De Nationale Cyber Security Strategie (NCSS)

Slagkracht door samenwerking

1. Inleiding

Nederland staat voor veilige en betrouwbare ICT[1] en het beschermen van de openheid en vrijheid van het internet. De toenemende afhankelijkheid van ICT maakt de samenleving steeds kwetsbaarder voor misbruik en (grootschalige) verstoring. Het kabinet komt daarom met deze Nationale Cyber Security Strategie die is opgesteld met bijdragen van een breed scala aan publieke en private partijen, kennisinstellingen en maatschappelijke organisaties. Met deze strategie komt het kabinet tegemoet aan de moties Knops en Hernandez[2] en geeft het kabinet vorm aan de in het regeerakkoord aangekondigde integrale aanpak voor cyber crime.

Leeswijzer
Deze strategie valt uiteen in twee delen. Het eerste deel (hoofdstukken 2 tot en met 4) bevat een analyse van het probleem, uitgangspunten voor het beleidsterrein cyber security en het te bereiken doel. Het tweede deel (hoofdstuk 5) bevat een aantal actielijnen en per lijn prioritaire activiteiten die dit kabinet zelf en met andere partijen wil uitvoeren om de cyber security te verbeteren.

2. Ontwikkelingen die om actie vragen

ICT is van fundamenteel belang voor onze samenleving en economie
Veilige en betrouwbare ICT is van fundamenteel belang voor onze welvaart en welzijn en vormt een katalysator voor (verdere) duurzame economische groei. In Europa is 50% van de productiviteitsgroei te danken aan de toepassing van ICT[3]. Nederland wil behoren tot de wereldtop als het gaat om gebruik én inzet van ICT in de samenleving en tegelijkertijd de veiligheid waarborgen van de digitale samenleving. De ambitie is om uit te groeien tot de *Digital Gateway to Europe*.

De samenleving is kwetsbaar
ICT biedt kansen, maar verhoogt ook de kwetsbaarheid van een samenleving waarin steeds meer vitale producten en diensten met elkaar verweven zijn. Een moedwillige of een onopzettelijke verstoring als gevolg van technisch of menselijk falen of door natuurlijke oorzaken kan leiden tot maatschappelijke ontwrichting. De complexiteit van ICT-voorzieningen en onze toenemende afhankelijkheid van deze voorzieningen leiden tot nieuwe kwetsbaarheden die misbruik en verstoring in de hand werken. Voorbeelden hiervan zijn de snelle ontwikkelingen van mobiel dataverkeer en cloud-computing die nieuwe kwetsbaarheden en nieuwe mogelijkheden van misbruik tot gevolg hebben. Ook de toename van het gebruik van internetdiensten waarbij persoonsgegevens gebruikt moeten worden en de stijging van de populariteit van sociale media zorgen voor nieuwe kwetsbaarheden en misbruik, bijvoorbeeld in de vorm van identiteitsdiefstal.

Recente voorbeelden
Recente incidenten geven gezicht aan dit besef van kwetsbaarheid en misbruik. Zo is in de tweede helft van 2010 geavanceerde malware - Stuxnet – ontdekt, die zich specifiek richt op industriële procesautomatisering. Analyse wees uit dat met de ontwikkeling hoge kosten moeten zijn gemoeid. Het vermoeden bestaat dat deze aanval door een staat gefinancierd is, gericht tegen de vitale infrastructuur in een andere staat, met wereldwijde neveneffecten bij andere (vitale) organisaties. In een internationaal gecoördineerde actie trad het KLPD eind 2010 in samenwerking met partners in binnen– en buitenland op tegen een groot botnet, een verzameling computers van veelal nietsvermoedende eigenaars die op afstand misbruikt kan worden voor bijvoorbeeld criminele handelingen. Het botnet, Bredolab genoemd, werd aangestuurd vanuit Armenië, had een zwaartepunt in Nederland en kende vertakkingen in verschillende andere landen. Wereldwijd waren miljoenen computers onderdeel van dit botnet, waarmee onder andere spam werd verstuurd en

[1] ICT is het geheel aan digitale informatie, informatie-infrastructuren, computers, systemen, toepassingen en de interactie tussen informatietechnologie en de fysieke wereld waarover communicatie en informatie-uitwisseling plaatsvindt.

