Bijlage 1 Stand van zaken actieprogramma NCSS-2, 2014-2016
De Nationale Cyber Security Strategie 2 (NCSS 2) kent 5 doelstellingen, namelijk Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het digitale domein, Nederland pakt cybercrime aan, Nederland investeert in veilige en privacy bevorderende ICT producten en diensten, Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het digitale domein en Nederland beschikt over voldoende cybersecuritykennis en –kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen. Ter verdere uitwerking van deze 5 doelstellingen zijn tien speerpunten benoemd. In deze bijlage worden de resultaten op de NCSS 2 toegelicht aan de hand van deze 10 speerpunten.

Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling
Uitval, verstoring of aantasting van de vitale infrastructuur kan grote gevolgen hebben voor de nationale veiligheid. Een hoge fysieke en digitale weerbaarheid is dan ook van cruciaal belang. Onder vitale infrastructuur verstaan we het samenstel van alle geïdentificeerde vitale processen[1]. Het is belangrijk om deze vitale processen te beschermen tegen uitval door bijvoorbeeld storingen, rampen, sabotage of aanslagen. Om het beschermingsniveau van de vitale infrastructuur in Nederland hoog te houden, werken overheid en vitale partners samen aan het verder verbeteren van continuïteit. Uw Kamer wordt in de voortgangsbrief nationale veiligheid nader geïnformeerd over de stand van zaken rondom het thema bescherming vitale infrastructuur.

Cybersecurity is geïntegreerd in de systematiek van het Alerteringssysteem Terrorismebestrijding. Verder heeft de Nationale Academie voor Crisisbeheersing cybersecurity in de basis- en verdiepingstraining opgenomen, waarbinnen een trainingsprogramma voor respons op grootschalige ICT-incidenten is opgenomen. Met en binnen vitale sectoren vinden regelmatig oefeningen plaats, zowel voor afzonderlijke als samenwerkende bedrijven. Van 22 tot 25 juni 2015 heeft een publiek-private operationele ICT-crisisoefening Isidoor op nationaal niveau plaatsgevonden. De deelnemers hebben in drie dagen de gelegenheid gehad met elkaar te werken aan het oplossen van het aan hen voorgelegde scenario. Hierdoor is het onderlinge vertrouwen in de samenwerking op operationeel niveau tussen publieke en private partijen sterk toegenomen.

Versterkte aanpak digitale spionage
Digitale spionage blijft één van de twee grootste cyberdreigingen waarmee Nederland wordt geconfronteerd die zich voortdurend ontwikkelt. Met name digitale politieke spionage en digitale economische spionage zijn op dit moment schadelijk voor Nederland. De jaarverslagen van de inlichtingen- en veiligheidsdiensten en het CSBN bevestigen de trend dat de frequentie, complexiteit en impact van digitale spionage aanvallen blijft toenemen. Een

[1] Kamerstuk 30821, nr. 23

constante aanscherping van de inspanningen om adequaat op deze dreiging te reageren is daarom gevraagd.

De voornaamste resultaten van het actieprogramma van het NCSS 2 zijn dat de onderzoeks- en analysecapaciteiten van de Militaire Inlichtingen en Veiligheidsdienst (MIVD) en het Nationaal Cyber Security Centrum (NCSC) zijn versterkt. Het versterken van de samenwerking in de keten van publieke partners is van groot belang voor het versterken van de cybersecurity. Zo is in een pilot CAT-5 (AIVD/MIVD/NCSC/Politie/OM) verkend hoe de samenwerking op het gebied van gezamenlijke analyses van botnets versterkt kan worden. De pilot is afgerond en er wordt thans bezien hoe een vervolg hierop, mede gelet op de wettelijke kaders, vorm kan krijgen. Een ander voorbeeld is de samenwerking tussen de AIVD en MIVD in een Joint Sigint Cyber Unit (JSCU) die op 15 juni 2014 van start is gegaan. Naar aanleiding van het rapport van de Commissie Dessens[2] wordt een wetsvoorstel voor een nieuwe Wet op de inlichtingen- en veiligheidsdiensten in procedure gebracht dat onder meer voorziet in een modernisering van de bevoegdheden van genoemde diensten en een versterking van de controle op de uitoefening van de bevoegdheden van deze diensten.

