Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1113

BRIEF VAN DE MINISTERS VAN ECONOMISCHE ZAKEN EN VAN JUSTITIE EN VEILIGHEID EN DE STAATSSECRETARIS VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 februari 2025

Hierbij bieden wij uw Kamer de geannoteerde agenda aan van de Informele Telecomraad op 4 en 5 maart 2025 in Warschau, Polen. Deze informele Telecomraad zal in het teken staan van cybersecurity. Gelet op zijn coördinerende verantwoordelijkheid ten aanzien van cybersecurity, zal de Minister van Justitie en Veiligheid hieraan deelnemen.

In verband met het grensoverschrijdende karakter van cyberdreigingen en het belang van het versterken van de digitale weerbaarheid van Nederland en de EU, verwelkomt het kabinet het initiatief van het Pools voorzitterschap van de Raad van Ministers van de Europese Unie om als Raad bijeen te komen en gedachten te wisselen over cybersecurity. Het kabinet kijkt uit naar de verspreiding van de uitgebreide agenda en stukken van deze Raad.

De Minister van Economische Zaken,
D.S. Beljaarts

De Minister van Justitie en Veiligheid,
D.M. van Weel

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
F.Z. Szabó

kst-21501-33-1113
ISSN 0921 - 7371
's-Gravenhage 2025

Geannoteerde agenda Informele Telecomraad, 4 en 5 maart 2025 in Warschau, Polen

In de Nederlandse Cybersecuritystrategie (NLCS) wordt de kabinetsbrede inzet voor het realiseren van een digitaal veilige samenleving uiteengezet en wordt, gelet op het grensoverschrijdende karakter van cyberdreigingen, het belang van internationale samenwerking op het gebied van cybersecurity in onder meer EU-verband benadrukt.[1] In lijn met de Kamerbrief Weerbaarheid tegen militaire en hybride dreigingen die 6 december jl. met uw Kamer is gedeeld, ondersteunt het kabinet de versterking van de (digitale) weerbaarheid in EU-verband en heeft het met interesse kennisgenomen van het rapport van speciaal adviseur Sauli Niinistö.[2, 3] Dit rapport dient als basis voor de aankomende *Preparedness Union Strategy* van de Europese Commissie (de Commissie), die ook zal werken aan Europese paraatheid en weerbaarheid.

Het kabinet zet zich actief in bij de verschillende Europese gremia en samenwerkingsverbanden die tot doel hebben de digitale weerbaarheid in de EU te vergroten en verwelkomt daarom het initiatief van het Pools voorzitterschap om als Raad bijeen te komen en gedachten te wisselen over cybersecurity. Op het moment van schrijven zijn er nog geen stukken of definitieve agenda voor deze Telecomraad verspreid. Het kabinet kijkt daarom uit naar de voorbereidende stukken en uitgebreide agenda en zal de besproken onderwerpen verder toelichten aan uw Kamer via het verslag.