[2] Motie Knops, Tweede Kamer, vergaderjaar 2009-2010, 32 123 X, nr. 66.
Motie Hernandez, Tweede Kamer, vergaderjaar 2010-2011, 32 500 X, nr. 76.

[3] Eurocommissaris Kroes tijdens de opening van de WCIT conferentie 2010 te Amsterdam.

DDoS-aanvallen werden uitgevoerd. De maatregelen die een aantal bedrijven namen tegen WikiLeaks lokten WikiLeaks aanhangers er toe uit wereldwijd DDoS-aanvallen uit te voeren tegen onder andere Paypal, Mastercard, het Openbaar Ministerie en de politie. Hierdoor zijn de websites van deze organisaties tijdelijk onbereikbaar geweest en is de eenvoud van hacktivisme duidelijk naar voren gekomen.

Cyber security *is het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.*

Samenwerking tussen bestaande partijen in de digitale samenleving is nodig, ook internationaal.
Bij een cyberaanval is het vaak moeilijk vast te stellen wie de veroorzaker is. Het kan gaan om een eenling, een organisatie, een staat of een combinatie hiervan. Ook is zelfs vaak niet direct duidelijk om welk type cyberdreiging[4] het gaat. Wel wordt bij een cyberaanval veelal gebruik gemaakt van dezelfde technieken en methoden[5]. Dit alles maakt verdergaande samenwerking tussen partijen die zich met cyber security bezig houden van groot belang; van overheidsorganisaties die zich richten op afzonderlijke typen dreigingen, bedrijven die de netwerk- en informatie-infrastructuur in stand houden, tot kennisinstellingen op het terrein van cyber security en de burger.

De digitale samenleving is mondiaal. Cyberaanvallen en -verstoringen overschrijden in een oogwenk landsgrenzen, culturele en juridische stelsels. Vaak is onduidelijk welke rechtsmacht van toepassing is en is het onzeker of het recht altijd effectief tot uitvoering kan worden gebracht. Het kabinet wil dat het gemakkelijker wordt om ook tegen misbruik in de digitale wereld op te treden, waar die ook vandaan komt.

3. Uitgangspunten

Investeren in cyber security betekent investeren in onze toekomst, onze economische groei en onze innovatie. Niet alleen doordat er veilige ICT en veilig gebruik van ICT mogelijk is in Nederland, maar ook omdat Nederland een belangrijke speler is in het kennis- en ontwikkelingsgebied van cyber security. Dit vereist een hoge prioriteit voor cyber security (civiel-militair, publiek-privaat, nationaal-internationaal, door de gehele veiligheidsketen) wat moet resulteren in een weerbare ICT-infrastructuur, in weerbare vitale sectoren, snelle en effectieve respons en een adequate rechtsbescherming in het digitale domein. Daarbij gelden de volgende uitgangspunten.

Verbinden en versterken van initiatieven
Er gebeurt al veel op het terrein van cyber security. Samenhang ontbreekt echter op een aantal punten. De bevindingen in het nationaal Trendrapport cybercrime en digitale veiligheid 2010 en het rapport ICT-kwetsbaarheid en Nationale Veiligheid van de Denktank Nationale Veiligheid ondersteunen dit. Daarom worden doublures verwijderd en initiatieven gebundeld. Waar mogelijk wordt voortgebouwd op bestaande initiatieven en zo nodig ontplooit het kabinet nieuwe initiatieven.

