Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

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

Nr. 3231

VERSLAG VAN EEN SCHRIFTELIJK OVERLEG

Vastgesteld 19 november 2021

De vaste commissie voor Digitale Zaken heeft een aantal vragen en opmerkingen voorgelegd aan de Minister van Justitie en Veiligheid over de brief van 27 augustus 2021 over het Fiche: Aanbeveling opbouw Joint Cyber Unit (Kamerstuk 22 112, nr. 3182).

De vragen en opmerkingen zijn op 14 oktober 2021 aan de Minister van Justitie en Veiligheid voorgelegd. Bij brief van 17 november 2021 zijn de vragen beantwoord.

De fungerend voorzitter van de commissie,
Leijten

Adjunct-griffier van de commissie,
Van Tilburg

kst-22112-3231
ISSN 0921 - 7371
's-Gravenhage 2021

Inhoudsopgave

I Vragen en opmerkingen vanuit de fracties

Vragen en opmerkingen van de leden van de VVD-fractie

De leden van de VVD-fractie hebben kennisgenomen van het voorstel tot oprichting van een Joint Cyber Unit (JCU), maar hebben nog enkele vragen en opmerkingen met betrekking tot de meerwaarde van het op te richten platform.

De leden van de VVD-fractie lezen dat de Joint Cyber Unit geen nieuwe instantie zal worden, maar een virtueel en fysiek platform zal betreffen voor het versterken van de samenwerking tussen de in de aanbeveling geïdentificeerde operationele en ondersteunende deelnemers. Deze leden vragen dan ook welke (nieuwe) rol het JCU zal gaan vervullen in het digitaal veilig houden van lidstaten. Welk mandaat zal het JCU precies krijgen? Op basis van welke probleemanalyse is men tot dit mandaat gekomen?

De leden van de VVD-fractie constateren voorts dat het JCU zich onder andere zal gaan bezighouden met het delen van informatie afkomstig uit verschillende cybersecuritygemeenschappen. Welke bevoegdheden zijn hierbij voorzien voor het JCU om ook deze informatie te kunnen ophalen en delen met andere partijen? Wordt hierbij een wettelijke grondslag voor informatiedeling tussen het JCU en andere organisaties geborgd? Zo nee, hoe zal het JCU dan in de praktijk dreigingsinformatie kunnen ophalen en delen? Kan de Minister ook toelichten wat wordt beoogd met cybersecuritygemeenschappen? Betreft het hier nationale samenwerkingsverbanden, waarbij bijvoorbeeld ook het Nederlandse Nationaal Cyber Security Centrum in de praktijk informatie kan gaan delen met het JCU of transnationale samenwerkingsverbanden? De Europese Unie kent meerdere reeds bestaande cybersecurityinitiatieven zoals het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) en CERT-EU (Computer Emergency Response Team voor de EU). Wat zijn precies hun taken? Welke knelpunten worden geïdentificeerd bij het uitvoeren van deze taken? In hoeverre is het voorzien dat het JCU op deze knelpunten acteert? Met andere woorden: hoe zal het JCU zich gaan verhouden qua takenpakket tot de bestaande initiatieven zoals ENISA en CERT-EU?

De leden van de VVD-fractie lezen dat een van de doelstellingen van de JCU is om te zorgen voor een gecoördineerde reactie binnen de Europese Unie op grootschalige cyberdreigingen en dat de Europese Commissie voorstelt om EU Cybersecurity Rapid Reaction Teams op te richten om de inzet te coördineren. Overwegende dat de NAVO al in 2012 een Rapid Reaction Team heeft opgezet om cyberaanvallen af te wenden, hoe zal het JCU zich gaan verhouden tot het Rapid Reaction Team van de NAVO? Hoe vaak is het Rapid Reaction Team tot nu toe ingezet? In hoeverre zijn er mogelijkheden om de JCU te laten samenwerken met het Rapid Reaction Team van de NAVO om cyberaanvallen op lidstaten tegen te gaan? Ook is het voor deze leden nog onduidelijk welke kosten komen kijken bij het

oprichten van het JCU. Wat is de begroting die hoort bij het oprichten van het JCU? Kan er een inschatting worden gemaakt in hoeverre deze kosten budgettaire gevolgen zullen hebben voor Nederland?

De leden van de VVD-fractie menen dat de oprichting van de JCU louter (financieel) te rechtvaardigen is wanneer de JCU daadwerkelijk een toevoeging vormt op de bestaande bevoegdheden en taakstellingen van eerdergenoemde bestaande diensten en daarmee van toegevoegde waarde is in het tegengaan van cyberaanvallen op lidstaten. Deelt de Minister deze mening? Zo ja, is de Minister bereid dit onder de aandacht te brengen bij de onderhandelingen? Zo nee, waarom niet?

Vragen en opmerkingen van de leden van de D66-fractie

De leden van de D66-fractie hebben met interesse kennisgenomen van de BNC-fiches met betrekking tot de Europese Joint Cyber Unit. Deze leden hebben kennisgenomen van de inzet van het kabinet op meer Europese samenwerking tussen bestaande organisaties die niet hoeft te leiden tot extra schakels maar tot effectievere samenwerking. Deze leden hebben nog enkele vragen.

De leden van de D66-fractie lezen dat de Europese cybereenheid uiterlijk 30 juni 2022 de operationele fase moet ingaan. Deze leden vragen de Minister toe te lichten welke volgende stappen vanuit het kabinet ondernomen zullen worden met betrekking tot de uitwerking van de Joint Cyber Unit. Deze leden lezen dat de noodzaak en urgentie van een Europese cybereenheid wordt ondersteund, maar wel bewaakt zal worden dat lidstaten zelf primair verantwoordelijk blijven voor het reageren op grote cyberveiligheidsincidenten en crises. De leden vragen de Minister toe te lichten wat de competentieverdeling zal zijn tussen de Europese Unie en de lidstaten in het geval van een cyberaanval. Onder welke omstandigheden zal Nederland zelf handelen? Welke maatstaf zal de Europese Commissie gebruiken voor de definitie van grote incidenten?

De leden van de D66-fractie constateren dat er via een Joint Cyber Unit veel kennis en tools gedeeld zullen worden binnen de Europese Unie. De leden vragen de Minister toe te lichten hoe er gewaarborgd zal worden dat belangrijke informatie beschermd zal blijven, bijvoorbeeld van externe mogendheden. Kan de Minister toelichten hoe het kabinet zal toezien op een hoog niveau van beveiliging van dit virtuele en fysieke platform? Deze leden vragen de Minister of er nog afwegingen gemaakt worden tussen welke lidstaten er wel of niet gedeeld wordt. Krijgen lidstaten die niet actief bijdragen aan de Joint Cyber Unit ook toegang tot alle kennis en tools die andere lidstaten delen?
De leden van de D66-fractie constateren dat middels de Europese cybereenheid, belangrijke informatie en kennis van Nederlandse organisaties richting het coördinatiepunt zal gaan. Deze leden vragen de Minister te specifiëren welke Nederlandse organisaties verbonden zullen zijn aan dit Europese netwerk.

De leden van de D66-fractie lezen dat de aanbeveling van de Joint Cyber Unit onderdeel is van een grotere EU Cybersecuritystrategie, onder andere een Europese wet op de cyberweerbaarheid. De leden vragen de Minister toe te lichten of er eventuele raakpunten of conflicten zijn tussen deze wetsvoorstellen en de Nederlandse wetten rondom cyberveiligheid, en welke uitdagingen hij hier ziet.

