Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

22 112 Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie

Nr. 4018 **BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 april 2025

Overeenkomstig de bestaande afspraken ontvangt u hierbij 4 fiches die werden opgesteld door de werkgroep Beoordeling Nieuwe Commissie voorstellen (BNC).

Fiche: Aanbeveling Blueprint Cyber
Fiche: Mededeling Europees actieplan omtrent kabelveiligheid (Kamerstuk 22 112, nr. 4019)
Fiche: Mededeling Clean Industrial Deal (Kamerstuk 22 112, nr. 4020)
Fiche: Mededeling Actieplan betaalbare energieprijzen (Kamerstuk 22 112, nr. 4021)

De Minister van Buitenlandse Zaken,
C.C.J. Veldkamp

kst-22112-4018
ISSN 0921 - 7371
's-Gravenhage 2025

Fiche: Aanbeveling Blueprint Cyber

1. Algemene gegevens

a) *Titel voorstel*
Voorstel voor een aanbeveling van de Raad voor een EU-blauwdruk voor crisisbeheer op het gebied van cyberbeveiliging
b) *Datum ontvangst Commissiedocument*
24 februari 2025
c) *Nr. Commissiedocument*
COM(2025) 66
d) *EUR-Lex*
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2025:66:FIN
e) *Nr. impact assessment Commissie en Opinie*
Niet opgesteld
f) *Behandelingstraject Raad*
Raad Justitie en Binnenlandse Zaken
g) *Eerstverantwoordelijk ministerie*
Ministerie van Justitie en Veiligheid

2. Essentie voorstel

Op 22 mei 2024 heeft de Europese Raad de Europese Commissie (hierna: de Commissie) opgeroepen om de aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises te herzien.[1] Sinds de publicatie in 2017 zijn er veel ontwikkelingen geweest binnen het cyberdomein, zowel met betrekking tot het beleid, als de dreiging en de opgave waar de EU mee te maken heeft. De Blueprint die in 2017 is uitgebracht is daarmee niet meer toepasbaar op het huidige EU cybercrisisstelsel. Op 24 februari jl. heeft de Commissie het voorstel voor een aanbeveling voor een EU Blueprint voor cybersecuritycrisismanagement (hierna: Blueprint Cyber) gepubliceerd. Deze vernieuwde Blueprint Cyber poogt de huidige uitdagingen en complexe cyberdreigingen aan te pakken, samenwerkingen tussen relevante crisisactoren op EU-niveau te bevorderen en bestaande cybercrisisnetwerken zoals het *European Cyber Crisis Liaison Organisation Network* (hierna: EU-CyCLONe) en het Computer Security Incident Response Teams CSIRTs-Netwerk (hierna: CNW) te versterken. Het herziene document sluit aan bij de bredere EU-aanbevelingen rondom paraatheid, zoals het Niinistö-rapport.[2]

Het doel van de nieuwe Blueprint Cyber is om een duidelijk en toegankelijk kader voor crisismanagement in de EU te bieden, relevante actoren te helpen effectief samen te werken en bestaande mechanismen en initiatieven optimaal te benutten. De Blueprint Cyber bestaat uit twee documenten; het voorstel voor de aanbeveling, bestaande uit acht thema's, en de annex.

In het eerste thema worden het doel en de reikwijdte van de Blueprint Cyber, en de relaties met andere thema's zoals hybride dreigingen, uiteengezet. Vervolgens wordt in het tweede thema ingegaan op de paraatheid op een cybercrisis, waaronder het belang van een gezamenlijk beeld op dreigingen, versterkte samenwerkingen met de private sector en *open-source* gemeenschappen en het opstellen van een continue cyclus van cyberoefeningen. Ook stelt de Commissie voor om vrijwillige samenwerkingsclusters te creëren waarin gemeenschappelijke zorgen kunnen worden gedeeld over afschrikking, detectie en respons op een

[1] COM(2027) 1584
[2] Kabinetsappreciatie Niinistö-rapport: Kamerstuk 33 694, nr. 70. Het Niinistö-rapport kunt u lezen via de website van de Commissie: 5bb2881f-9e29-42f2-8b77-8739b19d047c_en

bepaald type dreiging. Om de paraatheid verder te verhogen stelt de Commissie voor dat lidstaten en relevante EU-entiteiten een strategie ontwikkelen om diversificatie van Domain Name Systems (DNS-) resolutie te realiseren om de robuustheid hiervan te vergroten.

