ICT en Beleid
Brassersplein 2
Postbus 5050
2600 GB Delft

www.tno.nl

T 015 285 70 00
F 015 285 70 57
info-ict@tno.nl

TNO-rapport

ICT-veiligheidsbeleid in Nederland – een quickscan

Datum 25 september 2006

Auteur(s) Sandra Helmus
Linda Kool
André Smulders
Frans van der Zee

Exemplaarnummer
Oplage
Aantal pagina's 59
Aantal bijlagen 3

Inhoudsopgave

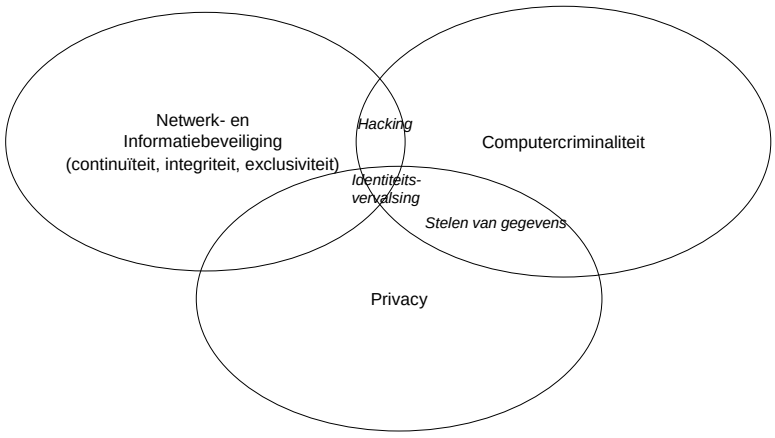
1 Inleiding

1.1 Achtergrond

Deze quickscan van het huidige ICT-veiligheidsbeleid maakt onderdeel uit van het Project 'Herijking ICT-veiligheidsbeleid' van het ministerie van Economische Zaken (EZ), Binnenlandse Zaken en Koninkrijksrelaties (BZK) en Justitie (JUS). Doel van de quickscan is om een inventarisatie te maken van het huidige beleid en de organisaties, programma's en projecten die voortkomen uit het beleid of het beleid uitvoeren.

De invalshoeken voor het project 'Herijking ICT-veiligheidsbeleid' zijn de drie domeinen netwerk- en informatiebeveiliging, computercriminaliteit en privacy zoals die in Europese kaders[1] zijn geformuleerd (zie figuur).

- Bij netwerk- en informatiebeveiliging gaat het om het zekerstellen dat informatie en diensten op de juiste momenten beschikbaar zijn voor gebruikers, dat gevoelige informatie is beschermd tegen onbevoegde kennisname (vertrouwelijkheid) en om het waarborgen van de correctheid (inclusief authenticiteit) en volledigheid van informatie en systemen (integriteit).
- Computercriminaliteit wordt meegenomen voor zover de computer naast middel ook doel is. Traditionele criminaliteit in een nieuw jasje, zoals verspreiding van kinderporno, waarbij de computer slechts als middel wordt gebruikt, valt buiten de scope van het project.
- Privacy betreft de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Onder de reikwijdte van het project vallen die privacy-issues die invloed hebben op het vertrouwen in het gebruik van ICT. Spam en phishing kunnen bijvoorbeeld afbreuk doen aan dit vertrouwen.[2]



Figuur 1. Domeinen op gebied van ICT-veiligheid

[1] Europese Commissie (2001), *Netwerk- en informatieveiligheid, voorstel voor een Europese beleidsaanpak*, COM(2001)298

[2] DGET (2006), Informatieblad interdepartementaal project 'Herijking ICT-Veiligheidsbeleid'

1.2 Doel

ICT-veiligheidsbeleid is een beleidsterrein dat niet onder één ministerie ressorteert, maar waarin meerdere ministeries rollen, taken en verantwoordelijkheden hebben. Dit komt onder meer voort uit aard en karakter van ICT-veiligheid, waarbij meerdere en verschillende infrastructuren (vast, mobiel, kabel, satelliet), diensten, toepassingen (inclusief software) en gebruik in verschillende maatschappelijke domeinen en sectoren in het geding zijn.

Tegelijkertijd dient het beleid dekkend, compleet en sluitend te zijn en dienen rollen, taken en verantwoordelijkheden duidelijk te zijn. Dit vergt afstemming tussen betrokken ministeries onderling en met en tussen partijen (bedrijven, organisaties, maar ook lagere overheden en het buitenland) in het veld.

Deze *quickscan* is enerzijds gericht op het in kaart brengen van het bestaande beleid inzake ICT-veiligheid, en anderzijds op het in kaart brengen van de bovenschetste rollen, taken en verantwoordelijkheden. In eerste instantie wordt daarbij gefocust op de initiatieven en acties van de ministeries BZK, EZ en Justitie. Omdat ICT-veiligheidsbeleid afhankelijk blijkt van andere partijen, soms binnen en soms buiten het publieke domein, worden ook andere spelers, acties en initiatieven in de inventarisatie betrokken. Er wordt daarmee een brede omschrijving van het begrip beleid gehanteerd, waarbij niet alleen wet- en regelgeving, maar ook bewustwording, informatievoorziening, coördinatie (inclusief vormen van zelfregulering) en andere vormen van beleid in beschouwing worden genomen en waarbij naast de (Rijks)overheid ook anderen een rol kunnen hebben.

