Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

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

Nr. 4089

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 25 juni 2025

De vaste commissie voor Digitale Zaken heeft enkele vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over de brief inzake het «Fiche: Aanbeveling Blueprint Cyber» (Kamerstuk 22 112, nr. 4018).

De vragen en antwoorden zijn op 15 mei 2025 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 25 juni 2025 zijn de vragen beantwoord.

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

kst-22112-4089
ISSN 0921 - 7371
's-Gravenhage 2025

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de PVV-fractie

De leden van de PVV-fractie hebben met interesse kennisgenomen van de stukken op de agenda van het schriftelijk overleg over de Fiche: Aanbeveling Blueprint Cyber (Kamerstuk 22 112-4018). Naar aanleiding hiervan hebben deze leden nog een aantal vragen.

De leden van de PVV-fractie constateren allereerst dat het kabinet benadrukt dat de beheersing van incidenten en crises in eerste instantie bij de lidstaten zelf ligt, en dat pas bij een grootschalig grensoverschrijdend incident wordt overgegaan op EU-structuren. Daarbij stelt het kabinet dat de Blueprint explicieter moet aangeven dat nationale structuren leidend zijn. Wat gaat de Minister doen om ervoor te zorgen dat dit door de Commissie geborgd gaat worden? Komt Nederland eventueel zelf met een voorstel hiertoe?

Daarnaast merken deze leden op dat het kabinet vragen stelt bij de inzet van gelden uit het Digital Europe Programme voor veilige communicatie, en verzoekt om verduidelijking over de wijze waarop dit gefinancierd kan worden binnen de bestaande budgettaire kaders. Is de Minister voornemens opheldering te vragen hoe deze veilige communicatie eruit zou moeten zien? Maakt IRIS2 («Infrastructure for Resilience, Interconnectivity and Security by Satellite») hier onderdeel van uit en hoe verhoudt zich dit tot bijvoorbeeld Starlink?

Ook nemen zij kennis van het feit dat het kabinet positief oordeelt over het niet-bindende karakter van de Blueprint Cyber (hierna ook: Blueprint). Tegelijkertijd spreekt het kabinet de wens uit dat de Blueprint handzaam en effectief in de praktijk wordt toegepast. Kan de Minister bij de implementatie van deze aanbeveling borgen dat dit niet leidt tot toenemende regeldruk? Wordt deze aanbeveling puur als facultatief beleidsinstrument gezien?

Voorts constateren de leden van de PVV-fractie dat het kabinet in de Nederlandse Cybersecuritystrategie inzet op versterking van het Nationaal Cyber Security Centrum (NCSC), onder andere door middel van een centraal meldportaal. Tegelijkertijd krijgt de EU-coördinatie via de Blueprint een nadrukkelijkere rol. Wat betekent de voorgestelde coördinatie op EU-niveau voor de positie, taken en bevoegdheden van het NCSC tijdens een cybercrisis? Moet het NCSC zijn werkwijze aanpassen aan Europese afspraken?

Tevens merken deze leden op dat het kabinet actief werkt aan de implementatie van de NIS2-richtlijn in de Nederlandse Cyberbeveiligingswet (Cbw), waarmee onder andere meldplichten en incidentenclassificatie geregeld zullen worden. Tegelijkertijd noemt de Blueprint aanvullende voorstellen over detectie, meldstrategieën en samenwerking. Hoe

verhoudt de Blueprint Cyber zich tot de NIS2-richtlijn en de Cyberbeveiligingswet? Zijn er tegenstrijdigheden of overlap in meldplichten en procedures?

Vervolgens lezen zij dat onder het thema «reageren op een cybercrisis» ook wordt stilgestaan bij de inzet en samenhang van bestaande initiatieven zoals de inzet van responsopties zoals handelsverboden op aanhoudende kwaadaardige cyberactiviteiten. Hoe verhoudt dit zich tot het huidige beleid, dat bestaat uit het overnemen van internationale sancties nadat de VN-veiligheidsraad hiervoor een resolutie heeft aangenomen en het opleggen van sancties vanuit het Gemeenschappelijk Buitenlands en Veiligheid Beleid van de EU? Hoe kijkt de Minister er tegenaan als hieruit een nieuw sanctiebeleid zou volgen?

Tot slot lezen de leden van de PVV-fractie dat het kabinet graag de betrokkenheid ziet van de NAVO bij oefeningen ter voorbereiding op een grootschalige cybercrisis, waarbij aandacht wordt behouden voor EU-lidstaten die niet bij de NAVO zijn aangesloten. Hoe ziet het kabinet dat voor zich? Wijken deze oefeningen af van «Locked Shields» (een jaarlijks georganiseerde grootschalige cyberoefening)?

Vragen en opmerkingen van de leden van de GroenLinks-PvdA-fractie

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de Blueprint Cyber en het bijbehorende BNC-fiche. Deze leden verwelkomen de stap richting een gecoördineerde EU-strategie voor het voorkomen en verhelpen van cybercrises. Daarvoor zijn harde afspraken nodig over acute zaken zoals de crisisrespons, maar ook het handhaven van standaarden zoals interoperabiliteit. Hierover hebben zij enkele vragen en opmerkingen.

De leden van de GroenLinks-PvdA-fractie benadrukken de noodzaak voor Europese samenwerking ten behoeve van de cyberveiligheid. Deze moet publiek-privaat worden vormgegeven, zodat kennis en kunde wordt uitgewisseld en hier snel op wordt gehandeld. Hierin dienen publieke organisaties een sturende rol te spelen, omdat cyberveiligheid een publiek algemeen belang is. Welke verantwoordelijkheden hebben overheidsorganisaties ten opzichte van private organisaties in de nieuwe Europese samenwerkingen? Kunt u uitleggen wat er in de praktijk verandert met de komst van de Blueprint Cyber? Welke aanvullende verantwoordelijkheden krijgen overheden en bedrijven? Wat verandert er ten opzichte van de huidige situatie en kunt u de voordelen van de maatregelen kwantificeren, bijvoorbeeld in de verwachte reactietijd van lidstaten bij een grootschalige netwerkstoring?

Deze leden willen dat de meest actuele dreigingsinformatie betrouwbaar wordt vormgegeven. Het monitoren van dreigingen ligt verspreid over verschillende publieke en private partijen. Zal de Blueprint leiden tot een intensievere samenwerking binnen bestaande nationale samenwerkingsverbanden, zoals het Nationaal Cyber Security Centrum (NCSC)? Kunt u expliciet maken welke ministeries betrokken zijn en welke nieuwe verantwoordelijkheden van hen worden verwacht? Wat schrijft de Blueprint Cyber voor nieuwe verantwoordelijkheden aan de inlichtingen- en veiligheidsdiensten AIVD en MIVD? Zij vragen u ook om in te gaan op wat de Blueprint voorschrijft op het gebied van informatiedeling tussen de EU en niet-EU partners.

De leden van de GroenLinks-PvdA-fractie steunen de suggestie van een continue cyclus van cyberoefeningen. Cyberaanvallen en -storingen zijn doorgaans abstract, waardoor de paraatheid noch bij burgers, noch de overheid, noch het bedrijfsleven wordt doorleefd. Hoe ziet u een dergelijke cyclus voor zich? Op welke organisaties en infrastructuur zijn deze oefeningen van toepassing? Doen Nederlandse organisaties al mee aan grootschalige cyberoefeningen en, zo ja, wat wordt er met de opgedane lessen gedaan? Via welke kanalen wordt deze informatie gecommuniceerd aan Europese partners en wat gaat de Blueprint Cyber daarin veranderen? Is het doel van de cyberoefeningen ook om het maatschappelijke bewustzijn te vergroten, of enkel om de paraatheid van organisaties te toetsen?

Deze leden steunen de roep om een robuuste en gediversifieerde Domain Name System (DNS)-infrastructuur. De roep om redundantie en soevereiniteit van het DNS geldt volgens hun voor alle onderdelen van onze kritieke digitale infrastructuur. Daarmee hoort het vergroten van de digitale soevereiniteit een expliciet doel te zijn van de Europese cyberveiligheidsagenda. Deelt u de mening dat digitale soevereiniteit onder de Blueprint Cyber moet vallen? Ziet u het tegengaan van de afhankelijkheid van enkele techmonopolies, met name van Amerikaanse en Chinese leveranciers, als onderdeel van de Europese paraatheid en veiligheid? Hoe bevordert de Blueprint dat streven?

