2025D21651

INBRENG VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Binnen de vaste commissie voor Digitale Zaken hebben enkele fracties de behoefte om enkele vragen en opmerkingen voor te leggen aan de Minister van Justitie en Veiligheid over de brief «Fiche: Aanbeveling Blueprint Cyber» (Kamerstuk 22 112, nr. 4018).

De voorzitter van de commissie,
Wingelaar

Adjunct-griffier van de commissie,
Muller

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 cloudpro-

viders. 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