraagd om bevestiging te krijgen dat het niet beschikt over wettelijke middelen[46] om de betrokken IP-adressen door ISP's te laten blokkeren. Hij antwoordde het volgende (vrije vertaling):

> "*Zoals aangegeven, heeft het CCB niet de bevoegdheid om ISP's te gelasten het inkomende en/of uitgaande verkeer van C2-servers te blokkeren, noch om dergelijke servers in beslag te laten nemen (zeker niet wanneer deze in het buitenland gevestigd zijn). De enige mogelijkheid voor het CCB is dus om zo snel mogelijk metagegevens te verzamelen, deze te analyseren, de verantwoordelijken voor de betrokken informatiesystemen te identificeren en hen te informeren.*
>
> *Een vrijwillige filtering/blokkering door een ISP zou afhangen van de bereidwilligheid van elke operator, van de middelen waarover hij beschikt, en van de verenigbaarheid van een dergelijke maatregel met zijn wettelijke/contractuele verplichtingen.* ***Een dergelijke blokkering/filtering zou weliswaar nieuwe slachtoffers kunnen voorkomen, maar zou niet noodzakelijkerwijs betekenen dat bestaande potentiële slachtoffers****, dat wil zeggen entiteiten/natuurlijke personen die al interactie hebben gehad met de betrokken server,* ***worden gewaarschuwd****. Gelet op het bovenstaande blijft het voorgestelde project de enige doeltreffende en evenredige maatregel om de slachtoffers te informeren*";
>
> "*Krachtens artikel 29 van het Wetboek van Strafvordering is elke ambtenaar die in de uitoefening van zijn ambt kennis krijgt van een misdaad of van een wanbedrijf, verplicht daarvan dadelijk bericht te geven aan de procureur des Konings en hem alle desbetreffende informatie te doen toekomen.* ***Wij kunnen ons echter niet uitspreken over wat er gebeurt met dergelijke aangiften bij het Openbaar Ministerie (dat volledig onafhankelijk en volgens zijn eigen vervolgingsprioriteiten handelt), en nog***

[46] In dit verband:

- Wat indien een ISP vrijwillig tot filtering/blokkering overgaat zodra het CCB (nationaal CSIRT) hem het IP-adres van een C2-server meedeelt?;
- Wat met de inschakeling van de gerechtelijke autoriteiten met het oog op de filtering/blokkering van IP-adressen van C2-servers (bijvoorbeeld artikel 39*bis*, § 1, van het Wetboek van Strafvordering)?;
- Wat met de mededeling van de lijsten met C2-servers aan de ADIV in het kader van de bevoegdheid waarover hij beschikt krachtens artikel 11, § 1, 2°/1, van de wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdiensten*?;

Met andere woorden, in het licht van het doeleinde van het project (het voorkomen van schade en van de betrokken inbreuken), worden sommige van deze maatregelen in het kader van het project overwogen, en zo ja, wanneer?

En ten slotte: wat met een evolutie in de wetgeving zoals artikel XVII.34/1 e.v. van het WER, *mutatis mutandis* aangepast aan de context van het CCB (zie ook artikel 9 van Verordening (EU) 2022/2065)?

minder over de beslissing om IP-adressen al dan niet te blokkeren/filteren of om de gerechtelijke autoriteiten in te schakelen met het oog op het filteren/blokkeren van IP-adressen van C2-servers *(bijvoorbeeld artikel 39bis, § 1, Wetboek van Strafvordering)*";

[redacted]

"*Bij een mededeling van informatie* ***zijn de doeleinden van de eventuele gegevensverwerkingen door de ADIV verschillend*** *(en zijn de mogelijkheden om informatie te delen niet dezelfde als die van het CCB)*";

"*Zie hierboven. In elk geval blijft artikel 29 van het Wetboek van Strafvordering van toepassing op het CCB.*
De waarschuwing van het slachtoffer door het CCB staat de toepassing van dit artikel niet in de weg";

"*Gelet op de context en de zeer dynamische en snelle activiteiten van C2-servers,* ***lijken deze gerechtelijke procedures moeilijk toepasbaar op de situatie die door het project wordt beoogd***." (in vet aangeduid door de Autoriteit)

76. De Autoriteit neemt akte van deze uitleg en formuleert daarover de volgende opmerkingen. Ten eerste blijft de mededeling aan de gerechtelijke autoriteiten van de in het kader van het project vastgestelde ongeoorloofde activiteiten van C2-servers in ieder geval relevant, en kan het strafrechtelijk beleid ter zake bovendien evolueren. Ten tweede is het weliswaar zo dat de ADIV en, ruimer, de inlichtingen- en veiligheidsdiensten andere doeleinden nastreven, maar dat neemt niet weg dat sommige van de in de aanvullende nota genoemde dreigingen ook onder de bevoegdheid van deze diensten kunnen vallen. Ten derde, wat betreft een mogelijke evolutie in de wetgeving die, *mutatis mutandis*, geïnspireerd zou zijn op artikel XVII.34/1 e.v. van het WER, binnen de normatieve context van het CCB (nationaal CSIRT), wijst de Autoriteit de aanvrager erop dat een vordering in kort geding op eenzijdig verzoekschrift mogelijk al binnen enkele dagen resultaat kan opleveren. Dat een dergelijke gerechtelijke procedure automatisch moeilijk toepasbaar is op de door het project beoogde situatie kan dus niet zonder meer worden aangenomen. Al deze maatregelen kunnen de dreiging doen stoppen, waardoor het door het project nagestreefde doeleinde kan worden bereikt zonder dat metagegevens van elektronische communicatie worden verzameld.

77. Dit gezegd zijnde en op basis van de antwoorden van de aanvrager, deelt de Autoriteit zijn visie dat **het project als zodanig een echte meerwaarde heeft, ongeacht deze maatregelen**.

78. Dit sluit niet uit dat, gelet op het doeleinde ervan[47] en in het licht van de beginselen van doelbinding en evenredigheid (die met name minimale gegevensverwerking opleggen), **het project vereist** dat het CCB (nationaal CSIRT), zodra het beschikt over betrouwbare en door hem gecontroleerde informatie over C2-servers in het kader van het project, **overweegt om gelijktijdig gebruik te maken van de middelen waarover het beschikt. Deze middelen zouden andere bevoegde autoriteiten in staat stellen de IP-adressen van de betrokken C2-servers door de betrokken operatoren te laten blokkeren/filteren**, waardoor wordt voorkomen dat de betreffende dreigingen worden verwezenlijkt. De maatregelen die in dit verband worden getroffen, zijn van dien aard dat zij de verzameling van metagegevens verminderen en vooral dat zij het door het project nagestreefde doeleinde (namelijk het voorkomen van schade bij potentiële slachtoffers) op doeltreffende wijze verwezenlijken, zeker als de betrokken middelen vóór of kort na de identificatie van de betrokken slachtoffers kunnen worden ingezet[48].