De leden van de GroenLinks-PvdA-fractie benadrukken dat weerbaarheid en paraatheid bij uitstek een maatschappelijke opgave is. Het aanjagen van actief burgerschap en sociale cohesie, door bestaande verenigingsstructuren te versterken en nieuwe netwerken op te bouwen, zijn een integraal deel van onze crisisrespons. Alleen door collectief te handelen kan een samenleving dreigingen te lijf gaan. Kunt u meer toelichten over hoe de afspraken uit de Blueprint Cyber worden uitgewerkt samen met civiele cybercrisisnetwerken? Welke netwerken betreft dit, en welke rol hebben maatschappelijke netwerken, zoals kerken, (sport)verenigingen en wijkteams, in de plannen van de Europese Commissie? Vindt u dat de Blueprint op dit punt toereikend is?

Deze leden steunen de komst van veilige, soevereine communicatiemiddelen. Informatiedeling tussen actoren en partners, maar ook de crisiscommunicatie richting burgers, moet in geen enkel geval afhankelijk zijn van systemen die Europa niet zelf in handen heeft. Zij willen meer informatie over de eisen die worden gesteld aan dergelijke communicatiemiddelen, welke alternatieven reeds beschikbaar zijn, en welke oplossingen Nederland te bieden heeft. De leden van de GroenLinks-PvdA-fractie zijn ervan overtuigd dat interoperabiliteit, dataportabiliteit, en soevereiniteitseisen voor alle digitale diensten – met name crisisdiensten – cruciaal zijn. Deze standaarden zouden evengoed moeten gelden voor cloudinfrastructuur, menen zij. Deze standaarden dienen breed te worden nageleefd en dragen direct bij aan de cyberveiligheid van Europa. Deelt u de mening dat er dwingende afspraken moeten worden gemaakt voor deze standaarden voor alle Europese overheidsdiensten en voor het ICT-inkoop en -aanbestedingsbeleid? Bent u bereid om te pleiten voor afdwingbare Europese standaarden voor interoperabiliteit, dataportabiliteit en soevereiniteit?

Deze leden dringen u aan om de Blueprint Cyber te zien als aanzet voor verdere beleidsvorming. Het is van belang dat informatiedeling wordt ingebed met harde afspraken, die voorzien zijn van goede «checks en balances». Data is kostbaar en gevoelig en dient ten strengste beveiligd te zijn. Daartoe vragen zij u om verder te definiëren wat een «significant incident» betekent. Deelt u de mening van deze leden dat incidenten,

waarin informatie van personen wordt buitgemaakt of uitgelekt, ook als «significant» moeten worden aangemerkt? De leden van de GroenLinks-PvdA-fractie vinden de opvatting dat alleen incidenten met grote materiële en immateriële schade voor entiteiten «significant» zijn, te beperkt is.

Deze leden zijn benieuwd naar het vervolg van de Blueprint Cyber. Zij vragen u om aan te geven welke onderdelen van de Blueprint wat u betreft moeten worden doorvertaald in harde afspraken en nieuw beleid. Ook horen zij graag hoe u de aanbevelingen uit de Blueprint proactief aan organisaties en burgers gaat communiceren, en deze zo praktisch mogelijk maakt.

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het BNC-fiche over de Blueprint Cyber. Deze leden verwelkomen de herziening van de Blueprint en delen de noodzaak om het cybersecurity-crisismanagement te herzien. Zij stellen nog enkele vragen over het BNC-Fiche.

De leden van de VVD-fractie vragen naar een nadere toelichting op de inzet van het kabinet ten aanzien van de versterkte publiek-private samenwerking bij de bestaande en nieuwe initiatieven. Hoe wordt deze samenwerking versterkt in de nieuwe Blueprint en maakt het uitwisselen van relevante gegevens hier ook onderdeel van uit?

Deze leden vragen wat de inzet is van het kabinet ten aanzien van de uitwerking van de rollen, taken en bevoegdheden van de Europese Commissie en van ENISA, het Europees agentschap voor cybersecurity.

Zij vragen verder of het kabinet kan nagaan of er een impact assessment zal worden gedaan door de Europese Commissie bij de herziening van de Blueprint, en zo niet, of dat alsnog kan worden gedaan.

Ook vragen de leden van de VVD-fractie of de grootschalige stroom-storing van onlangs in Spanje en Portugal nog nieuwe inzichten heeft opgeleverd, en of het kabinet bereid is te vragen naar de inzichten die deze lidstaten sindsdien hebben opgedaan en welke gevolgen dat heeft voor de gesprekken over de herziening van de Blueprint.

Vragen en opmerkingen van de leden van de NSC-fractie

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van het «Fiche: Aanbeveling Blueprint Cyber». Naar aanleiding hiervan hebben deze leden enkele vragen en opmerkingen.

In het BNC-fiche geeft het kabinet aan: «Het kabinet hecht waarde aan een praktisch document dat ten tijde van crisis daadwerkelijk door de betrokken actoren zal worden geraadpleegd.» De leden van de NSC-fractie vragen hoe het kabinet hier in Nederland invulling aan zou willen geven? Zou dit praktisch document specifiek moeten toezien op cybercrises of betreft het ook andere crises (met al dan niet een digitaal component)? Wat kan daarnaast verwacht worden van individuele burgers?

Het BNC-fiche vermeldt verder: «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 cybercrisis-management.» Deze leden vragen het kabinet om een nadere toelichting op dit standpunt. Hoe ziet het kabinet het onderscheid tussen cybercrisis-

management en andere vormen van crisismanagement, vooral in het licht van hybride dreigingen? Hoe definieert het kabinet een cybercrisis, en is het onderscheid tussen cybercrises en andere crises nog steeds relevant en goed af te bakenen?

Het BNC-fiche stelt ook: «Het kabinet ziet daarom graag duidelijker opgenomen dat de nationale structuren leidend zijn.» De leden van de NSC-fractie steunen deze visie vanuit het perspectief van subsidiariteit, maar hebben vragen over de aansluiting van de Nederlandse nationale structuren op de Blueprint Cyber bij opschaling naar EU-niveau. Gezien het feit dat systemen met elkaar verbonden zijn en incidenten zich over grenzen kunnen verspreiden, willen deze leden weten hoe het kabinet denkt dat deze structuren goed kunnen samenwerken met EU-structuren.

Daarnaast blijkt uit het fiche niet welke instantie de rol van nationaal aanspreekpunt zal krijgen voor EU-crisisstructuren, zoals het «European Cyber Crisis Liaison Organisation Network» (EU-CyCLONe). Zij vragen het kabinet wie zij voor deze rol in Nederland in gedachten heeft.

Tot slot vermeldt het BNC-fiche: «Het kabinet is echter van mening dat de Blueprint Cyber niet dit detailniveau moet hanteren. Bovendien ziet deze aanbeveling niet specifiek op cybercrisismanagement.» De leden van de NSC-fractie verzoeken het kabinet om een nadere toelichting op deze zienswijze. Zien zij geen risico in het ontbreken van expliciete richtlijnen, bijvoorbeeld met betrekking tot DNS-redundantie, die naar hun mening essentieel is? Hoe schat het kabinet het risico in van te grote vrijblijvendheid of te open normen als dergelijke zaken onvoldoende worden uitgewerkt? Welke andere vormen van diversificatie of redundantie acht het kabinet noodzakelijk, waar dit momenteel nog onvoldoende is geregeld?

Gegeven dat de Commissie het belang van veilige cloudinfrastructuur in crisissituaties benadrukt, maar niet definieert wat daaronder valt, vragen deze leden wat het kabinetsstandpunt op dit onderwerp is. Hoe verstrekkend zouden deze eisen moeten zijn als het gaat om cloudaanbieders? Ziet het kabinet daarnaast het belang ervan in dat de EU in het kader van de weerbaarheid bevordert dat er meer vormen van schaalbare cloudopslag beschikbaar zijn waarbij de betreffende data en digitale diensten niet toegankelijk zijn voor niet-Europese inlichtingendiensten en dat deze niet eenvoudig stopgezet kunnen worden door niet-Europese mogendheden?

Vragen en opmerkingen van de leden van de BBB-fractie

De leden van de BBB-fractie hebben kennisgenomen van de aanbeveling Blueprint Cyber, die gericht is op het verbeteren van de EU-brede coördinatie bij grootschalige cybercrises. Hoewel het voorstel op dit moment niet bindend is, achten deze leden het van belang om te benadrukken dat het richtinggevend kan zijn voor toekomstige Europese wet- en regelgeving. In dat licht hebben deze leden enkele opmerkingen en vragen.