1. Werksessie: Cybercrisismanagement

In pijler I van de NLCS stelt het kabinet het doel het vermogen van organisaties om te reageren, herstellen en leren van cyberincidenten te vergroten. Om dit te realiseren heeft het kabinet op nationaal niveau al stappen gezet om samenwerkingen ten tijde van grootschalige cybercrises en incidenten te versterken, onder andere door de publicatie van het Landelijk Crisis Plan Digitaal (LCP-D) en de grootschalige cyber oefening ISIDOOR IV van november 2023.[4] Waar relevant zal het kabinet nationale *best practices* dan ook opbrengen in de Raad.
Ook op Europees niveau wordt, zoals ook in het Niinistö rapport wordt onderstreept, door lidstaten tegenwoordig over het algemeen beter voorbereid op grootschalige cyber crises en incidenten, mede dankzij de cybersecuritywet- en regelgeving die deze laatste jaren is ontwikkeld en versterkt. Ook initiatieven zoals het *European Cyber Crisis Liaison Officers Network* (ook wel: CyCLONe), die in 2020 is gelanceerd, dragen sterk bij aan het versterken van de samenwerking ten tijde van grootschalige cyber crises en incidenten. Het kabinet ziet echter kansen om de samenwerking voor wat betreft de respons op (grootschalige) cyberincidenten nog verder te bevorderen en verwelkomt daarom het initiatief van de Commissie om de Blueprint inzake Grootschalige Cyber Incidenten (*Blueprint Cyber*) dit jaar te herzien. Wanneer de *Blueprint Cyber* tijdens de Raad wordt besproken, zal het kabinet voorstellen steunen om recente beleids- en stelselontwikkelingen op te nemen in de *Blueprint Cyber,* zodat dit document effectief en concreet kan bijdragen ten tijde van grootschalige grensoverschrijdende cybercrises en incidenten, waar volgens het kabinet de meerwaarde van dit document ligt. Het vergroten van de reikwijdte van de *Blueprint Cyber* buiten cybercrisismanagement, doet volgens het kabinet afbreuk aan de toegevoegde waarde. Wanneer de

---

[1] Kamerstuk 26 643, nr. 925, 10 oktober 2022.
[2] Kamerstuk 30 821, nr. 249, 6 december 2024.
[3] Uw Kamer wordt binnen afzienbare tijd geïnformeerd over de kabinetsappreciatie.
[4] Kamerstuk 26 643, nr. 955, 23 december 2022.

herziene *Blueprint Cyber* wordt gepubliceerd, zal het kabinet een uitgebreide appreciatie met uw Kamer delen via de reguliere BNC-procedure.

2. Werklunch: Civiel-militaire samenwerking

Het kabinet zet zich in om de digitale weerbaarheid van Nederland tegen militaire en hybride dreigingen versterken.[5] In voorgenoemde Niinistö-rapport wordt een *whole-of-society* samenwerking aangeraden ter versterking van onze weerbaarheid, onder meer door een versterkte civiel-militaire samenwerking. Het kabinet onderschrijft de waarde van goede civiel-militaire samenwerking en samenhang en zet zich hier zowel op nationaal als Europees niveau voor in. Hiertoe pleit het kabinet voor de instandhouding van de toekomstbestendigheid van het beleid dat betrekking heeft op civiel-militaire samenwerking, waarbij duplicatie binnen en tussen initiatieven van beide domeinen wordt voorkomen en samenhang wordt bevorderd. Hierbij is inspraak van lidstaten van groot belang, zeker waar het gaat om civiel-militaire initiatieven die kunnen raken aan de uitsluitende verantwoordelijkheid van lidstaten op het gebied van bescherming van nationale veiligheid (artikel 4, lid 2, VEU). Daarbij acht het kabinet het wenselijk dat de budgetten voor (Europese) defensie-investeringen op het gebied van cybersecurity ook zo veel mogelijk bijdragen aan en ten goede komen van civiele bescherming. Het kabinet ziet civiel-militaire initiatieven daarom graag geagendeerd in zowel de civiele als militaire (Raads)werkgroepen. Daarbij blijft betere samenwerking tussen de NAVO en EU een speerpunt van het kabinet.[6]

3. Werksessie II: Cyberinvesteringen

Het kabinet kijkt met interesse naar verdere toelichting van dit agendapunt en naar het voornemen van het Pools voorzitterschap ten aanzien van cyberinvesteringen op Europees niveau. Zoals omschreven in de NLCS is cybersecurity voor het kabinet een investering in onze toekomst en is het van belang om in te spelen op toekomstige kansen en dreigingen. Digitale weerbaarheid biedt concurrentievoordelen en versterkt onder meer innovatie, het vestigingsklimaat en de werkgelegenheid.