Haalbaarheidsonderzoek gescheiden netwerk vitaal
In de beleidsreactie bij het CSBN 2015 is uw Kamer geïnformeerd over het afronden van de verkenning naar een gescheiden ICT-netwerk voor (publieke en private) vitale processen, waarvan de bevindingen zijn toegelicht in mijn brief van 24 november 2014[3]. Het NCSC blijft een faciliterende rol spelen bij publiek-private en private initiatieven die bijdragen aan het verhogen van de weerbaarheid op dit vlak.

Versterking civiel-militaire samenwerking
Door de verwevenheid van militaire en civiele actoren in het digitale domein is een civiel-militaire aanpak ter vergroting van de digitale veiligheid noodzakelijk. In de beleidsreactie bij het CSBN 2015 is al gerapporteerd over belangrijke ontwikkelingen op dit vlak en ook het afgelopen jaar zijn een aantal forse stappen gezet. Na de oprichting van het Defensie Cyber Commando (DCC) in 2014 is in de loop van 2016 personele versterking gerealiseerd. Gewerkt wordt aan de opbouw van de operationele capaciteit van het DCC, die eind 2016 beschikbaar zal zijn. De doctrine voor de inzet van cybercapaciteiten in militaire missies is voor intern gebruik gerealiseerd. Deze wordt de komende periode becommentarieerd en geëvalueerd. In 2014 is ook een cyberreservistenbestand opgericht, met het oog op de beschikbaarheid van voldoende gekwalificeerd personeel in het geval van cyberincidenten. Er zijn inmiddels dertien cyberreservisten aangesteld, tien personen bevinden zich in de aanstellingsprocedure. Er vinden doorlopend

[2] Evaluatie Wet op de Inlichtingen en Veiligheidsdiensten 2002, Commissie Dessens, 2-12-2013
[3] Kamerstuk 26643, nr. 337

gesprekken plaats met publieke en private partijen over het verder vullen van het bestand.

In de beleidsreactie bij het CSBN 2015 bent u uitgebreid geïnformeerd over de samenwerking tussen het ministerie van Veiligheid en Justitie en het ministerie van Defensie, door middel van onder andere wederzijdse detacheringen en een samenwerkingsconvenant tussen DefCERT en het NCSC. De civiel-militaire samenwerking tussen beide partijen wordt onverkort doorgezet en verloopt naar tevredenheid.

Versterking Nationaal Cyber Security Centrum (NCSC)
De in 2014 ingezette personele versterking van het NCSC heeft verder vorm gekregen. Er zijn nog wel vacatures, vanwege de lastige situatie in het aantrekken van personeel in deze sterk gespecialiseerde sector en verloop. Het NCSC is 24/7 bereikbaar, waarbij verdere opschaling bij ernstige incidenten is voorzien. Het NCSC functioneert als meldpunt, signaleert nieuwe dreigingen en voorziet haar netwerk van contacten van opvolgbare informatie. Het NCSC zal, mede met behulp van het Nationaal Detectie Netwerk (NDN), zorgdragen voor het situationeel beeld ten aanzien van cyberdreigingen. In 2016 en 2017 ligt de nadruk bij de uitbreiding van het NDN en het eveneens publiek-private Nationaal Respons Netwerk (NRN) op het versneld aansluiten van meerdere organisaties en het optimaliseren van de dienstverlening door het NCSC, AIVD en MIVD.

Binnen de Rijksoverheid worden momenteel voorbereidingen getroffen voor het inrichten van een Threat Intel Platform waarmee, met inachtneming van de wettelijke kaders, informatie tussen het NCSC en andere Rijksoverheidsorganisaties kan worden gedeeld.

Als onderdeel van de verdere professionalisering van het NCSC is de Inspectie voor Veiligheid en Justitie verzocht een onderzoek uit te voeren naar het gebruik van beveiligingsadviezen, ofwel *advisories* van het NCSC. Dit onderzoek is met de vorige beleidsreactie gedeeld. De bevindingen uit het onderzoek zijn uitgewerkt in het project Advisories 2.0, wat momenteel in de tooling en werkwijze wordt geïmplementeerd. De belangrijkste wijziging is dat minder beveiligingsadviezen door het NCSC worden geschreven, maar dat meer tijd wordt genomen in het verdiepen van de achtergronden, remedies en impactanalyses.

