Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

26 643 Informatie- en communicatietechnologie (ICT)

30 821 Nationale Veiligheid

Nr. 1252 **BRIEF VAN MINISTER VAN BUITENLANDSE ZAKEN**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 6 december 2024

Zoals toegezegd in het schriftelijk overleg over de Internationale Cyberstrategie (ICS) d.d. 17 oktober 2023, bied ik u hierbij – mede namens de Ministers van Justitie en Veiligheid, Economische Zaken, Defensie, Binnenlandse Zaken en Koninkrijksrelaties, de Minister voor Buitenlandse Handel en Ontwikkelingshulp en de Staatssecretaris Digitalisering en Koninkrijksrelaties – de jaarlijkse voortgangsbrief aan over de uitvoering van de Internationale Cyberstrategie 2023–2028 (ICS).

De ICS die op 9 juni 2023 (Kamerstuk 26 643, nr. 1036) aan uw Kamer werd aangeboden, moet in nauwe samenhang worden bezien met de Nederlandse Cybersecuritystrategie 2022–2028 (NLCS). Over de voortgang van de NLCS ontving uw Kamer op 28 oktober jl. (Kamerstuk 26 643, nr. 1229) een brief.

De ICS richt zich primair op de diplomatieke inzet om een open, vrij en veilig digitaal domein te bevorderen. Deze inzet wordt voor een belangrijk deel vormgegeven door het Ministerie van Buitenlandse Zaken, inclusief het postennet, maar kenmerkt zich ook door intensieve samenwerking met de ministeries van Economische Zaken, Justitie en Veiligheid, Defensie, Binnenlandse Zaken en Koninkrijksrelaties alsook NCSC, AIVD en MIVD.

In deze brief zal worden ingegaan op de voortgang die in het afgelopen jaar is geboekt op de drie strategische doelstellingen binnen het internationaal cyberbeleid:
1. Tegengaan van cyberdreigingen van staten en criminelen
2. Versterken van democratische en mensenrechtelijke principes online
3. Behoud van een wereldwijd open, vrij en veilig internet

kst-26643-1252
ISSN 0921 - 7371
's-Gravenhage 2024

Doelstelling 1 – Tegengaan van cyberdreigingen van staten en criminelen

De aanhoudende Russische dreiging en overige geopolitieke spanningen hadden ook in 2024 duidelijk hun weerslag op het digitale domein. In hun jaarverslagen 2023 stellen de AIVD en MIVD respectievelijk dat het aantal landen dat grotere offensieve cybercapaciteiten ontwikkelt, alsook de dreiging die van die capaciteiten uitgaat, toeneemt. Zie in dat kader ook het Cybersecuritybeeld Nederland 2024.[1] Mede daardoor is in de afgelopen tijd het accent meer en meer op afschrikking en respons op cyberincidenten komen te liggen. Er zijn stappen gezet richting een meer proactieve omgang met cyberdreigingen. Onderdeel daarvan is intensievere informatie-uitwisseling tussen het Ministerie van Buitenlandse Zaken, de Inlichtingen- en veiligheidsdiensten, NCTV, NCSC, het Ministerie van Defensie, de Nationale Politie en het Openbaar Ministerie.

De attributie van de Chinese cyberoperatie tegen het Ministerie van Defensie[2], de verstoring van een Russische digitale campagne[3], en de waarschuwing voor cyberoperaties van hackers[4] van de Russische militaire geheime dienst zijn voorbeelden van deze nieuwe aanpak. Met deze acties maakt het kabinet heimelijke kwaadwillende cyberactiviteiten zichtbaar en poogt door middel van openbaarmaking te laten zien dat er kosten verbonden zijn aan dergelijke activiteiten. Hiermee geeft het kabinet tevens uitvoering aan de motie Erkens[5].

Volgend op de vraag van het lid Koekoek (Volt)[6] ligt de nadruk bij de aanpak van niet-statelijke dreigingen primair op weerbaarheid en opsporing. Bij het tegengaan van statelijke dreigingen gaat de aandacht vooral uit naar de inzet van inlichtingenoperaties, defensiemiddelen en diplomatieke instrumenten. Geconstateerd kan worden dat – onder andere vanwege de vrijheid waarmee cybercriminelen in sommige gevallen opereren – het onderscheid tussen beide categorieën diffuser wordt.