1.3 Inhoud

De structuur van deze quickscan is als volgt. In hoofdstuk 2 wordt een beeld geschetst van de lopende initiatieven inzake ICT-veiligheid. Deze inventarisatie is gebaseerd op de eerste resultaten van een enquête die door de interdepartementale projectgroep van EZ, BZK en JUS in april 2006 is uitgezet onder de drie verantwoordelijke ministeries en instellingen, op gesprekken met leden van de interdepartementale projectgroep en op projectplannen en factsheets die zijn ontvangen (zie ook inleiding hoofdstuk 2). In hoofdstuk 3 worden de eerste bevindingen geschetst rond overlap en witte vlekken in het huidige beleid en worden de rollen, taken en verantwoordelijkheden van een aantal projecten en programma’s kort beschreven. De annexen I en II geven een overzicht van het huidige (en eerdere) ICT-veiligheidsbeleid aan de hand van openbare beleidsdossiers en correspondentie met de Tweede Kamer aangevuld met een actietabel waarin de voorgenomen taken van de Rijksoverheid en de huidige stand van zaken zijn benoemd op het gebied van ICT-veiligheid. Deze actietabel geeft een beeld van wat er aan beleid geagendeerd is en wat tot op heden aan beleid is uitgevoerd. Het dient ook als eerste check of er ‘witte vlekken’ in het huidige ICT-veiligheidsbeleid zitten. De tussen haakjes geplaatste dikgedrukte letter- en cijfercombinatie in de tabel refereren naar uitgebreidere beschrijvingen in de tekst (hoofdstuk 2).

2 ‘State of play’ in het Nederlandse ICT-veiligheidsbeleid

2.1 Inleiding

Dit hoofdstuk bevat een overzicht van de initiatieven, organisaties, programma’s en projecten op het gebied van ICT-veiligheid. Uitgangspunt voor de inventarisatie van alle beleidsinitiatieven op ICT-veiligheidgebied zijn de resultaten uit de ingevulde door EZ, BZK en Justitie uitgezette enquêtes (zie Annex III) onder de verschillende betrokken partijen in het kader van het interdepartementale project Herijking ICT-veiligheid. Openbare stukken, waaronder correspondentie van betrokken ministers aan de Tweede Kamer en beleidsdocumenten vormden een kapstok voor verdere invulling van deze quickscan. Paragraaf 2.2 beschrijft de structuur en typologie van het ICT-veiligheidsbeleid die is gekozen om het grote scala aan initiatieven en activiteiten in te delen. Paragraaf 2.3 licht de taken, rollen en verantwoordelijkheden van de drie ministeries EZ, BZK en Justitie in relatie tot het ICT-veiligheidsbeleid nader toe.

2.2 Structuur en typologie van ICT-veiligheidsbeleid

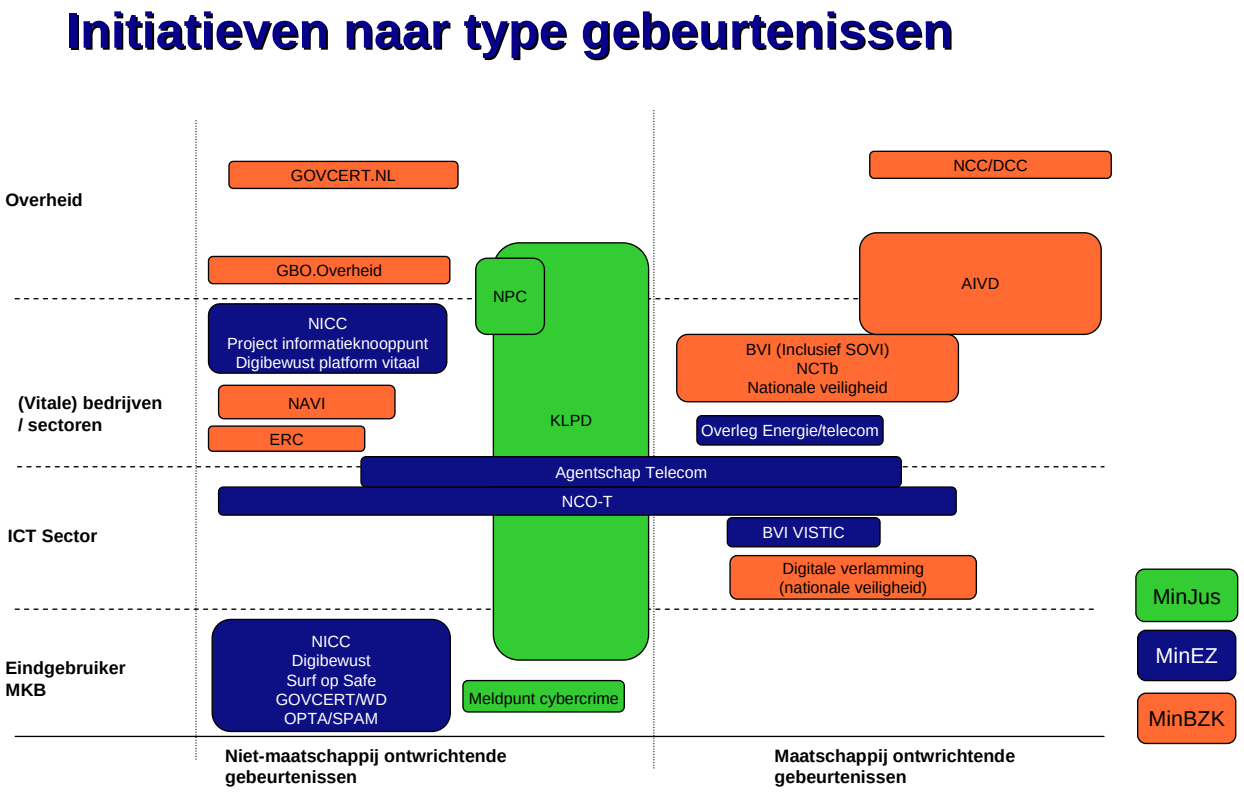
Het beleid op het gebied van ICT-veiligheid bestaat uit een groot aantal initiatieven, waaronder organisaties, publiek-private samenwerkingsverbanden, vormen van zelfregulering, en een veelheid van beleidsprogramma’s en projecten. Om hierin een nadere structuur aan te brengen is gekozen voor een indeling naar type gebeurtenis dat met de verschillende vormen van ICT-veiligheidsbeleid wordt beoogd.