Informatie via Cyber Threat Alerts

79. Ten tweede heeft de Autoriteit de aanvrager gevraagd waarom **de IP-adressen van de C2-servers niet zouden kunnen worden meegedeeld via "Cyber Threat Alerts"[49]**, samen met de relevante informatie om zich tegen de daaraan verbonden risico's te beschermen, in plaats van te proberen potentiële slachtoffers te informeren via de verzameling van metagegevens van elektronische communicatie. In dat geval zouden alle betrokken entiteiten automatisch de relevante informatie kunnen ontvangen en beschermingsmaatregelen – en desgevallend onderzoeksmaatregelen – kunnen treffen. Een dergelijke mededeling zou in voorkomend geval kunnen worden gericht aan de doelgroep van de betrokken dreigingen.

80. De aanvrager antwoordde het volgende (vrije vertaling):

> "*De Cyber Threat Alerts-service biedt algemene of gerichte informatie **aan entiteiten (al dan niet NIS2-entiteiten) die zich hebben geregistreerd op het platform van het CCB** SafeOnWeb@Work en die op deze service zijn geabonneerd. Deze service kan echter niet functioneren zonder relevante (meldingen van incidenten, van significante cyberdreigingen, van kwetsbaarheden, enz.) en geïndividualiseerde (lijst van geïnfecteerde IP-adressen, type getroffen informatiesystemen, enz.) informatie.*
>
> ***Om de informatiesystemen te identificeren die het "slachtoffer" zijn** van kwaadaardige activiteiten van C2-servers (door het CCB als dusdanig erkend op basis van*

[47] Zie de overwegingen nrs. 25 en 29.

[48] Deze oplossing houdt bovendien geen uitwisseling van informatie over essentiële of belangrijke entiteiten in (zie het antwoord van de aanvrager, geciteerd in overweging nr. 83, *in fine*).

[49] Zie voetnoot nr. 25 hierboven.

sterke aanwijzingen) ***en om de verantwoordelijken voor deze informatiesystemen te informeren*** *(via de Cyber Threat Alerts-service of een andere vorm van melding),* ***moet het CCB van de ISP's metagegevens verkrijgen over de elektronische communicatie tussen deze C2-servers en andere informatiesystemen. Het doel is om deze slachtoffers in staat te stellen zich te beschermen*** *tegen de kwaadaardige activiteiten die via deze C2-servers worden uitgevoerd.*

De Cyber Threat Alerts-service ***maakt het dus op zichzelf niet mogelijk om de slachtoffers*** *van deze C2-servers* ***te identificeren en te informeren***." (in vet aangeduid en onderstreept door de Autoriteit)

81. De Autoriteit neemt akte van dit antwoord en van het voornemen **om de betrokken slachtoffers specifiek en rechtstreeks te informeren**. Dit gezegd zijnde, **vereist het project**, gelet op het doeleinde ervan en overeenkomstig de beginselen van doelbinding en evenredigheid (met inbegrip van minimale gegevensverwerking), **dat** – voor zover mogelijk (op basis van de informatie waarover het CCB (nationaal CSIRT) beschikt en rekening houdend met de risico's voor de cyberveiligheid) – **wordt overwogen gelijktijdig algemene informatie te verstrekken (niet alleen ter attentie van de betrokken slachtoffers)**, in voorkomend geval uitsluitend ter attentie van de doelgroepen van de betrokken dreigingen, **over de betrokken C2-servers en IP-adressen via "Cyber Threat Alerts"**. Dit is namelijk **een minder ingrijpende manier** (waarbij geen metagegevens van elektronische communicatie moeten worden verzameld) om informatie te verstrekken over de betrokken dreigingen, en dit zodra het CCB (nationaal CSIRT) beschikt over betrouwbare en door hem gevalideerde informatie over C2-servers en hun IP-adressen. Een entiteit die de via een dergelijk kanaal verstrekte informatie ernstig behandelt, kan bovendien sneller interne preventiemaatregelen nemen (een individuele melding komt per definitie later, aangezien daarvoor een voorafgaande machtiging van de Autoriteit vereist is, behalve in dringende gevallen)[50]. In deze context begrijpt de Autoriteit dat de loutere publicatie van lijsten met IP-adressen van de betrokken C2-servers de daders van de betreffende ongeoorloofde activiteiten ertoe kan aanzetten om de getroffen maatregelen ter bestrijding van hun activiteiten gemakkelijker te omzeilen (door zo snel mogelijk andere IP-adressen te gebruiken). Zij begrijpt dat het CCB (nationaal CSIRT) **een beoordelingsmarge moet behouden bij de uitvoering van het project om te zorgen voor een zo goed mogelijk evenwicht tussen een bredere verspreiding van informatie over de aan de betrokken C2-servers toegewezen IP-adressen en specifieke mededelingen aan concrete potentiële slachtoffers**, en dus om te beslissen over het optimale evenwicht dat op het gebied van cyberveiligheid moet worden bereikt, bij de uitvoering van zijn taken in het kader van de NIS2-wet.

[50] Deze oplossing houdt bovendien geen uitwisseling van informatie over essentiële of belangrijke entiteiten in (zie het antwoord van de aanvrager, geciteerd in overweging nr. 83, *in fine*).

II.5.2. Minimale gegevensverwerking

82. Het CCB (nationaal CSIRT) moet de **IP-bereiken** ontvangen **die worden gebruikt door de entiteiten die onder de NIS2-wet vallen (inclusief updates daarvan), evenals hun contactgegevens**[51]. Met andere woorden, het is in principe niet nodig om de operatoren te raadplegen om deze entiteiten vervolgens te identificeren. De Autoriteit heeft de aanvrager gevraagd te preciseren of dit ook het geval zou zijn in het kader van het project. Zij heeft hem bovendien gevraagd waarom niet werd overwogen dat het CCB (nationaal CSIRT) deze IP-bereiken meteen zou meedelen aan de betrokken operator, in het kader van zijn verzoek om metagegevens van elektronische communicatie, zodat de operator rechtstreeks de metagegevens van elektronische communicatie kan filteren die het meest relevant zijn met betrekking tot het toepassingsgebied van de NIS2-wet.

83. De aanvrager antwoordde het volgende (vrije vertaling):

> *"Het CCB kan **inderdaad** aan de hand van de van een ISP ontvangen metagegevens controleren of de informatie overeenkomt met de informatie waarover het beschikt (IP-bereiken van de NIS2-entiteiten), **zonder dat daarvoor** noodzakelijkerwijs **een latere identificatie door een ISP moet worden gevraagd**. Voor de overige IP-adressen blijft identificatie door de elektronische-communicatieoperatoren echter noodzakelijk."*
>
> "*Zoals eerder toegelicht, is de taak bedoeld in artikel 19, § 1, eerste lid, 2°, van de NIS2-wet niet beperkt tot NIS2-entiteiten, maar strekt zij zich ook uit tot de bevoegde autoriteiten en andere relevante belanghebbenden. Uit de bovengenoemde bepaling blijkt dat de taak inzake vroegtijdige waarschuwing van het CCB niet beperkt is tot entiteiten die onderworpen zijn aan cyberbeveiligingsverplichtingen, maar ook geldt voor andere Belgische entiteiten, of het nu gaat om publieke of private entiteiten of om natuurlijke personen.*
>
> *Door enkel de IP-bereiken van NIS2-entiteiten mee te delen, kan het CCB zijn taak inzake vroegtijdige waarschuwing niet volledig vervullen. Bovendien moet het delen van informatie over NIS2-entiteiten worden beperkt tot wat strikt noodzakelijk is, overeenkomstig artikel 26, § 3, van de NIS2-wet.*" (in vet aangeduid door de Autoriteit)

84. De Autoriteit neemt akte van dit antwoord.

II.6. Verwerkingsverantwoordelijken, *accountability* en rechten van de betrokkenen

[51] Zie de artikelen 13 en 14 van de NIS2-wet.

