Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 793

BRIEF VAN DE MINISTER VAN BUITENLANDSE ZAKEN

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 29 september 2021

Hierbij bied ik u de kabinetsreactie aan op het rapport «Verbeter de verbinding», waarin de Directie Internationaal Onderzoek en Beleidsevaluatie (IOB) van het Ministerie van Buitenlandse Zaken (BZ) een evaluatie geeft van het internationaal cyberveiligheidsbeleid, zoals ontwikkeld en uitgevoerd door het ministerie in de periode 2015–2021[1].

Het kabinet wil allereerst zijn waardering uiten voor de grondige analyse en aanbevelingen die de IOB heeft gepresenteerd. De IOB-evaluatie biedt goede handvatten voor inhoudelijke en praktische versterking van het Nederlandse beleid ten aanzien van het internationaal cyberveiligheidsbeleid.

Het advies komt op een uitgelezen moment. Er is veel in beweging, in economisch en in geopolitiek opzicht: de wereld is complexer en onvoorspelbaarder geworden, machtsverhoudingen verschuiven en nieuwe grootmachten zoals China winnen aan invloed. Dat levert nieuwe kansen en dreigingen op. Technologische ontwikkelingen brengen nieuwe vraagstukken met zich mee. Door het digitale domein zijn we mondiaal steeds nauwer met elkaar verbonden. Dat is een groot goed. Tegelijkertijd vormen digitale dreigingen een van de grote veiligheidsvraagstukken van deze tijd.

Het meest recente Cybersecuritybeeld Nederland (CSBN2021) (Kamerstuk 26 643, nr. 767) schetst de urgentie: cyberdreigingen vanuit het buitenland blijven zich ontwikkelen, de weerbaarheid daartegen is onvoldoende en de spanning tussen veiligheid, vrijheid en economische groei neemt toe. Gezien de toenemende ernst van de dreiging is een bestendige aandacht voor internationaal cyberbeleid noodzakelijk.

Cyberveiligheid speelt zich af binnen een domein waar binnen- en buitenland in elkaar overlopen. Deze evaluatie van het internationale

[1] Raadpleegbaar via www.tweedekamer.nl

kst-26643-793
ISSN 0921 - 7371
's-Gravenhage 2021

cyberveiligheidsbeleid kan dan ook niet los gezien worden van de recente evaluatie van het brede kabinetsbeleid op dit vlak, zoals neergelegd in de Nederlandse Cybersecurity Agenda (NCSA). Het kabinet heeft de Kamer zijn visie op die evaluatie samen met het CSBN2021 gestuurd in een eerdere brief van de Minister van Justitie en Veiligheid[2]; onderstaande kabinetsreactie hangt dus samen met het gestelde in die brief.

Ik wil voorop te stellen dat de algemene teneur van het IOB-rapport positief is: uit het rapport is af te leiden dat de basis van de analyse en de daarop gebaseerde inzet voor het internationale cyberveiligheidsbeleid goed is. De inzet en de activiteiten van BZ, zoals geschetst in hoofdstuk 4 van de IOB-evaluatie, en de daarbij behorende organisatorische opzet van het werk (hoofdstuk 5) leiden tot een overwegend positief beeld.

Met name de waarneming van de IOB dat Nederland in diplomatieke zin in een hoge gewichtsklasse bokst, sterkt mij in de overtuiging dat Nederland op de goede weg is. Ik hecht eraan te benadrukken dat dit gunstige oordeel niet alleen het gevolg van de inzet van BZ: het is ook het onmiddellijke product van de goede samenwerking tussen de verschillende departementen die bij het internationaal cyberveiligheidsbeleid betrokken zijn, zoals bijvoorbeeld plaatsvindt in het interdepartementale kader voor diplomatieke respons en de voorbereiding van de Europese raadswerkgroep voor cyberaangelegenheden. Ook hier geldt: doeltreffend internationaal beleid begint met goede nationale samenwerking.

Terecht wijst de IOB erop (en de NCSA-evaluatie maakt dat ook duidelijk) dat de doeltreffendheid van ons internationaal cyberveiligheidsbeleid gebaat is bij het verder verbeteren van die samenwerking. De samenwerking moet bovendien gestoeld zijn op een samenhangende beleidsvisie, die uiteenlopende interpretaties vermijdt van begrippen als capaciteitsopbouw of «open, vrij en veilig internet», om twee door de IOB aangehaalde voorbeelden te noemen. En analoog aan wat mijn ambtgenoot van J&V uw Kamer heeft geschreven in zijn brief, zal in een nieuwe (internationale) cybersecurityaanpak ook aandacht moeten zijn voor de meetbaarheid van de (verwachte) effecten van de strategie, zodat er bij een toekomstige evaluatie duidelijker zicht kan worden verkregen op de doeltreffendheid ervan.