Publiek-Private Samenwerking
ICT-infrastructuur, –producten en -diensten worden voor het grootste deel geleverd door private sectoren. Continuïteit en leveringszekerheid zijn niet alleen voor het bedrijfsleven van belang vanwege hun voortbestaan. Ook de maatschappij heeft daar belang bij, bijvoorbeeld om maatschappelijke ontwrichting door verstoringen te voorkomen. Wederzijds vertrouwen is essentieel om samen te werken en informatie met elkaar te delen. Overheid en bedrijfsleven werken dan ook samen als gelijkwaardige partners. Daarbij moet elke betrokken partij meerwaarde

[4] cybercrime, cyberterrorisme, cyberactivisme, cyberspionage of cyberconflict
[5] zoals malware, botnets, spam, phishing en targeted attacks

ontlenen aan participatie in gezamenlijke initiatieven. Een goed samenwerkingsmodel met daarbij duidelijke taken, verantwoordelijkheden, bevoegdheden en waarborgen ondersteunt dit.

Eigen verantwoordelijkheid
Alle gebruikers (burgers, bedrijven, instellingen en overheden) nemen passende maatregelen om hun eigen ICT-systemen en –netwerken te beveiligen en veiligheidsrisico's voor anderen te voorkomen. Zij zijn zorgvuldig met het opslaan en delen van gevoelige informatie en respecteren de informatie en de systemen van andere gebruikers.

Verantwoordelijkheidsverdeling departementen
De minister van Veiligheid en Justitie heeft, in lijn met de uitgangspunten van de Strategie Nationale Veiligheid, de regie op de samenhang en samenwerking binnen het onderwerp cyber security en is daarop aanspreekbaar. Daarnaast behoudt iedere partij zijn eigen taken en verantwoordelijkheden.

Actieve internationale samenwerking
Het grensoverschrijdende karakter van dreigingen maakt het noodzakelijk sterk in te zetten op internationale samenwerking. Uitgangspunt is een internationaal 'level playing field'. Veel maatregelen zullen pas effect sorteren als ze internationaal worden afgestemd dan wel getroffen. Nederland steunt en draagt actief bij aan de inspanningen van bijvoorbeeld de EU (Digitale agenda voor Europa en de Interne Veiligheidsstrategie), de NAVO (ontwikkelen van cyber defence beleid in het kader van het nieuwe strategische concept), het Internet Governance Forum en andere samenwerkingsverbanden. Nederland zet zich in voor een wijdverspreide ratificatie en uitvoering van het Cybercrime Verdrag van de Raad van Europa.

Te nemen maatregelen zijn proportioneel
Honderd procent veiligheid bestaat niet. Nederland maakt keuzes in het oppakken van cyber security activiteiten op basis van een risicoafweging. Belangrijk onderdeel daarbij vormt een aantal kernwaarden van onze samenleving. Privacy, respect voor anderen en fundamentele rechten als de vrijheid van meningsuiting en informatievergaring dienen overeind te blijven. Er moet een goede balans blijven bestaan tussen enerzijds onze wens voor publieke en nationale veiligheid en anderzijds voor het waarborgen van onze grondrechten. Maatregelen moeten proportioneel zijn. Hiervoor worden waarborgen en toetsingsmechanismen, waaronder de bestaande toezichtfuncties, benut en waar nodig versterkt.

Zelfregulering als het kan, wet- en regelgeving als het moet
Overheid en bedrijven bereiken de gewenste digitale veiligheid allereerst door zelfregulering. Wanneer zelfregulering niet werkt wordt gekeken naar mogelijkheden van wet- en regelgeving. Uitgangspunten daarbij zijn dat regelgeving niet onnodig concurrentieverstorend werkt en zoveel mogelijk zorgt voor een level playing field, dat de administratieve lasten niet onevenredig worden verhoogd en de kosten in een redelijke verhouding staan tot de baten.
Ontwikkelingen gaan snel. Wetgeving kan daardoor snel verouderen. Het kabinet gaat na of de wetgeving aangepast moet worden aan de ontwikkelingen in het digitale domein.

4. Doel van de strategie

Veiligheid en vertrouwen in een open en vrije digitale samenleving
Doel van deze strategie is het versterken van de veiligheid van de digitale samenleving om daarmee het vertrouwen in het gebruik van ICT door burger, bedrijfsleven en overheid te verhogen. Daartoe wil de Nederlandse overheid met andere partijen slagvaardiger werken aan de veiligheid en de betrouwbaarheid van een open en vrije digitale samenleving.