II.6.1. Lijst van C2-servers met contextuele gegevens

85. Het CCB, **dat optreedt als nationaal CSIRT**, is verwerkingsverantwoordelijke voor de persoonsgegevens die in het kader van het project worden verwerkt. **Ook de betrokken ISP is een** volwaardige **verwerkingsverantwoordelijke** met betrekking tot de gegevensverwerkingen die hij uitvoert (uitvoering van een wettelijke verplichting die op hem rust krachtens artikel 21 van de NIS2-wet). Als verwerkingsverantwoordelijke **moet hij dus eveneens toezien op de rechtmatigheid van de gegevensverwerkingen waarvoor hij verantwoordelijk is**.

86. In de nota staat het volgende: "*De*[…] *CCB C2-list wordt* ***zonder context*** *gedeeld met Belgische ISP's samen met een officiële aanvraag tot het delen aan het CCB van meta-data over de communicatie van en naar deze IP-adressen. Enkel de IP-adressen van deze lijst worden door het CCB gedeeld met de ISP's (zonder context),* ***dit bijvoorbeeld om te vermijden dat een ISP direct op hoogte is dat een bepaalde klant slachtoffer is van een specifieke dreigingsactor***." (in vet aangeduid door de Autoriteit) [redacted]

87. De Autoriteit is van mening dat **het weglaten van deze contextuele informatie de operatoren** verhindert te kunnen nagaan of het aan hen gerichte verzoek in overeenstemming is met het toepasselijke normatieve kader. Zij heeft de aanvrager daarom gevraagd welk doel deze beperking dient. Temeer omdat operatoren zelf informatie kunnen inwinnen over dreigingen om hun eigen infrastructuur te beschermen, misschien zelfs via dezelfde private bronnen als die van het CCB (nationaal CSIRT).

88. De aanvrager antwoordde het volgende (vrije vertaling):

> "*In het project wordt gepreciseerd dat de lijst met C2-servers en alle updates, met context, ter beschikking worden gesteld van de GBA in het kader van de controle zoals bedoeld in artikel 21, §§ 2 en 4, van de NIS2-wet, om die controle door de GBA mogelijk te maken. De lijst met C2-servers wordt inderdaad zonder context ter beschikking gesteld van de ISP's. Het doel van dit project is dat het CCB metagegevens van elektronische communicatie analyseert* ***om verdachte communicatie op te sporen*** *en slachtoffers te identificeren.* ***Aangezien het om informatie over slachtoffers gaat, wil het CCB het delen van informatie beperken tot wat strikt noodzakelijk is om de operator in staat te stellen op het verzoek in te gaan.*** *Na de analyse van deze metagegevens wordt de ISP verzocht de identiteit van het slachtoffer in kwestie te verifiëren om deze te kunnen waarschuwen. Het is belangrijk dat het CCB een gestructureerde procedure heeft voor het informeren van slachtoffers.*

Bovendien is het CCB ***verplicht om de toegang tot de informatie in het kader van de NIS2-wet te beperken tot de personen die ervan op de hoogte moeten zijn en er toegang tot moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van de NIS2-wet*** *(artikel 26, § 3, van de NIS2-wet). Bijgevolg kan bepaalde informatie niet vrijelijk met alle partijen worden gedeeld.* ***Het lijkt er*** *echter* ***niet op dat de elektronische-communicatieoperatoren alle informatie nodig hebben om hun verplichtingen na te komen****.*" (in vet aangeduid door de Autoriteit)

89. Allereerst herhaalt de Autoriteit dat **het verzoek om medewerking van de operatoren aan het project per definitie een uitwisseling van informatie met hen inhoudt**. Als verwerkingsverantwoordelijken zijn zij verplicht toe te zien op de rechtmatigheid van de gegevensverwerkingen die zij uitvoeren krachtens de wettelijke verplichting die op hen rust. Daarnaast zijn de operatoren gehouden samen te werken met andere entiteiten, zoals de gerechtelijke autoriteiten en zelfs de inlichtingen- en veiligheidsdiensten[52]. De omgang met mogelijk bijzonder gevoelige gegevens is dus niet nieuw voor hen, en zij moeten hiervoor de nodige passende technische en organisatorische maatregelen treffen[53]. De Autoriteit is dan ook van mening dat **contextuele gegevens zoals die welke in het kader van deze aanvraag zijn meegedeeld (eerste lijst van C2-servers die door de aanvrager is verstrekt) ten minste ook aan de operatoren moeten worden meegedeeld**. **Hetzelfde geldt, *a fortiori*, in dringende gevallen** wanneer geen voorafgaande machtiging aan de Autoriteit wordt gevraagd en het verzoek om verzameling van metagegevens rechtstreeks aan de betrokken operator wordt gericht.

90. Dit gezegd zijnde, benadrukt de Autoriteit dat deze **contextuele informatie, zoals oorspronkelijk meegedeeld aan de Autoriteit** in het kader van deze aanvraag, **onvoldoende** is **om na te gaan of het verzoek daadwerkelijk onder het toepassingsgebied van het project valt**. Deze informatie is namelijk **hoofdzakelijk stereotiep** en laat niet toe te begrijpen op welke basis de vermelde IP-adressen daadwerkelijk verband houden met een dreiging die onder het project valt. Bijgevolg **kan de Autoriteit op basis daarvan geen controle uitvoeren in het kader van de machtigingsprocedure**.

[redacted]

[52] Zie de artikelen 16/2, 18/7, 18/8 en 18/17 van de wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdiensten*.

[53] Zie in het bijzonder artikel 127/3 van de WEC, dat voorziet in de oprichting bij elke operator van een Coördinatie-cel die belast is met het verstrekken aan de wettelijk bevoegde autoriteiten, op hun verzoek, van de elektronische-communicatiegegevens, en in het bijzonder paragraaf 2 daarvan.

92. De aanvrager heeft eerst aangegeven dat de aanvullende documenten later zouden worden meegedeeld[54]. Vervolgens heeft hij een **aanvullende nota** verstrekt, **waarin met name de context met betrekking tot de vermelde IP-adressen meer in detail werd toegelicht**. Ten slotte heeft hij de door zijn bronnen verstrekte informatie nog concreter geïllustreerd [redacted], met betrekking tot drie categorieën van deze bronnen [redacted]

93. De Autoriteit is van mening dat **elk verzoek om machtiging in het kader van het project, evenals elk verzoek om latere controle in geval van dringendheid, de bewijskrachtige documenten moet bevatten** (**zoals de aanvullende nota**; onverminderd de mogelijkheid voor de Autoriteit om bij latere aanvragen de overlegging te vragen van de documenten op basis waarvan het CCB (nationaal CSIRT) de betrokken IP-adressen identificeert) **op basis waarvan de IP-adressen die aan de C2-servers zijn toegewezen, worden geïdentificeerd als relevant in het kader van het project**. Deze documenten moeten **ook de vreemde landen vermelden** waaruit de betrokken adressen afkomstig zijn (aangezien het project tot deze adressen beperkt is).

