Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 1128

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

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 april 2025

Hierbij bieden wij uw Kamer het verslag van de informele *Telecomraad* van 4 en 5 maart 2025 in Warschau, Polen aan.

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-21501-33-1128
ISSN 0921 - 7371
's-Gravenhage 2025

Verslag informele Telecomraad 4–5 maart 2025, te Warschau, Polen

1. Werksessie I: Cybercrisismanagement

In de eerste sessie schetste het Poolse voorzitterschap en de Europese Commissie (hierna: Commissie) een duidelijk beeld van digitale dreigingen en dagelijkse cyberaanvallen, merendeels vanuit Rusland.

De digitale weerbaarheid van Europa is een topprioriteit van de Commissie en de Commissie gaf aan dat de herziening van de *Blueprint Cyber*, het *EU Cable Security Action Plan* en het *European Cyber Crisis Liaison Officers Network* (ook wel: CyCLONe) hierbij van groot belang zullen zijn. De Commissie deed een oproep aan alle lidstaten om gebruik te maken van de beschikbare financiering om nationale cyberhubs op te richten.

Veel lidstaten, waaronder Nederland, verwelkomden de herziening van de *Blueprint Cyber,* riepen op tot het delen van kennis en informatie en benadrukten de noodzaak voor gecoördineerde, grensoverschrijdende responses voor gedegen cybercrisismanagement. Nederland specificeerde hierin, samen met een grote groep lidstaten, dat er een duidelijke verdeling van rollen en verantwoordelijkheden moet zijn, en dat dit gepaard gaat met het maximaal benutten van bestaande initiatieven en structuren en vereenvoudiging van het cyberlandschap. Daarnaast benadrukten verschillende lidstaten het belang van gemeenschappelijk crisissimulaties en oefeningen, tussen lidstaten en ook in samenwerking met de NAVO. Enkele lidstaten riepen op tot uitgebreidere publiek-private samenwerking vanwege de grote invloed van private partijen op onze cyberveiligheid en de veiligheid van onze kritieke infrastructuur.

2. Werklunch: Civiel-militaire samenwerking

Tijdens de besloten werklunch opende het Poolse voorzitterschap met het benadrukken van het belang van gedegen civiel-militaire samenwerking. De Commissie benoemde de overlap tussen civiele en militaire doelen van cyberdreigingen. Veel civiele infrastructuur is ook voor een militaire context relevant. Daarom is het belangrijk dat lidstaten met een integrale blik risk assessments doen op alle kritieke infrastructuur en ook rekening houden met deze overlap in de inzet om het industriële concurrentievermogen van de EU te versterken. Het doel is om tijdens crises snel te kunnen handelen, met een grote rol voor de *Blueprint Cyber* en samenwerking tussen de EU en de NAVO.

Een kleine groep lidstaten nam tijdens de lunch het woord. Nederland benadrukte het belang voor toekomstbestendig beleid dat civiel-militaire samenwerking versterkt, waarbij duplicatie tussen beide domeinen wordt voorkomen, een punt dat door meerdere lidstaten werd benoemd. Een aantal lidstaten, waaronder Nederland, gaf aan dat er winst te behalen is door het verminderen van de complexiteit van het cyberlandschap. Voor een aantal lidstaten zou dit erg helpen bij het beschermen van kritieke infrastructuur. Enkele lidstaten gaven aan dat de samenwerking vanuit het militaire domein verbeterd kan worden, en dat het militaire domein meer middelen zou kunnen inbrengen ten behoeve van het civiele domein. Een enkele lidstaat gaf aan al vergevorderde operationele samenwerking te hebben tussen civiele en militaire partijen.

Het Poolse voorzitterschap concludeerde met een oproep om meer te investeren in het *Europese Kenniscentrum voor Cyberbeveiliging* (ECCC), om meer onderzoek en kennisdeling te faciliteren. Ook zouden er meer cyberoefeningen plaats moeten vinden om zwakheden te blijven testen.

3. Werksessie II: Cyberinvesteringen

Tijdens deze tweede werksessie stond de Europese interne markt voor cyberveiligheidsdiensten centraal. De Commissie benadrukte dat EU-aanbieders op deze markt slechts 25% marktaandeel hebben. De andere 75% van het aanbod wordt ingevuld door partijen uit andere landen en voornamelijk uit de Verenigde Staten. Daarmee heeft de EU aanzienlijke afhankelijkheden op het gebied van cyberveiligheid. De Commissie schetste een viertal handelingsopties op het terrein van aanbestedingen, investeringen, inzet van AI-fabrieken en vaardigheden, waarna lidstaten hun prioriteiten communiceerden.

Op het gebied van investeringen gaf de Commissie aan dat ENISA (EU-Agentschap voor cyberbeveiliging) en ECCC (Europees kenniscentrum voor cyberbeveiliging) lidstaten verder helpen met innovatie en investeringen op cyberveiligheidsgebied. Een grote groep lidstaten, benadrukte het belang van AI en kwantum oplossingen voor cyberveiligheid. Nederland legde nadruk op AI-gedreven systemen en post-quantum cryptografie om ook in de toekomst weerbaar te blijven tegen aanvallen. Een groep lidstaten stipte het belang van meer nationale en Europese publieke investeringen in cyberveiligheid aan, het belang van het stimuleren van het MKB en het eventueel verhogen van cofinanciering voor cyberveiligheidsprojecten. Recente publieke investeringen in defensie moeten volgens hen ook bij cyberveiligheidsbedrijven terecht komen.

De Commissie ziet grote potentie in het gebruik van AI-fabrieken voor cyberveiligheid. In sommige EU-landen bieden AI-fabrieken hun capaciteit al aan om de meest geavanceerde AI modellen toe te passen op cyberveiligheidsvraagstukken. In het komende *InvestAI* initiatief zal de Commissie hier verder op ingaan. De Commissie gaf ook aan dat lidstaten kunnen sturen op de inzet van het Digital Europe Programma en Horizon middelen om daarin cyberveiligheid meer prioriteit te geven. Ook zogenaamde *dual use technologieën* kunnen hiervan profiteren. Een enkele lidstaat merkte op dat EU-fondsen voor MKB-bedrijven moeilijk toegankelijk zijn.

Volgens de Commissie heeft de EU bovengemiddeld veel last van een gebrek aan vaardigheden en talent op cyberveiligheidsgebied, vergeleken met VS en Azië. De Commissie zet daarom in op een nieuwe *Cybersecurity Skills Academy*, een specifieke *European Digital Innovation Hub (EDiH)* om cybersecurity capaciteit door de gehele Unie te verspreiden. Ook de ontwikkeling van *European Cyber Hubs* wordt versneld. Op dit moment zijn slechts twee van deze hubs actief. In reactie hierop benadrukte een grote groep lidstaten, waaronder Nederland, het belang van talentontwikkeling voor de ontwikkeling van de markt van cyberdiensten.

De Commissie benadrukte dat lidstaten het Europese aanbestedingssysteem gerichter kunnen inzetten, zodat Europese bedrijven een kans hebben en het niet automatisch afleggen tegen grote niet-Europese spelers («Buy European»). Nederland vroeg specifiek aandacht voor het principe van cybersecurity-by-design, het beter benutten van het European Cybersecurity Competence Centre (ECCC) en het netwerk van nationale coördinatiecentra. Andere individuele lidstaten benadrukten het

belang van internationale samenwerking én de recente aanvallen op fysieke infrastructuur die ook voor de cyberveiligheid een risico vormen.