Hiermee wordt de economie gestimuleerd en welvaart en welzijn verhoogd. Een goede rechtsbescherming in het digitale domein wordt gegarandeerd en maatschappelijke ontwrichting wordt voorkomen dan wel er wordt adequaat opgetreden als het toch mis gaat.

5. Werkplan "Werk in uitvoering"

Om het doel van deze Nationale Cyber Security Strategie te bereiken zijn de volgende actielijnen gekozen:

- Nederland zorgt voor een integrale aanpak door publieke en private partijen;
- Nederland zorgt voor adequate en actuele dreiging- en risicoanalyses;
- Nederland versterkt de weerbaarheid tegen ICT-verstoringen en cyberaanvallen;
- Nederland versterkt responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
- Nederland intensiveert opsporing en vervolging van cybercrime;
- Nederland stimuleert onderzoek en onderwijs.

Hieronder worden bij de actielijnen concrete acties uitgewerkt.

Werk in uitvoering
Voor het onderwerp van cyber security als geheel geldt dat er al veel gebeurt. Hieronder wordt een aantal prioritaire nieuwe of te versterken activiteiten uitgewerkt. De mate waarin deze activiteiten zijn uitgewerkt verschilt. Voor een aantal activiteiten bevindt het proces zich nog in een vroeg stadium, waardoor op dit moment geen breed gedragen beeld kan worden geschetst van de invulling van de activiteit. Hier is dus duidelijk sprake van werk in uitvoering. Na publicatie van dit actieplan wordt met betrokken partijen verder gewerkt aan uitwerking van deze punten.

5.1. Inrichten Cyber Security Raad en Nationaal Cyber Security Centrum

De zorg voor digitale veiligheid is in Nederland belegd bij veel verschillende partijen. Op dit moment is er nog onvoldoende samenhang tussen het geheel van goede beleidsinitiatieven, voorlichting en operationele samenwerking. Het kabinet vindt het daarom belangrijk dat er een gezamenlijke aanpak is met bedrijfsleven en kennis- en onderzoeksinstellingen. Doel is het versterken van het netwerk en het zorgen voor coördinatie van strategisch tot uitvoerend niveau.

- Het kabinet vindt een nieuwe netwerkgerichte samenwerkingsvorm nodig om de integrale en samenhangende aanpak van cyber security te bereiken. Inzet van het kabinet is het oprichten van een Cyber Security Raad, waarin op strategisch niveau vertegenwoordigers van alle relevante partijen zitting hebben en waarin afspraken worden gemaakt over uitvoering en uitwerking van deze strategie. De komende maanden wordt in overleg met alle relevante partijen uitgewerkt hoe de Raad in te richten. De overheid faciliteert de Raad.

- Wens van het kabinet is dat publieke en private partijen, op basis van hun eigen taken en binnen de wettelijke mogelijkheden, informatie, kennis en expertise in een op te richten Nationaal Cyber Security Centrum bij elkaar brengen, zodat inzicht kan worden verkregen in ontwikkelingen, dreigingen en trends, en ondersteuning kan worden geboden bij incidentafhandeling en crisisbesluitvorming. Het kabinet nodigt publieke en private partijen uit zich aan te sluiten bij dit Centrum. Om dit mogelijk te maken wordt een samenwerkingsmodel ontwikkeld.

- Het kabinet zal het huidige GOVCERT.NL[6] uitbreiden, versterken en inbrengen in dit Centrum.

Inzet van het kabinet is dat de Raad op 1 juli van dit jaar en het Centrum op 1 januari 2012 kunnen starten.

5.2. Opstellen dreiging- en risicoanalyses

Het versterken van de veiligheid begint met inzicht in kwetsbaarheden en dreigingen. Door kennis en informatie van (inter)nationale publieke en private organisaties[7] bij elkaar te brengen en te

[6] GOVCERT.NL richt zich op versterking van de informatiebeveiliging binnen de Nederlandse overheid en doet dat door het monitoren van bronnen via internet, het uitgeven van adviezen over ICT-kwetsbaarheden en waarschuwingen bij dreigingen en door ondersteuning te bieden aan overheidsorganisaties bij de afhandeling van ICT-gerelateerde incidenten.