Zij sluiten zich aan bij het standpunt van het kabinet dat nationale crisisstructuren, zoals het Landelijk Crisisplan Digitale Veiligheid (LCP-D), leidend moeten blijven in de aanpak van cybercrises. De leden van de BBB-fractie maken zich daarnaast zorgen over het ontbreken van voldoende waarborgen voor de rechtsstaat en fundamentele rechten, met name waar het gaat om informatie-uitwisseling.

Voorts vragen deze leden om een nadere toelichting op het standpunt van het kabinet ten aanzien van vrijwillige aanbevelingen die mogelijk kunnen leiden tot verplichte datalokalisatie of de uitsluiting van niet-EU cloudproviders. Waarom verzet het kabinet zich tegen deze aanbevelingen, ondanks hun niet-bindende karakter?

De leden van de BBB-fractie onderschrijven de zorgen van het kabinet over het gebrek aan duidelijke prioritering voor acute crisisrespons binnen het voorgestelde financieringskader. Hoewel het voorstel formeel niet juridisch bindend is, rijst de vraag hoe groot de kans is dat de Blueprint op termijn alsnog zal uitmonden in bindende regelgeving. Op welke onderdelen zou dat volgens het kabinet met name het geval kunnen zijn? Denk hierbij aan domeinen zoals kunstmatige intelligentie, cloudbeveiliging en crisiscommunicatie.

Deze leden willen daarnaast weten op welke wijze het kabinet waarborgt dat nationale crisisstructuren daadwerkelijk de regie behouden wanneer de EU-coördinatie bij een cybercrisis wordt opgeschaald. Ook vragen zij hoe wordt voorkomen dat besluitvorming op Europees niveau ten koste gaat van nationale autonomie in crisissituaties.

Met betrekking tot de paragraaf over civiel-militaire samenwerking en de rechtsstatelijke aspecten daarvan vragen de leden van de BBB-fractie welke juridische en ethische kaders het kabinet voor ogen heeft bij informatie-uitwisseling tussen civiele en militaire actoren binnen het kader van de Blueprint. Tevens willen deze leden weten op welke wijze parlementaire betrokkenheid en democratische controle op dergelijke samenwerking worden geborgd.

Tot slot vragen zij waarom het kabinet van mening is dat de aanbeveling over DNS-diversificatie niet thuishoort binnen het Blueprint-kader. Overweegt het kabinet, mede in het licht van deze aanbeveling, om in Nederland strategische publieke DNS-capaciteit op te bouwen?

II Antwoord/reactie van de bewindspersoon

Antwoorden op vragen van de PVV-fractie

1.
De leden van de PVV-fractie constateren allereerst dat het kabinet benadrukt dat de beheersing van incidenten en crises in eerste instantie bij de lidstaten zelf ligt, en dat pas bij een grootschalig grensoverschrijdend incident wordt overgegaan op EU-structuren. Daarbij stelt het kabinet dat de Blueprint explicieter moet aangeven dat nationale structuren leidend zijn. Wat gaat de Minister doen om ervoor te zorgen dat dit door de Commissie geborgd gaat worden?

Tijdens de onderhandelingen in de Raadswerkgroep voor Cyberaangelegenheden (HWPCI) heeft Nederland zich ingezet om in de Blueprint Cyber die op 6 juni voorligt in de Telecomraad als hamerstuk duidelijk op te nemen dat nationale structuren leidend zijn voor het beheersen en mitigeren van cyberincidenten en cybercrises.

Zo staat inmiddels expliciet aangegeven dat nationale structuren en lidstaat-gedreven netwerken (zoals het CSIRTs-Netwerk en het *European cyber crisis liaison organisation network* (hierna: EU-CyCLONe)) leidend zijn. Ook wordt in deze herziene Blueprint Cyber meer aandacht besteed aan nationale actoren en verantwoordelijkheden, mededankzij de toevoeging van sectie III in de Blueprint «Cyber Nationale Cybercrisisbe-

heersingsstructuren en Verantwoordelijkheden», waarin de nationale verantwoordelijkheden uiteengezet worden.

2.
Komt Nederland eventueel zelf met een voorstel hiertoe?

Nederland heeft het voorstel gedaan voor het toevoegen van bovengenoemde sectie III van de Blueprint Cyber: «Nationale Cybercrisisbeheersingsstructuren en Verantwoordelijkheden». Daarnaast heeft Nederland in samenwerking met andere lidstaten het visuele overzicht aangepast waarin het Europese cybercrisisbeheersingsstelsel wordt weergegeven. Zo is er een extra kolom toegevoegd die de nationale structuren weergeeft en de koppeling tussen nationale cyber- en crisisautoriteiten met het Europese niveau.

3.
Daarnaast merken deze leden op dat het kabinet vragen stelt bij de inzet van gelden uit het Digital Europe Programme voor veilige communicatie, en verzoekt om verduidelijking over de wijze waarop dit gefinancierd kan worden binnen de bestaande budgettaire kaders. Is de Minister voornemens opheldering te vragen hoe deze veilige communicatie eruit zou moeten zien?

Verschillende lidstaten, waaronder Nederland, hebben om verduidelijking gevraagd over de verwijzingen naar veilige communicatiemiddelen in de Blueprint Cyber. In de versie van de Blueprint Cyber die als hamerstuk voorligt in de Telecomraad wordt aanbevolen dat de Europese Commissie een voorstel zal maken voor een set veilige communicatiemiddelen die ingezet kunnen worden door Europese instellingen op basis van een eerder uitgevoerde inventarisatie.

4.
Maakt IRIS2 («Infrastructure for Resilience, Interconnectivity and Security by Satellite») hier onderdeel van uit en hoe verhoudt zich dit tot bijvoorbeeld Starlink?

Europa werkt actief aan versterking van de strategische autonomie op dit terrein. De Europese Commissie ontwikkelt in dat kader het programma IRIS^2: een Europese satellietconstellatie van circa 300 satellieten in verschillende banen om veilige, robuuste en wereldwijde communicatie mogelijk te maken. Het systeem is bedoeld als aanvulling op bestaande netwerken en kan dienen als terugval infrastructuur voor publieke telecommunicatie bij uitval of crises. Dit wordt verkend in het kader van bijvoorbeeld hybride of militaire dreigingen. In de Lange-termijn Ruimtevaartagenda, die in januari 2024 aan de Kamer is gestuurd, bent u hierover geïnformeerd.[1] De IRIS^2-wetgeving bevat bovendien bepalingen die zorgen voor deelname van het midden- en kleinbedrijf aan aanbestedingen, wat past bij het Nederlandse belang van diverse industriële toegang. Nederland ondersteunt de ontwikkeling van IRIS^2 en zet, binnen de beschikbare middelen, in op gerichte deelname van Nederlandse partijen aan dit strategisch belangrijke Europese project. Tegelijk blijft internationale samenwerking – o.a. binnen NAVO-verband – van belang voor interoperabiliteit en toegang tot kritieke infrastructuur in de ruimte.

5.
Kan de Minister bij de implementatie van deze aanbeveling borgen dat dit niet leidt tot toenemende regeldruk?

[1] https://www.rijksoverheid.nl/documenten/rapporten/2024/01/25/bijlage-bij-kamerbrief-bij-rapport-vanuit-de-ruimte-voor-de-aarde

Ja, zoals in het BNC-fiche benoemd heeft de aanbeveling inzake de Blueprint Cyber enkel impact op de werking en afspraken tussen EU instituties en lidstaten ten tijde van een cybercrisis of -incident en doet binnen de bestaande kaders niet-bindende aanbevelingen voor het bevorderen van de samenwerking tussen EU instellingen ten tijde van een cyberincident of crisis. Hierbij is geen sprake van verwachtingen voor burgers, bedrijven of organisaties.

6.
Wordt deze aanbeveling puur als facultatief beleidsinstrument gezien?

De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen verder te bevorderen. Hiermee kan dit document door lidstaten geraadpleegd worden ten tijde van een cyberincident of crisis om het cybercrisisbeheersingsproces op Europees niveau te begrijpen.

7.
Wat betekent de voorgestelde coördinatie op EU-niveau voor de positie, taken en bevoegdheden van het NCSC tijdens een cybercrisis?

Er verandert hierdoor niets aan de taken en bevoegdheden van het Nationaal Cyber Security Centrum (NCSC) tijdens een cybercrisis. De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen verder te bevorderen.

8.
Moet het NCSC zijn werkwijze aanpassen aan Europese afspraken?

Nee, het NCSC hoeft zijn werkwijze niet aan te passen. De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen verder te bevorderen. Er worden geen aanbevelingen gedaan die zien op de werkwijzen van nationale cyberorganisaties zoals het NCSC.