De twee belangrijkste typen gebeurtenissen die onderscheiden kunnen worden op het gebied van ICT-veiligheid zijn: maatschappij ontwrichtende gebeurtenissen en niet-maatschappij ontwrichtende gebeurtenissen. Alle bestaande initiatieven en activiteiten richten zich op het voorkomen of bestrijden van (een van) deze twee typen gebeurtenissen. Deze twee categorieën sluiten aan bij de terminologie ‘uit te sluiten gebeurtenissen’ en ‘uitruilbare betrouwbaarheid’ zoals gebruikt in het DGET-paper ‘*Een strategische visie; overheidsrol en beleidsrichting op basis van omgevingsscan’*. Met ‘maatschappij ontwrichtende gebeurtenissen’ worden die situaties of gebeurtenissen bedoeld die de overheid ten koste van alles wil voorkomen en waar een publiek belang in het geding is dat uitgaat boven individuele deelbelangen. Het betreft gebeurtenissen die vergaande maatschappelijke en potentieel maatschappij ontwrichtende consequenties hebben op financieel, economisch of sociaal vlak. Voorbeelden hiervan zijn een terroristische aanslag, het uitvallen van een groot deel van de ICT-infrastructuur of een andere vitale infrastructuur (bijv. drinkwater, energie). De overheid zal in deze gevallen sturend willen optreden om deze gebeurtenissen zoveel mogelijk te voorkomen (bijvoorbeeld door middel van wet- en regelgeving) dan wel de consequenties zoveel mogelijk aan banden te leggen (mitigeren).

De categorie niet-maatschappij ontwrichtende gebeurtenissen omvat al die gebeurtenissen die geen maatschappij ontwrichtende consequenties hebben. Daarbij kan een (beperkt) publiek belang in het geding zijn. Echter, voor individuele (of een groep) slachtoffers kunnen deze gebeurtenissen verstrekkende gevolgen hebben. Voorbeelden hiervan zijn spam, spyware, virussen, hacking, phishing, autodialers. De overheid treedt

in deze gevallen voornamelijk faciliterend op (bijvoorbeeld door het geven van voorlichting, bewustwordingscampagnes etc.).

Naast de indeling naar type gebeurtenis is een (grove) indeling naar doelgroep te maken. De indeling zoals in deze quickscan gehanteerd is gebaseerd op de informatie uit de ingevulde vragenlijsten en bestaande projectplannen van de verschillende activiteiten. Er worden vier 'doelgroepen' van beleid onderscheiden: 1. de overheid, 2. de ICT-sector, 3. vitale sectoren/bedrijven en 4. de consument en overige bedrijven (waaronder het MKB). Veel initiatieven richten zich op één of meerdere doelgroepen. In onderstaande figuur zijn de meeste initiatieven weergegeven[3]. In paragraaf 2.4 tot en met 2.6 worden deze nader beschreven. Voorafgaand zal in paragraaf 2.3 kort de rolverdeling worden besproken tussen de drie meest relevante ministeries op het gebied van ICT-veiligheid.



Figuur 2. Initiatieven naar type gebeurtenis en doelgroep

[3] Deze indeling is naar beste kunnen gemaakt op basis van de beschikbare informatie. Voor dit rapport dient deze indeling met name om initiatieven die verwantheid in doelstelling (type gebeurtenis) en doelgroep lijken te hebben, dicht bij elkaar te kunnen beschrijven. De kleurindeling duidt op welk departement het meest dominant is in het project, waarbij tegelijkertijd opgemerkt dient te worden dat veel projecten betrokkenheid van meerdere departementen kennen.

2.3 De verantwoordelijke ministeries

2.3.1 Ministerie van Economische Zaken (DGET)

Binnen het ministerie van Economische Zaken is het Directoraat-Generaal Energie en Telecom (DGET) verantwoordelijk voor het creëren van de juiste randvoorwaarden voor een goede werking van elektronische netwerken en -diensten. Een van de hoofddoelstellingen van DGET is een veilig en betrouwbaar gebruik van telecommunicatie en ICT en het garanderen en bewaken van de continuïteit, betrouwbaarheid, veiligheid en kwaliteit van informatienetwerken en -diensten. Onder deze twee noemers kunnen de meeste activiteiten van EZ worden geschaard. Voorts heeft EZ een coördinerende verantwoordelijkheid voor het kabinetsbrede ICT-beleid en het beleid ten aanzien van informatienetwerken en -diensten. DGET vervult een belangrijke rol als beleidsmaker op het gebied van ICT-veiligheid naar de markt en de eindgebruikers.