94. **In principe zouden** deze stukken **ook aan de operator moeten worden meegedeeld, op zijn verzoek, in het bijzondere geval waarin hij** beschikt over objectieve elementen die de juistheid van de meegedeelde IP-adressen en contextuele gegevens in twijfel trekken. **Dit geldt *a fortiori* ook wanneer in datzelfde geval, omwille van dringendheid**, geen voorafgaande machtiging aan de Autoriteit wordt gevraagd en het verzoek om verzameling van metagegevens rechtstreeks aan de operator wordt gericht.

95. Het kan **echter** niet worden uitgesloten dat de **verstrekking van deze documenten aan de operator wordt beperkt door het toepasselijke recht** (artikel 26, § 3, van de NIS2-wet; onvermijdelijke contractuele verplichting tot vertrouwelijkheid; andere). In dat geval **mag** het CCB (nationaal CSIRT) **deze documenten niet verstrekken en volstaat het om de operatoren mee te delen waarom** ze niet worden verstrekt.

II.6.4. Relaties tussen de operator en de betrokken benadeelde entiteit

96. In de door de aanvrager verstrekte nota staat het volgende: "*Het CCB zal de ISP op de hoogte stellen wanneer het contact opneemt met/of waarschuwing stuurt naar een klant,* ***zodat de ISP een complementaire rol kan spelen in de communicatie en ondersteuning van de klant.*** *Dit zorgt ervoor dat de respons op cyberdreigingen gecoördineerd en effectief is, en voorkomt verwarring of tegenstrijdige informatie tussen de betrokken partijen.* ***De ISP contacteert zijn klant over de vaststelling enkel in overleg met het CCB.*** […] *Wanneer CCB en ISPs (potentiële) slachtoffers*

[redacted]

waarschuwen is het belangrijk hierbij zorgvuldig te werk gaan en via goede informering ***te voorkomen dat klanten overhaast zaken gaan verwijderen of blokkeren, wat zou kunnen leiden tot het verdwijnen van de kwaadaardige infrastructuur (C2) voordat het CCB het incident volledig heeft kunnen onderzoeken***."

97. In dit verband heeft de Autoriteit de aanvrager gevraagd op welke wettelijke basis het CCB (nationaal CSIRT) kan bepalen hoe de operator met de betrokken entiteit communiceert. Bovendien heeft zij hem verzocht te bevestigen dat het incident in kwestie wel degelijk het incident is dat de betrokken entiteit heeft getroffen (ervan uitgaande dat de benadeelde entiteit om tussenkomst van het CCB verzoekt). De aanvrager antwoordde het volgende (vrije vertaling):

> "***Het gaat hier niet om het creëren van een verplichting*** *voor de ISP (om te communiceren met of bijstand te verlenen aan zijn klanten na de melding van het CCB), maar veeleer* ***om op vrijwillige basis een doeltreffende coördinatie*** *tussen de ISP en het CCB* ***te waarborgen*** *bij de communicatie met betrekking tot de beoogde meldingen (of in het kader van eventuele bijstand die de ISP aan de slachtoffers verleent om de door het CCB vastgestelde dreigingen te verhelpen).*" (in vet aangeduid door de Autoriteit)

> "*De passage gebruikt het begrip incident zoals gedefinieerd in artikel 8, 5°, van de NIS2-wet: een gebeurtenis die de beschikbaarheid, authenticiteit, integriteit of vertrouwelijkheid van opgeslagen, verzonden of verwerkte gegevens of van de diensten die worden aangeboden door of toegankelijk zijn via netwerk- en informatiesystemen, in gevaar brengt. De passage* ***heeft betrekking op een mogelijk incident dat het slachtoffer*** *(al dan niet een NIS2-entiteit)* ***heeft ondergaan*** *en dat werd veroorzaakt via een C2-server. In een dergelijk geval* ***kan*** *de verantwoordelijke voor het getroffen systeem* ***al dan niet de bijstand van het CCB inroepen***." (in vet aangeduid door de Autoriteit)

98. De Autoriteit neemt akte van dit antwoord en merkt op dat **de documentatie met betrekking tot het project moet worden aangepast in functie van het antwoord van de aanvrager** (coördinatie met de operator op vrijwillige basis).

II.6.3. Rechten van de betrokkenen

99. De Autoriteit heeft de aanvrager verzocht om, op basis van de normatieve bepalingen die van toepassing zijn op het CCB (nationaal CSIRT), aan te geven of en in hoeverre een betrokkene (in de zin van de AVG) zijn rechten kan uitoefenen op grond van de artikelen 15 (inzage), 16 (rectificatie),

17 (gegevenswissing) en 18 (beperking) van de AVG in het kader van het project[55]. Hij antwoordde het volgende (vrije vertaling): "*Betrokkenen kunnen hun rechten uitoefenen in het kader van het project. De NIS2-wet beperkt, in voorkomend geval, de uitoefening van de rechten van de betrokkenen enkel in het kader van het toezicht op de entiteiten die onderworpen zijn aan de cyberbeveiligingsverplichtingen, wat in dit geval niet aan de orde is.*"

100. Hoewel dit *a priori* niet het geval lijkt te zijn[56], heeft de Autoriteit de aanvrager gevraagd of de betrokkenen het voorwerp kunnen uitmaken van een besluit dat uitsluitend gebaseerd is op een geautomatiseerde verwerking van gegevens zoals bedoeld in artikel 22 van de AVG. De aanvrager antwoordde het volgende (vrije vertaling): "*Het project voorziet niet in besluiten die uitsluitend gebaseerd zijn op een geautomatiseerde verwerking van gegevens. De gegevens zullen worden geanalyseerd en gevalideerd door deskundigen van het CCB.*"

101. De antwoorden op deze vragen blijven relevant, zelfs wanneer de metagegevens betrekking hebben op de elektronische communicatie van een abonnee die een rechtspersoon is. Zodra een incident aan de betrokken entiteit wordt gemeld, kan deze[57] immers binnen haar privénetwerk vaststellen welke informatiesystemen betrokken zijn en mogelijk verband houden met communicatie waarbij haar werknemers of bezoekers betrokken zijn[58], die in voorkomend geval verantwoording moeten afleggen en hun handelingen moeten rechtvaardigen.

102. Wat betreft het recht om bezwaar te maken tegen de verwerking van persoonsgegevens, heeft de aanvrager met name bevestigd dat het mogelijk is om bij het CCB bezwaar te maken en dat de NIS2-wet de uitoefening van de rechten van de betrokkenen in het kader van het project niet beperkt.

II.7. Verdere verwerking van gegevens

103. De Autoriteit heeft de aanvrager verzocht om te identificeren aan welke wettelijke verplichtingen tot gegevensverstrekking (op eigen initiatief of op verzoek) het CCB (nationaal CSIRT) onderworpen is met betrekking tot gegevens waarover het beschikt[59], en om uit te leggen hoe hij deze verplichtingen

---

[55] Zoals voorgelegd aan de Autoriteit, dat wil zeggen wanneer de verzamelde metagegevens betrekking kunnen hebben op andere personen dan essentiële of belangrijke entiteiten.