In het derde thema gaat de aanbeveling in op tijdige detectie van incidenten. Zo stelt de aanbeveling onder andere voor dat er detectiestrategieën geïmplementeerd kunnen worden bij zowel publieke als private partijen en roept de aanbeveling de civiele cybercrisisnetwerken op om procedurele afspraken te maken om coördinatie te waarborgen bij grote incidenten. Ook refereert de aanbeveling naar de landsgrensoverschrijdende cyber hubs en hun potentiële bijdrage aan het gedeeld situationeel bewustzijn. Waar het gaat om cyberincidenten met mogelijke multisectorale impact, raadt de aanbeveling aan dat de Commissie een rol speelt om informatiestromen tussen horizontale en sectorale crisismechanismen te faciliteren.

Vervolgens noemt de aanbeveling de taken en verantwoordelijkheden van actoren die op Unieniveau een rol spelen bij het reageren op een grootschalige cybercrisis. Onder het thema «reageren op een cybercrisis» wordt ook stilgestaan bij de inzet en samenhang van bestaande initiatieven zoals de *EU Cybersecurity Reserve* en de inzet van responsopties zoals handelsverboden op aanhoudende kwaadaardige cyberactiviteiten. Ook spoort de aanbeveling aan om geleerde lessen uit incidenten en oefeningen te borgen. In een zesde thema wordt ingegaan op interoperabele oplossingen voor veilige communicatie tussen EU-entiteiten. De Commissie stelt voor dat EU-cybercrisisactoren voor het eind van 2026 overeenstemming moeten bereiken over veilige communicatiemiddelen. Hiervoor wordt aangespoord om te onderzoeken of gelden uit het *Digital Europe Programme* ingezet kunnen worden om deze communicatiemiddelen in te zetten. Ook gaat de aanbeveling in op het bevorderen van informatiedeling tussen rechtshandhavingsnetwerken en cybersecuritynetwerken.

Tot slot wordt ingegaan op coördinatie met militaire actoren en strategische partners. Zo wordt onder andere aanbevolen dat meer samenwerking gezocht kan worden tussen civiele cybernetwerken en hun militaire tegenhangers om gedeeld situationeel bewustzijn tussen civiele en militaire actoren op te zetten.

De Commissie raadt in dat kader ook aan dat binnen de EU contactpersonen worden aangewezen om EU-NAVO informatiedeling te bewerkstelligen en om een *«joint staff exercise»* te organiseren tussen de EU en de NAVO. Daarnaast stelt de Commissie voor dat lidstaten zowel militaire als civiele cybercrisisnetwerken informeren als ze defensie-initiatieven inzetten. Ten aanzien van strategische partners worden de Hoge Vertegenwoordiger, Commissie en andere Unie-entiteiten opgeroepen om informatiedeling met strategische partners te versterken in het kader van de inzet van de *Cyber Diplomacy Toolbox*.

De annex van de Blueprint Cyber is drieledig. Allereerst wordt middels een diagram de inhoud van de Blueprint Cyber weergegeven. Hierbij wordt op technisch, operationeel en politiek niveau gekeken naar de relevante actoren, de escalatielijnen, het gedeelde situationeel bewustzijn en relevante responsinstrumenten. Ook zijn er verschillende tabellen opgenomen waarbij relevante actoren en hun verantwoordelijkheden worden weergegeven. De annex sluit af met een overzicht van relevante horizontale en verticale crisismechanismen.