De leden van de D66-fractie lezen dat uit de IOB Cybersecurity evaluatie van juni 2021 blijkt dat ambtenaren van het Ministerie van Buitenlandse Zaken vaak werken met verouderde en onveilige middelen, waardoor de

communicatie niet goed verloopt. Welke stappen zijn er sindsdien genomen om dit recht te zetten? Deze leden concluderen dat het voorstel vooral gaat om het delen van kennis en tools binnen de Europese Unie. Deze leden vragen de Minister of deze Europese Cybereenheid ook zal samenwerken met landen die geen lidstaat zijn, en welke extra kansen een sterkere Europese samenwerking biedt tot meer mondiale samenwerking. Deze leden horen specifiek graag van de Minister op welke manier dit voorstel samenkomt en een aanvulling vormt met het door de Europese Commissie aangekondigde Cyber Resilience Act en daarnaast met de door de Verenigde Staten aangekondigde verbond tegen ransomware, het Counter-Ransomware Initiative.
De leden van de D66-fractie lezen dat de Joint Cyber Unit gebaseerd is op inbreng van lidstaten op vrijwillige basis. Deze leden lezen dat onder andere de inbreng van een nationaal cybersecurity incident- en crisisresponsplan alleen vrijwillig kan gebeuren. Acht de Minister het wenselijk dat er eventueel grote verschillen tussen lidstaten ontstaan met betrekking tot digitale veiligheid?

De leden van de D66-fractie lezen dat het kabinet als prioriteit heeft om vertrouwen en veilige informatie-wisseling op te bouwen tussen deelnemers. Deze leden vragen de Minister om voorbeelden van voorstellen om het vertrouwen tussen lidstaten op te bouwen wat betreft digitale veiligheid. Ziet de Minister kansen om lidstaten aan te moedigen zich aan te sluiten bij de Europese Cyber Unit? Zo ja, op welke manier gaat de Minister zich hiervoor inzetten? Deze leden constateren dat het kabinet vervolggesprekken met alle betrokkenen wenst over uitwerking van randvoorwaarden van informatie-uitwisseling en het garanderen van de vertrouwelijkheid van informatie. Deze leden vragen de Minister om toe te lichten wat de inzet is van het kabinet om zoveel mogelijk te waarborgen dat de informatie vertrouwelijk is en blijft tegenover derde landen.

Vragen en opmerkingen van de leden van de CDA-fractie

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het fiche over de Joint Cyber Unit. Deze leden lezen dat het kabinet het uitgangspunt om te streven naar versterkte informatie-uitwisseling steunt, maar dat over vervolggesprekken met alle betrokkenen over de uitwerking en randvoorwaarden er nog veel vragen zijn. Deze leden lezen weinig over de concrete inzet van het kabinet bij deze gesprekken. Zij hopen dat de Minister daar verder over kan uitweiden. In het bijzonder welke punten er absoluut onacceptabel zullen zijn.

De leden van de CDA-fractie hebben begrip voor de inzet van het kabinet op behoud van eigen autonomie waar het gaat om crisisbeheersing. Deze leden merken wel op dat cyberdreigingen grens overstijgend zijn en dat informatiedeling cruciaal is. Op nationaal niveau is de informatiedeling ook nog niet waar het zou moeten zijn en in dat kader vragen deze leden of de Minister wel in Europees verband gaat inzetten op adequate deling van dreigingsinformatie tussen lidstaten.

De leden van de CDA-fractie vragen naar de uitsluitende verantwoordelijkheid en de opvatting van het kabinet dat de plannen rondom het JCU daarmee op gespannen voet kunnen staan. Deze leden vragen welke ideeën de Minister heeft om de samenwerking te bevorderen. Ook vragen deze leden wat er gedaan kan worden wanneer andere lidstaten hun cyberveiligheid niet op orde hebben en op welke wijze er dan gehandeld moet worden door andere lidstaten. Tot slot vragen deze leden op dit punt onder welke omstandigheden en in welke gevallen Nederland aan zet

dient te zijn en in welke gevallen er sprake zou moeten zijn van een Europese aanpak.

De leden van de CDA-fractie zien een logica in de voorstellen van de Europese Commissie wat betreft de wijze waarop zij de structuur willen vormgeven. Deze leden vragen naar de structuur van signalering van cyberdreigingen in eigen land en wat er geleerd kan worden van de Europese plannen. Functioneert de huidige structuur afdoende. Deze leden vragen welke organisaties vanuit Nederland verbonden zullen zijn aan de Joint Cyber Unit.

Vragen en opmerkingen van de leden van de Volt-fractie

De leden van de Volt-fractie hebben met interesse kennisgenomen van het Fiche «aanbeveling opbouw Joint Cyber Unit» van de demissionair Minister van Buitenlandse Zaken. Deze leden zijn uiteraard voorstander van betere Europese samenwerking op het gebied van cyberveiligheid.

De leden van de Volt-fractie merken allereerst in algemene zin op dat het demissionair kabinet op een groot aantal onderwerpen van het voorstel eerst nadere uitwerking en duidelijkheid vereist. De demissionair Minister noemt daarbij een aantal onderdelen. Om welke onderdelen gaat het, anders dan de onderdelen die worden genoemd op pagina 5 van het fiche? Waar gaat de demissionair Minister specifiek op letten bij deze uitwerking? Hoe gaat de demissionair Minister de verdere uitwerking van een JCU concreet bewaken? Hoe zal de demissionair Minister bewerkstelligen dat de oprichting en ontwikkeling van een JCU in een gedegen en gefaseerd proces zal verlopen en er tegelijkertijd op wordt toegezien dat er geen onnodige vertraging optreedt? Hoe gaat het demissionair kabinet zich ervoor inzetten dat lidstaten in het gehele proces van verdere uitwerking en het operationeel maken van een JCU vertegenwoordigd zijn? Op welke momenten en op welke wijze zal de demissionair Minister deze Kamer daarbij betrekken? Welke gemeenschappelijke doelen als bedoeld op pagina 5 ziet de demissionair Minister op dit moment voor zich bij het oprichten van een JCU?

De leden van de Volt-fractie merken op dat de demissionair Minister in de brief noemt dat het demissionair kabinet zich actief inzet bij de verschillende Europese gremia die tot doel hebben de digitale weerbaarheid te vergroten. Om welke gremia gaat het anders dan de organisaties genoemd in voetnoot 15? Op welke manier zet de demissionair Minister zich in bij deze organisaties? Wat is daarbij de Nederlandse inzet en met welke andere lidstaten trekt Nederland in dit verband op? Welke andere ministeries zijn betrokken bij de voorbereiding van een JCU? Op welke manier gaat de demissionair Minister samenwerken met de andere betrokken ministeries? Welke ministeries dragen daarbij welke verantwoordelijkheden?
De leden van de Volt-fractie vragen met het oog op de doelstellingen genoemd op pagina 4 van het fiche hoe deze doelstellingen volgens de demissionair Minister zouden moeten worden uitgewerkt. Op welke manier moet de samenwerking volgens de demissionair Minister moeten worden vormgegeven? Hoe ziet de demissionair Minister de rol van Nederland in een JCU?