2.3.2 Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK)

Nationale veiligheid is een van de hoofddoelstellingen van BZK. ICT-veiligheid is daar een onderdeel van. Onderwerpen als crisisbeheersing, bescherming van vitale infrastructuren en cyberterrorisme maken onderdeel uit van de ICT-veiligheid. Scheidslijnen tussen nationale veiligheid en ICT-veiligheid zijn vaak lastig te trekken.
Daarnaast is BZK beheerder en grootgebruiker van informatiesystemen en netwerken binnen de rijksoverheid. Vanuit deze taak draagt het ministerie de verantwoordelijkheid voor de bescherming en veiligheid van de overheidsinformatie-infrastructuur. Bovendien is dit ministerie verantwoordelijk voor de ontwikkeling van elektronische dienstverlening en is om die reden ook verantwoordelijk voor de veiligheid van deze elektronische diensten.

De verdeling binnen het ministerie is als volgt: twee DG's houden zich bezig met aspecten van (publieke) ICT-veiligheid: DG Veiligheid (DGV) richt zich hoofdzakelijk op de sector openbare orde en veiligheid en daarmee op de coördinatie en afstemming van het nationale veiligheidsbeleid, waar ICT-veiligheid onderdeel van uitmaakt. Directie Crisisbeheersing, het agentschap Korps Landelijke Politiedienst (KLPD) en brandweer en hulpdiensten vallen hieronder. De directie Crisisbeheersing is tevens coördinator van Nationaal Crisis Centrum (NCC). De afdeling risicobeleid binnen DG Veiligheid beheert het dossier Bescherming Vitale Infrastruur (BVI).

De Directie Innovatie en Informatiebeleid (DIIOS) van DG Management Openbare sector (MOS) is verantwoordelijk voor de ontwikkeling van elektronische dienstverlening (e-government) en de veiligheid van deze diensten. DIIOS is opdrachtgever voor diverse programma's in de clusters "Identificatie en Authenticatie" en "Informatiebeveiliging" van GBO.Overheid, waaronder DigiD, PKI-overheid, GOVCERT en eNIK. Verder is het directoraat betrokken bij totstandkoming Nationale Infrastructuur Bescherming Cybercrime (NICC). DIIOS werkt vooral samen met GBO/ICTU, medeoverheden en andere departementen.

2.3.3 Ministerie van Justitie (JUS)

Het ministerie van Justitie staat borg voor de strafrechtelijke handhaving van de wet- en regelgeving op het gebied van ICT-veiligheid door middel van opsporing en vervolging. Het ministerie bepaalt het beleid, het Openbaar Ministerie (OM) en de landelijke en regionale politiediensten zijn verantwoordelijk voor de uitvoering ervan.[4] Nieuwe criminele activiteiten in de digitale wereld, zoals phishing, het inbreken op computernetwerken en het verspreiden van spam en malware, vinden steeds vaker plaats en hebben een groeiende impact op de maatschappij. Daarnaast wordt ook veel traditionele criminaliteit gepleegd met ICT als middel. Deze laatste categorie valt echter buiten de scope van dit onderzoek.

Naast EZ, BZK en Justitie zijn zijdelings ook andere ministeries betrokken bij vraagstukken van ICT-veiligheid, waaronder OCW en Defensie. Deze worden echter buiten beschouwing gelaten in deze rapportage.

Hieronder zullen zowel organisaties en initiatieven worden besproken die op grond van een duidelijke wettelijke of beleidsbasis een bepaalde rol, taak en verantwoordelijkheid hebben binnen het dossier ICT-veiligheid, als een groot aantal andere activiteiten zoals (tijdelijke) programma's en projecten. De nadruk in de beschrijvingen zal liggen op de doelstelling, aard en inhoud van de activiteiten en de verdeling van rollen en verantwoordelijkheden.

2.4 Maatschappij ontwrichtende gebeurtenissen

Allereerst zullen de organisaties worden beschreven die over het algemeen een duidelijke wettelijke of beleidsbasis hebben. Voorts zullen de overige initiatieven worden besproken.

2.4.1 Nationaal Crisiscentrum (NCC) / Departementaal Crisiscentrum (DCC)

Wanneer zich een omvangrijke nationale crisis voordoet is de minister van Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk voor de afstemming van de orde- en veiligheidsmaatregelen op centraal niveau. Het Nationaal Crisiscentrum (NCC) speelt bij de uitvoering van deze verantwoordelijkheid een centrale rol. Het NCC verzorgt de informatievoorziening tussen de verschillende bestuurslagen en, als er buitenlandse aspecten meespelen, voor de contacten met de omringende landen. Het Departementaal Crisiscentrum (DCC) heeft dezelfde taak op departementaal niveau. Het NCC verleent tevens faciliteiten voor een goed functioneren van de beleidsteams en ambtenaren tijdens de opgeschaalde situatie. Afspraken over interdepartementale coördinatie en besluitvormingsstructuren zijn vastgelegd in het Nationaal Handboek Crisisbesluitvorming. Doelgroep van de NCC is primair de rijksoverheid.

Het NCC heeft geen specifieke taken op het gebied van ICT-veiligheid, maar zou zeker een belangrijke rol kunnen vervullen in het geval een ernstige crisis op het gebied van ICT-veiligheid gevolgen heeft voor het functioneren van andere maatschappelijk vitale sectoren. Andere organisaties die bij nationale crises op aanpalende gebieden verantwoordelijkheid hebben voor de coördinatie zijn de Nationaal Coördinator Terrorismebestrijding (NCTb), die bij terroristische dreiging de regie heeft, en de

[4] De landelijke en regionale politiediensten vallen onder verantwoordelijkheid van BZK.