9.
Hoe verhoudt de Blueprint Cyber zich tot de NIS2-richtlijn en de Cyberbeveiligingswet?

De NIS2-richtlijn heeft als doel de cyberweerbaarheid van essentiële en belangrijke entiteiten binnen de EU te versterken. De Cyberbeveiligingswet zal de wet betreffen waarmee de NIS2-richtlijn in nationale wetgeving wordt geïmplementeerd. De Blueprint cyber is een niet-bindend document dat door lidstaten gebruikt kan worden als praktisch hulpmiddel bij een grootschalig cyberincident. Cyberincidenten die entiteiten bijvoorbeeld bij hun CSIRT worden gemeld zouden kunnen leiden tot een internationaal cyberincident, waar de Blueprint voor ingezet zou kunnen worden.

10.

Zijn er tegenstrijdigheden of overlap in meldplichten en procedures?

Nee, de Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen binnen dat stelsel verder te bevorderen. Het zet geen nieuwe meldplichten of procedures op.

11.
Hoe verhoudt dit zich tot het huidige beleid, dat bestaat uit het overnemen van internationale sancties nadat de VN-veiligheidsraad hiervoor een resolutie heeft aangenomen en het opleggen van sancties vanuit het Gemeenschappelijk Buitenlands en Veiligheid Beleid van de EU?

De Blueprint Cyber brengt de bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart en doet binnen die bestaande kaders aanbevelingen om samenwerking binnen dat stelsel te bevorderen. Onder de bestaande verantwoordelijkheden vallen ook handelingsopties van de verschillende Europese actoren, waaronder ook beleidsinstrumenten zoals de inzet van sancties onder de cyberdiplomatie en hybride toolboxen tegen individuen of entiteiten die betrokken waren bij operaties die leidden tot de cybercrisis. Van een nieuw sanctiebeleid is geen sprake.

12.
Hoe kijkt de Minister er tegenaan als hieruit een nieuw sanctiebeleid zou volgen?

Dit is een niet-bindend document waarin de rollen en verantwoordelijkheden van de verschillende actoren binnen het Europese cybercrisisbeheersingsstelsel worden omschreven. Van een nieuw sanctiebeleid is geen sprake.

13.
Tot slot lezen de leden van de PVV-fractie dat het kabinet graag de betrokkenheid ziet van de NAVO bij oefeningen ter voorbereiding op een grootschalige cybercrisis, waarbij aandacht wordt behouden voor EU-lidstaten die niet bij de NAVO zijn aangesloten. Hoe ziet het kabinet dat voor zich?

Het kabinet zet zich in haar internationale cyberbeleid in voor nauwere EU-NAVO samenwerking en moedigt de deelname van de NAVO staf bij EU-cyberoefeningen aan en vice versa, zoals bij veel EU-cyberoefeningen reeds staande praktijk is. Zo laten we cyber-crisismechanismes van de EU en NAVO zo goed mogelijk op elkaar aansluiten om onnodige duplicatie te voorkomen.

14.
Wijken deze oefeningen af van «Locked Shields» (een jaarlijks georganiseerde grootschalige cyberoefening)?

Binnen de EU en NAVO worden diverse grootschalige cyberoefeningen georganiseerd, waar «Locked Shields» er één van is. De Blueprint Cyber creëert geen nieuwe cyberoefeningen maar creëert een overzicht van bestaande cyberoefening ter bevordering van de voorbereidingen op deze oefeningen.

Antwoorden op vragen van de GL-PvdA-fractie

15.
Welke verantwoordelijkheden hebben overheidsorganisaties ten opzichte van private organisaties in de nieuwe Europese samenwerkingen?

De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen binnen dat stelsel verder te bevorderen. Het bevat geen nieuwe voorstellen inzake private organisaties.

16.
Kunt u uitleggen wat er in de praktijk verandert met de komst van de Blueprint Cyber?

In de praktijk wijzigt de Blueprint Cyber niets aan de huidige verhoudingen, verantwoordelijkheden of taken van organisaties. De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen binnen dat stelsel verder te bevorderen.

Wel biedt de Blueprint Cyber een actualisering van de bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel, gelet op de ontwikkelingen binnen het stelsel sinds die tijd waaronder de instelling van het CSIRTs-netwerk en EU-CyCLONe.[2]

Daarnaast is duidelijker weergegeven hoe het cybercrisisbeheersingsstelsel zich verhoudt met andere sectorale en horizontale crisismechanismen. Zo heeft de Commissie een rol in het verbinden van cybercrisisbeheersingsmechanismen en actoren zoals EU-CyCLONe met andere sectorale mechanismen, en is opgenomen hoe het cybercrisisbeheersingsstelsel zich verhoudt met het overkoepelende geïntegreerde Regeling Politieke Crisisrespons (IPCR).

17.
Welke aanvullende verantwoordelijkheden krijgen overheden en bedrijven?

De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen binnen dat stelsel verder te bevorderen. Overheden en bedrijven krijgen geen aanvullende verantwoordelijkheden in de Blueprint Cyber.

18.
Wat verandert er ten opzichte van de huidige situatie en kunt u de voordelen van de maatregelen kwantificeren, bijvoorbeeld in de verwachte reactietijd van lidstaten bij een grootschalige netwerkstoring?

---

[2] In de 2017 versie van de Blueprint Cyber stonden bijvoorbeeld het CSIRTs-netwerk en EU-CyCLONe, twee belangrijke actoren binnen het huidige Europese cybercrisisbeheersingsstelsel, nog niet opgenomen gezien deze pas na de publicatie in 2017 zijn opgezet.

De Blueprint Cyber is een niet-bindend document, dat bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart brengt en binnen die bestaande kaders aanbevelingen doet om samenwerkingen binnen dat stelsel verder te bevorderen. Hiermee verandert er ten opzichte van de huidige situatie niets voor bijvoorbeeld de verwachte reactietijd van lidstaten.

19.
Zal de Blueprint leiden tot een intensievere samenwerking binnen bestaande nationale samenwerkingsverbanden, zoals het Nationaal Cyber Security Centrum (NCSC)?

De Blueprint Cyber bevat hier geen bepalingen over.

20.
Kunt u expliciet maken welke ministeries betrokken zijn en welke nieuwe verantwoordelijkheden van hen worden verwacht?

Meerdere ministeries hebben meegelezen tijdens de ontwikkeling van de Blueprint Cyber, zowel bij het opstellen van het BNC-fiche en de daaropvolgende discussies in de Europese Raadswerkgroep voor Cyber aangelegenheden. Onder penvoerderschap van het Ministerie van Justitie en Veiligheid zijn onder andere het Ministerie van Defensie, het Ministerie van Economische Zaken en het Ministerie van Buitenlandse Zaken betrokken. Er worden van deze ministeries geen nieuwe verantwoordelijkheden verwacht.

21.
Wat schrijft de Blueprint Cyber voor nieuwe verantwoordelijkheden aan de inlichtingen- en veiligheidsdiensten AIVD en MIVD?

De Blueprint Cyber schrijft geen nieuwe verantwoordelijkheden voor aan de inlichtingen- en veiligheidsdiensten.

22.
Zij vragen u ook om in te gaan op wat de Blueprint voorschrijft op het gebied van informatiedeling tussen de EU en niet-EU partners.

De Blueprint Cyber raadt aan om informatiedeling tussen de Europese Unie en de NAVO in het kader van cybercrisisbeheersing verder te versterken. Onder andere door te onderzoeken welke mogelijkheden bestaan om informatie tijdig uit te wisselen ten behoeve van het beheersen van een cyberincident of crisis. De daadwerkelijke uitwerking van deze informatiedeling moet verder worden uitgewerkt door de EU en de NAVO in aparte discussies.

23.
De leden van de GroenLinks-PvdA-fractie steunen de suggestie van een continue cyclus van cyberoefeningen. Cyberaanvallen en -storingen zijn doorgaans abstract, waardoor de paraatheid noch bij burgers, noch de overheid, noch het bedrijfsleven wordt doorleefd. Hoe ziet u een dergelijke cyclus voor zich?

De cyclus waar in de Blueprint Cyber over gesproken wordt is een aanbeveling tot het opstellen van een overzicht van bestaande grootschalige cyberoefeningen waaronder Cyber Europe, Cyber Storm, Locked Shields, PACE, CMX en BlueOLEx ter bevordering van de voorbereidingen op deze oefeningen. Nederland draagt actief bij en neemt deel aan

verschillende EU en NAVO cyberoefeningen. Nederland steunt deze aanbeveling in de Blueprint Cyber.