Daarnaast is het wetsvoorstel gegevensverwerking en meldplicht cybersecurity[4] bij uw Kamer ingediend.

Legacysystemen, toezicht en accreditatie
In 2015 heeft het NCSC een self-assessmentmethode ontwikkeld om organisaties zelf in staat te stellen de risico's voor legacy systemen in kaart te brengen.

[4] Kamerstuk 34 388, nr.2

Gezien het Europese akkoord op de NIB-richtlijn is besloten dit onderwerp ter voorkoming van overlap onder te brengen bij de implementatie van de NIB richtlijn. Tenslotte is in 2015 een verkenning gestart naar diverse internationale accreditatiesystemen voor bedrijven die als 'digitale brandweer' kunnen optreden. Deze verkenning is afgerond. In het rapport "verkenning accreditatiesysteem voor trusted hulpverleners" wordt aanbevolen om op basis van de thans gestarte discussie over standaardisering van cybersecurity in Europa, in de diverse Europese gremia actief te pleiten voor de opzet van een certificeringssysteem voor cybersecuritydienstverleners dat breed in Europa van toepassing is. Tevens wordt aanbevolen het Britse systeem CREST voor deze Europese oplossing als basis te gebruiken. In de tussentijd wordt voor Nederland het systeem van trusted Introducer aanbevolen om tot een voorlopig overzicht te komen van vertrouwde cybersecuritydienstverleners voor de Nederlandse cybersecuritymarkt.

Internationale aanpak cybercriminaliteit
Cybercrime is naast digitale spionage de andere grote dreiging op het gebied van cybersecurity. Om de aanpak van cybercrime stevig aan te pakken wordt de (straf)wetgeving versterkt. Hiertoe is het wetgevingstraject voor de wet computercriminaliteit III ingezet. De wet computercriminaliteit III geeft de politie meer slagkracht voor de opsporing in cyberspace. Het wetsvoorstel is eind 2015 naar de Tweede Kamer gestuurd.

Internationaal wordt ingezet op het versterken van de samenwerking en het harmoniseren van wetgeving. De onderwerpen die tijdens de GCCS2015 zijn besproken, versterking van de samenwerking en jurisdictie in cyberspace, zijn tijdens het Nederlandse EU voorzitterschap geagendeerd voor de JBZ-raad. Er zijn raadsconclusies aangenomen over *criminal justice* in cyberspace, die door de commissie worden uitgevoerd, in samenwerking met de lidstaten en private partijen. Ter bevordering van de samenwerking zijn raadsconclusies aangenomen over de start van een Europees netwerk van openbaar aanklagers, met ondersteuning van Eurojust. Daarnaast heeft COSI, op basis van ervaringen uit de praktijk, concrete aanbevelingen aangenomen voor versterking van de operationele samenwerking.

Op operationeel niveau heeft de politie in 2014 een personele versterking van onderzoeks- en analysecapaciteiten gerealiseerd doordat het Team High Tech Crime (THTC) van politie op sterkte is gekomen, namelijk 120 fte. Voor de komende periode is de aandacht daarom gericht op het verruimen van de aanpak van high tech crime zaken op het niveau van de landelijke eenheid naar de aanpak van cybercrime op het niveau van alle eenheden van de politie. Een randvoorwaarde daarvoor is het versterken van de digitale expertise. In 2015 is gestart met het (extern) werven van digitaal experts die ondersteunen bij de aanpak van alle criminaliteit met een complexer digitale component, waaronder cybercrime. Ook is een start gemaakt met

investeringen in de benodigde technische ondersteuning en zijn standaarden vastgelegd en geïmplementeerd. Het vrijmaken van voldoende tactische capaciteit binnen de bestaande sterkte van de eenheden en het realiseren van de noodzakelijke ondersteunende ICT middelen om tegen de snelle groei van cybercrime op te kunnen treden blijkt echter een lastige opgave.

Er wordt verder onverminderd ingezet op bewustwording en toerusting van betrokken medewerkers van de politie om de benodigde bijdrage aan de aanpak van cybercrime en gedigitaliseerde criminaliteit te kunnen leveren. Het afgelopen jaar zijn updates verschenen voor handreikingen (voor de intake van cybercrime en het betreden van een plaats delict in een gedigitaliseerde omgeving) en is de ambitie om het trainings- en opleidingsaanbod op dit thema uit te breiden.