Om scherper zicht te krijgen op de cyberdreiging heeft het kabinet fors geïnvesteerd in de onderzoekscapaciteit van de Inlichtingen- en Veiligheidsdiensten ten behoeve van inlichtingenmatig-diepteonderzoek. Om de AIVD en MIVD in staat te stellen hun taken efficiënter en slagvaardiger te kunnen uitvoeren, is in juli 2024 de herziene Tijdelijke wet cyberoperaties in werking getreden. Daarmee zorgt het kabinet dat de diensten hun bevoegdheden in het digitale domein sneller en effectiever kunnen inzetten, terwijl waarborgen behouden blijven. Dit draagt bij aan het beperken van digitale dreigingen, zorgt voor een versterkte informatie-uitwisseling en verhoging van de weerbaarheid voor Nederland en zijn bondgenoten. Wel heeft de Commissie van toezicht op de Inlichtingen-en Veiligheidsdiensten (CTIVD) aangegeven vanwege huisvestingsproblemen en het daaruit volgende capaciteitsgebrek slechts beperkt toezicht te kunnen houden op de Tijdelijke Wet. Om die reden wordt de wet nog niet volledig toegepast. Hierdoor is het voor de AIVD en de MIVD op dit moment nog niet mogelijk om sneller en effectiever op te treden in het digitale domein, zoals beoogd. Over dit knelpunt vindt overleg plaats met de CTIVD.

---

[1] Cybersecuritybeeld Nederland 2024 | Publicatie | Nationaal Coördinator Terrorismebestrijding en Veiligheid (nctv.nl)
[2] MIVD onthult werkwijze Chinese spionage in Nederland | Nieuwsbericht | Defensie.nl
[3] Nederland en VS verstoren Russische digitale beïnvloedingsoperatie | Nieuwsbericht | Defensie.nl
[4] MIVD waarschuwt: Russen hebben het gemunt op westerse hulp aan Oekraïne | Nieuwsbericht | Defensie.nl
[5] Kamerstuk 36 410 X, nr. 46
[6] Vraag gesteld tijdens de begrotingsbehandeling Buitenlandse Zaken d.d. 21 november 2024

Ook het Ministerie van Defensie heeft het afgelopen jaar verdere stappen gezet om bij te dragen aan de weerbaarheid van de gedigitaliseerde samenleving door middel van investeringen in de digitale slagkracht. Naast het onderkennen en verstoren van cyberdreigingen vanuit de inlichtingen- en veiligheidstaak van de MIVD, kan de krijgsmacht militaire cyberoperaties uitvoeren. Daarnaast levert Defensie waar mogelijk op verzoek ondersteuning aan bondgenoten gericht op het verhogen van cyberweerbaarheid, zoals capaciteitsopbouw, handhaving, detectie en respons. Tevens investeert Defensie in de digitale slagkracht van de krijgsmacht om militaire cyberoperaties uit te kunnen voeren, die zowel defensief of offensief van aard kunnen zijn. Defensie onderzoekt de mogelijkheden voor een specifieke wettelijke grondslag om in het grijze gebied tussen oorlog en vrede met militaire capaciteiten te kunnen bijdragen aan de digitale bescherming van onze samenleving.[7]

Op diplomatiek vlak bouwt Nederland verder aan coalities om tegenspel te bieden aan landen met een offensief cyberprogramma gericht tegen onze belangen. Dit doet het kabinet in eerste instantie binnen de EU en NAVO. Daarnaast beoogt het kabinet de samenwerking hierover met belangrijke partnerlanden verder te intensiveren. Zo voerde Nederland afgelopen jaar cyberconsultaties met de VS, het VK, Zuid-Korea, India en Zuid-Afrika.

EU-samenwerking tegen cyberdreigingen kent uitdagingen, zoals beperkingen in informatie-uitwisseling met als gevolg langdurige attributieprocessen. Vaak ook komt de lezing van de aard en omvang van de cyberdreiging niet in alle lidstaten overeen. Nederland neemt daarom binnen de EU het initiatief het geheel aan gezamenlijke maatregelen om te kunnen reageren op cyberdreigingen, verder te ontwikkelen. Zo maakt Nederland zich hard voor het frequenter toepassen en ontwikkelen van het cyber-sanctie instrumentarium.