3. Nederlandse positie ten aanzien van het voorstel

a) Essentie Nederlands beleid op dit terrein

In de Nederlandse Cybersecuritystrategie 2022–2028 (hierna: NLCS) wordt in vier pijlers de kabinetsbrede inzet voor het realiseren van een digitaal veilige samenleving uiteengezet. In pijler I van de NLCS stelt het kabinet het doel het vermogen van organisaties om te reageren, herstellen en leren van cyberincidenten te vergroten. Om dit te realiseren heeft het kabinet op nationaal niveau al stappen gezet om publiek, private en internationale samenwerkingen ten tijde van grootschalige cybercrises en incidenten te versterken, onder andere door de publicatie van het Landelijk Crisis Plan Digitaal (LCP-D). De afspraken in het LCP-D worden geoefend door middel van de terugkerende grootschalige ISIDOOR cyber-oefening, waarvan de laatste plaatsvond in november 2023. De *lessons learned* van de meest recente ISIDOOR oefening worden meegenomen in de lopende herijking van het LCP-D.

Ook werkt het kabinet aan de implementatie van de nieuwe Europese *Network and Information Security Directive* (hierna: de NIS2-richtlijn) in de Cyberbeveiligingswet (hierna: Cbw). De NIS2-richtlijn heeft als doel om een hoog niveau van cyberbeveiliging bij bedrijven en andere organisaties te bereiken. Deze NIS2-richtlijn beoogt in dit verband door meer Europese harmonisatie verschillen tussen lidstaten weg te nemen. Een van de speerpunten van de Cbw is de meldplicht. Het wetsvoorstel schrijft voor dat essentiële en belangrijke entiteiten significante incidenten binnen 24 uur moeten melden bij het Computer Security Incident Response Team (CSIRT) en de toezichthouder. Het gaat om incidenten die bijvoorbeeld de verlening van de diensten van de organisatie ernstig (kunnen) verstoren. CSIRTs kunnen vervolgens bijstand verlenen. De (sectorspecifieke) drempelwaarden voor het aanmerken van incidenten als significant incident worden nog nader uitgewerkt. Voorbeelden van factoren die incidenten tot een significant incident kunnen maken zijn de omvang van de financiële verliezen voor de betrokken entiteit én de mate van materiële en immateriële schade voor andere (mogelijk) getroffen entiteiten.

Voor het doen van meldingen wordt een centraal meldportaal ingericht door het Nationaal Cyber Security Centrum (NCSC). Dat portaal zal tevens kunnen dienen voor het doen van vrijwillige meldingen door entiteiten van andere dan significante incidenten of van bijna-incidenten.

b) Beoordeling + inzet ten aanzien van dit voorstel

In lijn met de NLCS verwelkomt het kabinet de herziening van de Blueprint Cyber om de samenwerking voor wat betreft de respons op (grootschalige) cyberincidenten verder te bevorderen. Het kabinet ziet daarbij het belang van een praktisch document dat ten tijde van (grootschalige grensoverschrijdende) crises en incidenten in de praktijk effectief kan worden gebruikt. Het kabinet zal in de beoordeling van de verdere uitwerking van de verschillende elementen uit deze aanbeveling goed kijken naar de effectiviteit van de Blueprint Cyber.

Het kabinet staat positief tegenover de verbetering van leesbaarheid van de nieuwe Blueprint Cyber. Het document is overzichtelijker geworden door het opdelen van de aanbevelingen in acht thema's, wat het document tevens handzamer maakt dan voorheen. Ook vindt het kabinet het diagram met de weergave van de verschillende taken en verantwoordelijkheden van de betrokken actoren ten tijde van grootschalige cybercrises een waardevolle toevoeging. Het kabinet hecht daarnaast meerwaarde aan de weergave van cybercrisismanagement in samenhang

met sectoraal en generiek crisismanagement, wat in de nieuwe Blueprint Cyber en de bijlagen al beter naar voren komt.

Het kabinet verwelkomt de uiteenzetting in sectie IV, over hoe er op Unieniveau kan worden gereageerd op een cybercrisis vanuit de verschillende betrokken actoren. Het kabinet hecht waarde aan een praktisch document dat ten tijde van crisis daadwerkelijk door de betrokken actoren zal worden geraadpleegd. Sectie IV vormt daarom een goede basis van een handzame Blueprint Cyber. Het kabinet ziet graag dat de andere secties, waaronder ook de preambules, net zo handzaam worden ingestoken. Zo voldoet de Blueprint Cyber beter aan het doel om een duidelijk en toegankelijk kader voor cybercrisismanagement in de EU te schetsen.