[56] De NIS2-wet is in principe van toepassing op rechtspersonen. Een melding van het CCB (nationaal CSIRT) zal echter in principe een directe interne impact hebben binnen de betrokken entiteit, die zeker zal trachten de apparaten (en hun gebruikers) te identificeren waarmee de C2-server zou hebben gecommuniceerd.

[57] Of het CCB (nationaal CSIRT) indien zijn bijstand vereist is; of elke entiteit die een onderzoek zou instellen naar het incident binnen het betrokken systeem.

[58] Bijvoorbeeld werknemers die op een phishing-e-mail hebben geklikt, het apparaat van een werknemer van waaruit op frauduleuze wijze gegevens worden ontfutseld, de werknemer wiens login wordt gebruikt om in te loggen op een systeem, enzovoort.

[59] Bijvoorbeeld artikel 29, § 1, van het Wetboek van Strafvordering; artikel 14, tweede lid, van de wet van 30 november 1998 *houdende regeling van de inlichtingen- en veiligheidsdiensten*; beslag door de gerechtelijke autoriteiten, enz.

denkt toe te passen met betrekking tot de gegevens (metagegevens van elektronische communicatie en achteraf verzamelde contact- en identificatiegegevens) die in het kader van het project worden verzameld.

104. Hij antwoordde met name het volgende (vrije vertaling):

> "*Het CCB **overweegt geen andere verwerkingen dan die welke in de projectfiche worden vermeld**. Net als andere overheidsinstanties **is het CCB echter wel onderworpen aan bepaalde wettelijke bepalingen, die in voorkomend geval kunnen leiden tot het delen van informatie met andere autoriteiten** (artikel 29, § 1, van het Wetboek van Strafvordering, artikel 14, tweede lid, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, beslag door de gerechtelijke autoriteiten, enz.).*
>
> *Artikel 25 van de NIS2-wet voorziet in samenwerking op nationaal niveau, waaronder een adequate uitwisseling van informatie over de beveiliging van netwerk- en informatiesystemen. Het betreft samenwerking met het NCCN, de administratieve diensten van de Staat, de administratieve overheden, met inbegrip van de nationale autoriteiten krachtens Verordening (EG) nr. 300/2008 en nr. 2018/1139, de toezichthoudende organen uit hoofde van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, de Nationale Bank van België, de Autoriteit voor Financiële Diensten en Markten, het Instituut, de krachtens de wet van 1 juli 2011 bevoegde autoriteiten, de gerechtelijke overheden, de inlichtingen- en veiligheidsdiensten bedoeld in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, de politiediensten bedoeld in de wet van 7 december 1998 tot organisatie van een geïntegreerde politiedienst, gestructureerd op twee niveaus, en de gegevensbeschermingsautoriteiten. Het CCB heeft een coördinatie- en evaluatieplatform opgericht dat de bevoegde autoriteiten (artikel 15 van de NIS2-wet) en het NCCN toelaat informatie uit te wisselen en hun optreden in het kader van de uitvoering van de NIS2-wet op elkaar af te stemmen.*
>
> *Bovendien is het CCB verplicht om de toegang tot de informatie in het kader van de NIS2-wet te beperken tot de personen die ervan op de hoogte moeten zijn en er toegang tot moeten hebben voor de uitoefening van hun functie of opdracht die verband houdt met de uitvoering van de NIS2-wet. Bijgevolg kan bepaalde informatie niet vrijelijk worden gedeeld met alle partijen.*" (in vet aangeduid en onderstreept door de Autoriteit)
>
> […]."

105. De Autoriteit herinnert er vooreerst aan dat de normatieve bepalingen die de bij haar ingediende machtigingsaanvraag regelen, in het bijzonder artikel 21, § 4, van de NIS2-wet en artikel 23, § 3, van de WOG, een **specifiek normatief dispositief** vormen (een *lex specialis* en bovendien een *lex posterior*) **voor de toegang tot metagegevens van elektronische communicatie die door de operatoren worden verwerkt**. De in het kader van het project verzamelde metagegevens **mogen** met andere woorden **niet verder worden verwerkt voor andere doeleinden dan die welke door het project worden beoogd** (met inbegrip van uiteraard de verwerkingen in verband met de toepassing van de rechtsregels die op het project zelf van toepassing zijn). Elke verdere verwerking voor andere doeleinden zou in strijd zijn met de Belgische wetgeving inzake de toegang tot metagegevens van elektronische communicatie die door de operatoren in het kader van hun activiteiten worden verwerkt[60].

106. Voorts is het CCB naar Belgisch recht de nationale autoriteit zoals bedoeld in artikel 16 van de NIS2-wet[61], en vervult het op grond van deze bepaling "*de taken van bevoegde autoriteit voor essentiële en belangrijke entiteiten, van nationaal CSIRT, van centraal nationaal contactpunt voor de uitvoering van deze wet, en vertegenwoordigt zij België in de samenwerkingsgroep, het CSIRT-netwerk en het Europees netwerk van verbindingsorganisaties voor cybercrises (EU-CyCLONe) bedoeld in artikel 16 van de NIS2-richtlijn*". Overweging nr. 41 van de NIS2-richtlijn bepaalt het volgende: "*Om de vertrouwensrelatie tussen de entiteiten en de CSIRT's te versterken, moeten de lidstaten, indien een CSIRT deel uitmaakt van een bevoegde autoriteit, een* ***functionele scheiding*** *kunnen overwegen* ***tussen de operationele taken van de CSIRT's****, met name met betrekking tot de aan de entiteiten verleende informatie-uitwisseling en bijstand,* ***en de toezichtsactiviteiten van de bevoegde autoriteiten****.*" (in vet aangeduid door de Autoriteit) De Autoriteit heeft de aanvrager gevraagd welke maatregelen in dit verband binnen het CCB zijn getroffen.

107. De aanvrager heeft een antwoord gegeven waarin hij voornamelijk de nadruk legde op de onafhankelijkheid van de inspectiedienst van het CCB[62].

---

[60] Zie in dezelfde zin (verleende) machtiging nr. 001/2024 van 6 november 2024 *betreffende een machtigingsaanvraag zoals bedoeld in artikel 15, § 2, tweede lid, van de wet van 17 januari 2003 met betrekking tot het statuut van de regulator van de Belgische post- en telecommunicatiesector (AH-2024-0010)*, overweging nr. 76.

[61] Zie artikel 16, tweede lid, van de NIS2-wet en artikel 3, § 1, van het koninklijk besluit van 9 juni 2024 *tot uitvoering van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid*.