Dat leidde in 2024 tot het sanctioneren van een aantal Russische cybercriminelen.[8] Dit resultaat kwam tot stand door intensieve en strategische samenwerking tussen het Ministerie van Buitenlandse Zaken, Politie, OM en het Ministerie van Justitie en Veiligheid. Daarnaast werden – eveneens naar Nederlands voorstel – onder de «Rusland-sancties» verschillende bedrijven gesanctioneerd die als ICT-toeleverancier opereren voor de Russische inlichtingendiensten en zo kwaadwillende cyberoperaties mede mogelijk maken.

Binnen de NAVO richtte de discussie zich ook in het afgelopen jaar vooral op het vergroten van de cyberweerbaarheid van het Bondgenootschap. In dat kader organiseerde Nederland op 16 en 17 mei jl. samen met Roemenië de NAVO *Cyber Defence Pledge Conference*.[9] De *pledge* belicht de stand van zaken van de nationale cyberweerbaarheid van de bondgenoten en spoort aan om investeringen in die weerbaarheid te vergroten.

Tot slot heeft het kabinet Oekraïne bijgestaan zich beter te wapenen tegen de Russische cyberdreiging; zo financierde Nederland cyberveiligheidsproducten en toegang tot het internet via Starlink-satellieten. Ook droeg Nederland via het Tallinn Mechanisme – een samenwerkingsverband van de belangrijkste donoren op cybersecuritygebied – bij aan niet-militaire cybersteun aan Oekraïne.

---

[7] Kamerstuk 33 321, nr. 10: Optreden Defensie in het cyberdomein

[8] Cyber-attacks: six persons added to EU sanctions list for malicious cyber activities against EU member states and Ukraine – Consilium (europa.eu)

[9] NATO – News: NATO Deputy Secretary General: we must be big on cyber defence ambitions, 17-May.-2024

Versterking en bestendiging van normen voor verantwoord statelijk gedrag

Ondanks de geopolitieke spanningen heeft Nederland ook het afgelopen jaar een concrete bijdrage kunnen leveren aan de lopende VN-onderhandelingen over de normen voor verantwoordelijk statelijk gedrag en de toepassing van internationaal recht in het cyberdomein. Breed gedragen normen zijn daarbij een manier om overtreders van die normen ter verantwoording te roepen. Zo is Nederland er samen met gelijkgezinde landen in geslaagd de bescherming van internationale organisaties tegen cyberaanvallen, alsook de dreiging van ransomware-aanvallen, hoger op de agenda van de VN te krijgen. Nederland werkt met gelijkgezinde landen toe naar een VN-mechanisme voor implementatie van het zogenaamde normatief kader voor verantwoordelijk statelijk gedrag in het cyberdomein. Over de contouren van een dergelijk mechanisme wordt in de zomer van 2025 besloten.

Versterkte internationale samenwerking tegen cybercriminaliteit

Nederland heeft zich ingezet om landen aan te moedigen zich aan te sluiten bij de Boedapest-Conventie. Dit leidde tot stappen richting toetreding door onder andere Malawi, Kenia en Fiji. Parallel hieraan werd in augustus 2024 het VN-cybercrimeverdrag met consensus overeengekomen. Dit verdrag is qua inhoud vergelijkbaar met de Boedapest-Conventie (uit 2004) van de Raad van Europa en kan later mogelijk de samenwerking met VN-lidstaten mogelijk maken. Er zal echter eerst op Europees en nationaal niveau een besluit moeten worden genomen of het verdrag moeten worden geratificeerd, een voorwaarde om partij te worden bij het verdrag. Nederland heeft tijdens de onderhandelingen sterk ingezet op solide waarborgen voor mensenrechten en een beperkte reikwijdte van het verdrag, opdat het verdrag zich richt op de bestrijding van *cyber*criminaliteit en geen breed verdrag wordt op internationale strafvordering.