Het Kabinet streeft verder naar het bevorderen van de bewustwording binnen de samenleving door middel van de Nederlandse Cybersecuritystrategie (NLCS). Deze is in publiek-privaat verband tot stand gekomen onder bewind van de Minister van Justitie en Veiligheid. In de NLCS geeft het kabinet aan te streven naar een digitaal veilig Nederland waarin burgers en bedrijven ten volle kunnen profiteren van deelname aan de digitale samenleving, vrij van zorgen over cyberrisico's.

De concrete beleidsinzet van het kabinet – ter verwezenlijking van de ambities in de strategie – is uitgewerkt in een actieplan. De Kamer wordt jaarlijks geïnformeerd over de voortgang. Zo is de voortgangsrapportage 2024 op 28 oktober j.l. aangeboden aan de Kamer.[3]

Om in te kunnen spelen op trends, actuele dreigingen en risico's, worden de acties in de loop van de tijd uitgewerkt, aangepast of versterkt. Het actieplan kan daarom jaarlijks op punten worden geactualiseerd, waardoor adequaat ingespeeld kan worden op de snelle ontwikkelingen in relatie tot digitale veiligheid en bijgestuurd kan worden als daar aanleiding toe is. Mogelijke aanleidingen kunnen gesignaleerd worden door het jaarlijkse Cybersecurity Beeld Nederland (CSBN) wat een actueel beeld geeft van de digitale dreiging, de belangen die daardoor kunnen worden aangetast, de weerbaarheid en digitale risico's. Het actieplan kan ook worden aangepast op basis van inzichten van publieke, private- of wetenschapspartijen. Dit kan daarnaast verwoord zijn in nationale dan wel internationale rapporten of adviezen die gedurende de looptijd van de NLCS worden uitgebracht. Tot slot kan ook de Cyber Security Raad adviseren over strategische ontwikkelingen die volgens hen meegewogen moeten worden bij de uitvoering van het beleid.

Nederland is een koploper binnen de Europese Unie waar het gaat om oefenen dankzij de ISIDOOR oefening. ISIDOOR is een cyber-specifieke crisisoefening waar het bedrijfsleven ook aan deelneemt. Voorgaande ISIDOOR oefening telde 120 deelnemende organisaties en meer dan 3000 individuele deelnemers. Er is drie dagen volop geoefend (technisch operationeel deel), plus een aparte dag voor hoog-ambtelijke besluitvorming.

24.
Op welke organisaties en infrastructuur zijn deze oefeningen van toepassing?

Dat verschilt per oefening. Cyber Europe bijvoorbeeld, is een cyber-incident- en crisisbeheersing oefening op EU-niveau georganiseerd door ENISA. Tijdens Cyber Europe oefenen organisaties zowel de publieke als de private sectoren binnen de EU en de Europese Vrijhandelsassociatie (EVA). Aan de Locked Shields oefening, georganiseerd door de NAVO's *Cooperative Cyber Defence Centre of Excellence* (CCDCOE), doen teams van cyberspecialisten mee.[4] Tijdens de nationale ISIDOOR-oefening, oefent de Rijksoverheid met organisaties die een rol hebben tijdens of betrokken zijn bij een (dreigende) digitale crisis. Dit zijn organisaties

[3] https://www.rijksoverheid.nl/documenten/rapporten/2024/10/28/tk-bijlage-2-nlcs-voortgangsrapportage-2024

[4] https://www.defensie.nl/actueel/nieuws/2022/04/22/grootste-cyberaanvaloefening-navo-zet-systemen-onder-druk

binnen de vitale infrastructuur, maar ook veiligheidsregio's en organisaties uit het Cyberweerbaarheidsstelsel (CWN).[5]

25.
Doen Nederlandse organisaties al mee aan grootschalige cyberoefeningen en, zo ja, wat wordt er met de opgedane lessen gedaan?

Nederlandse organisaties doen al mee aan grootschalige cyberoefeningen op zowel Europees als nationaal niveau. Zo oefent de Rijksoverheid mee tijdens verschillende oefeningen, zoals de CMX, PACE en Cyber Europe. Aan oefeningen zoals Locked Shields kunnen Nederlandse organisaties participeren. Op nationaal niveau organiseert de Rijksoverheid, zoals bij vraag 23 benoemd, de ISIDOOR oefening. Aan deze cyber-specifieke crisisoefening neemt naast de Rijksoverheid ook het bedrijfsleven ook aan deel. Voorgaande ISIDOOR oefening telde 120 deelnemende organisaties en meer dan 3000 individuele deelnemers.

Het ISIDOOR evaluatierapport met aanbevelingen heeft uw kamer op 11 april 2024 ontvangen. De aanbevelingen uit de evaluatie van ISIDOOR IV worden interdepartementaal opgevolgd. Binnen de reikwijdte van de Nederlandse Cyber Security Strategie zijn meerdere acties ondernomen voor de opvolging van de aanbevelingen. De aanbevelingen uit de ISIDOOR evaluatie worden ook meegenomen in de actualisatie van het LCP-Digitaal. De evaluatie wordt tevens meegenomen in de uitwerking van het bouwplan van het Cyberweerbaarheidsnetwerk, dat momenteel wordt vormgegeven door het NCSC.

26.
Via welke kanalen wordt deze informatie gecommuniceerd aan Europese partners en wat gaat de Blueprint Cyber daarin veranderen?

Relevante informatie over cyberoefeningen wordt doorgaans door het NCSC en haar partners verspreidt. De Blueprint Cyber brengt hier geen verandering bij aan.

27.
Is het doel van de cyberoefeningen ook om het maatschappelijke bewustzijn te vergroten, of enkel om de paraatheid van organisaties te toetsen?

Zoals cyberoefeningen nu zijn ingeregeld zijn deze voornamelijk ten behoeve van het verhogen van de paraatheid van organisaties. Voor het verhogen van het maatschappelijk bewustzijn worden andere methoden ingezet, zoals publiekscampagnes.[6]

28.
Deelt u de mening dat digitale soevereiniteit onder de Blueprint Cyber moet vallen?

De Blueprint Cyber ziet alleen op de beheersing van een cyberincident of -crisis op Europees niveau. Zoals in het BNC-fiche benoemd, hecht het kabinet waarde aan een document dat het huidige Europese cybercrisisstelsel in kaart brengt. De Blueprint Cyber is volgens het kabinet daarom niet het juiste document om vraagstukken omtrent digitale soevereiniteit onder te brengen.

---

[5] ISIDOOR. https://www.ncsc.nl/wat-doet-het-ncsc-voor-jou/isidoor
[6] NLCS Actieplan, Pijler IV, doel 1 «burgers zijn goed beschermd tegen digitale risico's».

29.
Ziet u het tegengaan van de afhankelijkheid van enkele techmonopolies, met name van Amerikaanse en Chinese leveranciers, als onderdeel van de Europese paraatheid en veiligheid? Hoe bevordert de Blueprint dat streven?

Het kabinet vindt het belangrijk om de Europese capaciteiten op strategische digitale technologieën te versterken en de risico's voor het borgen van publieke belangen zoals veiligheid door strategische afhankelijkheden van partijen uit derde landen te mitigeren, zoals onder meer staat geformuleerd in de Agenda Digitale Strategische Autonomie. Tegelijkertijd is niet iedere afhankelijkheid een kwetsbaarheid voor de veiligheid.

De Blueprint Cyber draagt in algemene zin bij aan de Europese veiligheid en paraatheid door duidelijk en toegankelijk het kader voor crisismanagement in de EU weer te geven om relevante actoren te helpen effectief samen te werken en bestaande mechanismen en initiatieven optimaal te benutten bij eventuele incidenten die kunnen ontstaan door afhankelijkheden van partijen uit derde landen op het terrein van cyberdreigingen.

30.
Kunt u meer toelichten over hoe de afspraken uit de Blueprint Cyber worden uitgewerkt samen met civiele cybercrisisnetwerken?

Zoals eerder benoemd, bestaan er binnen de Europese Unie twee lidstaat-gedreven civiele cybercrisisnetwerken: het CSIRTs-Netwerk en EU-CyCLONe. De Blueprint Cyber benoemt de huidige afspraken, rollen en verantwoordelijkheden van onder andere deze twee netwerken. Bij een aantal aanbevelingen in de Blueprint Cyber wordt verwezen naar deze netwerken om deze verder uitwerken.

31.
Welke netwerken betreft dit, en welke rol hebben maatschappelijke netwerken, zoals kerken, (sport)verenigingen en wijkteams, in de plannen van de Europese Commissie?

Deze maatschappelijke netwerken komen niet aan bod in de Blueprint Cyber.