[62] "*Het CCB maakt het voorwerp uit van een functionele scheiding tussen de inspectiedienst van het CCB (NCCA) en de andere diensten (met name CERT en CyTRIS, die voornamelijk de taken van nationaal CSIRT vervullen). In het kader van de uitvoering van de wet van 20 juli 2022 inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit (CSA-wet) heeft het CCB namelijk een eigen inspectiedienst (NCCA) gekregen. Deze inspectiedienst is belast met het toezicht op de NIS2-wet. Verschillende wettelijke bepalingen waarborgen de onafhankelijkheid van deze dienst in het kader van zijn inspectietaken.*

Overeenkomstig artikel 58, § 4, van Verordening (EU) 2019/881, artikel 13 van bovengenoemde wet van 20 juli 2022 en artikel 3ter, §§ 2 en 3, van het koninklijk besluit van 10 oktober 2014 tot oprichting van het Centrum voor Cybersecurity België, vervult de inspectiedienst zijn opdrachten volledig onafhankelijk van de overige diensten van het CCB en van andere publieke of private entiteiten. Daartoe beschikt hij over een eigen directeur.

108. Wat mogelijke **verdere verwerkingen van gegevens door het CCB zelf** betreft, heeft de Autoriteit de aanvrager gevraagd of het CCB, op basis van de bevoegdheden die het overigens krachtens de NIS2-wet geniet, een dwangmaatregel tegen het betrokken potentiële slachtoffer overweegt. Meer bepaald heeft de Autoriteit hem verzocht te bevestigen dat het CCB geen verdere verwerking van de in het kader van het project verzamelde metagegevens en identificatiegegevens overweegt, ongeacht zijn functie. De aanvrager antwoordde het volgende (vrije vertaling):

> "*Het CCB heeft enkel de bevoegdheid om een dwangmaatregel op te leggen aan het betrokken slachtoffer wanneer dit een essentiële of belangrijke NIS2-entiteit is (in het kader van zijn inspectietaken).*"
>
> "*Alleen de hierboven genoemde verwerkingen (het informeren van verantwoordelijken van getroffen systemen en het onderzoeken van problemen bij informatiesystemen) die door het CCB worden uitgevoerd, zijn voorzien in het kader van dit project.*"

109. Toen het CCB (nationaal CSIRT) opnieuw werd bevraagd over de zojuist genoemde onderwerpen[63], antwoordde het met name als volgt (vrije vertaling):

> "[...] *In het kader van de beoogde procedure* ***behoren de leden van de inspectiedienst niet tot de personeelsleden die toegang hebben tot de door de ISP's verstrekte metagegevens van communicatie en identificatiegegevens*** *(zij zullen dus geen toegangsrechten hebben tot deze bestanden en de daaraan toegewezen informatiesystemen).*" (in vet aangeduid door de Autoriteit);
>
> "*De in het kader van het project beoogde verwerkingen hebben niet tot doel de eventuele betrokken NIS2-entiteiten te controleren of te sanctioneren, maar zijn veeleer bedoeld* ***om***

Krachtens artikel 47, § 2, van de NIS2-wet mogen de leden van de inspectiedienst van de nationale cyberbeveiligingsautoriteit en van de eventuele bevoegde sectorale overheid of sectorale inspectiedienst en de experten die deelnemen aan de inspectie, geen enkel rechtstreeks of onrechtstreeks belang hebben in de ondernemingen of instellingen waarvoor zij met het toezicht belast zijn, waardoor hun objectiviteit in het gedrang zou kunnen komen.

Overeenkomstig artikel 64 van de NIS2-wet is de inspectiedienst van de nationale cyberbeveiligingsautoriteit of, in voorkomend geval, de sectorale inspectiedienst die door de Koning is aangewezen voor de overheidssector, bij de uitvoering van zijn toezichthoudende taken operationeel onafhankelijk van de overheidsinstanties waarop hij toezicht houdt." (vrije vertaling)

[63] Meer bepaald heeft de Autoriteit de volgende twee aanvullende vragen gesteld (vrije vertaling):

Er wordt weliswaar melding gemaakt van de volledige onafhankelijkheid van de inspectiedienst, maar hoe zit het met het (nationale) CSIRT? Kan de inspectiedienst de gegevens die door het CSIRT in het kader van het project worden verwerkt, verzamelen voor eigen doeleinden? Of bestaat er in het kader van het project een *Chinese wall* tussen het nationale CSIRT en de NCCA?

De aanvrager werd verzocht te bevestigen dat de in het kader van het project en de latere ontwikkelingen verzamelde gegevens niet door het CCB zullen worden verwerkt met het oog op controle of sanctionering van de betrokken entiteiten. Het CCB (inspectiedienst of andere) zal bijvoorbeeld niet controleren of de in het kader van het project geïnformeerde entiteiten al dan niet een melding bij het CCB hebben ingediend.

hen te helpen dreigingen in hun netwerken te identificeren en incidenten sneller te mitigeren/voorkomen*. De inspectiedienst van het CCB zal standaard geen toegang hebben tot deze gegevens (zie bovenstaand antwoord).*

Echter, de CERT- of CyTRIS-diensten van het CCB kunnen, indien een NIS2-entiteit niet binnen een redelijke termijn reageert (na ontvangst van een melding), besluiten om bepaalde beperkte informatie door te geven aan de inspectiedienst *(naam van de entiteit, betrokken sector, geïdentificeerde dreiging, datum van de melding – zonder andere elementen of gegevens).* ***Deze zou dan contact kunnen opnemen met de entiteit om haar aan te moedigen de nodige maatregelen te treffen om haar informatiesystemen te beschermen*** *(eventueel op dwingende wijze).*

Er zij echter op gewezen dat het feit dat men slachtoffer is van een C2-server niet noodzakelijkerwijs betekent dat er sprake is van een inbreuk op de cyberbeveiligingsverplichtingen of de verplichtingen tot melding van significante incidenten die voortvloeien uit de NIS2-wet." (in vet aangeduid door de Autoriteit)

110. De Autoriteit neemt akte van dit antwoord, maar benadrukt dat zij niet inziet waarom de inspectiedienst zou moeten tussenkomen in het kader van het project. **Er dient te worden opgemerkt dat de NIS2-wet geen specifieke verplichting oplegt aan degene** (slachtoffer of andere) **die een melding ontvangt** (en het project doet dat overigens evenmin) **om te antwoorden op de mededeling die hem wordt toegestuurd**. Weliswaar **is het**, zoals eerder werd vermeld (overweging nr. 26), afhankelijk van het geval **mogelijk dat de betrokken essentiële of belangrijke entiteit**, naar aanleiding van de door het CCB (nationaal CSIRT) ontvangen mededeling, **verplicht is om overeenkomstig de NIS2-wet een incidentmelding te doen**. Maar dat betreft een andere hypothese dan die waarbij men verplicht zou zijn om een "antwoord" te geven op een melding die wordt ontvangen in het kader van het project. **In ieder geval begrijpt de Autoriteit niet waarom, gelet op het doeleinde van het project** (dat geen controledoeleinde is), **het CCB als nationaal CSIRT** niet zelf zou kunnen zorgen voor een aangepaste communicatie naar de betrokken slachtoffers, om hen aan te moedigen de nodige maatregelen te treffen (en desgevallend een beroep te doen op zijn bijstand), zelfs als dat betekent dat er meerdere keren contact met hen moet worden opgenomen.