Om ervoor te zorgen dat de Blueprint Cyber een effectief en overzichtelijk document blijft, is het voor het kabinet essentieel dat de Blueprint Cyber zich alleen richt op cybercrisismanagement. De beheersing van incidenten en crises ligt voor een groot deel bij de EU-lidstaten zelf. Pas bij een grootschalig grensoverschrijdend incident wordt er overgegaan op EU-structuren. Het kabinet ziet daarom graag duidelijker opgenomen dat de nationale structuren leidend zijn, zowel in de aanbevelingen als in de diagram in de bijlage.

Het kabinet ziet graag een verduidelijking van hoe de samenhang met horizontale en verticale crisismechanismen wordt gezocht, daar waar cybercrises vaak connecties hebben met verschillende domeinen en sectoren. Het kabinet vindt dat deze samenhang nog niet voldoende naar voren komt en acht het van belang voor het doel van de Blueprint Cyber om relevante actoren te helpen effectief samen te werken en bestaande mechanismen en initiatieven optimaal te benutten.

De aanbeveling gaat ook in op een aantal technische afhankelijkheden, waaronder het domeinnaamsysteem (DNS). Het kabinet steunt de aanbeveling aan beheerders van infrastructuur om middels diversificatie tussen leveranciers voldoende redundantie aan te brengen. Hierbij geldt wel dat er veel andere essentiële diensten zijn die paraatheid van EU-entiteiten kunnen verhogen. Het kabinet is echter van mening dat de Blueprint Cyber niet dit detailniveau moet hanteren. Bovendien ziet deze aanbeveling niet specifiek op cybercrisismanagement.

Het kabinet ondersteunt de aanbeveling voor lidstaten om noodmaatregelen in te stellen wanneer het reguliere telecommunicatienetwerk verstoord is. Het kabinet heeft echter vragen over de inzet van gelden uit het *Digital Europe Programme* van het *European Cyber Competence Centre and Network* (ECCC) voor inzet van veilige communicatiemiddelen. De Blueprint Cyber stelt voor dat het *Digital Europe Programme* lidstaten financieel bijstaat voor de inzet van middelen voor *real-time* communicatie. Het kabinet ziet graag verduidelijking over hoe het *Digital Europe Programme* dit zal financieren omdat er veel beroep wordt gedaan op de gelden binnen dit programma.

Met betrekking tot het diagram in de bijlage ziet het kabinet graag extra verduidelijking op de weergegeven stappen. Het kabinet ziet het diagram als essentieel onderdeel van de Blueprint en ziet de meerwaarde in van een gedetailleerdere beschrijving van stappen en lagen van het diagram, zodat deze ten tijde van grootschalige cybercrises een snelle weergave kan bieden van de uit te lopen stappen voor de verschillende EU-entiteiten. Het kabinet ziet daarnaast graag dat wordt uitgewerkt wat de rollen zijn van de Commissie en van ENISA, het Europees agentschap

voor cybersecurity, ten tijde van een grootschalig grensoverschrijdende cybercrisis.

Tot slot, is het kabinet positief over het benoemen van de EU-NAVO samenwerking en de *Cyber Diplomacy Toolbox* in de Blueprint Cyber. Echter vindt het kabinet dat de aanwezigheid van dit onderdeel in de aanbevelingen kan worden versterkt en geconcretiseerd. Zo zou bijvoorbeeld expliciet benoemd kunnen worden dat de NAVO wordt betrokken bij oefeningen ter voorbereiding op een grootschalige cybercrisis, waarbij uiteraard aandacht wordt behouden voor die EU-lidstaten die niet bij NAVO zijn aangesloten. Daarnaast kan ook worden aangescherpt wat vervolgstappen zijn ten aanzien van de voorgestelde coördinatie en het delen van informatie met militaire actoren ten tijde van crisis.

c) Eerste inschatting van krachtenveld

In algemene zin verwelkomen EU-lidstaten de herziening van Blueprint Cyber gezien er veel ontwikkelingen zijn geweest in recente jaren met impact op het cybercrisisstelsel. Met een steeds omvangrijkere dreiging zien veel EU-lidstaten de toegevoegde waarde van een vernieuwde Blueprint Cyber. De positie van het Europees Parlement is nog onbekend.