Algemene Inlichtingen en Veiligheidsdienst (AIVD) die een belangrijke rol speelt bij cybercrime, waarbij de nationale veiligheid in het geding is. Het is onduidelijk of voor deze drie partijen, maar ook voor de doelgroepen die gebruikmaken van de diensten van deze organisaties, voldoende helderheid bestaat over waar de taken en verantwoordelijkheden van de ene organisatie ophouden en die van de andere organisatie beginnen. De genoemde organisaties worden hieronder besproken.

2.4.2 Nationaal Coördinator Terrorismebestrijding (NCTb)

In Nederland zijn ongeveer twintig instanties betrokken bij terrorismebestrijding. De Nationaal Coördinator Terrorismebestrijding (NCTb) is op grond van een wettelijke regeling aangesteld om de samenwerking tussen al deze instanties te verbeteren. De NCTb legt verantwoording af aan de minister van Justitie (als coördinator Terrorismebestrijding). Naast het ministerie van Justitie moet de NCTb ook verantwoording afleggen aan het ministerie van BZK. Organisatorisch en beheersmatig is de organisatie van de NCTb ondergebracht bij het ministerie van Justitie, op vergelijkbare wijze als een directoraat-generaal.

De coördinator is verantwoordelijk voor:
- Analyse van (inlichtingen-)informatie
- Beleidsontwikkeling
- Regie over te nemen beveiligingsmaatregelen bij de bestrijding van terrorisme

Doel is de slagvaardigheid van de overheid vergroten.

Tot het werkterrein van de NCTb behoren:

1. Zorgdragen voor de ontwikkeling van een helder en eenduidig beleid op het vlak van terrorismebestrijding, daaronder begrepen strategische en internationale beleidsontwikkeling en communicatiestrategie;
2. Regisseren van de samenwerking van de verschillende partijen op het specifieke terrein van terrorismebestrijding via structurele (procesgerichte) en incidentele (actiegerichte) regie en het – mede daardoor – realiseren van een hoge samenwerkingsgraad tussen die partijen;
3. Bijeenbrengen, combineren en veredelen van informatie van inlichtingenverschaffende diensten en bestuurlijke en wetenschappelijke bronnen ten behoeve van integrale analyses en dreigingsbeelden inzake terrorisme;
4. Zorgdragen voor de beveiliging van de burgerluchtvaart tegen met name terrorisme;
5. Toezicht op de inrichting van de keten van de beveiliging van de burgerluchtvaart en het toezicht op de kwaliteit van de beveiliging van de burgerluchtvaart;
6. Onderhouden, uitvoeren en vernieuwen van het nationaal stelsel van bewaken en beveiligen;
7. Regisseren van de voorlichting en woordvoering over terrorismebestrijding.

Ten aanzien van ICT-veiligheid komt de NCTb in beeld als er een terroristische dreiging is gericht tegen de ICT infrastructuur. De omgeving waarin de NCTb opereert, is bestuurlijk en politiek complex. Politieke afstemming vindt plaats in de Raad voor de Nationale Veiligheid (RNV). De RNV staat onder leiding van de minister-president. In de Raad overleggen de meest betrokken bewindspersonen op het terrein van terrorismebestrijding en inlichtingen- en veiligheidsdiensten met elkaar. Het

Gezamenlijk Comité Terrorismebestrijding (GCT) bereidt het overleg voor. In de GCT zijn de bij terrorismebestrijding betrokken ministeries en overheidsdiensten vertegenwoordigd.

2.4.3 Algemene Inlichtingen en Veiligheidsdienst (AIVD)

De AIVD houdt zich bezig met ICT-dreigingen die een gevaar vormen voor de democratische rechtsorde, de veiligheid of andere gewichtige belangen van de staat. Daarnaast bevordert de AIVD de beveiliging van gegevens waarvan geheimhouding door de nationale veiligheid wordt geboden en van die onderdelen van de overheid en het bedrijfsleven die van vitaal belang zijn voor de instandhouding van het maatschappelijke leven. De rol van de AIVD inzake bijzondere informatie is die van beleidsbepaler en deskundige. De minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de AIVD. Hij legt verantwoording af aan de Tweede Kamer. De Kamer heeft voor de controle op de inlichtingen- en veiligheidsdiensten een aparte commissie ingesteld, die in alle vertrouwelijkheid door de minister wordt geïnformeerd.

De AIVD heeft een wettelijke taak op grond van de Wet op inlichtingen- en veiligheidsdiensten. De AIVD onderneemt de volgende activiteiten op het gebied van ICT veiligheid:

1. AIVD bevordert de beveiliging van staatsgeheime informatie en ontwikkelt mede het beleid hieromtrent, waaronder het ICT-beveiligingsregime. In dit kader werd bijvoorbeeld het VIR-bi[5] geschreven en worden verbindingsbeveiligingsvoorschriften beheerd.
2. AIVD voert Tempest-metingen uit en geeft adviezen over de elektromagnetische uitstralingen van apparatuur.
3. AIVD evalueert apparatuur en software die gebruikt wordt voor het verwerken van staatsgeheime informatie.
4. AIVD produceert en levert sleutels die gebruikt worden in cryptoapparatuur.
5. AIVD levert bijdragen in (inter)nationale werkgroepen die verantwoordelijk zijn voor respectievelijk voorstellen doen voor de totstandkoming van informatiebeveiligingsbeleid (onder meer in Nato en EU-verband)
6. AIVD is *overseeer* van het Nederlandse Common-Criteria certificatieschema. AIVD vertegenwoordigt Nederland in de management board, executive board en onderliggende Common Criteria werkgroepen.
7. De AIVD voert als Appropriately Qualified Agency (AQUA) tweede land evaluaties uit ten behoeve van de Raad van de Europese Unie.