[7] Onder andere GOVCERT.NL, AIVD en MIVD[7], politie, Buitengewone Opsporingsdiensten (bijv. FIOD, SIOD), toezichthouders (bijv. OPTA en Consumentenautoriteit), Rijksinspecties (bijv. Inspectie Volksgezondheid),

analyseren, ontstaat een beter inzicht in actuele en mogelijke nieuwe kwetsbaarheden en dreigingen. Hierbij wordt aangesloten bij de werkwijze van de strategie nationale veiligheid; dat wil zeggen: risico's in kaart brengen en capaciteiten identificeren die versterkt moeten worden om dreigingen te voorkomen en op verstoringen te kunnen reageren. Met deze kennis kunnen alle doelgroepen maatregelen treffen in de gehele keten van preventie tot respons en opsporing en vervolging.

- Een van de taken van het Nationaal Cyber Security Centrum is het creëren van één gezamenlijk en integraal beeld van de actuele dreigingen van ICT, onder andere in de vorm van het Trendrapport Cybercrime en digitale veiligheid, dat in 2010 voor het eerst is verschenen.

- AIVD en MIVD[8] brengen kennis in ten behoeve van dit beeld. Waar nodig versterken zij hun cyber capaciteit.

- Het kabinet wordt jaarlijks via de Nationale Risicobeoordeling[9] op de hoogte gesteld van dreigingen voor de nationale veiligheid. Cyber security zal hierin extra aandacht krijgen.

5.3. Vergroten weerbaarheid van vitale infrastructuur

Maatschappelijke ontwrichting door ICT-verstoringen of cyberaanvallen moet worden voorkomen. Verschillende partijen hebben daarbij een verantwoordelijkheid, van burger tot leverancier. De gebruiker moet erop kunnen vertrouwen dat een ICT-product of -dienst veilig gebruikt kan worden. De leverancier moet daarom een voldoende veilig ICT-product of -dienst aanbieden. De gebruiker moet ook zelf de nodige veiligheidsmaatregelen treffen.

- De Telecommunicatiewet wordt in 2011 geactualiseerd. Een aantal bestaande afspraken met de grootste telecombedrijven over de continuïteit van hun vitale telecommunicatie-infrastructuur zal in regelgeving worden omgezet. Dit gaat om het melden van verstoring of uitval van diensten, minimum eisen op het gebied van continuïteit van dienstverlening, en het aansluiten bij internationale standaarden. Waar mogelijk wordt aangesloten bij een Europese gezamenlijke aanpak van deze onderwerpen.

- De komende jaren wordt het Informatieknooppunt Cybercrime onder de vlag van CPNI.nl voortgezet[10]. Nog dit jaar wordt bezien hoe de samenwerking tussen CPNI.nl en het op te richten Nationaal Cyber Security Centrum vorm krijgt.

- De overheid gaat samen met de vitale organisaties het gebruik van de gangbare minimale ICT beveiligingsstandaarden op basis van good practices stimuleren. Het kabinet werkt met vitale sectoren aan het verkrijgen van inzicht in mogelijke maatregelen tegen verstoring van hun vitale ICT-voorzieningen. Op basis hiervan dringt de overheid er bij vitale sectoren op aan om de geïdentificeerde maatregelen ook te treffen. Een voorbeeld daarvan is de Noodcommunicatievoorziening (NCV) die per 1 mei 2011 het huidige Noodnet vervangt. Vitale organisaties krijgen de gelegenheid zich op deze Noodcommunicatievoorziening aan te sluiten.

---

private partijen (bijv. ISP's en security vendors), nationale en internationale kennis- en onderzoeksinstellingen.

8 De AIVD en MIVD beschikken over een unieke informatiepositie aangaande cyberdreiging (zoals digitale spionage, cyberterrorisme en cyberextremisme) door het onderzoek dat wordt gedaan in het belang van de nationale veiligheid.