II.8. Bewaartermijn van de gegevens

111. In de verstrekte nota staat het volgende: "*CCB slaat de ontvangen data beveiligd op voor maximaal 1 jaar, dit om* ***grondige analyses*** *te kunnen maken over meerdere gegevens*." (in vet aangeduid door de Autoriteit) De GEB vermeldt dat de gegevens zullen worden bewaard "*tot het einde van het*

onderzoek en de waarschuwing van de slachtoffers ***en*** *tot maximaal één jaar vanaf de verzameling*" (in vet aangeduid door de Autoriteit; vrije vertaling). Aangezien de Autoriteit niet inziet waarom de metagegevens van elektronische communicatie langer zouden moeten worden bewaard dan noodzakelijk voor het onderzoek en de waarschuwing van de slachtoffers, namelijk tot maximaal één jaar[64], heeft zij de aanvrager verzocht de eerste antwoorden te concretiseren om de noodzaak van de beoogde bewaring te verduidelijken.

112. De aanvrager antwoordde het volgende (vrije vertaling):

> "*Het is de bedoeling dat de gegevens worden bewaard gedurende de tijd die nodig is voor de verwerking (informatie en analyse), dat wil zeggen tot het einde van het onderzoek en de waarschuwing van de slachtoffers, en tot* ***maximaal*** *één jaar vanaf de initiële verzameling.* ***Ze zullen uiterlijk bij het verstrijken van deze termijn worden verwijderd, onverminderd de onderzoeksresultaten en de rapporten die door het CCB zullen zijn opgesteld in het kader van de onderzoeken naar de C2-servers die zijn gestart na de vaststelling van communicatie tussen deze servers en slachtoffers.***
>
> *Deze termijn moet het CCB in staat stellen om gedurende een redelijke termijn de informatie over de activiteiten van de verschillende C2-servers op zinvolle wijze te kruisen (analyse van de dreiging en de ontwikkeling ervan in de tijd). Deze termijn stelt het CCB eveneens in staat om, indien nodig, de uitgevoerde verwerkingen te kunnen aantonen en rechtvaardigen (accountability AVG en gemeenrechtelijke aansprakelijkheidsregels).*" (vetgedrukte opmaak gewijzigd door de Autoriteit en onderstreept door de Autoriteit)

113. In het licht van deze toelichting is de Autoriteit van mening dat de verzamelde metagegevens kunnen worden **bewaard tot het einde van het onderzoek en de waarschuwing van de slachtoffers, en tot maximaal één jaar vanaf de initiële verzameling, om de informatie over de activiteiten van de verschillende C2-servers op zinvolle wijze te kruisen (analyse van de dreiging en de ontwikkeling ervan in de tijd) en met het oog op *accountability***.

114. Deze bewaartermijn kan **echter <u>niet</u> gelden** "*onverminderd de onderzoeksresultaten en de rapporten die door het CCB zullen zijn opgesteld in het kader van de onderzoeken naar de C2-servers die zijn gestart na de vaststelling van communicatie tussen deze servers en slachtoffers*" (vrije vertaling). Ten eerste ziet de Autoriteit geen concreet scenario (noch doeleinde) voor deze gegevensverwerking, dat niet werd vermeld in de oorspronkelijke aanvraag aan de Autoriteit en de bijgevoegde nota. Ten tweede herinnert de Autoriteit eraan dat het doeleinde van het project bestaat

[64] Zeker omdat de metagegevens door de betrokken operatoren moeten worden meegedeeld zolang de betrokken C2-server actief is.

in het waarschuwen van slachtoffers teneinde de verwezenlijking van de betrokken dreiging te voorkomen (met inbegrip van het uitvoeren van de daartoe noodzakelijke analyses), en benadrukt zij in ieder geval dat zowel de NIS2-wet als de WOG de machtigingsbevoegdheid van de Autoriteit beperken tot niet-strafrechtelijke doeleinden.

II.9. Beslissing

OM DEZE REDENEN,
beslist de Autoriteit, binnen de grenzen zoals vermeld in de overwegingen nrs. 12-17, het volgende:

1. De aanvrager moet de Autoriteit binnen 10 werkdagen vanaf de kennisgeving van deze beslissing (de datum van verzending van de e-mail van de Autoriteit aan de aanvrager geldt als bewijs) duidelijk aangeven welke passages van haar beslissing volgens hem niet mogen worden gepubliceerd om de door hem aangevoerde redenen (**overwegingen nrs. 6-11**);

2. Elk concreet verzoek om toestemming voor toegang tot metagegevens van elektronische communicatie bij een operator moet vooraf ter goedkeuring worden voorgelegd aan de Autoriteit. Dit sluit niet uit dat daaropvolgende verzoeken om machtiging of om latere controle in dringende gevallen kunnen verwijzen naar deze beslissing, mits zij verder uitvoerig gemotiveerd blijven.

Aangezien het om een eerste aanvraag in het kader van het specifieke project van de aanvrager gaat, staat de Autoriteit positief tegenover de door hem gevolgde aanpak om haar een voorafgaande machtiging te vragen, in plaats van – ervan uitgaande dat in het kader van zijn aanvraag een beroep op dringendheid zou kunnen worden gedaan – de Autoriteit voor een voldongen feit te plaatsen in een situatie van latere controle (**overwegingen nrs. 18-24**);

3. Het project steunt op artikel 19, § 1, 2°, van de NIS2-wet. Het betreft het verspreiden van meldingen en informatie over cyberdreigingen en kwetsbaarheden onder de betrokken entiteiten en personen die potentieel slachtoffer zijn, nadat de daarvoor nodige analyse- en opsporingswerkzaamheden zijn uitgevoerd (**overwegingen nrs. 25-29**);

4. In elk verzoek om voorafgaande machtiging moet(en) de operator(en) worden vermeld waarop de machtigingsaanvraag betrekking heeft (**overwegingen nrs. 33-36**);

5. Het project kan betrekking hebben op de metagegevens van elektronische communicatie tussen de C2-servers en de essentiële of belangrijke entiteiten waarop de NIS2-wet van toepassing is, alsook op de metagegevens van elektronische communicatie tussen deze C2-servers en andere entiteiten (**overwegingen nrs. 37-44**).