32.
Vindt u dat de Blueprint op dit punt toereikend is?

De Blueprint Cyber heeft tot doel het in kaart brengen van het Europese cybercrisisbeheersingsstelsel. Belangrijk hierbij is een duidelijk onderscheid in de rollen en verantwoordelijkheden die Europese instellingen wel en niet hebben ten tijde van een cyberincident of -crisis. De Blueprint Cyber heeft zich gehouden aan deze reikwijdte.

33.
Zij willen meer informatie over de eisen die worden gesteld aan dergelijke communicatiemiddelen, welke alternatieven reeds beschikbaar zijn, en welke oplossingen Nederland te bieden heeft.

In de versie van de Blueprint Cyber die voorligt in de Telecomraad als hamerstuk worden geen eisen gesteld aan veilige communicatiemiddelen, wel wordt benoemd dat deze veilige communicatiemiddelen moeten voldoen aan gemeenschappelijk gedefinieerde vereisten voor de bescherming van gevoelige, niet-geheime informatie. Ook adviseert de

Blueprint Cyber om zoveel mogelijk gebruik te maken van oplossingen gebaseerd op een open protocol met open-source-implementaties die geschikt zijn voor realtimecommunicatie en beheerd worden door een in de EU gevestigde entiteit.

34.
Deelt u de mening dat er dwingende afspraken moeten worden gemaakt voor deze standaarden voor alle Europese overheidsdiensten en voor het ICT-inkoop en -aanbestedingsbeleid?

Gemeenschappelijke dwingende inkoop- en aanbestedingsvereisten kunnen zeker ondersteunen in de aanpak van cyberrisico's. Nationale inzet hierop vindt onder meer plaats middels de momenteel in ontwikkeling zijnde IT-Sourcingstrategie. Voor zaken waar nationale veiligheid aan bod is, zijn de Algemene Beveiligingseisen Rijksoverheidsopdrachten (ABRO) in ontwikkeling. Dit betreft echter wel nationale veiligheid, wat een nationale aangelegenheid is en niet binnen het mandaat van de EU valt.

35.
Bent u bereid om te pleiten voor afdwingbare Europese standaarden voor interoperabiliteit, dataportabiliteit en soevereiniteit?

Interoperabiliteit en dataportabiliteit komen in het kader van de Data Act al aan de orde. Op 1 april, 2022 bent u via het BNC Fiche Dataverordening geïnformeerd over de Nederlandse inzet, waaronder ook voor versterkte interoperabiliteit en dataportabiliteit in de Data Act.[7] Daarnaast lopen er verschillende dossiers waarbij Nederland zich inzet op soevereiniteit.

36.
Daartoe vragen zij u om verder te definiëren wat een «significant incident» betekent.

In lijn met de NIS2-richtlijn, hanteert de Blueprint Cyber de volgende definitie van een significant incident: een incident dat a. een ernstige operationele verstoring van de diensten of financieel verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of b. andere natuurlijke of rechtspersonen heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

37.
Deelt u de mening van deze leden dat incidenten, waarin informatie van personen wordt buitgemaakt of uitgelekt, ook als «significant» moeten worden aangemerkt?

De definitie van «significant incident», zoals deze ook is opgenomen in de NIS2-richtlijn, moet naar het oordeel van het kabinet bepalend zijn. In de Cyberbeveiligingswet (CBW), die dient ter implementatie van de NIS2-richtlijn, wordt in relatie tot de meldplicht geregeld dat de criteria op basis waarvan wordt vastgesteld of er sprake is van een significant incident worden uitgewerkt in lagere regelgeving.

Deze zogeheten drempelwaarden zullen naar verwachting in ministeriële regelingen worden vastgesteld onder coördinatie van het Ministerie van Justitie en Veiligheid. Een datalek van persoonsgegevens ziet een dergelijk incident op de Algemene verordening gegevensbescherming (AVG).

---

[7] https://www.eerstekamer.nl/eu/behandeling/20220401/brief_van_de_minister_van_buza

38.
Deze leden zijn benieuwd naar het vervolg van de Blueprint Cyber. Zij vragen u om aan te geven welke onderdelen van de Blueprint wat u betreft moeten worden doorvertaald in harde afspraken en nieuw beleid.

Er zijn geen harde afspraken of nieuw beleid dat moet worden opgesteld aan de hand van de Blueprint Cyber. Het overzicht van het Europese cybercrisisstelsel zal wel door het kabinet worden meegenomen tijdens de herziening van het Landelijk Crisisplan Digitaal (LCP-D).

39.
Ook horen zij graag hoe u de aanbevelingen uit de Blueprint proactief aan organisaties en burgers gaat communiceren, en deze zo praktisch mogelijk maakt.

De Blueprint Cyber heeft zoals hierboven benoemd geen impact op bedrijven, organisaties en burgers en dient vooral de betrokken instanties bij de lidstaten. Het kabinet acht het daarom niet nodig om de Blueprint Cyber proactief te communiceren met organisaties en burgers

Antwoorden op vragen van de VVD-fractie

40.
De leden van de VVD-fractie vragen naar een nadere toelichting op de inzet van het kabinet ten aanzien van de versterkte publiek-private samenwerking bij de bestaande en nieuwe initiatieven. Hoe wordt deze samenwerking versterkt in de nieuwe Blueprint en maakt het uitwisselen van relevante gegevens hier ook onderdeel van uit?

De Blueprint Cyber is in de kern een document dat de respons op Unieniveau weergeeft. Hoe de publiek-private samenwerking met betrekking tot cybercrisisbeheersing in de lidstaten zelf is geregeld of geregeld dient te worden gaat de Blueprint Cyber niet op in.

Wel doet de Blueprint Cyber algemene aanbevelingen ten aanzien van het betrekken van private organisaties bij het herstel van cyberincidenten, het waar mogelijk uitwisselen van informatie met de private sector ten tijde van cyberincidenten, en het opnemen van oefeningen waar de private sector aan meedoet in het overzicht van grootschalige cyberoefeningen.

41.
Deze leden vragen wat de inzet is van het kabinet ten aanzien van de uitwerking van de rollen, taken en bevoegdheden van de Europese Commissie en van ENISA, het Europees agentschap voor cybersecurity.

De Blueprint Cyber weerspiegelt daarmee alleen de bestaande afspraken, rollen en verantwoordelijkheden, waaronder ook van de Europese Commissie en ENISA.

42.
Zij vragen verder of het kabinet kan nagaan of er een impact assessment zal worden gedaan door de Europese Commissie bij de herziening van de Blueprint, en zo niet, of dat alsnog kan worden gedaan.

Zoals in het BNC-fiche inzake de Blueprint Cyber is opgenomen is er geen impact assesment opgesteld. De Blueprint Cyber is immers een niet-bindend document gericht op het in kaart brengen van bestaande afspraken, rollen en verantwoordelijkheden op Europees niveau.

Gezien de herziene Blueprint Cyber op 6 juni al ter aanname in de Telecomraad wordt gepresenteerd kan er geen verzoek tot impact assessment worden gedaan. Het kabinet acht dit echter ook niet nodig gezien het karakter van het document.

43.
Ook vragen de leden van de VVD-fractie of de grootschalige stroomstoring van onlangs in Spanje en Portugal nog nieuwe inzichten heeft opgeleverd, en of het kabinet bereid is te vragen naar de inzichten die deze lidstaten sindsdien hebben opgedaan en welke gevolgen dat heeft voor de gesprekken over de herziening van de Blueprint.

De definitieve oorzaak voor de stroomstoring in Spanje en Portugal is vooralsnog niet bekend. Het kabinet kan hier op dit moment geen uitspraken over doen.

Antwoorden op vragen van de NSC-fractie

44.
In het BNC-fiche geeft het kabinet aan: «Het kabinet hecht waarde aan een praktisch document dat ten tijde van crisis daadwerkelijk door de betrokken actoren zal worden geraadpleegd.» De leden van de NSC-fractie vragen hoe het kabinet hier in Nederland invulling aan zou willen geven?

Hoewel de Blueprint Cyber een niet-bindend document betreft heeft Nederland er in de onderhandelingen in de Raadswerkgroep voor Cyberaangelegenheden naar gestreefd om aanpassingen aan het document voor te stellen die de bruikbaarheid op nationaal niveau zullen stimuleren. Zo heeft Nederland het voorstel gedaan om de Blueprint Cyber duidelijker te structureren zodat de kern van het document – het in kaart brengen van de bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel – duidelijk is opgenomen. Ook heeft Nederland het voorstel gedaan voor het toevoegen van bovengenoemde sectie III van de Blueprint Cyber: «Nationale Cybercrisisbeheersingsstructuren en Verantwoordelijkheden». Daarnaast heeft Nederland in samenwerking met andere lidstaten het visuele overzicht aangepast waarin het Europese cybercrisisbeheersingsstelsel wordt weergegeven. Zo is er een extra kolom toegevoegd die de nationale structuren weergeeft en de koppeling tussen nationale cyber- en crisisautoriteiten met het Europese niveau.

