[illegible]

Aan de Voorzitter van de
Tweede Kamer der Staten-Generaal
Binnenhof 4
Den Haag

Directie Veiligheidsbeleid
Bezuidenhoutseweg 67
2594 AC Den Haag
Postbus 20061
Nederlandfalse Nederland
www.rijksoverheid.nl

Onze Referentie
DVB/Cyber-004/2017

Bijlage(n)
1

Datum 12 februari 2017
Betreft Internationale Cyberstrategie

Hierbij bied ik u, mede namens de Ministers van Economische Zaken, Defensie, Binnenlandse Zaken en Koninkrijksrelaties en de Staatssecretaris van Veiligheid en Justitie, de Internationale Cyberstrategie aan. Met deze strategie geeft het Kabinet gestalte aan de toezegging vervat in de kabinetsreactie op de rapporten ‘Het internet, een onbegrensde ruimte met beperkte staatsmacht’ van de AIV en ‘De publieke kern van het internet: naar een buitenlands internetbeleid’ van de WRR. Hierin kondigde het kabinet een aanzet tot een internationale cyberstrategie aan.[1]

De wereld om ons heen verandert in snel tempo. Zowel in economisch als in geopolitiek opzicht. Machtsverhoudingen verschuiven, nieuwe grootmachten zoals China winnen aan invloed. De wereld is complexer en onvoorspelbaarder geworden. Dat levert nieuwe kansen en dreigingen op. Technologische ontwikkelingen brengen nieuwe vraagstukken met zich mee. Door internet zijn we mondiaal steeds nauwer met elkaar verbonden. Dat is een groot goed. Tegelijkertijd vormen digitale dreigingen een van de grote veiligheidsdreigingen van deze tijd.

Een veilig, vrij en open cyberdomein is dan ook geen vanzelfsprekendheid. Het vergt continue investering. We moeten daar, in de snel veranderde wereld om ons heen, hard aan werken. Samen met andere landen, internationale organisaties, private partijen, de technische gemeenschap, academici en maatschappelijke organisaties. ‘Bruggen slaan’ is ook in het internationaal cyberbeleid het devies. Een veilig, vrij en open cyberdomein begint en eindigt niet bij onze landsgrenzen of bij de buitengrenzen van de Europese Unie.

Moderne dreigingen laten zich weinig gelegen liggen aan grenzen of dijken. Interne en externe veiligheid zijn steeds minder goed van elkaar te scheiden. Dit geldt vooral voor het cyberdomein. Wat daar gebeurt, raakt direct aan onze eigen veiligheid en welvaart. Nederland loopt wereldwijd voorop in de digitalisering met razendsnelle netwerken, een uitstekende digitale infrastructuur en één van de

1
Kamerbrief met kabinetsreactie op advies nr. 92 ‘Het internet: Een wereldwijde vrije ruimte met begrensde staatsmacht’ van de Adviesraad Internationale Vraagstukken (AIV) en het advies nr. 94 ‘De publieke kern van het internet: naar een buitenlands internetbeleid’ van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR), Kamerstuk 26643-411, 19 mei 2016.

grootste internetknooppunten ter wereld, de Amsterdam Internet Exchange. Hiermee heeft Nederland een van de meest ICT-intensieve economieën van Europa. De digitale infrastructuur vormt, naast Schiphol en de Rotterdamse haven, de derde mainport van ons land.

De dreiging van cyberaanvallen is de afgelopen jaren steeds duidelijker geworden. Zoals weergegeven in de beleidsreactie Cyber Security Beeld Nederland 2016 is internationaal een trend waarneembaar dat digitale capaciteiten worden ingezet in conflictsituaties, al dan niet als onderdeel van hybride oorlogsvoering.[2] De meest voorkomende verschijningsvormen zijn de zogenaamde informatie operaties, die als doel hebben de publieke opinie te beïnvloeden. De hacks van de digitale systemen van politieke partijen in de aanloop naar de Amerikaanse presidentsverkiezingen ten behoeve van politieke beïnvloeding zijn hiervan een actueel voorbeeld. Geopolitieke ontwikkelingen hebben een belangrijke invloed op de ontwikkeling van de dreiging. Steeds meer staten ontwikkelen (militaire) cybercapaciteiten en het is voorstelbaar dat wanneer Nederland berokken raakt bij oplopende geopolitieke spanningen of een internationaal conflict, zij doelwit kan worden van digitale sabotage of andere ernstige cyberaanvallen. Het ontbreken van overeenstemming over duidelijke gedragsregels draagt bij aan deze instabiliteit. Dit is nog grotendeels onontgonnen terrein.

Nederland heeft zich met de Global Conference on Cyber Space 2015 en de daarop volgende initiatieven zoals het Global Forum on Cyber Expertise in de voorhoede van de internationale discussies over cyberbeleid geplaatst. Dit leverde onder meer op dat Nederland nu deelneemt aan het overleg in de UN Group of Governmental Experts over normen voor een veilig en stabiel cyberdomein. Binnenkort gaat bovendien op Nederlands initiatief de Global Commission on the Stability of Cyberspace aan het werk. Dit platform kan door zijn verscheidenheid aan deelnemers (bedrijven, academici en vertegenwoordigers van de technische gemeenschap en maatschappelijke organisaties) een open discussie over nieuwe gedragsnormen in het cyberdomein faciliteren. Hiermee wordt een bijdrage geleverd aan breed gedragen afspraken voor verantwoordelijk gedrag en stabiliteit in het cyberdomein.

Om optimaal te kunnen blijven inspelen op de bedreigingen, kansen en uitdagingen zal Nederland de internationale samenwerking en diplomatie binnen dit domein nog verder moeten versterken. Een aanzet daartoe is vervat in deze Internationale Cyberstrategie. De hierin aangekondigde inspanningen zijn complementair aan en in lijn met de Nationale Cyber Security Strategie (NCSS 2), de Digitale Agenda 2016-2017, de Mensenrechtenstrategie 2, de Defensie Cyber Strategie en de Nederlandse Internationale Veiligheidsstrategie. Er wordt bovendien aangesloten bij de snelle ontwikkelingen op dit terrein in internationale organisaties zoals de NAVO en de EU.

De Internationale Cyberstrategie is in consultatie met publieke en private partijen, academici, de technische gemeenschap en organisaties uit het maatschappelijk middenveld tot stand gekomen.
De Cyber Security Raad, bestaande uit vertegenwoordigers van publieke en private partijen en wetenschap, is eveneens geconsulteerd.

Nederland wil internationaal een voortrekkersrol blijven spelen binnen het

2
Kamerbrief met beleidsreactie Cyber Security Beeld Nederland 2016, Kamerstuk 26643-420, 5 september 2016.

cyberdomein. Alleen zo kunnen we een bijdrage leveren aan een veilig, vrij en open cyberdomein realiseren, waarin de kansen die digitalisering onze samenleving biedt volop worden benut, dreigingen het hoofd worden geboden en fundamentele rechten en waarden worden beschermd.

Onze Referentie
DVB/Cyber-004/2017

De Minister van Buitenlandse Zaken,

Bert Koenders