Wat deze andere entiteiten betreft, is de Autoriteit echter van mening dat deze interpretatie van de NIS2-wet op korte termijn door de wetgever moet worden bevestigd, hetzij door een interpretatieve wet, hetzij door een wijziging van de NIS2-wet, om met name de rechtszekerheid van de uitgevoerde gegevensverwerkingen te waarborgen. Het komt het CCB toe om in dit verband de nodige stappen te ondernemen, en de Autoriteit zal hierop letten in het kader van toekomstige verzoeken om machtiging (of latere controle) (**overweging nr. 45**);

6. Volgens de door de aanvrager verstrekte informatie gebeurt de identificatie van een slachtoffer op basis van verschillende elementen: [redacted] (**overwegingen nrs. 46-**Error! Reference source not found.);

7. De verzameling van bronnen voor de identificatie van IP-adressen die door de aanvrager worden vermeld in het kader van het project, moet in overeenstemming zijn met de NIS2-wet. Bovendien vereist het project de invoering van een doeltreffend proces voor de controle van de kwaliteit van de informatie over C2-servers die door al deze bronnen wordt verstrekt, en dus ook van het feit dat de betrokken IP-adressen daadwerkelijk bestemd zijn voor het verkeer van C2-servers die zijn geselecteerd op basis van de ernst van de impact van hun activiteiten. Dit proces moet de relevante combinaties van technische maatregelen omvatten die zijn opgenomen in de aanvullende nota van de aanvrager, alsmede, indien van toepassing, alle andere extra maatregelen die volgens de stand van de techniek op dit gebied vereist zijn. Ten slotte moet de aanvrager het betrouwbaarheidsniveau van de informatiebronnen, diensten en dienstverleners waarop hij in het kader van de uitvoering van het project een beroep doet, beoordelen en aangeven. Deze processen en de uitvoering ervan moeten worden gedocumenteerd overeenkomstig het beginsel van *accountability* (**overwegingen nrs. 52-61**);

8. Het project vereist de invoering van een doeltreffend proces dat ten minste dagelijks plaatsvindt om te controleren of de IP-adressen van de betrokken C2-servers actueel zijn (indien nodig vaker, indien de stand van de techniek dit toelaat en vereist), op basis van de in de overwegingen nrs. 57 en 59 bedoelde controlemaatregelen. Dit proces en de uitvoering ervan moeten worden gedocumenteerd overeenkomstig het beginsel van *accountability* (**overwegingen nrs. 62-66**);

9. Het project vereist dat zodra het CCB (nationaal CSIRT) de vaststelling maakt dat een IP-adres niet langer gekoppeld is aan de betrokken C2-server, de betrokken operator hiervan onmiddellijk in kennis wordt gesteld via een passend kanaal en vanaf dat moment stopt met het verzamelen van metagegevens met betrekking tot het verkeer van en naar het betrokken adres. Het project moet ook voorzien in een doeltreffende kennisgevingsprocedure ter attentie van het CCB (nationaal CSIRT) wanneer de betrokken operator over objectieve elementen beschikt die de juistheid van de betrokken gegevens in twijfel trekken. De Autoriteit moet op de hoogte worden gebracht van de updates die in dit verband aan de lijst van C2-servers worden aangebracht, bij het volgende verzoek om machtiging (of latere controle) dat haar in het kader van het project wordt voorgelegd (**overwegingen nrs. 67-70**);

10. Ondanks de echte meerwaarde van het project, vereist het dat het CCB (nationaal CSIRT) overweegt om gelijktijdig gebruik te maken van de middelen waarover het beschikt. Deze middelen zouden andere autoriteiten in staat stellen de IP-adressen van de betrokken C2-servers door de betrokken operatoren te laten blokkeren/filteren, waardoor wordt voorkomen dat de betreffende dreigingen worden verwezenlijkt (**overwegingen nrs. 73-77**);

11. Gelet op het doeleinde ervan en overeenkomstig de beginselen van doelbinding en evenredigheid (met inbegrip van minimale gegevensverwerking) vereist het project dat – voor zover mogelijk (op basis van de informatie waarover het CCB (nationaal CSIRT) beschikt en de risico's voor de cyberveiligheid) – wordt overwogen gelijktijdig algemene informatie te verstrekken (niet alleen ter attentie van de betrokken slachtoffers) over de betrokken C2-servers en IP-adressen via "Cyber Threat Alerts" (**overwegingen nrs. 79-81**);

12. Contextuele gegevens zoals die welke in het kader van deze aanvraag zijn meegedeeld (eerste lijst van C2-servers die door de aanvrager is verstrekt) moeten ten minste ook aan de operatoren worden meegedeeld. Hetzelfde geldt, *a fortiori*, in dringende gevallen wanneer geen voorafgaande machtiging aan de Autoriteit wordt gevraagd en het verzoek om verzameling van metagegevens rechtstreeks aan de operatoren wordt gericht (**overwegingen nrs. 85-89**);

13. Elk verzoek om machtiging in het kader van het project, evenals elk verzoek om latere controle in geval van dringendheid, moet de bewijskrachtige documenten bevatten (zoals de aanvullende nota; onverminderd de mogelijkheid voor de Autoriteit om bij latere aanvragen de overlegging te vragen van de documenten op basis waarvan het CCB (nationaal CSIRT) de betrokken IP-adressen identificeert) op basis waarvan de IP-adressen die aan de C2-servers zijn toegewezen, worden geïdentificeerd als relevant in het kader van het project. In principe

zouden deze stukken ook aan de operator moeten worden meegedeeld in het bijzondere geval waarin hij beschikt over objectieve elementen die de juistheid van de meegedeelde IP-adressen en contextuele gegevens in twijfel trekken. Dit geldt *a fortiori* ook wanneer in datzelfde geval, omwille van dringendheid, geen voorafgaande machtiging aan de Autoriteit wordt gevraagd en het verzoek om verzameling van metagegevens rechtstreeks aan de operatoren wordt gericht. Tenzij de verstrekking van deze documenten aan de operator wordt beperkt door het toepasselijke recht, wat moet worden gedocumenteerd (**overwegingen nrs. 90-95**);

14. De documentatie met betrekking tot het project moet worden aangepast om weer te geven dat de medewerking van de operator bij de communicatie aan potentiële slachtoffers op vrijwillige basis gebeurt (**overwegingen nrs. 96-98**);

15. In het kader van de uitvoering van het project wordt, overeenkomstig de door de aanvrager verstrekte antwoorden, geen afwijking van de rechten van de betrokkenen overwogen (**overwegingen nrs. 99-102**);

16. De door het CCB (nationaal CSIRT) verzamelde metagegevens van elektronische communicatie mogen niet verder worden verwerkt voor andere doeleinden dan die welke door het project worden beoogd (**overwegingen nrs. 103-110**);

17. De verzamelde metagegevens mogen worden bewaard tot het einde van het onderzoek en de waarschuwing van de slachtoffers, en tot maximaal één jaar vanaf de initiële verzameling, om de informatie over de activiteiten van de verschillende C2-servers op zinvolle wijze te kruisen (analyse van de dreiging en de ontwikkeling ervan in de tijd) en met het oog op *accountability* (**overwegingen nrs. 111-114**);

18. Onder de hierboven en in deze beslissing genoemde voorwaarden en beperkingen is het CCB, dat optreedt als nationaal CSIRT, gemachtigd om bij de operator Belnet de volgende metagegevens van elektronische communicatie te verzamelen: *Source-IP, Destination-IP, Timestamps, Duration, Ports, Protocol, Number of packets, Number of Bytes*, met betrekking tot elektronische communicatie van en naar de 14 IP-adressen die zijn toegewezen aan C2-servers, zoals gecontextualiseerd in de aanvullende nota en opgenomen in de lijst die op 8 juli 2025 door de aanvrager is verstrekt en in de bijlage hierna, vanaf de datum waarop het verzoek om mededeling van deze metagegevens aan Belnet wordt gericht en zolang de betrokken IP-adressen aan de betrokken C2-servers zijn toegewezen;

19. Tegen deze beslissing kan beroep worden aangetekend bij de Raad van State.

Voor de Autorisatie- en Adviesdienst,
(get.) Alexandra Jaspar, directeur