De leden van de Volt-fractie vragen of de demissionair Minister dan ruimte ziet om de samenwerking verplicht te stellen, voor zover samenwerking binnen een JCU niet op vrijwillige basis tot stand komt (zoals genoemd op pagina 5). Zo ja, op welke grond? Zo nee, waarom niet? De demissionair Minister merkt op dat ten aanzien van een groot aantal van de cybersecurityincidenten al in de praktijk samenwerking bestaat tussen

de lidstaten binnen reeds bestaande netwerken. Om welke samenwerkingsverbanden gaat het? Welke landen en organisaties zijn daarbij betrokken en om wat voor samenwerking gaat het? Voor welke specifieke (categorieën van) cases, waar op dit moment nog onvoldoende samenwerking tussen de verschillende lidstaten en EU-instellingen tot stand komt, ziet de demissionair Minister met name meerwaarde voor een JCU? Waar plaatst de demissionair Minister een JCU ten opzichte van andere cybersecurity samenwerkingsverbanden? Hoe ziet een «virtueel en fysiek platform», wat het JCU zou moeten worden, er volgens de demissionair Minister uit? Hoe verschilt een «virtueel en fysiek platform» volgens de demissionair Minister van een instelling? Hoe gaat de demissionair Minister er in concrete zin voor zorgen dat duplicatie met bestaande structuren waarbinnen reeds samenwerking plaatsvindt wordt voorkomen?
De leden van de Volt-fractie vragen op basis waarvan de demissionair Minister verwacht dat diverse lidstaten aandacht zullen vragen voor de rol en mate van invloed van lidstaten in het totstandkomingsproces en de activiteiten van een JCU, en de onderdelen van de aanbeveling die op gespannen voet staan met de uitsluitende verantwoordelijkheid van de lidstaten op het terrein van nationale veiligheid (als bedoeld op pagina 5). Om welke onderdelen van de aanbeveling gaat het? Om welke lidstaten gaat het? Met welke lidstaten heeft de demissionair Minister hierover contact en wat is de inhoud van dat contact?

II Reactie van de Minister van Justitie en Veiligheid

De leden van de VVD-fractie hebben kennisgenomen van het voorstel tot oprichting van een Joint Cyber Unit (JCU), maar hebben nog enkele vragen en opmerkingen met betrekking tot de meerwaarde van het op te richten platform.
De leden van de VVD-fractie lezen dat de Joint Cyber Unit geen nieuwe instantie zal worden, maar een virtueel en fysiek platform zal betreffen voor het versterken van de samenwerking tussen de in de aanbeveling geïdentificeerde operationele en ondersteunende deelnemers. Deze leden vragen dan ook welke (nieuwe) rol het JCU zal gaan vervullen in het digitaal veilig houden van lidstaten. Welk mandaat zal het JCU precies krijgen? Op basis van welke probleemanalyse is men tot dit mandaat gekomen?

De Europese Commissie bracht op 23 juni 2021 een aanbeveling uit over de opbouw van een Joint Cyber Unit (JCU). Hierin constateert de Commissie dat er nog geen gemeenschappelijk EU-platform bestaat waar informatie, afkomstig uit verschillende cybersecuritygemeenschappen efficiënt en veilig kan worden uitgewisseld en waar operationele capaciteiten kunnen worden gecoördineerd en gemobiliseerd. De Commissie heeft geconcludeerd dat een JCU nodig is om samenwerking te versterken op dit terrein op basis van een analyse door ENISA naar de sterktes en zwaktes van het EU cybersecurity landschap. In de aanbeveling wordt het proces geschetst om te komen tot het instellen van een JCU met de volgende drie doelstellingen: zorgen voor een gecoördineerde reactie binnen de EU op grootschalige cyberdreigingen, -incidenten en -crises; verbeteren van het situationeel bewustzijn; en het verbeteren van gezamenlijke paraatheid.

In recent aangenomen conclusies van de Europese Raad is door de lidstaten aangegeven dat de JCU bestaande taken en bevoegdheden van de lidstaten en de EU-instellingen, -organen en -agentschappen (EU-IOA's) onverlet dient te laten. Daarnaast dient er in de ontwikkeling van de JCU rekening gehouden te worden met de volgende beginselen, waaronder evenredigheid, subsidiariteit, inclusiviteit, complementariteit, voorkoming

van dubbel werk en vertrouwelijkheid van informatie.[1] De genoemde uitgangspunten sluiten grotendeels aan bij de inzet van het kabinet, zoals vastgelegd in het BNC-fiche inzake een JCU.[2] Deze beginselen en uitgangspunten vormen het kader waarbinnen de uitwerking van de plannen voor de JCU vorm moet krijgen. ENISA zal de komende tijd verdiepende workshops organiseren om op basis van de Raadsconclusies, samen met experts van de lidstaten en EU IOA's, de verschillende componenten van het plan voor de JCU verder uit te werken.

De verwachting is dat samenwerking binnen de JCU plaatsvindt op basis van de taken en bevoegdheden van de deelnemende partijen. Momenteel wordt nader bezien op welke juridische basis samenwerking en informatie-uitwisseling plaats zou moeten vinden binnen de JCU.

De leden van de VVD-fractie constateren voorts dat het JCU zich onder andere zal gaan bezighouden met het delen van informatie afkomstig uit verschillende cybersecuritygemeenschappen. Welke bevoegdheden zijn hierbij voorzien voor het JCU om ook deze informatie te kunnen ophalen en delen met andere partijen? Wordt hierbij een wettelijke grondslag voor informatiedeling tussen het JCU en andere organisaties geborgd? Zo nee, hoe zal het JCU dan in de praktijk dreigingsinformatie kunnen ophalen en delen? Kan de Minister ook toelichten wat wordt beoogd met cybersecuritygemeenschappen? Betreft het hier nationale samenwerkingsverbanden, waarbij bijvoorbeeld ook het Nederlandse Nationaal Cyber Security Centrum in de praktijk informatie kan gaan delen met het JCU of transnationale samenwerkingsverbanden?

In de aanbeveling wordt door de Commissie aangegeven dat de JCU zich zal richten op het verbeteren van de samenwerking tussen bestaande cybersecuritygemeenschappen. Met cybersecuritygemeenschappen wordt gedoeld op bestaande Europese netwerken, zoals het CSIRT Netwerk, het *Cyber Crisis Liaison Organisation Network (*CyCLONe) en de *Joint-Cybercrime Action Taskforce* (J-CAT) die bestaan uit vertegenwoordigers van de lidstaten en EU IOA's. De JCU gaat zich naar verwachting voornamelijk richten op het tot stand brengen en verbeteren van samenwerking tussen verschillende netwerken en organisaties die onderdeel zijn van de door de Commissie zogenoemde cybersecuritygemeenschappen binnen de EU, en niet zozeer tussen van die gemeenschappen deel uitmakende individuele organisaties. Er zal de komende tijd nader worden bezien in hoeverre toekomstige activiteiten binnen de JCU kunnen worden uitgevoerd op basis van de bestaande grondslagen voor de activiteiten van de deelnemende netwerken en organisaties. De Raad heeft opgeroepen om tijdens het proces van de totstandkoming van de JCU te blijven afwegen of een rechtsgrondslag voor de activiteiten binnen een JCU vereist is, en indien het nodig blijkt, welk instrument hiervoor dan aangewezen moet worden geacht.

De Europese Unie kent meerdere reeds bestaande cybersecurityinitiatieven zoals het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) en CERT-EU (Computer Emergency Response Team voor de EU). De leden van de VVD-fractie vragen wat zijn precies hun taken? Welke knelpunten worden geïdentificeerd bij het uitvoeren van deze taken? In hoeverre is het voorzien dat het JCU op deze knelpunten acteert? Met andere

[1] COM (2021) 12534.
[2] Kamerstuk 22 112, nr. 3182

woorden: hoe zal het JCU zich gaan verhouden qua takenpakket tot de bestaande initiatieven zoals ENISA en CERT-EU?