Een van de pijlers van de NLCS is het beschikken over veilige en innovatieve digitale producten en diensten, waarvoor versterking van kennisontwikkeling en innovatie in cybersecurity noodzakelijk is. Dit wordt nader uitgewerkt in de cybersecurity-agenda van de Nationale Technologiestrategie (NTS).[7] Essentiële uitgangspunten bij die versterking van kennisontwikkeling en innovatie zijn het verwezenlijken van het principe van *cybersecurity-by-design* en het versterken van *onderzoeks- en innovatie-ecosystemen* op het gebied van cybersecurity, zowel op nationaal als op Europees niveau. Om bij te dragen aan het inherent minder kwetsbaar maken van producten, diensten, organisaties en systemen is het kabinet daarom van mening dat de EU onderzoek en innovatie moet prioriteren bij de vormgeving van de Europese agenda voor cybersecurity. Daarbij moet er meer aandacht worden gegeven aan onderzoek naar nieuwe systeemontwerpen, weerbare organisatie inrichting, menselijk gedrag en mens-ondersteunende technologie. Langs die lijn zou er aanvullend beleid moeten worden ontwikkeld voor innovatie op cybersecuritygebied. De Europese agenda zou daarnaast nadruk moeten leggen op onderwerpen zoals AI-gedreven systemen, dreigingsanalyse, post-quantum cryptografie

---

[5] Kamerstuk 30 821, nr. 249, 6 december 2024.
[6] Kamerstuk 28 676, nr. 417, Verslag NAVO-top Madrid, Ministerie Buitenlandse Zaken en Defensie.
[7] Kamerstuk 33 009, nr. 140, 19 januari 2024.

en talentontwikkeling. Om dit te realiseren moet de EU volgens het kabinet de randvoorwaarden helpen creëren voor een *concurrerende cybersecuritymarkt*. Daarbij pleit het kabinet voor het versterken van de samenwerking tussen wetenschap, bedrijven en investeerders en het stimuleren van grensoverschrijdend en multidisciplinair samenwerken binnen Europa. Het Europees kenniscentrum voor cyberbeveiliging (ECCC) en het netwerk van nationale coördinatiecentra (NCC's) kan hierin een belangrijke rol spelen. Dit netwerk moet verder worden versterkt om Europese ecosystemen met elkaar te verbinden, en gezamenlijke benaderingen te vinden voor onderzoek en innovatie.

Mogelijke ondertekening van een cybersecurityverklaring

Onder dit (mogelijke) agendapunt zal het Poolse Voorzitterschap naar verwachting aansturen op de ondertekening van een gemeenschappelijke verklaring ten aanzien van cybersecurity. Voor het kabinet zijn een aantal standpunten van belang om in deze (mogelijke) verklaring op te nemen. Zo pleit het kabinet voor toekomstbestendigheid van het Europese cybersecurity beleid- en regelgeving in een steeds veranderende wereld van technologische en geopolitieke ontwikkelingen. Om te voorkomen dat cybersecuritybeleid- en wetgeving in de EU wordt ingehaald door specifieke technologische ontwikkelingen of geopolitieke verhoudingen, zal het kabinet inzetten op het vormgeven van beleid en wetgeving op basis van zoveel mogelijk onafhankelijke en technologie-neutrale principes. In lijn met het eerdere Nederlandse non-paper[8], zal het kabinet oproepen tot meer aandacht voor en duiding van de impact (risico's en kansen) van nieuwe technologieën op het digitale veiligheidsdomein. Daarbij is het voor een toekomstbestendig Europees cybersecuritybeleid van belang dat de complexiteit en overlap in het EU-cybersecurity-landschap wordt verminderd en er wordt gefocust op succesvolle implementatie, harmonisatie en innovatie van bestaande en toekomstige initiatieven en wetgeving.

[8] Nederlands non-paper «Non paper Effective EU cybersecurity legislation and decisive diplomacy in the cyberdomain», d.d. 26 april 2024 (Bijlage bij Kamerstuk 32 317, nr. 877; 2024D17688).