De AIVD werkt op het vlak van ICT-beveiliging samen met o.a.:

- Buitenlandse zusterdiensten
- Andere departementen, bijvoorbeeld via IB-overleg, WBI
- CBIB (vervanger van de contactkring van BVAs)
- NATO en Defensie
- Ministerie van BZK (POI-rijk, IIOS, Govcert)
- Europese Commissie via CSPAG

[5] Voorschrift informatiebeveiliging rijksdienst - bijzondere informatie (Virbi) geeft regels voor beveiliging van bijzondere informatie bij de rijksdienst. Deze regels strekken ertoe het aantal personen dat met bijzondere informatie in aanraking komt zo beperkt mogelijk te houden en zo spoedig mogelijk tot actie over te gaan bij kennisname door niet-gerechtigden.

- Raad van de Europese Unie: Council Security Committee Infosec, Accreditation Panels, Aqua Reference Group
- AQUA 2e land evaluaties tbv Raad vd EU
- Raadssecretariaat Infosec Office

De AIVD ziet als onbenutte kans intensievere interdepartementale samenwerking. Als algemene verbeterpunten in het ICT veiligheidsbeleid van de overheid wordt genoemd het verbeteren van de samenhang en coördinatie, en de synchronisatie met het EU en NATO beleid.

2.4.4 Agentschap Telecom (AT)

Het Agentschap Telecom (AT) valt rechtstreeks onder het ministerie van Economische Zaken en legt aan de minister van Economische Zaken verantwoording af. Dat is geregeld in het Besluit Aanwijzing toezichthouders Telecommunicatiewet.[6] Aandachtsgebieden van AT zijn continuïteit, integriteit en beschikbaarheid van elektronische netwerken en diensten. Hieronder vallen activiteiten als crisismanagement in buitengewone omstandigheden en frequentie-verwerving en -uitgifte, monitoring en toezicht om de continuïteit te waarborgen van draadloze communicatiediensten, zoals nooddiensten, C2000, alarmeringsystemen, radionavigatie. Daarnaast houdt het AT toezicht op de Grondroerdersregeling[7] en toezicht op het aanwezig zijn van tapvoorzieningen bij service providers in het geval politie en justitie daarvan gebruik willen maken in het kader van terrorisme- en criminaliteitsbestrijding.

Doel van de activiteiten van AT is het voorkomen van ontwrichting van de samenleving, het leveren van een bijdrage aan (het gevoel van) veiligheid en streven naar continuïteit in netwerken en voorzieningen, waardoor economische groei bevorderd kan worden. De activiteiten van AT richten zich dus zowel op het voorkomen en bestrijden van maatschappij ontwrichtende gebeurtenissen als op het vlak van niet-maatschappij ontwrichtende gebeurtenissen. De doelgroep van het AT bevindt zich op het snijvlak van vitale sectoren en bedrijven en specifiek de ICT-sector.

AT werkt samen met onder andere de volgende organisaties met een veiligheidsrol: Nationaal Coördinatie Centrum (NCC), DGET, KLPD, politieregio's, Landelijk Operationeel Coördinatie Centrum, Ministerie van Defensie, marechaussee, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Ministerie van Buitenlandse Zaken, Directoraat Generaal Transport en Logistiek, Kustwacht, Luchtverkeersleiding Nederland, Eurocontrol, aanbieders van (openbare) netwerken en diensten, en alle (groot) zakelijke telecommunicatiegebruikers.

AT merkt op dat het huidige ICT-veiligheidsbeleid te veel versnipperd is over verschillende ministeries. Belangrijk is helder te krijgen welk ministerie welke rol heeft. AT pleit ervoor alle activiteiten op het gebied van ICT-veiligheid zoveel mogelijk bij één departement onder te brengen. Daarnaast merkt AT op dat de verschillende interpretaties en belangen rond veiligheid onduidelijkheid en zelfs tegenstrijdigheid kunnen opleveren. Daarom zal EZ (door AT gewenst coördinator van het ICT-veiligheidsbeleid) tevens moeten streven naar het inzichtelijk maken van deze dilemma's en belangen en invalshoeken rondom veiligheid.

---

[6] Staatscourant 1998, 230.

[7] De grondroerdersregeling is wetgeving met als doel het aantal graafincidenten (met gepaard gaande storingen) te verminderen.

*2.4.5 Bescherming Vitale Infrastructuur (BVI) **[D2]*** [8]

In april 2002 is het project Bescherming Vitale Infrastructuur (BVI) gestart. BZK voert de rijksbrede interdepartementale coördinatie, monitoring en toetsing over het dossier vanuit haar coördinerende verantwoordelijkheid voor veiligheid, crisisbeheersing en bescherming vitale infrastructuur. Binnen BVI wordt nauw samengewerkt met alle departementen, het bedrijfsleven en de medeoverheden.
BVI omvat:

1. De ontwikkeling van een samenhangend pakket maatregelen ter bescherming vitale infrastructuur, waaronder ICT;
2. De verankering van maatregelen binnen bedrijfsvoering overheid en bedrijfsleven.

In Annex I wordt uitgebreid ingegaan op het beleidsdossier Bescherming Vitale Infrastructuur (BVI). In deze alinea worden hoofdzakelijk de resultaten van de beantwoorde vragenlijsten beknopt weergegeven.