9 In de Nationale Risicobeoordeling worden verschillende typen bedreigingen voor de nationale veiligheid met een uniforme methode in scenario's voor de middellange termijn uitgewerkt en op waarschijnlijkheid en impact gescoord. Vervolgens worden voorstellen gedaan voor versterking van capaciteiten om de (gevolgen van de) bedreigingen te verminderen.

10 Het Informatieknooppunt Cybercrime biedt een platform waar vitale sectoren en overheidspartijen in een vertrouwde omgeving informatie uitwisselen over incidenten, dreigingen, kwetsbaarheden en good practices op het gebied van cybercrime en cyber security. Doel is de weerbaarheid van deze partijen tegen verstoringen te verhogen.

- Specifiek ter voorkoming van (digitale) spionage heeft het kabinet een maatregelenpakket ontwikkeld. Voor bedrijven is er een handleiding Kwetsbaarhedenanalyse Spionage beschikbaar waarmee zij hun weerbaarheid tegen spionage kunnen vergroten.

- De overheid vindt het vergroten van de eigen weerbaarheid belangrijk. Daarom werkt het kabinet eraan dat 80% van de vitale organisaties in de vitale sectoren Openbaar Bestuur en Openbare Orde en Veiligheid eind 2011 beschikt over een continuïteitsplan waarin het scenario van grootschalige verstoring van ICT en elektriciteit is opgenomen.

- Het kabinet stelt medio 2011 één beveiligingskader vast voor informatiebeveiliging van de rijksdienst en komt met een nieuw Voorschrift Informatiebeveiliging Gerubriceerde Informatie[11]. Ook wordt een rijksbrede controlecyclus voor informatiebeveiliging ingericht.

- In de loop van 2011 besluit het kabinet of in reisdocumenten een elektronische identiteitskaart kan worden opgenomen die voldoet aan het hoogste betrouwbaarheidsniveau voor burgers. Burgers kunnen zich dan via het internet betrouwbaar identificeren en een gekwalificeerde elektronische handtekening zetten waarbij de privacy gewaarborgd is.

- De overheid implementeert de Europese meldplicht voor datalekken met betrekking tot de Telecomsector. Verder wordt op grond van het regeerakkoord een voorstel voor een meldplicht uitgewerkt in geval van verlies, diefstal of misbruik van persoonsgegevens voor alle diensten van de informatiemaatschappij.

- Het kabinet zal in 2011 keuzes maken over veiligheid in relatie tot de verwerking van persoonsgegevens. De Europese ontwikkelingen op het gebied van privacy zijn daarbij richtinggevend. Het kabinet zal de Tweede Kamer binnen afzienbare tijd informeren over het standpunt over privacy. De meldplicht wordt daarin meegenomen.

- Het kabinet wil in overleg met de ICT-leveranciers zoeken naar mogelijkheden om de veiligheid van hard- en software te verbeteren en zet zich ervoor in om ook op internationaal niveau afspraken te maken over veilige hard- en software. Daarnaast neemt Nederland actief deel in het Internet Governance Forum dat door de Verenigde Naties wordt gefaciliteerd. Doel hiervan is om een actieve rol te spelen om in de mondiale context van een open en transparante dialoog onderwerpen aan te snijden die kunnen bijdragen aan deze strategie, zoals de spelregels op het internet te verbeteren en misbruik tegen te gaan.

- Het kabinet wil met leveranciers in overleg om informatie over de veiligheid van ICT-producten en -diensten beter beschikbaar te maken voor de gebruiker[12]. De overheid zal samen met leveranciers van ICT-producten en -diensten doelgerichte nationale campagnes voor burgers, bedrijven en overheid blijven ontwikkelen die zijn toegesneden op actuele ontwikkelingen en kwetsbaarheden[13].

5.4. Responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren

Om adequaat te kunnen reageren op verschillende dreigingen en om bij een verstoring of aanval terug te kunnen keren naar een stabiele situatie zijn verschillende responsactiviteiten nodig. ICT-incidenten die leiden tot een inbreuk op de beschikbaarheid, integriteit of exclusiviteit van de netwerk- en informatie-infrastructuur pakt de betreffende organisatie in eerste instantie zelf aan.