4. Grondhouding ten aanzien van bevoegdheid, subsidiariteit, proportionaliteit, financiële gevolgen en gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

a) Bevoegdheid

Het oordeel van het kabinet is positief. De aanbeveling heeft betrekking op de uitwisseling van informatie tussen Unie-entiteiten en lidstaten zoals vastgesteld in Verordening 2023/2841. De aanbeveling is gebaseerd op artikel 292 van het Verdrag betreffende de werking van de Europese Unie (VWEU). Dit artikel geeft de onder andere de Raad de bevoegdheid om aanbevelingen vast te stellen. De aanbeveling heeft betrekking op de ruimte van veiligheid, vrijheid en recht, specifiek de uitwisseling van informatie tussen Unie-entiteiten en lidstaten zoals vastgesteld in Verordening 2023/2841. Op het terrein van de ruimte van vrijheid, veiligheid en recht is sprake van een gedeelde bevoegdheid tussen de EU en lidstaten op grond van artikel 4, lid 2, sub j VWEU.

b) Subsidiariteit

De grondhouding van het kabinet is positief. De aanbeveling heeft tot doel om de paraatheid van de Unie tegen grootschalige cyberincidenten te verhogen. Gezien de potentieel grensoverschrijdende aard van cyberincidenten en hun effect of kritieke informatie-infrastructuren, kan dit onvoldoende door lidstaten op centraal, regionaal of lokaal niveau worden verwezenlijkt. Daarom is een EU-aanpak wel nodig. Door deze aanbeveling kan de samenwerking op Europees niveau met betrekking tot cyberincidenten worden bevorderd. Om die redenen is optreden op het niveau van de EU gerechtvaardigd.

c) Proportionaliteit

De grondhouding van het kabinet is positief. De aanbeveling heeft tot doel om de paraatheid van de Unie tegen grootschalige cyberincidenten te verhogen. Het voorgestelde optreden is geschikt om deze doelstelling te bereiken, nu het een duidelijk en toegankelijk kader biedt voor cybercrisismanagement in de EU en hiermee de relevante actoren helpt samen te werken. Bovendien gaat het voorgestelde optreden ook niet verder dan

noodzakelijk. De Blueprint Cyber schetst immers een beeld van hoe Lidstaten en EU-entiteiten gebruik kunnen maken van bestaande crisismechanismen. Een niet-bindend document is hierbij passend.

d) Financiële gevolgen

Vooralsnog worden er geen directe financiële gevolgen verwacht uit de Blueprint Cyber voor de EU-begroting of Nederland. Wel worden er voorstellen gemaakt voor de toekomstige inzet van *Digital Europe Programme* gelden, bijvoorbeeld ten behoeve van het uitrollen van veilige communicatiemiddelen. Het kabinet is van mening dat de benodigde EU-middelen gevonden dienen te worden binnen de in de Raad afgesproken financiële kaders van de EU-begroting 2021–2027 en dat deze moeten passen bij een prudente ontwikkeling van de jaarbegroting. Het kabinet wil echter niet vooruit lopen op de integrale afweging van middelen na 2027. Eventuele budgettaire gevolgen worden ingepast op de begroting van het/de beleidsverantwoordelijk(e) departement(en), conform de regels van de budgetdiscipline.

e) Gevolgen voor regeldruk, concurrentiekracht en geopolitieke aspecten

Het is in dit stadium nog onduidelijk of de aanbevelingen in de Blueprint gevolgen hebben voor de regeldruk in de lidstaten. Er zijn geen gevolgen voor regeldruk voorzien voor burgers en

het bedrijfsleven/ De Blueprint schetst een beeld van hoe EU-entiteiten en lidstaten met elkaar gebruik kunnen maken van de bestaande crisismechanismen. Het biedt handelingsperspectief en samenwerkingsmogelijkheden in het geval een cybercrisis op Unieniveau plaatsvindt.

Er zijn geen gevolgen voor de concurrentiekracht van de EU. De Blueprint draagt bij aan de weerbaarheid van de EU tegen grootschalige, grensoverschrijdende cybercrises en bevordert samenwerking van crisisactoren op Unie-niveau.