Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

21 501-33 Raad voor Vervoer, Telecommunicatie en Energie

Nr. 923

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 april 2022

Hierbij bied ik u, mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties, het verslag aan van de informele Telecomraad van 8 en 9 maart 2022 in Parijs en Nevers. De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties heeft namens Nederland het woord gevoerd tijdens de informele Telecomraad.

Zoals gemeld in de Kamerbrief[1] met de beantwoording van het schriftelijk overleg heeft het Franse voorzitterschap de agenda van de informele Telecomraad volledig aangepast vanwege de oorlog in Oekraïne. De focus van de informele Raad lag op de thema's desinformatie, de weerbaarheid van de digitale infrastructuur en cybersecurity. De bijeenkomsten op 8 maart stonden in het teken van hybride dreigingen en desinformatie en de weerbaarheid van de digitale infrastructuur.
Op 9 maart vond er een bijeenkomst plaats met als discussieonderwerp het beschermen van de Europese cyberspace. In het kader van de informele Raad zijn er twee gezamenlijke oproepen gedaan, waarvan één over hybride oorlogsvoering en desinformatie en één over het versterken van de cybersecurity capaciteit.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

[1] Kamerstuk 21 501-33, nr. 920

kst-21501-33-923
ISSN 0921 - 7371
's-Gravenhage 2022

Verslag informele Telecomraad 8–9 maart

Hybride oorlogsvoering

Informele lunchdiscussie

Tijdens de informele lunchdiscussie heeft de Raad van gedachten gewisseld over de problemen rond desinformatie tegen de achtergrond van de oorlog in Oekraïne en over hybride oorlogsvoering. Bij de bijeenkomst waren diverse vertegenwoordigers van online platformen aanwezig.

Er was een gedeelde visie onder de lidstaten dat deze oorlog naast een gewapend conflict ook een informatieoorlog is. Diverse lidstaten riepen de online platformen op om meer te doen om desinformatie te adresseren en te voorkomen en pleitten voor een coherent instrumentarium van de EU. Enkele lidstaten uit kleine lidstaten vroegen aandacht voor het beperkte aantal *fact checkers* dat online platformen in dienst hebben binnen deze lidstaten om desinformatie te adresseren. Lidstaten riepen de online platformen op om zoveel als mogelijk te doen, waarbij de fundamentele rechten van burgers gewaarborgd blijven.

De online platformen gaven aan deze oproep serieus te nemen. Zij gaven tevens aan dat de uitzonderlijke omstandigheden als gevolg van de oorlog in Oekraïne het lastig maken om snel te reageren. Tegelijkertijd benadrukten de platforms wel zo hard mogelijk aan de slag te willen.

Nederland heeft steun uitgesproken voor de hybride toolbox[2] van de EU en heeft gepleit voor proportionele maatregelen om desinformatie te adresseren en te voorkomen. Daarbij heeft Nederland het belang van betrouwbare informatie over de oorlog in Oekraïne, ook voor Russische burgers, benadrukt. Als laatste sprak Nederland steun uit voor de oproep van diverse lidstaten richting de online platformen om meer te doen om desinformatie te adresseren en te voorkomen.

Het Frans voorzitterschap heeft het initiatief genomen om een gezamenlijke oproep vanuit de Raad te doen aan vertegenwoordigers van technologiebedrijven, grote online platformen, social media en aanbieders van bemiddelings- of informatiediensten om verantwoordelijkheid te nemen bij het tegengaan van desinformatie. Lidstaten hebben unaniem steun uitgesproken voor deze gezamenlijke oproep[3].

Elektronische communicatie infrastructuren en netwerken in Europa

Verdiepende sessie

In deze verdiepende sessie is van gedachten gewisseld over elektronische communicatie-infrastructuren en -netwerken in Europa. De sessie werd geopend door de Franse Staatssecretaris voor de digitale economie Cédric O en Eurocommissaris voor de Interne Markt Thierry Breton. Er is in deze sessie gesproken over de manier waarop de EU de weerbaarheid van haar communicatie-infrastructuur kan versterken. Tevens is er van

---

[2] Een hybride toolbox moet leiden tot een gecoördineerde en geïntegreerde benutting van bestaande en toekomstige EU-instrumenten voor het tegengaan van hybride dreigingen.

[3] Gezamenlijke oproep over desinformatie en hybride oorlogsvoering: https://presse.economie.gouv.fr/download?id=91749&pn=3020%20-%20Joint%20appeal%20by%20EU%20ministers%20responsible%20for%20digital%20and%20electronic%20communications-pdf

gedachten gewisseld over de balans tussen een open en innovatieve oplossingen en de gevolgen daarvan voor de veiligheid.

Vrijwel alle aanwezige lidstaten onderstreepten het belang van een spoedige afronding van de triloogonderhandelingen over de herziening van de richtlijn netwerk- en informatiebeveiliging (NIB2-richtlijn). Ook benadrukte een grote groep lidstaten het belang van goede kennis en capaciteit binnen de publieke sector en private partijen om de digitale infrastructuur te kunnen beschermen.

Nederland heeft het belang benadrukt van het versterken van de digitale weerbaarheid van de (digitale) infrastructuur. Hierbij benadrukte Nederland dat deze versterking niet alleen moet worden gezocht op de korte termijn via technische en organisatorische maatregelen in bestaande netwerken en informatie-uitwisseling over actuele dreigingen, maar ook op de langere termijn door bijvoorbeeld het verminderen van ongewenste strategische afhankelijkheden.

Europese cyberspace

Plenaire sessie

In de plenaire sessie vroeg het voorzitterschap aandacht voor de bescherming van de Europese *cyberspace*. Eurocommissaris Breton vroeg aandacht voor het vergroten van de detectiecapaciteit, het verbeteren van de governance, de solidariteit tussen lidstaten (waarbij er ook gekeken zou moeten worden naar het ondersteunen van elkaar op het gebied van kennis) en maatregelen gericht op de interne markt. Breton vroeg aandacht voor de NIB2-richtlijn en gaf aan dat de *Cyber Resilience Act* later dit jaar zal verschijnen.

Er was onder de lidstaten brede steun voor de reeds lopende initiatieven van de Commissie op het terrein van cybersecurity. Diverse lidstaten benadrukten het belang van het opbouwen van eigen kennis en capaciteiten ter voorbereiding op cyberincidenten en crisissituaties. Enkele lidstaten wezen op het belang van crisisvoorbereiding en lessen die uit gemeenschappelijke oefeningen getrokken konden worden. Er was onder lidstaten brede steun om de gezamenlijke EU-regels te versterken. Diverse lidstaten wezen op het belang van de aangekondigde *Cyber Resilience Act* waarover Nederland een non-paper[4] heeft geschreven. Dat non-paper kreeg van diverse lidstaten steun.

Nederland heeft in het overleg aangegeven dat EU-regulering op het gebied van cybersecurity ook een cruciale rol speelt in de versterking van de digitale weerbaarheid. Nederland heeft daarom opgeroepen tot snelle afronding van de NIB2-richtlijn. Na afloop van het overleg werd een tweede oproep[5] aangenomen om de cybersecurity-capaciteiten in de EU te versterken. Ook deze oproep werd unaniem door de lidstaten gesteund.

---

[4] Kamerstuk 21 501-33, nr. 900

[5] Gezamenlijke oproep over de versterking van EU cybersecurity capaciteiten: https://presse.economie.gouv.fr/download?id=92261&pn=2123%20-%20Joint%20appeal%20by%20EU%20ministers%20responsible%20for%20digital%20and%20electronic%20communications-pdf