Tot slot is tijdens de jaarlijkse bijeenkomst van het *Counter Ransomware Initiative* (CRI) van 2 oktober jl. een oproep gedaan aan CRI leden om ransomware-actoren gezamenlijk ter verantwoording te roepen en hen een veilige haven te ontzeggen met behulp van alle cyberdiplomatie- en wetshandhavingsinstrumenten die tot hun beschikking staan.[10]

Doelstelling 2 **– Versterken van democratische en mensenrechtelijke principes online**

Nederland heeft zich, in samenwerking met een brede coalitie van landen, onderzoekers, bedrijven en maatschappelijke organisaties, ook in het afgelopen jaar ingezet voor de verankering van internationale afspraken in het digitale domein. Zo is Nederland in 2024 voorzitter van de *Freedom Online Coalition* (FOC), een strategische coalitie om internationaal recht en mensenrechten in het digitale domein te bevorderen. Door gezamenlijk aandacht te vragen voor onderwerpen als internet governance, basisprincipes voor kunstmatige intelligentie (AI), en belang van veilige toegang tot het internet, beïnvloeden we de internationale discussies hierover. Binnen de VN zet de FOC zich in tegen internet shutdowns, censuur en surveillance en bevordert digitale inclusie en de betrouwbaarheid van online-informatie. Om niet-westerse landen bij de coalitie te betrekken, organiseerde Nederland regionale dialogen in Ghana, Brazilië en Taiwan. Dit leidde tot de toetreding van Zuid-Korea, Kaapverdië, Slovenië en Colombia tot de coalitie.

---

[10] International Counter Ransomware Initiative 2023 Joint Statement | The White House

Het nastreven van de toepassing van mensenrechten online betekent ook het zoeken naar een balans tussen het tegengaan van statelijke desinformatie en het bevorderen van een vrij online medialandschap. Nederland heeft samen met Canada de *Global Declaration on Information Integrity*[11] opgesteld, die niet-bindende normen bevat rondom online informatie-integriteit. Deze verklaring, ondertekend door 35 landen, richt zich op het tegengaan van online desinformatie en behoud van vrijheid van meningsuiting. Nederland en Canada stimuleren meer landen om zich bij de verklaring aan te sluiten. Middels de OESO *Hub on Information Integrity*[12] delen beleidsmakers kennis en bespreken ze uitdagingen om zo samen effectieve oplossingen te vinden.

Deze inzet sluit aan bij de EU-verordening *Digital Services Act* (DSA) voor online contentbeheer. Het kabinet zal een conferentie organiseren over het belang van mensenrechten bij contentmoderatie onder de DSA; hiermee wordt aangesloten op de geactualiseerde Rijksbrede strategie tegen desinformatie[13].

In de ICS heeft het kabinet zich ook gecommitteerd aan het borgen van mensenrechten en democratische beginselen bij de ontwikkeling van standaarden voor opkomende technologieën. Op dit gebied werkt het Ministerie van Buitenlandse Zaken nauw samen met de Ministeries van Binnenlandse Zaken en Economische Zaken. Zo hebben deze ministeries in VN-resoluties, de Global Digital Compact, de Pact for the Future, en in FOC-verklaringen voorstellen gedaan hoe actiever bij te dragen aan internationale standaarden voor digitale technologieën, met aandacht voor mensenrechten, economie en geopolitiek.[14]

Nederland wordt internationaal erkend als belangrijke speler op het gebied van verantwoorde inzet van AI[15]; zo heeft Nederland actief bijgedragen aan de UN High Level Advisory Body on AI en maakte Nederland deel uit van de kerngroep van landen voor de eerste AVVN-resolutie over AI[16]. Hierin streeft Nederland nadrukkelijk naar erkenning van de toepasbaarheid van internationaal recht en mensenrechten.

Doelstelling 3 **– Behoud van een wereldwijd open, vrij en veilig internet**

Nederland heeft zich het afgelopen jaar in VN-onderhandelingen ingezet voor het behoud van het multistakeholder-model voor internetbeheer, een cruciaal moment met de aanstaande WSIS+20-evaluatie van bestaande afspraken.[17] Zo is Nederland in organisaties zoals de Internet Corporation for Assigned Names and Numbers (ICANN) en International Telecommunications Union (ITU), en platformen zoals de FOC, intensief in gesprek met partnerlanden en -organisaties om hen mee te nemen in de belangen die op het spel staan en in de nadelen van andere, door staten gestuurde, vormen van *internet governance*.