Om de vragen van de VVD-fractie te kunnen beantwoorden, is het van belang om allereerst te schetsen wat de taken zijn van respectievelijke ENISA en CERT-EU. ENISA heeft als doel een hoog gemeenschappelijk cyberbeveiligingsniveau te bereiken in de hele Unie, onder meer door actief steun te verlenen aan de lidstaten en de EU-IOA's. ENISA fungeert als referentiepunt voor advies en expertise op het gebied van cyberbeveiliging. De taken en bevoegdheden van ENISA zijn vastgelegd in de Cybersecurity Act.[3]CERT-EU fungeert sinds 11 september 2012 als CERT voor EU-IOA's en bestaat uit IT-beveiligingsexperts van de belangrijkste EU-instellingen (Europese Commissie, secretariaat-generaal van de Raad, Europees Parlement, Comité van de Regio's, Economisch en Sociaal Comité). De reikwijdte van de activiteiten van CERT-EU omvat preventie, detectie, respons, en herstel. Om het cyberbeveiligingsniveau van EU-IOA's te verhogen en CERT-EU beter in staat te stellen om nieuwe cybersecuritymaatregelen toe te passen en EU-IOA's te ondersteunen met het verhogen van hun weerbaarheid is versterking van het mandaat van CERT-EU en een versterkt financieringsmechanisme noodzakelijk volgens de Commissie. Eind dit jaar worden een Verordening voor gezamenlijke cybersecurityregels voor EU-IOA's en een Verordening voor informatieveiligheid van EU-IOA's verwacht om dit te waarborgen.

De JCU is in de eerste plaats bedoeld om de samenwerking tussen bestaande organisaties en netwerken te versterken en ondersteunen. Zoals aangegeven in het BNC-fiche wil het kabinet waken voor duplicatie tussen het werk van de JCU en bestaande structuren. Dit is ook onderschreven door de lidstaten in eerdergenoemde Raadsconclusies. CERT-EU en ENISA zijn door de Commissie geïdentificeerd als operationele deelnemers aan een JCU die op basis van hun eigen taken en bevoegdheden kunnen bijdragen aan het bevorderen van de activiteiten van een JCU.

De leden van de VVD-fractie lezen dat een van de doelstellingen van de JCU is om te zorgen voor een gecoördineerde reactie binnen de Europese Unie op grootschalige cyberdreigingen en dat de Europese Commissie voorstelt om EU Cybersecurity Rapid Reaction Teams op te richten om de inzet te coördineren. Overwegende dat de NAVO al in 2012 een Rapid Reaction Team heeft opgezet om cyberaanvallen af te wenden, hoe zal het JCU zich gaan verhouden tot het Rapid Reaction Team van de NAVO? Hoe vaak is het Rapid Reaction Team tot nu toe ingezet? In hoeverre zijn er mogelijkheden om de JCU te laten samenwerken met het Rapid Reaction Team van de NAVO om cyberaanvallen op lidstaten tegen te gaan?

Het kabinet wacht nog op verduidelijking op welke wijze de ontwikkeling van EU Cybersecurity Rapid Reaction Teams zal worden vormgegeven en heeft meer uitleg nodig over de praktische uitwerking hiervan en de toegevoegde waarde ten opzichte van bijvoorbeeld de Cyber Rapid Response Teams in het kader van Permanente Gestructureerde Samenwerking (PESCO). De Raad heeft het belang van deze verdere uitleg en uitwerking onderschreven in haar conclusies, ook in relatie tot het respecteren van de taken en bevoegdheden van deelnemers aan een JCU. Ook wordt benadrukt gebruik te blijven maken van bestaande initiatieven, waarbij kan worden gedacht aan PESCO's Cyber Rapid Response Teams project waar Nederland een van de zeven deelnemers is.

[3] COM (2019) 881.

Het Rapid Reaction Team van de NAVO valt onder het NAVO CERT (NCIRC). Het NCIRC heeft taken in relatie tot de NAVO-systemen maar kan ook ultimo ingezet worden voor ondersteuning van CERT-EU, daartoe zijn vertrouwelijke afspraken gemaakt. De Raad heeft in haar conclusies het belang van samenwerking tussen de EU en de NAVO nogmaals herbevestigd.

Het is op dit moment nog niet mogelijk verdere uitspraken te doen over de mogelijkheden tot samenwerking tussen de JCU en het Rapid Reaction Team van de NAVO vanwege de verdere reflectie die de Raad verzocht heeft over de toegevoegde waarde en werking van EU Cybersecurity Rapid Reaction Teams. Het uitgangspunt van het kabinet is echter wel dat er wordt gestreefd naar interoperabiliteit en standaardisatie binnen EU en NAVO zodat optimaal samengewerkt kan worden.

Ook is het voor deze leden nog onduidelijk welke kosten komen kijken bij het oprichten van het JCU. Wat is de begroting die hoort bij het oprichten van het JCU? Kan er een inschatting worden gemaakt in hoeverre deze kosten budgettaire gevolgen zullen hebben voor Nederland? De leden van de VVD-fractie menen dat de oprichting van de JCU louter (financieel) te rechtvaardigen is wanneer de JCU daadwerkelijk een toevoeging vormt op de bestaande bevoegdheden en taakstellingen van eerdergenoemde bestaande diensten en daarmee van toegevoegde waarde is in het tegengaan van cyberaanvallen op lidstaten. Deelt de Minister deze mening? Zo ja, is de Minister bereid dit onder de aandacht te brengen bij de onderhandelingen? Zo nee, waarom niet?

Zoals aangegeven in het BNC-fiche verwelkomt het kabinet het initiatief om te komen tot een JCU omdat het essentieel is om te blijven inzetten op versterking van de samenwerking tussen verschillende gemeenschappen binnen de EU, met oog op de toegenomen digitalisering en het permanente karakter van digitale dreigingen. Een beter situationeel bewustzijn is benodigd om adequaat te kunnen reageren op cyberincidenten en -crises. Met betrekking tot de financiële aspecten beschikt het kabinet niet over nieuwe informatie ten opzichte van hetgeen is verwoord in het BNC-fiche. De Commissie heeft in haar aanbeveling aangegeven dat de JCU voornamelijk gefinancierd zal worden op basis van financiële middelen vanuit het programma Digitaal Europa. Op dit moment is de inschatting van het kabinet dat er geen grote budgettaire gevolgen zijn voor Nederlandse overheidsorganisaties als gevolg van het voorstel voor een JCU. Vanzelfsprekend deelt het kabinet de mening van de VVD-fractie dat de te maken kosten proportioneel moeten zijn in relatie tot de toegevoegde waarde voor lidstaten.

De leden van de D66-fractie hebben met interesse kennisgenomen van de BNC-fiches met betrekking tot de Europese Joint Cyber Unit. Deze leden hebben kennisgenomen van de inzet van het kabinet op meer Europese samenwerking tussen bestaande organisaties die niet hoeft te leiden tot extra schakels maar tot effectievere samenwerking. Deze leden hebben nog enkele vragen.