Een van de doelen van BVI was dat departementen een goede kwetsbaarheidsanalyse van de vitale sectoren zouden maken om op grond daarvan maatregelen te nemen. Doel hiervan is discontinuïteit en daarmee maatschappelijke ontwrichting tegengaan. ICT/Telecom is een van de twaalf vitale sectoren die onder BVI vallen en waarmee een directe link ligt met ICT-veiligheid.

2.4.6 BVI (VISTIC)

Bovengenoemde kwetsbaarheidsanalyse en de implementatie van de daaruit voortvloeiende maatregelen voor de ICT/Telecom–sector zijn ondergebracht bij het ministerie van EZ, onder het project VISTIC. Het in 2003 gestarte project analyseert welke mogelijke zaken de continuïteit van de ICT/Telecom-sector bedreigen. Er wordt expliciet bekeken wat de afhankelijkheid van andere sectoren is, waarin ook terrorisme als mogelijke bedreiging wordt meegenomen. Waar het Nationaal Continuïteitsoverleg Telecom (NCO-T) zich (tot voor kort) hoofdzakelijk op telefonie richtte, neemt VISTIC ook internet mee in zijn analyse. De uit VISTIC voortvloeiende maatregelen voor de ICT/Telecom-sector zijn (voor een deel) belegd in activiteiten als de wettelijke maatregelen in geval van buitengewone omstandigheden (H14 Tw), het overlegorgaan NCO-T, de activiteiten van Agentschap Telecom, de activiteiten van Digibewust (waaronder de oprichting van een Nationaal Platform Continuïteit Vitale ICT – ofwel Platform Vitaal), GOVCERT, de Waarschuwingsdienst en Surf op Safe.

Aangezien het structurele overleg ten aanzien van bescherming van de vitale infrastructuur tussen de overheid en het bedrijfsleven vooral sectoraal (verticaal) is gestructureerd (vergelijk NCO-T voor de ICT/Telecom-sector), heeft BZK (BVI) in overleg met VNO-NCW besloten tot de oprichting van een Strategisch Overleg Vitale Infrastructuur (SOVI).

[8] De tussen haakjes geplaatste dikgedrukte letter- en cijfercombinatie refereren naar de tabel in Annex I. Dit geldt ook voor de hierna volgende identieke vermeldingen.

2.4.7 Strategisch Overleg Vitale Infrastructuur (SOVI)

SOVI is een publiek-privaat platform, bij ministeriële regeling ingesteld in 2006, waarin zowel de overheid als het bedrijfsleven vanuit verschillende sectoren zijn vertegenwoordigd (horizontaal). Op de agenda van het SOVI staan overkoepelende, strategische onderwerpen die alle partijen aangaan, zoals de in september 2005 aan de Tweede Kamer gemelde bovensectorale maatregelen. Voorts zullen onderwerpen aan de orde komen als de bundeling van veiligheidskennis, de financiering van maatregelen, het structureel inbedden van veiligheidsmaatregelen, de noodzaak tot oefenen, en de informatievoorziening. Deelnemers aan het overleg komen uit de top van het bedrijfsleven en de overheid en staan onder leiding van een onafhankelijke voorzitter. Bescherming van de vitale infrastructuur is daarom een zaak van overheid en bedrijfsleven gezamenlijk. Het overleg komt ongeveer twee keer per jaar bijeen.

2.4.8 Het Nationaal Noodnet en het Nationaal Continuïteitsoverleg Telecom (NCO-T)

[B1] Het Nationaal Noodnet vindt zijn wettelijke basis in de Tw (H14). Van oudsher rust op KPN een wettelijke verplichting om het (gesloten) Nationale Noodnet in stand te houden, zodat telecommunicatiediensten in buitengewone – en crisisomstandigheden beschikbaar blijven voor partijen die een functie hebben die omstandigheden te managen (o.a.bestuurders en hulpdiensten). **[C2]** Daarnaast heeft de minister van EZ in buitengewone omstandigheden een bevoegdheid (H14 Tw) om alle aanbieders van openbare elektronische communicatienetwerken en diensten aanwijzingen te geven met betrekking tot de exploitatie en het gebruik van hun netwerken. In het publiek-private samenwerkingsverband NACOTEL werd in 2001 een convenant gesloten tussen een aantal aanbieders en het ministerie van EZ over hoe te voldoen aan de verplichtingen van H14 Tw en om te bevorderen dat de beschikbaarheid van communicatiediensten ook in gewone omstandigheden zo goed mogelijk is geborgd.

[E2] Het Nationaal Continuïteitsoverleg Telecom (NCO-T) is een vervolg op NACOTEL, maar dan in een meer geformaliseerde vorm. Het NCO-T is sinds maart 2006 ingesteld bij ministeriële regeling, wat inhoudt dat de in de regeling genoemde aanbieders verplicht zijn deel te nemen aan het overleg. Huidige deelnemers aan het overleg zijn @Home (Essent), BT, Enertel, KPN, MCI, Orange, T-Mobile, Telfort, Tiscali, UPC, Chello (UPC), Tele2-Versatel, Vodafone en Wanadoo. NCO-T heeft tot doel nader vorm te geven aan de hierboven beschreven verplichtingen. Daarnaast is het NCO-T bedoeld als platform om kennis te delen op het gebied van continuïteitsplanning van de ICT-infrastructuur: hoe te zorgen dat communicatiediensten zo min mogelijk uitvallen en het professionaliseren van de crisisorganisatie van deelnemende partijen mocht dit onverhoopt toch gebeuren. Het NCO-T houdt zich dus zowel met maatschappij-ontwrichtende gebeurtenissen als niet-maatschappij-ontwrichtende gebeurtenissen bezig.