Gedragen standaarden en security en privacy by design
Veel oudere ICT systemen die thans in gebruik zijn, waren niet altijd ontwikkeld met privacy en veiligheid in gedachte. Om op de lange termijn over veiligere ICT-systemen te kunnen beschikken, zet het kabinet in op het stimuleren van de ontwikkeling en aanschaf van veilige hard- en software. Het belang van aantoonbaar veilig ontwikkelde software is in de voortgangsbrief Visie Telecom, Media en Internet en de Nationale Cyber Security Strategie geduid. Om dit te realiseren hebben diverse marktpartijen, in nauwe samenwerking met het ministerie van Economische Zaken en ECP, een nieuw “Normenkader Secure Software” ontwikkeld. Dit normenkader en het gebruik ervan wordt verder ontwikkeld en gestimuleerd binnen een onafhankelijke stichting, de Secure Software Foundation.

Voorts is in 2014 een publiek privaat platform internetstandaarden ingericht om de toepassing van moderne internetstandaarden te stimuleren. De website www.internet.nl, gelanceerd tijdens de GCCS 2015, checkt op de compliance met internetstandaarden zoals IPv6, DNSSEC en veiligheidsstandaarden van websites. De website is inmiddels 100.000 maal bezocht en heeft daarmee bijgedragen aan bewustwording én geleid tot aanpassingen bij diverse marktpartijen en overheden.

Standaarden en certificering om veiligheid en privacy van ICT producten- en diensten te bevorderen was één van de vier hoofdthema’s van de Hoogambtelijke bijeenkomst cybersecurity in april 2016, resulterend in aanbevelingen aan de Commissie om acties op te pakken.

Cyberdiplomatie: veiligheid, kennis en capaciteitsopbouw
Het internationale karakter van cybersecurity kwam nadrukkelijk naar voren bij de GCCS 2015 waarvan Nederland gastheer was. Deze internationale top met vertegenwoordigers op ministerieel niveau, van internationale organisaties en leiders uit de private sector benadrukte het belang van internationale samenwerking tussen alle stakeholders en kennisuitwisseling in het digitale domein. De successen van de GCCS 2015 zijn het afgelopen jaar verder ontwikkeld. Een voorbeeld hiervan is het, tijdens de GCCS 2015

gelanceerde, mondiale Global Forum on Cyber Expertise (GFCE). In het GFCE worden initiatieven voor het delen van kennis en kunde over digitale veiligheid samengebracht. Hieronder vallen het ontwikkelen van cybersecurity strategieën, het versterken van de positie van zogenaamde internetnooddiensten en het aanmoedigen van de samenwerking met ethische hackers. De leden van het GFCE onderschrijven een vrij, open en veilig internet. Nederland heeft als voorzitter van het GFCE een sterke en zichtbare rol.

De internationale visie van de Nationale Cyber Security Strategie 2 gaat uit van een geïntegreerde aanpak van veiligheid, waarin naast het belang van *defence* en *development*, in de vorm van capaciteitsopbouw, ook middels *diplomacy* wordt bijgedragen aan meer stabiliteit in het cyberdomein.

Nederland is op de ingeslagen weg voortgegaan. Er is een actieve bijdrage geleverd aan het tot stand komen van een tweede set vertrouwenwekkende maatregelen (CBMs) in de OVSE. De ontwikkeling van soortgelijke CBMs in Azië is gestimuleerd door de organisatie van scenario-oefeningen, onder andere in het ASEAN Regional Forum. Nederland heeft samen met de Verenigde Staten een International Security Cyber Issues Workshop Series in de VN gefinancierd, om een grotere groep landen in staat te stellen aan deze discussie deel te nemen. Internationale veiligheid in cyberspace werd daarin voor het eerst in de VN volgens een multistakeholderaanpak benaderd. Ook is voor de juridische adviseurs van meer dan 50 landen een tweede consultatiebijeenkomst gehouden over de *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, die eind dit jaar gepubliceerd zal worden. In het kader van *The Hague Process* zal deze waardevolle discussie verder worden voortgezet na het aflopen van het NCSS2.0 actieplan.