De leden van de D66-fractie lezen dat de Europese cybereenheid uiterlijk 30 juni 2022 de operationele fase moet ingaan. Deze leden vragen de Minister toe te lichten welke volgende stappen vanuit het kabinet ondernomen zullen worden met betrekking tot de uitwerking van de Joint Cyber Unit. Deze leden lezen dat de noodzaak en urgentie van een Europese cybereenheid wordt

ondersteund, maar wel bewaakt zal worden dat lidstaten zelf primair verantwoordelijk blijven voor het reageren op grote cyberveiligheidsincidenten en crises. De leden vragen de Minister toe te lichten wat de competentieverdeling zal zijn tussen de Europese Unie en de lidstaten in het geval van een cyberaanval. Onder welke omstandigheden zal Nederland zelf handelen? Welke maatstaf zal de Europese Commissie gebruiken voor de definitie van grote incidenten? De leden van de CDA-fractie vragen onder welke omstandigheden en in welke gevallen Nederland aan zet dient te zijn en in welke gevallen er sprake zou moeten zijn van een Europese aanpak.

Zoals vermeld in antwoord op de vragen van de VVD-fractie, zal ENISA de komende tijd verdiepende workshops organiseren om op basis van de Raadsconclusies, samen met experts van de lidstaten en EU IOA's, de verschillende componenten van het JCU-plan verder uit te diepen. Hierbij is onder meer aandacht voor het opstellen van een nieuwe tijdlijn, proces en mijlpalen, alvorens wordt toegewerkt naar een implementatieplan. Vanuit Nederland zullen hierbij experts van verschillende ministeries betrokken zijn die deel uitmaken van de verschillende genoemde cybersecuritygemeenschappen om te borgen dat aansluiting wordt gezocht bij de praktijk en de behoeften.

De aanbeveling inzake een JCU ziet op grootschalige cyberincidenten en -crises, zoals gedefinieerd in de Commissie Aanbeveling inzake een gecoördineerde respons op grootschalige cyberincidenten en -crises.[4] Het is primair de verantwoordelijkheid van de lidstaten om te reageren als zij getroffen worden door grootschalige cyberincidenten of -crises. Op initiatief van lidstaten bestaan er ook mogelijkheden bijv. via het CSIRT Netwerk om, waar mogelijk, een gecoördineerde reactie op incidenten te bepalen en elkaar bijstand bij de aanpak van incidenten te verlenen. Ook heeft de Raad nogmaals benadrukt dat bijdragen van lidstaten aan een JCU gebaseerd zijn op vrijwilligheid en dat samenwerking op EU-niveau wat betreft grootschalige cyberincidenten en -crises gevoerd wordt in overeenstemming met de beginselen van subsidiariteit, evenredigheid, complementariteit, voorkoming van dubbel werk, en vertrouwelijkheid.

De leden van de D66-fractie constateren dat er via een Joint Cyber Unit veel kennis en tools gedeeld zullen worden binnen de Europese Unie. De leden vragen de Minister toe te lichten hoe er gewaarborgd zal worden dat belangrijke informatie beschermd zal blijven, bijvoorbeeld van externe mogendheden. Kan de Minister toelichten hoe het kabinet zal toezien op een hoog niveau van beveiliging van dit virtuele en fysieke platform? De leden van de D66-fractie constateren dat het kabinet vervolggesprekken met alle betrokkenen wenst over uitwerking van randvoorwaarden van informatie-uitwisseling en het garanderen van de vertrouwelijkheid van informatie. Deze leden vragen de Minister om toe te lichten wat de inzet is van het kabinet om zoveel mogelijk te waarborgen dat de informatie vertrouwelijk is en blijft tegenover derde landen.

---

[4] «*Cyberincidenten die verstoringen veroorzaken die te groot zijn om door een getroffen lidstaat alleen te worden verholpen of die zodanig verstrekkende en significante technische of politieke gevolgen hebben voor twee of meer lidstaten of EU-instellingen dat tijdige coördinatie en respons op het politieke niveau van de Unie vereist zijn. Dergelijke grootschalige cyberincidenten worden als een «cybercrisis» beschouwd*» [COM (2017) 6100].

De Commissie stelt in haar aanbeveling dat ENISA verantwoordelijk zal zijn om een veilig virtueel platform op te zetten en daarnaast een fysieke locatie ter beschikking te stellen voor ad hoc samenwerking van deelnemers binnen de JCU. Binnen de EU bestaat reeds een stelsel voor informatiebeveiliging, waar regelgeving voor fysieke beveiliging en beveiliging van ICT-systemen onderdeel van is. Dit stelsel zal ook van toepassing zijn op het faciliteren van ENISA van een dergelijk JCU-platform. De hoofdverantwoordelijkheid voor het toezicht op de naleving van de regelgeving ligt bij de EU IOA's zelf. Daarnaast kunnen lidstaten specifieke eisen aan de beveiliging op (laten) nemen in de verdere uitwerking van de JCU-plannen om toe te zien op een hoog niveau van beveiliging van het platform.

Verder wil het kabinet verwijzen naar de eerdere beantwoording van de VVD-fractie waarin uiteengezet is wat reeds op EU-niveau wordt ondernomen om de vertrouwelijkheid van informatie te waarborgen.[5] Tenslotte heeft de Raad in haar conclusies, mede op basis van inzet van het kabinet, benadrukt dat er met prioriteit aandacht uit zal moeten gaan naar de adequate beveiliging van het platform en veilige communicatiekanalen voor het uitwisselen van informatie.

De leden van de D66-fractie vragen de Minister of er nog afwegingen gemaakt worden tussen welke lidstaten er wel of niet gedeeld wordt. Krijgen lidstaten die niet actief bijdragen aan de Joint Cyber Unit ook toegang tot alle kennis en tools die andere lidstaten delen? De leden van de D66-fractie lezen dat de Joint Cyber Unit gebaseerd is op inbreng van lidstaten op vrijwillige basis. Deze leden lezen dat onder andere de inbreng van een nationaal cybersecurity incident- en crisisresponsplan alleen vrijwillig kan gebeuren. Acht de Minister het wenselijk dat er eventueel grote verschillen tussen lidstaten ontstaan met betrekking tot digitale veiligheid?

Een belangrijk uitgangspunt voor het kabinet is dat de JCU gebaseerd zal zijn op vrijwillige bijdragen van lidstaten en ten dienste moet staan van lidstaten. Dit is mede op basis van Nederlandse inzet ook opgenomen in de Raadsconclusies. Daarbij heeft de Raad opgeroepen dat de nodige aandacht moet blijven uitgaan naar veilige communicatiekanalen voor de uitwisseling van gerubriceerde en gevoelige informatie.
Gelet op de onderlinge verwevenheid van lidstaten binnen de EU en het grensoverschrijdende karakter van digitale dreiging, acht het kabinet het van belang dat alle lidstaten toegang hebben tot de JCU zodat lidstaten de schaarse capaciteiten op het gebied van cybersecurity zo effectief mogelijk kunnen inzetten en lidstaten die minder mogelijkheden hebben om actief bij te dragen ook kunnen leren van meer volwassen lidstaten en in staat worden gesteld hun capaciteiten verder op te bouwen. Het kabinet verwacht dat samenwerking en informatie-uitwisseling binnen een JCU een gunstig effect kan hebben op het verbeteren van de paraatheid van alle lidstaten.

De leden van de D66-fractie constateren dat middels de Europese cybereenheid, belangrijke informatie en kennis van Nederlandse organisaties richting het coördinatiepunt zal gaan. Deze leden, en de leden van het CDA, vragen de Minister te specifiëren welke Nederlandse organisaties verbonden zullen zijn aan dit Europese netwerk.

[5] Eind dit jaar worden een Verordening voor gezamenlijke cybersecurityregels voor EU-IOA's en een Verordening voor informatieveiligheid van EU-IOA's verwacht die zien op een hoog niveau van informatieveiligheid en cybersecurity van EU IOA's.