---

11 Het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD bevordert de beveiliging van bijzondere informatie door gekeurde en zelf ontwikkelde beveiligingsproducten beschikbaar te stellen, door hulp te verlenen bij de implementatie daarvan, door bijdragen te leveren aan beleid en regelgeving op dit gebied en door advies te geven over informatiebeveiliging.

12 Goede voorbeeelden zijn de “3 keer kloppen” campagne van de banken en gericht op de burger, het initiatief “Bescherm uw onderneming” van brancheverenigingICT~Office om MKB-ondernemingen te stimuleren tot een risicoanalyse en goede informatiebeveiliging, de campagne “Cybersafe yourself” voor hogescholen en universiteiten en “Webwijs” van Bits of Freedom.

13 Voorbeelden hiervan zijn de campagnes “Veilig Internetten”, “Digivaardig en Digibewust” (van ECP-EPN). Ook de “Waarschuwingsdienst.nl” voor actuele bedreigingen van GOVCERT.NL dient dit doel.

Daar waar incidenten kunnen leiden tot maatschappelijke ontwrichting of aantasting van vitale objecten, processen of personen, zal de overheid adequaat reageren.

- Het kabinet levert in de zomer van 2011 het Nationaal Crisisplan ICT op. Onderdeel hiervan is een oefenplan, dat zowel nationale als internationale oefeningen op elkaar afstemt.

- De ICT Response Board (IRB), een publiek-private samenwerking die de crisisbesluitvormingsorganisaties advies geeft over maatregelen om grootschalige ICT-verstoring tegen te gaan of te bestrijden, wordt in 2011 geoperationaliseerd en als functie ondergebracht in het Nationaal Cyber Security Centrum.

- Internationaal wordt ingezet op de versterking van de samenwerking bij de operationele respons tussen de CERT-organisaties in Europa en wordt gestreefd naar versterking van het International Watch and Warning Network (IWWN) dat nu als informeel mondiaal operationeel overleg fungeert bij ICT-incidenten.

- De maatschappelijke impact van een grootschalige terroristische aanval op of via het internet kan groot zijn. Het Alerteringsysteem Terrorismebestrijding (ATb) wordt daarom uitgebreid met een cyber component en beoefend.

- Defensie ontwikkelt kennis en capaciteiten om in het digitale domein effectief te kunnen opereren. Hierbij wordt maximaal ingezet op mogelijkheden om kennis en expertise uit te wisselen met civiele en internationale partners. Tevens wordt onderzocht hoe Defensie kennis en capaciteiten voor haar derde (hoofd)taak beschikbaar kan stellen binnen de ICMS (Intensivering Civiel-Militaire Samenwerking) afspraken.

- Er wordt een cyber opleidings- en trainingscentrum (OTC) opgericht.

- Om de weerbaarheid van de eigen netwerken en systemen verder te verbeteren worden de taken van het Defensie Computer Emergency Response Team (DefCERT) in de komende jaren verder uitgebreid. Tevens wordt geïnvesteerd in het vergroten van het beveiligingsbewustzijn bij het personeel en wordt gezorgd voor accreditatie van systemen en processen.

- Een doctrine voor cyber operations wordt ontwikkeld voor de respons op een aanval ter bescherming van eigen middelen en eenheden.

5.5. Intensiveren opsporing en vervolging van cybercrime

De zich snel ontwikkelende cyber criminaliteit vereist effectieve bestrijding om het vertrouwen in de digitale samenleving hoog te houden. Hiertoe moeten de uitvoeringsorganisaties in de strafrechtelijke keten (voornamelijk de politie en andere opsporingsdiensten maar ook het Openbaar Ministerie en de rechterlijke macht) die belast zijn met de bestrijding van cybercrime, beschikken over voldoende specialisten. Het gaat hierbij om de zeer specialistische behandeling van complexe zaken (high tech crime) en om behandeling van de meer eenvoudige (high volume) zaken die het vertrouwen in ICT van burgers, MKB en het overig bedrijfsleven aantasten. Doel is dat de aangiftebereidheid en de pakkans stijgen en dat overtreders steviger worden aangepakt. Ook met internationale samenwerking wordt grensoverschrijdende criminaliteit beter aangepakt.