Ook op andere manieren speelt Nederland een vooruitstrevende rol op het gebied van cyberdiplomatie. Zo is tijdens het EU voorzitterschap de aanzet gegeven voor het ontwikkelen voor een diplomatiek instrumentarium voor een gezamenlijke EU respons op ernstige cyberaanvallen. De EU kan daarmee de militaire benadering van de NAVO complementeren. Daarnaast werkt Nederland op basis van de kabinetsreactie op het rapport van de WRR over de publieke kern van het internet aan het ontwikkelen van een gedragsnorm welke bijdraagt aan conflictpreventie.

Het kennisknooppunt op het gebied van cyberdiplomatie waar in de NCSS 2 naar gestreefd wordt, is momenteel in oprichting. Het ministerie van Buitenlandse Zaken werkt hieraan in een samenwerkingsverband met de Universiteit Leiden, om meer kennis en expertise te genereren op het gebied van internationale betrekkingen en conflictpreventie in cyberspace.

Nederland heeft zicht het afgelopen jaar ook sterk ingezet voor internetvrijheid. Het belang van stevige bescherming van fundamentele rechten en vrijheden is onder meer onder de aandacht gebracht tijdens VN bijeenkomsten (IGF 2015 en de Mensenrechtenraad 32) en tijdens de toonaangevende internetconferentie RightsCon. In de Freedom Online Coalitie (FOC) zijn er drie statements uitgebracht en Nederland bekleedt een actieve rol in de werkgroep die de strategische evaluatie van de FOC trekt.

Cybersecurity onderwijs en het stimuleren van innovatie in cybersecurity
In 2015 is een stevige impuls gegeven aan de acties op het gebied van onderwijs uit de NCSS2. Gelet op het belang van een veilige digitale omgeving wordt de noodzaak van voldoende cybersecurityspecialisten breed onderschreven. Zo maakt de beroepsgroep cybersecurityspecialisten onderdeel uit van de Human Capital Agenda die door het ministerie van Economische Zaken wordt ontwikkeld[5]. Cybersecurityspecialisten is een van de doelgroepen waar de acties uit de HCA ICT-innovatie zich op richten.

In april 2016 is het startschot gegeven voor het Dutch cybersecurity platform for higher education and research (Dcypher)[6]. Met de realisatie van Dcypher wordt ook invulling gegeven aan de doelstelling uit de NCSS2 over cybersecurity kennis en –kunde en ICT-innovatie. Het zorgt voor agendering en coördinatie van (wetenschappelijk en praktijkgericht) cybersecurity onderzoek en –hoger onderwijs. Met Dcypher wordt beoogd te bereiken dat het aantal cybersecurity specialisten groeit en dat meer studenten in het hoger onderwijs zich voor relevante curricula inschrijven en succesvol afronden. Dcypher vormt de opvolger van het voormalige ICT Innovatieplatform Veilig Verbonden (IIP-VV), dat zich vooral richtte op de agendering van het onderzoek naar security en privacy.

Een ander project in dit kader is de pilot Scientist on the Job (SotJ) van de NWO. Met de introductie van het SotJ-instrument stimuleert NWO personele uitwisselingen tussen (in Nederland gevestigde) publieke- en private ondernemingen en de Nederlandse cybersecurity onderzoekscommunity. Het doel is om snel concreet wetenschappelijke resultaten in die ondernemingen te boeken en om binnen een publiek-private samenwerking meer van elkaar te leren.
Om onderzoek en innovatie in cybersecurity te stimuleren is vanaf 2012 een tweetal onderzoek tenders uitgevoerd binnen de kaders van de Nationale Cyber Security Research Agenda (NCSRA). Met de opgedane ervaringen wordt thans aan een vervolgtender vorm gegeven. Zo zijn tijdens het NCSRA-Symposium op 2 november 2015 lopende onderzoeksprojecten gepresenteerd die uit deze tenders zijn voortgekomen.

[5] Stcrt. 2014, nr. 28095
[6] Dcypher is geïnitieerd door het ministerie van Veiligheid en Justitie, het ministerie van Economische Zaken, het ministerie van Onderwijs, Cultuur en Wetenschap en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek, gebied Exacte Wetenschappen.