Het is nog te vroeg om uitspraken te doen over welke specifieke kennis en informatie vanuit Nederland met een JCU zouden worden gedeeld. Dit zal in grote mate afhankelijk zijn van de verdere uitwerking van de doelen en functionaliteiten van een JCU. Het is voorstelbaar dat Nederlandse organisaties die actief zijn binnen de genoemde netwerken uit de aanbeveling in de toekomst in enigerlei vorm betrokken zullen zijn bij de activiteiten binnen de JCU om toe te werken naar een sneller en beter situationeel beeld. Dit betreft onder andere het NCSC, de NCTV, de Nationale Politie en het Ministerie van BZ en Defensie.

De leden van de D66-fractie lezen dat de aanbeveling van de Joint Cyber Unit onderdeel is van een grotere EU Cybersecuritystrategie, onder andere een Europese wet op de cyberweerbaarheid. De leden vragen de Minister toe te lichten of er eventuele raakpunten of conflicten zijn tussen deze wetsvoorstellen en de Nederlandse wetten rondom cyberveiligheid, en welke uitdagingen hij hier ziet. De leden van de D66-fractie horen specifiek graag van de Minister op welke manier dit voorstel samenkomt en een aanvulling vormt met het door de Europese Commissie aangekondigde Cyber Resilience Act en daarnaast met de door de Verenigde Staten aangekondigde verbond tegen ransomware, het Counter-Ransomware Initiative.

In de EU Cyberstrategie wordt onder andere ook verwezen naar het voorstel van de Commissie voor de herziening van de NIB-richtlijn (NIB2) en het voorstel voor de richtlijn veerkracht kritieke entiteiten.[6] De onderhandelingen over beide richtlijnen vinden op dit moment plaats. Eerstgenoemde regelt onder andere ook de werking van het CSIRT Netwerk en CyCLONe, die naar verwachting ook een rol zullen krijgen in het kader van samenwerking binnen de JCU. Veel Nederlandse wetgeving op het gebied van cybersecurity betreft implementatie van Europese regelgeving, zoals de Wet beveiliging netwerk- en informatiesystemen (Wbni).

Op dit moment is er bij het kabinet nog weinig bekend over de recent door de Commissie aangekondigde Cyber Resilience Act. Naar verwachting zal deze verordening zich voornamelijk richten op minimum standaarden voor apparaten die op het internet zijn aangesloten. Beide voorstellen beogen bij te dragen aan de digitale weerbaarheid van de EU vanuit verschillende invalshoeken, maar de directe raakvlakken lijken beperkt.
Verder kan het kabinet mededelen dat een gedetailleerd beeld van de praktische uitwerking van het recent door de Verenigde Staten gelanceerde *Counter-Ransomware Initiative* nog ontbreekt waardoor het lastig is om te bezien of en hoe de samenwerking van een JCU samenkomt met dit initiatief.

De leden van de D66-fractie lezen dat uit de IOB Cybersecurity evaluatie van juni 2021 blijkt dat ambtenaren van het Ministerie van Buitenlandse Zaken vaak werken met verouderde en onveilige middelen, waardoor de communicatie niet goed verloopt. Welke stappen zijn er sindsdien genomen om dit recht te zetten?

BZ werkt sinds 2019 aan de vernieuwing van de systemen voor staatsgeheime communicatie met de posten. Door COVID-19 is de uitrol van dit project sterk vertraagd vanwege de noodzaak om naar verschillende

[6] COM (2020) 18.

posten te reizen. De uitrol van de nieuwe middelen is weer hervat gelet op het opheffen van reisbeperkingen en quarantaine eisen. De planning is dat eind dit jaar alle posten waarmee communicatie op niveau (staats)geheim noodzakelijk is, zullen zijn voorzien van de nieuwe apparatuur, mits de COVID-19 beperkingen dat toelaten.

De leden van de D66-fractie concluderen dat het voorstel vooral gaat om het delen van kennis en tools binnen de Europese Unie. Deze leden vragen de Minister of deze Europese Cybereenheid ook zal samenwerken met landen die geen lidstaat zijn, en welke extra kansen een sterkere Europese samenwerking biedt tot meer mondiale samenwerking.

In het ontwikkelproces van een JCU heeft de Commissie voorzien dat vanuit JCU-verband op termijn zou kunnen worden samengewerkt met internationale partners buiten de EU. Het proces richt zich in de eerste fase op het opbouwen van vertrouwen en operationeel krijgen van de samenwerking van organisaties binnen de EU en zal daarna aandacht besteden aan de externe dimensie.

De leden van de D66-fractie lezen dat het kabinet als prioriteit heeft om vertrouwen en veilige informatie-wisseling op te bouwen tussen deelnemers. Deze leden vragen de Minister om voorbeelden van voorstellen om het vertrouwen tussen lidstaten op te bouwen wat betreft digitale veiligheid. Ziet de Minister kansen om lidstaten aan te moedigen zich aan te sluiten bij de Europese Cyber Unit? Zo ja, op welke manier gaat de Minister zich hiervoor inzetten?

Vanwege de ontwikkelingen in het dreigingsbeeld en de toenemende verwevenheid vindt het kabinet Europese samenwerking en informatie-uitwisseling op het gebied van cybersecurity van groot belang. Het kabinet is dan ook tevreden dat de noodzaak daartoe door de lidstaten wordt onderschreven in de Raadsconclusies. Zoals aangegeven, is een belangrijk uitgangspunt voor het kabinet dat de JCU gebaseerd zal zijn op vrijwillige bijdragen van lidstaten en ten dienste moet staan van lidstaten. Op dit moment wordt al op reguliere basis informatie uitgewisseld tussen de lidstaten binnen de verschillende netwerken, zoals het CSIRT netwerk. Het kabinet vertrouwt er dan ook op dat lidstaten bereid zullen zijn om informatie uit te wisselen binnen de JCU, mits onder meer aan de randvoorwaarden van vrijwilligheid en vertrouwelijkheid wordt voldaan.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het fiche over de Joint Cyber Unit. Deze leden lezen dat het kabinet het uitgangspunt om te streven naar versterkte informatie-uitwisseling steunt, maar dat over vervolggesprekken met alle betrokkenen over de uitwerking en randvoorwaarden er nog veel vragen zijn. Deze leden lezen weinig over de concrete inzet van het kabinet bij deze gesprekken. Zij hopen dat de Minister daar verder over kan uitweiden. In het bijzonder welke punten er absoluut onacceptabel zullen zijn.

Het kabinet benadrukt in de gesprekken inzake de verdere uitwerking van de JCU onder meer het belang van goede samenhang en aansluiting van de JCU op bestaande netwerken en initiatieven binnen de EU, zoals het CSIRT Netwerk, CyCLONe, de NIB-Samenwerkingsgroep, de Raadswerkgroep Cyber, de Joint-Cybercrime Action Taskforce en EU-INTCEN. Ook zet het kabinet in op het voorkomen van duplicatie met bestaande structuren waarbinnen reeds samenwerking plaatsvindt. In navolging hiervan heeft de Raad in haar conclusies onderstreept dat de

informatiebehoeften- en lacunes in en tussen cybergemeenschappen verder in kaart gebracht dienen te worden om activiteiten van de JCU beter te kunnen richten. Ook heeft de Raad de noodzaak van veilige communicatiekanalen voor samenwerking en informatie-uitwisseling benadrukt waarbij rekening gehouden dient te worden met reeds beschikbare infrastructuur.