Daarnaast is dankzij de toevoegingen in het visuele overzicht duidelijker weergegeven hoe het cybercrisisbeheersingsstelsel zich verhoudt met andere sectorale en horizontale crisismechanismen. Ook is opgenomen hoe het cybercrisisbeheersingsstelsel zich verhoudt met het overkoepelende geïntegreerde Regeling Politieke Crisisrespons (IPCR).

45.
Zou dit praktisch document specifiek moeten toezien op cybercrises of betreft het ook andere crises (met al dan niet een digitaal component)?

De Blueprint Cyber ziet op de respons op een grootschalig cyberincident, cybercrisis of crisis met een cyberaspect. Het kabinet steunt deze lijn.

46.
Wat kan daarnaast verwacht worden van individuele burgers?

De Blueprint Cyber brengt bestaande afspraken, rollen en verantwoordelijkheden binnen het Europese cybercrisisbeheersingsstelsel in kaart en doet binnen die bestaande kaders aanbevelingen om samenwerkingen verder te bevorderen. Het legt geen rechten of plichten op aan (individuele) burgers.

47.
Deze leden vragen het kabinet om een nadere toelichting op dit standpunt. Hoe ziet het kabinet het onderscheid tussen cybercrisismanagement en andere vormen van crisismanagement, vooral in het licht van hybride dreigingen?

In Nederland staat de generieke aanpak van een nationale crisis beschreven in het Nationaal Handboek Crisisbeheersing.[8] Hierin wordt, op nationaal niveau, de algemene werkwijze beschreven ten aanzien van crisisbeheersing op nationaal niveau. Ten aanzien van specifieke crisistype, waaronder een cybercrisis, kan er besloten worden om specifiek crisisplan (c.q. landelijk crisisplan) op te stellen. Een landelijk crisisplan geeft op hoofdlijnen overzicht en inzicht van de gemaakte afspraken over de beheersing van een specifieke crisis. Voor een cybercrisis is het Landelijk Crisisplan Digitaal opgesteld, waarin de specifieke aanpak voor een cybercrisis wordt beschreven. De specifieke aanpak kenmerkt zich door de betrokken actoren, het juridisch kader, de specificaties ten aanzien van crisisprocessen en de specifieke sleutelbesluiten bij een cybercrisis. Zowel decentrale overheden, (private) organisaties en andere betrokken actoren zijn dan genoodzaakt om hun operationeel uitgewerkte plannen en draaiboeken in lijn te brengen met het National Handboek Crisisbeheersing en/of het Landelijk Crisisplan Digitaal.

In het kader van de geopolitieke ontwikkelingen groeit de huidige hybride dreiging, een van die dreigingen zijn cyberaanvallen. Het kabinet werkt ook dan ook aan het verhogen van de weerbaarheid ten aanzien de militaire en hybride dreiging, in dat kader wordt ook de digitale weerbaarheid verhoogd. Deze elementen komen ook terug in de actualisatie van de Landelijk Crisisplan Digitaal.

48.
Hoe definieert het kabinet een cybercrisis, en is het onderscheid tussen cybercrises en andere crises nog steeds relevant en goed af te bakenen?

Het Landelijk Crisisplan Digitaal richt zich op crises in de digitale ruimte. De digitale ruimte betreft het conglomeraat van digitale middelen en -diensten en bevat permanente, tijdelijke en plaatselijke (digitale) verbindingen en gegevens, waarbij geen geografische beperkingen zijn gesteld. Alle entiteiten in de samenleving kunnen in de digitale ruimte verbonden zijn. Binnen de digitale ruimte richt het Landelijk Crisisplan Digitaal zich op de beheersing van crises met betrekking tot de beveiliging van netwerken en informatiesystemen met aanzienlijke maatschappelijke gevolgen en daaraan gerelateerde cascade- en gevolgeffecten. Het plan

[8] Nationaal Handboek Crisisbeheersing (NHC), 2022.

ziet toe op crises waarbij de (veronderstelde) oorzaak zich eveneens in de digitale ruimte bevindt.

Digitale middelen en- diensten zijn vaak randvoorwaardelijk voor dienstverlening, waaronder bij vitale- en andere maatschappelijk relevante processen. Door de digitalisering zijn fysieke processen steeds meer verweven met digitale systemen; hierbij wordt nadrukkelijk aandacht besteed aan de fysieke (maatschappelijke) effecten bij een cybercrisis.

Desondanks is een cybercrisis nog steeds af te bakenen van andersoortige crises. Digitale crisisbeheersing onderscheidt zich door intensieve samenwerking tussen verschillende sectoren, netwerken en publieke en private actoren die parallel en gelijktijdig betrokken kunnen zijn bij de beheersing van de digitale en fysieke (gevolg) effecten van een crisis. Tussen al deze partners bestaat een omvangrijk web aan informatiestromen, ook over grenzen heen, waarin duiding, handelingsperspectieven, technische en niet-technische informatie, die van belang zijn voor de crisisbeheersing zo veel als mogelijk worden gedeeld.

49.
Het BNC-fiche stelt ook: «Het kabinet ziet daarom graag duidelijker opgenomen dat de nationale structuren leidend zijn.» De leden van de NSC-fractie steunen deze visie vanuit het perspectief van subsidiariteit, maar hebben vragen over de aansluiting van de Nederlandse nationale structuren op de Blueprint Cyber bij opschaling naar EU-niveau. Gezien het feit dat systemen met elkaar verbonden zijn en incidenten zich over grenzen kunnen verspreiden, willen deze leden weten hoe het kabinet denkt dat deze structuren goed kunnen samenwerken met EU-structuren.

Met nationale structuren wordt in dit geval nationale crisismechanismen en afspraken bedoeld. EU-CyCLONe en CSIRTs-netwerk zijn voorbeelden van EU lidstaat-gedreven netwerken waarin afgevaardigden van nationale crisisorganisaties samenkomen en samenwerken t.b.v. cybercrisismanagement. Indien er grootschalige cyberincidenten of cybercrises plaatsvinden zijn dit de structuren die gebruikt kunnen worden om samen cybercrises het hoofd te bieden. Nederland heeft ingezet op een versterking van de rol van beiden gremia in de Blueprint.

Daarnaast is in de versie van de Blueprint Cyber die als hamerstuk voorligt in de Telecomraad duidelijker weergegeven hoe het Europese cybercrisisbeheersingsstelsel waar deze lidstaat-gedreven netwerken onderdeel van uitmaken zich verhoudt met andere sectorale en horizontale crisismechanismen. Zo heeft de Commissie een rol in het verbinden van cybercrisisbeheersingsmechanismen en actoren, zoals EU-CyCLONe met andere sectorale mechanismen, en is opgenomen hoe het cybercrisisbeheersingsstelsel zich verhoudt met het overkoepelende geïntegreerde Regeling Politieke Crisisrespons (IPCR).

50.
Daarnaast blijkt uit het fiche niet welke instantie de rol van nationaal aanspreekpunt zal krijgen voor EU-crisisstructuren, zoals het «European Cyber Crisis Liaison Organisation Network» (EU-CyCLONe). Zij vragen het kabinet wie zij voor deze rol in Nederland in gedachten heeft.

EU-CyCLONe en het CSIRTs-netwerk zijn EU-crisisstructuren waar Nederland reeds aan deelneemt. Namens Nederland is de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) aangesloten bij EU-CyCLONe en het NCSC bij het CSIRTs-netwerk.

51.
Tot slot vermeldt het BNC-fiche: «Het kabinet is echter van mening dat de Blueprint Cyber niet dit detailniveau moet hanteren. Bovendien ziet deze aanbeveling niet specifiek op cybercrisismanagement.» De leden van de NSC-fractie verzoeken het kabinet om een nadere toelichting op deze zienswijze. Zien zij geen risico in het ontbreken van expliciete richtlijnen, bijvoorbeeld met betrekking tot DNS-redundantie, die naar hun mening essentieel is?