Bij het vormgeven van de nieuwe inzet en prioriteiten op het gebied van internationaal cyberveiligheidsbeleid is het waarborgen van maximale doeltreffendheid noodzakelijk, gegeven de vaststelling dat onze digitale veiligheid kwetsbaar is en blijft. Zij wordt bedreigd door statelijke actoren die de intentie en de capaciteiten hebben om digitale aanvallen uit te voeren. Zij kunnen spioneren, saboteren en ongewenste invloed uitoefenen met cybermiddelen. Deze aanvallen worden uitgevoerd met methoden en technieken die detectie, analyse en attributie moeilijk maken. In soortgelijke zin – zo luidt ook een van de conclusies van het CSBN2021 – is cybercriminaliteit aan te merken als factor die de nationale veiligheid kan raken. Dit geldt m.n. indien een aanval leidt tot omvangrijke schade, zoals door het verstoren van vitale processen. Ook kan het voorkomen dat cybercriminelen bescherming genieten van de staat van waaruit zij opereren of is er sprake van samenwerking met een staat.

Het uitgangspunt van een nieuwe strategie is en blijft het versterken en naleven van het internationale normatieve kader in cyberspace. Wanneer landen op enigerlei manier in strijd daarmee handelen, is een reactie op zijn plaats. De diplomatieke respons die kan volgen, dient meerdere doelen, waaronder het onderstrepen van het belang dat we hechten aan

[2] Kamerstuk 26 643, nr. 767 d.d. 28 juni 2021

de rechtsorde, het verhogen van de prijs van onverantwoord gedrag in het cyberdomein en het verhogen van het publieke bewustzijn over cyberdreigingen.

De afgelopen jaren heeft Nederland actief bijgedragen aan dat normatieve kader, op basis van het centrale uitgangspunt dat bestaand internationaal recht (met inbegrip van mensenrechten) van toepassing is in *cyberspace*. Dat doen we niet alleen, maar in hechte samenwerking met EU, NAVO en gelijkgezinde partners. Vaak zijn we daarin voortrekker. Het is mede vanwege deze inzet dat alle VN-lidstaten in maart 2021 herbevestigd hebben dat het internationaal recht van toepassing is op het cyberdomein. De komende tijd zal de aandacht moeten verschuiven van het formuleren van normen naar het implementeren ervan. In dat kader zet Nederland bijvoorbeeld met de EU in op het uitwerken van *best practices* en het delen daarvan met derde landen (m.n. landen van de G-77). Ook is het wenselijk verder te verkennen hoe het bedrijfsleven nauwer te betrekken bij het handhaven van normen.

De IOB-evaluatie is niet het eerste rapport dat de noodzaak van een doeltreffend cyberveiligheidsbeleid onderstreept. De dreigingen nemen toe, en zo ook onze afhankelijkheid van digitale middelen. De digitale ruimte biedt onuitputtelijke mogelijkheden. Tegelijkertijd is het onderdeel van een geopolitieke krachtenstrijd. Het is essentieel dat we nu en in de toekomst blijven werken aan digitale autonomie en cybersecurity om ongewenste strategische afhankelijkheden weg te nemen of te voorkomen[3].

Ook moet rekening worden gehouden met het toenemen van dreigingen en kwetsbaarheden, zoals teweeggebracht door de verdere ontwikkeling van methoden als *ransomware* en desinformatie en technologieën als kunstmatige intelligentie, 5G, *Internet of Things* en kwantumcomputers. De IOB wijst terecht op ervaringen in andere landen die nuttig zijn bij het vormgeven van een integrale cybersecuritystrategie m.n. Australië, het Verenigd Koninkrijk en de Verenigde Staten.

Gelet op deze ontwikkelingen, de permanente digitale dreiging en de toenemende afhankelijkheid van digitale middelen zal stevige inzet op het blijven versterken van een assertief internationaal cyberbeleid onder een nieuw kabinet noodzakelijk zijn. Daarvoor zullen de benodigde menskracht, kennis en middelen ter beschikking moeten worden gesteld. Zoals het volgende kabinet een besluit zal nemen over de opvolging van de NCSA, zo zal mijn opvolger werken aan een nieuwe strategie voor internationaal cybersecuritybeleid van BZ, als onderdeel van of aansluitend op een nieuwe departement-overstijgende cybersecuritystrategie. Deze zal putten uit de waardevolle inzichten en nuttige aanbevelingen die de IOB heeft gedaan.

Tot dat moment zal ik op basis van de bestaande beleidsstukken voortgaan met de drieslag internationale rechtsorde – respons – capaciteitsopbouw, en voorbereidingen treffen die noodzakelijk zijn om te komen tot het versterken van het internationale cyberbeleid. Uw Kamer zal ik blijvend informeren over de actuele stand van zaken in het internationale digitale domein.

De Minister van Buitenlandse Zaken,
H.P.M. Knapen

---

[3] Gewezen zij op het advies van de Cyber Security Raad van 6 mei 2021: Nederlandse Digitale Autonomie en Cybersecurity