Om als Nederland goed aangesloten te zijn bij de verdere uitwerking van de JCU, heeft het kabinet ingezet op betrokkenheid en een juiste balans tussen afvaardigingen van lidstaten en EU-IOA's binnen het totstandkomingsproces van de JCU. Enkele zaken acht het kabinet op dit moment onwenselijk, zoals verplichte bijdragen van lidstaten aan een JCU of de oprichting van een nieuwe entiteit.

De leden van de CDA-fractie hebben begrip voor de inzet van het kabinet op behoud van eigen autonomie waar het gaat om crisisbeheersing. Deze leden merken wel op dat cyberdreigingen grens overstijgend zijn en dat informatiedeling cruciaal is. Op nationaal niveau is de informatiedeling ook nog niet waar het zou moeten zijn en in dat kader vragen deze leden of de Minister wel in Europees verband gaat inzetten op adequate deling van dreigingsinformatie tussen lidstaten.

Zoals aangegeven in antwoord op de vragen van de leden van de D66-fractie onderschrijft het kabinet het belang van Europese samenwerking op het gebied van cybersecurity, inclusief informatiedeling. Zowel nationaal als internationaal wordt informatie gedeeld over cyberdreigingen en -kwetsbaarheden. Op nationaal niveau gebeurt dit bijvoorbeeld via schakelorganisaties die deel uitmaken van het Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden, binnen de Cyber Info/Intel Cel en via het interdepartementale diplomatieke responskader voor cyber-incidenten.[7] Diverse Nederlandse overheidsorganisaties dragen actief bij aan informatie- en expertise-uitwisseling binnen Europese netwerken geïdentificeerd als deelnemers binnen een JCU.

Het kabinet zal zich dan ook blijven inzetten voor het verbeteren van informatiedeling, zowel op nationaal als Europees niveau. Over het verbeteren van informatiedeling op nationaal niveau heb ik uw Kamer reeds geïnformeerd.[8]

De leden van de CDA-fractie vragen naar de uitsluitende verantwoordelijkheid en de opvatting van het kabinet dat de plannen rondom het JCU daarmee op gespannen voet kunnen staan. Deze leden vragen welke ideeën de Minister heeft om de samenwerking te bevorderen. Ook vragen deze leden wat er gedaan kan worden wanneer andere lidstaten hun cyberveiligheid niet op orde hebben en op welke wijze er dan gehandeld moet worden door andere lidstaten.

Het kabinet acht gezien de onderlinge verwevenheid van lidstaten binnen de EU en het grensoverschrijdende karakter van digitale dreiging, het van belang dat alle lidstaten toegang hebben tot de JCU, zodat lidstaten de

---

[7] Binnen deze cel werken AIVD, MIVD, NCSC, OM en Politie samen ten behoeve van het versterken van een landelijk situationeel beeld ten aanzien van cyberdreigingen en -incidenten, het op basis daarvan door partijen in relatie tot die dreigingen en incidenten beter kunnen uitoefenen van hun wettelijke taken, het meer en sneller bieden van handelingsperspectief aan andere belanghebbende organisaties inzake cyberdreigingen, en het hierdoor vergroten van de digitale slagkracht van genoemde organisaties en versterken van de veiligheid in het digitale domein. De CIIC is bij Convenant opgericht (Stcrt. 2020, nr. 30702).

[8] Kamerstuk 26 643, nr. 738; Kamerstuk 26 643, nr. 767.

schaarse capaciteiten op het gebied van cybersecurity zo effectief mogelijk kunnen inzetten. Daarnaast is het belangrijk dat lidstaten die minder mogelijkheden hebben om actief bij te dragen aan een JCU ook kunnen leren van lidstaten met verder ontwikkelde cybercapaciteiten en zo in staat worden gesteld hun capaciteiten verder op te bouwen.

Deelname op basis van vrijwilligheid dient volgens het kabinet het uitgangspunt te zijn. Het kabinet wijst er daarbij op dat op dit moment het voorstel voor de herziening van de NIB-richtlijn in onderhandeling is, die de lidstaten onder andere verplicht om nationale capaciteiten op het gebied van cybersecurity te ontwikkelen en een mechanisme introduceert voor peer-reviews om het wederzijds leren tussen lidstaten te versterken.

De leden van de CDA-fractie zien een logica in de voorstellen van de Europese Commissie wat betreft de wijze waarop zij de structuur willen vormgeven. Deze leden vragen naar de structuur van signalering van cyberdreigingen in eigen land en wat er geleerd kan worden van de Europese plannen. Functioneert de huidige structuur afdoende.

Om te komen tot een nationale structuur waarin cyberdreigingen adequaat en tijdig worden onderkend zijn met de uitwerking van de Nederlandse Cybersecurity Agenda (NCSA) diverse beleidsinitiatieven gestart. De structuur voor het signaleren van cyberdreigingen is in Nederland de afgelopen jaren sterk doorontwikkeld, waartoe bijvoorbeeld de Cyber Info/Intel Cel is opgericht. Naast het signaleren van cyberdreigingen door overheidspartijen zelf, wordt ook ingezet op een Landelijk Dekkend Stelsel van cybersecurity samenwerkingsverbanden, waarbinnen schakelorganisaties zo veel als mogelijk relevante informatie over digitale dreigingen en incidenten kunnen uitwisselen, ten behoeve van de informatievoorziening richting hun onderscheidenlijke doelgroepen. Omdat het veld en de dreiging zich blijven ontwikkelen, zijn voortdurend investeringen nodig om de dreiging het hoofd te kunnen blijven bieden.

De leden van de Volt-fractie hebben met interesse kennisgenomen van het Fiche «aanbeveling opbouw Joint Cyber Unit» van de demissionair Minister van Buitenlandse Zaken. Deze leden zijn uiteraard voorstander van betere Europese samenwerking op het gebied van cyberveiligheid.

De leden van de Volt-fractie merken allereerst in algemene zin op dat het demissionair kabinet op een groot aantal onderwerpen van het voorstel eerst nadere uitwerking en duidelijkheid vereist. De demissionair Minister noemt daarbij een aantal onderdelen. Om welke onderdelen gaat het, anders dan de onderdelen die worden genoemd op pagina 5 van het fiche? Waar gaat de demissionair Minister specifiek op letten bij deze uitwerking? Hoe gaat de demissionair Minister de verdere uitwerking van een JCU concreet bewaken? Hoe zal de demissionair Minister bewerkstelligen dat de oprichting en ontwikkeling van een JCU in een gedegen en gefaseerd proces zal verlopen en er tegelijkertijd op wordt toegezien dat er geen onnodige vertraging optreedt? Hoe gaat het demissionair kabinet zich ervoor inzetten dat lidstaten in het gehele proces van verdere uitwerking en het operationeel maken van een JCU vertegenwoordigd zijn? Op welke momenten en op welke wijze zal de demissionair Minister deze Kamer daarbij betrekken? Welke gemeenschappelijke doelen als bedoeld op pagina 5 ziet de demissionair Minister op dit moment voor zich bij het oprichten van een JCU?

Het kabinet heeft binnen de Raad gepleit voor een sterke rol van de lidstaten in het verdere ontwikkelproces van de JCU, en dit is ook zo opgenomen in de Raadsconclusies. De rol van lidstaten zal geborgd worden via de Raadswerkgroep Cyber, onder andere door regelmatige bespreking van voortgangsrapportages over het proces van de totstandkoming van de JCU. Om onnodige vertraging te voorkomen zal het kabinet inzetten op voldoende betrokkenheid van verschillende (nationale) experts vanuit de verschillende cybergemeenschappen. Dit om een bijdrage te leveren aan de uitwerking en implementatie van een JCU en het verder opbouwen van vertrouwen tussen de betrokken cybergemeenschappen. Het kabinet zal de Tweede Kamer over voortgang informeren indien daar aanleiding toe is.