- Het kabinet zet in op expert-poulevorming en inrichting van een deskundigenregister voor overheid, universiteiten en bedrijfsleven, zodat schaars beschikbare expertise gedeeld kan worden en specialisten een uitdagend carrièreperspectief wordt geboden.

- Voor de rechtshandhaving zet het kabinet in op meer grensoverschrijdende onderzoeken met opsporingsdiensten uit landen binnen Europa en met andere internationale partners. Verder zet het kabinet in op verdere internationale wet- en regelgeving voor cybercrime.

- Landelijk wordt een stuurgroep opgezet voor de aanpak van prioritaire criminaliteit. Voor cybercrime is het doel dat er in de gehele strafrechtketen voldoende specialisten zijn om cybercrime zaken adequaat aan te kunnen pakken. De voorzitter van deze stuurgroep neemt

deel in de Cyber Security Raad. De Inspectie Openbare Orde en Veiligheid zal onderzoek verrichten naar het functioneren van de politie bij de opsporing van cybercrime.

- Binnen het huidige budgettaire kader van de politie vindt de komende jaren een verschuiving plaats naar meer recherchecapaciteit en daarbinnen ook richting opsporing en vervolging van cyber criminaliteit. Het betreft internetsurveillanten en -specialisten binnen de regio's en bij het team high tech crime van het KLPD. Inzet is dat het team high tech crime in 2014 ongeveer twintig zaken draait. De opsporings- en vervolgingsdiensten zullen deelnemen aan het Nationaal Cyber Security Centrum.

- Het programma aanpak cybercrime speelt de komende jaren een centrale rol in onder meer: het opzetten van een kenniscentrum binnen de politie, de versterking van de politieorganisatie en het effectief verschuiven binnen de bestaande capaciteiten. Het OM en de rechterlijke macht gaan beschikken over voldoende en gespecialiseerde officieren van justitie, parketsecretarissen, rechters en cyberrechter commissarissen.

5.6. Stimuleren onderzoek en onderwijs

Wetenschappelijk en toegepast onderzoek en het stimuleren van de ontwikkeling van innovatieve veiligheidsoplossingen zijn een aanjager voor cyber security. Goede scholing op alle niveaus is noodzakelijk om betrouwbare ICT te kunnen blijven maken en weerstand te kunnen blijven bieden aan dreigingen. Een professionele beroepsgroep is een voorwaarde voor de groei van de digitale economie in Nederland.

- Het kabinet zal onderzoeksprogramma's van in ieder geval de overheid en waar mogelijk van wetenschappelijke onderzoekscentra en het bedrijfsleven beter op elkaar afstemmen in de Nationale Cyber Security Raad. Daarnaast gaat de overheid de genoemde partijen nog actiever dan nu begeleiden bij het aanboren van multiplicerende onderzoeksgelden bij bijv. Europese en Euregionale fondsen.

- Versterking van scholing op alle niveaus is noodzakelijk om weerstand te kunnen blijven bieden aan dreigingen en betrouwbare ICT te kunnen blijven maken en is een voorwaarde voor de groei van de digitale economie in Nederland. Met de beroepsgroepen en het onderwijsveld wordt een plan ontwikkeld voor het uitbreiden van het aandeel van ICT-veiligheid in de daarvoor geschikte opleidingen. Ook wordt voortgebouwd op een onderzoek naar de mogelijkheden van certificering en kwalificering van informatiebeveiligingsprofessionals. Daarbij hoort helderheid over de inhoud van opleidingen. Een goed voorbeeld daarvan is het initiatief van de beroepsgroep van informatiebeveiligers om de kenmerken van de verschillende opleidingen te expliciteren.

6. Financiële gevolgen

Bovenstaande activiteiten zullen binnen de bestaande begrotingen worden opgevangen.