---

[11] Canada and the Netherlands launch the Global Declaration on Information Integrity Online | News item | Government.nl

[12] https://www.oecd.org/en/blogs/2023/03/oecd-hub-on-information-integrity-joining-forces-to-fight-dis--and-misinformation.html

[13] Kamerstuk 30 821 nr. 230

[14] Freedom Online Coalition | Joint Statement on Technical Standards and Human Rights in the Context of Digital Technologies

[15] The Global Index on Responsible AI (global-index.ai)

[16] AVVN Res 78/L.49 Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development

[17] World Summit on the Information Society: zie voor meer achtergrondinformatie omtrent *internet governance* en deze processen H3 van de Internationale Cyber Strategie.

Toch is een aantal niet-westerse landen voorstander van een grotere coördinerende rol van de VN en de ITU op *internet governance*. Een dergelijke verschuiving naar een meer multilaterale en gecentraliseerde constructie zal volgens Nederland, de EU en gelijkgezinde landen een negatieve impact hebben op de weerbaarheid, veiligheid en algemene beschikbaarheid van het internet. Zo bestaat het risico dat de technische laag van het internet, die oorspronkelijk ontworpen is voor maximale functionaliteit, in de toekomst om meer politieke redenen aangepast kan worden, met als gevolg surveillance, censuur en internet fragmentatie. Daarnaast zou centralisering de verdere ontwikkeling van het internet en daarmee de digitalisering van minder ontwikkelde landen vertragen.
In de ICS is aangekondigd dat het kabinet de risico's en de economische, technische en geopolitieke gevolgen van internet fragmentatie wil laten onderzoeken. Het afgelopen jaar is gesproken met Nederlandse en internationale experts op het gebied van *internet governance* en economische modellen. Uit dit vooronderzoek bleek dat experts van mening verschillen over de kans dat het internet daadwerkelijk zal fragmenteren. Begin oktober is een ronde-tafel-bijeenkomst met Nederlandse stakeholders georganiseerd om deze bevindingen te bespreken en op basis daarvan wordt een onderzoeksvoorstel nader uitgewerkt.

Nederland is recent verkozen tot vicevoorzitter van de *Governmental Advisory Committee* (GAC) binnen ICANN. ICANN is opgericht om het wereldwijde beheer van het internetdomeinnamensysteem (DNS) uit te voeren, en daarmee onderdeel van het stelsel van multistakeholder-organisaties die de publieke kern van het internet te beheren. Daarnaast wordt binnen ICANN het beleid bepaald waaronder generieke topleveldomeinnamen (gTLD) en landcode topleveldomeinnamen (ccTLD) aan het DNS systeem worden toegevoegd. Onze betrokkenheid bij de GAC draagt bij aan een stabiele en effectieve toepassing van het multistakeholder model voor *internet governance* en biedt tevens de mogelijkheid om met andere landen en stakeholders het gesprek aan te gaan over hoe een open, vrij, veilig en wereldwijd verbonden internet behouden kan worden.

Om de dialoog tussen landen en de betrokkenheid van het maatschappelijk middenveld, overheden en bedrijven in de prioriteitsregio's Westelijke Balkan, Indo-Pacific en zuidelijk Afrika te vergroten, organiseert Nederland regionale consultaties. Hier worden actuele thema's besproken op het gebied van cyberveiligheid, cybercriminaliteit, *internet governance* etc. Op het gebied van capaciteitsopbouw is het Ministerie van Buitenlandse Zaken samenwerkingsrelaties aangegaan met o.a. HCSS, Clingendael, ESIWA, NCSC, Wereldbank en UNODC.

Het met Nederlandse steun in 2015 opgerichte *Global Forum on Cyber Expertise* organiseerde de eerste *Global Conference on Cyber Capacity Building in Accra*, Ghana, in november 2023. Meer dan 100 overheidsvertegenwoordigers en experts uit de ontwikkelings- en technische cybergemeenschap discussieerden over het belang om cyberveiligheid te verbinden aan de nationale en internationale ontwikkelingsagenda's. Over hetzelfde thema werd de *Accra Call* gelanceerd; een verklaring gesteund door 73 landen, bedrijven en organisaties. Immers, om van de voordelen van een gedigitaliseerde maatschappij te kunnen profiteren, is bescherming tegen cyberkwetsbaarheden onontbeerlijk.

De Minister van Buitenlandse Zaken,
C.C.J. Veldkamp