De leden van de Volt-fractie merken op dat de demissionair Minister in de brief noemt dat het demissionair kabinet zich actief inzet bij de verschillende Europese gremia die tot doel hebben de digitale weerbaarheid te vergroten. Om welke gremia gaat het anders dan de organisaties genoemd in voetnoot 15? Op welke manier zet de demissionair Minister zich in bij deze organisaties? Wat is daarbij de Nederlandse inzet en met welke andere lidstaten trekt Nederland in dit verband op? Welke andere ministeries zijn betrokken bij de voorbereiding van een JCU? Op welke manier gaat de demissionair Minister samenwerken met de andere betrokken ministeries? Welke ministeries dragen daarbij welke verantwoordelijkheden?

Dit betreft andere Europese gremia waarin Nederlandse overheidsorganisaties kennis en expertise delen met organisaties van andere lidstaten ter vergroting van de digitale weerbaarheid zoals de *Joint-Cybercrime Action Taskforce* waarin de politie Nederland vertegenwoordigd, het *European Judicial Cybercrime Network* waarin het OM namens Nederland plaatsheeft en cyber defensie gerelateerde projecten gelanceerd onder PESCO zoals de Cyber Rapid Response Teams waarbinnen het Ministerie van Defensie actief is.
Onder coördinatie van het Ministerie van JenV wordt in nauwe afstemming tussen de ministeries JenV, BZ, BZK, EZK en Defensie de Nederlandse inbreng in de overleggen over de JCU voorbereid. Deze ministeries zijn betrokken bij de JCU vanwege hun verantwoordelijkheden voor beleidsterreinen die in het geding zijn bij de JCU-plannen.

De leden van de Volt-fractie vragen met het oog op de doelstellingen genoemd op pagina 4 van het fiche hoe deze doelstellingen volgens de demissionair Minister zouden moeten worden uitgewerkt. Op welke manier moet de samenwerking volgens de demissionair Minister moeten worden vormgegeven? Hoe ziet de demissionair Minister de rol van Nederland in een JCU?

Nederland zal verder invulling geven aan zijn bijdrage aan de eerdergenoemde workshops georganiseerd door ENISA en verdere vervolgstappen in het proces op basis van de kabinetsinzet, zoals vastgelegd in het BNC-fiche.

De leden van de Volt-fractie vragen of de demissionair Minister dan ruimte ziet om de samenwerking verplicht te stellen, voor zover samenwerking binnen een JCU niet op vrijwillige basis tot stand komt (zoals genoemd op pagina 5). Zo ja, op welke grond? Zo nee, waarom niet?

Zoals aangegeven in het BNC-fiche is het uitgangspunt voor Nederland dat samenwerking binnen de JCU op vrijwillige basis plaatsvindt. Een verplichte samenwerking is wat het kabinet betreft dus niet aan de orde.

De demissionair Minister merkt op dat ten aanzien van een groot aantal van de cybersecurityincidenten al in de praktijk samenwerking bestaat tussen de lidstaten binnen reeds bestaande netwerken. De leden van de Volt-fractie vragen om welke samenwerkingsverbanden gaat het? Welke landen en organisaties zijn daarbij betrokken en om wat voor samenwerking gaat het? Voor welke specifieke (categorieën van) cases, waar op dit moment nog onvoldoende samenwerking tussen de verschillende lidstaten en EU-instellingen tot stand komt, ziet de demissionair Minister met name meerwaarde voor een JCU?

Reeds bestaande samenwerking in de EU op cyberincidenten vindt onder andere plaats binnen het CSIRT Netwerk, EU-CyCLONe, de NIB-Samenwerkingsgroep, de Raadswerkgroep Cyber, de Joint Cybercrime Taskforce en EU INTCEN waarin lidstaten en EU-organisaties vertegenwoordigd zijn. Deze netwerken hebben ieder een specifieke rol in samenwerking, informatie-uitwisseling, en eventuele coördinatie. Een voorbeeld hiervan is het CSIRT Netwerk, waarin de CSIRT's die lidstaten hebben ingericht krachtens de NIB-richtlijn technische informatie over dreigingen en incidenten waar mogelijk uitwisselen. Aangezien het instellen van en de activiteiten binnen de JCU nog nader moeten worden uitgewerkt, kan het kabinet in deze fase nog geen specifieke (categorieën) van cases noemen waarvoor de samenwerking binnen de JCU in het bijzonder meerwaarde ten opzichte van bestaande samenwerkingsvormen zou hebben.

De leden van de Volt-fractie vragen waar de demissionair Minister een JCU plaatst ten opzichte van andere cybersecurity samenwerkingsverbanden? Hoe ziet een «virtueel en fysiek platform», wat het JCU zou moeten worden, er volgens de demissionair Minister uit? Hoe verschilt een «virtueel en fysiek platform» volgens de demissionair Minister van een instelling? Hoe gaat de demissionair Minister er in concrete zin voor zorgen dat duplicatie met bestaande structuren waarbinnen reeds samenwerking plaatsvindt wordt voorkomen?

Een JCU beoogd een gemeenschappelijk EU-platform te organiseren waar informatie, afkomstig uit verschillende cybersecuritygemeenschappen efficiënt en veilig kan worden uitgewisseld. De Commissie omschrijft het fysiek platform als een locatie die beschikbaar is voor deelnemers aan de JCU wanneer benodigd om bij te dragen aan de volgende drie doelstellingen van de JCU: zorgen voor een gecoördineerde reactie binnen de EU op grootschalige cyberdreigingen, -incidenten en -crises; verbeteren van het situationeel bewustzijn; en het verbeteren van gezamenlijke paraatheid. Het virtueel platform zal bestaan uit digitale middelen die veilige informatie-uitwisseling en samenwerking tussen de deelnemers binnen een JCU ondersteunen.

Het kabinet zet erop in dat de JCU zich ontwikkelt tot een samenwerkingsplatform ten dienste van genoemde gemeenschappen, dat geen nieuwe organisatie wordt én waarvan de activiteiten niet overlappen met die van bestaande structuren en samenwerkingsverbanden.

De leden van de Volt-fractie vragen op basis waarvan de demissionair Minister verwacht dat diverse lidstaten aandacht zullen vragen voor de rol en mate van invloed van lidstaten in het

totstandkomingsproces en de activiteiten van een JCU, en de onderdelen van de aanbeveling die op gespannen voet staan met de uitsluitende verantwoordelijkheid van de lidstaten op het terrein van nationale veiligheid (als bedoeld op pagina 5). Om welke onderdelen van de aanbeveling gaat het? Om welke lidstaten gaat het? Met welke lidstaten heeft de demissionair Minister hierover contact en wat is de inhoud van dat contact?

Nederland kan vanwege de vertrouwelijkheid waarin deze onderhandelingen en gesprekken plaatsvinden geen uitspraak doen over de inzet van individuele lidstaten. De gezamenlijke positie van de lidstaten is uiteengezet in de Raadsconclusies waarin lidstaten onder andere oproepen tot reflectie inzake de plannen op het gebied van EU Cybersecurity Rapid Reaction Teams en het EU-plan voor incident- en crisisrespons met oog op het onder meer respecteren van de uitsluitende verantwoordelijkheid van de lidstaten op het terrein van nationale veiligheid.