DNS is voor het kabinet zeker een belangrijk onderwerp. Vanuit verschillende instrumenten, waaronder de Telecomwet (TW) en Wet Beveiliging Netwerk- en Informatiesystemen, zijn reeds eisen opgesteld t.a.v. weerbaarheid van het DNS. Ook is DNS een vitaal proces binnen de digitale infrastructuur[9] Voor niet vitale partijen zijn er binnen de keten van DNS leveranciers en DNS registratiediensten veelal contractuele eisen die toezien op redundantie van het DNS. Zo stelt de Stichting Internetdomeinregistratie Nederland (SIDN) als beheerder van het nl-domein de voorwaarde dat: «Voor elk domein dat we in de .nl-zonefile opnemen, is er een *primary nameserver*. En minimaal 1 *secondary nameserver*. Die *nameservers* zijn redundant en gebruiken verschillende (sub)netten[10].» Het kabinet is derhalve van mening dat opname van details t.a.v. het DNS in de Blueprint Cyber niet nodig zijn en mogelijk slechts verwarring schept.

52.
Hoe schat het kabinet het risico in van te grote vrijblijvendheid of te open normen als dergelijke zaken onvoldoende worden uitgewerkt?

Zie antwoord op vraag 51.

53.
Welke andere vormen van diversificatie of redundantie acht het kabinet noodzakelijk, waar dit momenteel nog onvoldoende is geregeld?

Het Kabinet zag de noodzaak om de rollen en verantwoordelijkheden van de verschillende betrokken actoren op Europees niveau verder te verduidelijken in de Blueprint Cyber. In de versie van de Blueprint Cyber die als hamerstuk voorligt in de Telecomraad wordt in sectie VII «Reageren op een grootschalig cyberincident of cybercrisis op Unieniveau» in detail ingegaan op deze aspecten.

54.
Gegeven dat de Commissie het belang van veilige cloudinfrastructuur in crisissituaties benadrukt, maar niet definieert wat daaronder valt, vragen deze leden wat het kabinetsstandpunt op dit onderwerp is. Hoe verstrekkend zouden deze eisen moeten zijn als het gaat om cloudaanbieders?

---

[9] https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/04/vitaal-beoordeling-datacenters-en-dns-dienstverleners

[10] https://www.sidn.nl/nl-domeinnaam/technische-eisen-voor-registratie-en-gebruik-van-nl-domeinnamen

De NIS-richtlijn heeft een meldplicht, op basis van de NIS-richtlijn wordt een verlener van cloudcomputerdiensten gedefinieerd. Voor deze aanbieders is dus al een dergelijke meldplicht ingeregeld waardoor zij in crisissituaties, zoals grootschalige uitval, moeten melden. Ook zijn er vanuit de NIS-richtlijn andere vereisten voor verleners van cloudcomputerdiensten.

Naast de voorgenoemde meldplicht voor significante incidenten dienen cloudaanbieders zich ook te houden aan de zorgplicht. In geval van cloudcomputingdiensten dienen zij zich te houden aan de door de Europese Commissie opgestelde uitvoeringsverordening (EU) 2024/2690. Hierin wordt zowel de meldplicht als zorgplicht voor deze sector nader ingekleurd en daarmee geeft de Europese Commissie inzicht in wat zij verstaat onder een veilige cloudinfrastructuur. De uitvoeringsverordening gaat uit van een riscogebaseerde aanpak, waardoor de te nemen maatregelen per cloudcomputingdienst kunnen verschillen. Daarnaast is het zo dat wanneer partijen die onder de Cbw vallen een clouddienst afnemen voor haar dienstverlening, zij vanuit die hoedanigheid ook eisen zullen opleggen aan de leverancier van haar cloudinfrastructuur die zij afnemen.

55.
Ziet het kabinet daarnaast het belang ervan in dat de EU in het kader van de weerbaarheid bevordert dat er meer vormen van schaalbare cloudopslag beschikbaar zijn waarbij de betreffende data en digitale diensten niet toegankelijk zijn voor niet-Europese inlichtingendiensten en dat deze niet eenvoudig stopgezet kunnen worden door niet-Europese mogendheden?

Het kabinet vindt de beschikbaarheid van voldoende schaalbare Europese cloudopslag belangrijk. We stimuleren het Europese aanbod van clouddiensten, bijvoorbeeld via IPCEI CIS, om innovatie te bevorderen en zo het Europese cloudaanbod te verdiepen en verbreden. Daarbij streven we naar een open ecosysteem, waarbij niet één partij dominant is. In zo'n federatieve opzet bieden meerdere Europese aanbieders samen een geïntegreerd marktaanbod aan.

Antwoorden op vragen van de BBB-fractie

56.
Voorts vragen deze leden om een nadere toelichting op het standpunt van het kabinet ten aanzien van vrijwillige aanbevelingen die mogelijk kunnen leiden tot verplichte datalokalisatie of de uitsluiting van niet-EU cloudproviders. Waarom verzet het kabinet zich tegen deze aanbevelingen, ondanks hun niet-bindende karakter?

Dit punt is niet aan bod gekomen tijdens de discussies omtrent de Blueprint Cyber. Verplichte datalokalisatie of de uitsluiting van niet-EU cloudproviders is tevens geen onderdeel van de Blueprint Cyber.

57.
Hoewel het voorstel formeel niet juridisch bindend is, rijst de vraag hoe groot de kans is dat de Blueprint op termijn alsnog zal uitmonden in bindende regelgeving. Op welke onderdelen zou dat volgens het kabinet met name het geval kunnen zijn?

Het kabinet kan geen uitspraken doen over de eventuele toekomstige omzetting van de Blueprint Cyber naar een ander initiatief van de Europese Commissie dat wel bindend is. Het kabinet acht de Blueprint

Cyber, in z'n huidige niet-bindende vorm, echter een goed instrument om samenwerking in geval van grootschalige cybercrises- of incidenten te bevorderen.

58.
Deze leden willen daarnaast weten op welke wijze het kabinet waarborgt dat nationale crisisstructuren daadwerkelijk de regie behouden wanneer de EU-coördinatie bij een cybercrisis wordt opgeschaald.

Nederland heeft tijdens de onderhandelingen ingezet op het versterken van de aanwezigheid van de rol van nationale crisisstructuren. Zo is er momenteel duidelijk opgenomen dat lidstaten de verantwoordelijkheid hebben voor de mitigatie van een cybercrisis, en is de integrale rol die lidstaat-gedreven netwerken zoals het CSIRTs-netwerk en EU-CyCLONe spelen prominent opgenomen.

59.
Ook vragen zij hoe wordt voorkomen dat besluitvorming op Europees niveau ten koste gaat van nationale autonomie in crisissituaties.

Zoals omschreven in vraag 44, is in de Blueprint Cyber opgenomen dat lidstaten verantwoordelijk zijn voor het mitigeren van cybercrises. Op Europees niveau kan er informatie uitgewisseld worden, of, op initiatief van een lidstaat, coördinatie gezocht worden. Besluitvorming op Europees niveau gaat hierbij niet ten koste van de nationale autonomie.

60.
Met betrekking tot de paragraaf over civiel-militaire samenwerking en de rechtsstatelijke aspecten daarvan vragen de leden van de BBB-fractie welke juridische en ethische kaders het kabinet voor ogen heeft bij informatie-uitwisseling tussen civiele en militaire actoren binnen het kader van de Blueprint.

De Blueprint stelt voor dat het CSIRTs-netwerk en EU-CyCLONe identificeren hoe zij het beste samen kunnen werken met militaire actoren uit de EU. Een goede samenwerking tussen civiele en militaire actoren is van groot belang om het hoofd te blijven bieden aan cyberdreigingen. Afhankelijk van de betreffende omstandigheden en de organisaties in kwestie, vindt gegevensuitwisseling – waaronder cyberdreigingsinformatie – plaats binnen de daarvoor geldende wettelijke kaders. Relevante wetgeving is in dat kader de Wet beveiliging netwerk- en informatiesystemen (Wbni), de Algemene Verordening Gegevensbescherming (AVG) en de Wet op de inlichtingen- en veiligheidsdiensten 2017 (WIV 2017).

61.
Tevens willen deze leden weten op welke wijze parlementaire betrokkenheid en democratische controle op dergelijke samenwerking worden geborgd.

De Kamer wordt volgens reguliere lijnen geïnformeerd voor wat betreft zaken over informatie-uitwisseling tussen civiel-militaire actoren.

62.
Tot slot vragen zij waarom het kabinet van mening is dat de aanbeveling over DNS-diversificatie niet thuishoort binnen het Blueprint-kader. Overweegt het kabinet, mede in het licht van deze aanbeveling, om in Nederland strategische publieke DNS-capaciteit op te bouwen?

De Europese Commissie heeft middels het DNS4EU initiatief al het voortouw genomen in de opbouw van publieke DNS-capaciteit binnen de EU en gebruikmakend van Europese leveranciers.