2.4.9 Nationale veiligheid (Digitale verlamming)

Het doel van het project Nationale Veiligheid is het borgen van de nationale veiligheid, en het voorkomen van maatschappelijke ontwrichting. Om dit te bereiken wordt met diverse departementen samengewerkt. Daarnaast werkt het project Nationale Veiligheid aan de ontwikkeling van een rijksbrede strategie voor nationale veiligheid.

Het project Nationale Veiligheid heeft de opdracht om knelpunten en blinde vlekken in het huidige pro-actieve beleid t.a.v. een negental dreigingen in kaart te brengen, waaronder digitale verlamming. Hierover is gerapporteerd in een interdepartementale zelfevaluatie 'Digitale verlamming'. Digitale verlamming omvat gebeurtenissen (met een langdurig karakter) in alle vitale sectoren die kunnen leiden tot maatschappelijke ontwrichting. Het verwerken van de onderzoeksresultaten van het rapport 'Digitale verlamming' is onderdeel van de ontwikkeling van een rijksbrede strategie. Bij dit onderzoek zijn EZ, Justitie en BZK betrokken. De Stuurgroep (DG-niveau van betrokken ministeries) moet nog bepalen hoe de resultaten opgepakt zullen worden. De grote lijnen in de resultaten van het rapport zijn dat de ministeries onderling een betere rolverdeling zouden moeten afspreken en beter met elkaar zouden moeten samenwerken.

Als uitgangspunt voor de inrichting van een rijksbrede strategie voor nationale veiligheid is gekozen voor de capaciteitenbenadering. Deze benadering komt oorspronkelijk uit de militaire wereld, maar wordt steeds vaker toegepast in het civiele domein. Doel van deze methodiek is om in kaart te brengen wat de overheid moet kunnen om de nationale veiligheid te borgen (taak) en wat de overheid nodig heeft (o.a. middelen, mensen, methoden) om uitvoering te geven aan de taken (capaciteiten).

2.5 Niet-maatschappij ontwrichtende gebeurtenissen

Net als bij de maatschappij ontwrichtende gebeurtenissen heeft zowel een aantal staande organisaties als vele (tijdelijke) programma's, projecten, instanties in oprichting en pilots activiteiten geformuleerd rondom het voorkomen en bestrijden van niet-maatschappij ontwrichtende gebeurtenissen. Allereerst zullen de activiteiten van de organisaties worden besproken en vervolgens het grote aantal overige initiatieven.

2.5.1 GBO.Overheid

Sinds 1 januari 2006 is de Gemeenschappelijke Beheer Organisatie (GBO.Overheid) verantwoordelijk voor beheer en doorontwikkeling van een aantal overheidsbrede ICT-voorzieningen. Verder worden gemeenschappelijke standaarden ontwikkeld om informatie-uitwisseling tussen overheden, burgers en bedrijven te vergemakkelijken. GBO.Overheid is een serviceorganisatie in het publieke domein en levert onder meer diensten op het gebied van authenticatie (DigiD/PKIoverheid), berichtenverkeer (Overheidstransactiepoort), ICT-veiligheid (GOVCERT en Waarschuwingsdienst) en open standaarden (Overheids Open Standaarden).

GBO.Overheid past binnen het streven van de overheid de dienstverlening aan burgers en bedrijven te verbeteren. Continuïteit, betrouwbaarheid en integriteit van ICT-voorzieningen zijn daarvoor eerste vereisten. De sturing is in handen van een Programmaraad waarin gebruikers vertegenwoordigd zijn. Organisatorisch valt GBO.Overheid onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), maar GBO.Overheid staat ten dienste van alle ministeries.

2.5.2 GOVCERT

Een van de acties die mede zijn voortgekomen uit de KWINT-nota en het programma KWINT is de start van een Computer Emergency and Response Team (CERT) voor de overheid in 2002: GOVCERT. GOVCERT valt onder verantwoordelijkheid van het

ministerie van BZK. Voorheen werden de activiteiten van GOVCERT gecoördineerd door uitvoeringsorganisatie stichting ICTU[9]. Sinds 1 januari 2006 is GOVCERT een zelfstandige organisatie en maakt onderdeel uit van GBO.Overheid.

GOVCERT heeft als doel het verhogen van het niveau van informatiebeveiliging binnen de overheid, en, via de aan GOVCERT gelieerde Waarschuwingsdienst, het verhogen van ICT-veiligheid bij thuisgebruikers/kleinbedrijf. GOVCERT verwacht kennis en bewustzijn bij gebruikers, beheerders en management te vergroten en incidenten te voorkomen. Belangrijkste doelgroep van GOVCERT is de overheid, maar ook partijen daarbuiten kunnen gebruikmaken van de kennis en expertise van GOVCERT.

GOVCERT onderneemt de volgende activiteiten:

- Kennisdeling/verspreiding binnen overheid
- Incidentafhandeling
- Bewustzijn creëren (overheid, burger/kleinbedrijf)
- Adviseren

GOVCERT werkt samen met:

- Ketenpartijen, zoals KLPD, AIVD, OM, OPTA, etc.
- Private partijen zoals ISP's, banken, software/hardware leveranciers, etc.
- Incident response teams en abuse teams in Nederland
- CERTs, high tech crime units en vendors internationaal
- Awareness programma's zoals ECP.nl, Digibewust, etc.

Deze samenwerking richt zich onder meer op kennisuitwisseling, incident response en bewustwording. De samenwerking wordt vormgegeven door (deelname aan en organiseren van) internationale bijeenkomsten en conferenties, structurele periodiek overleg, soms door GOVCERT.NL georganiseerd (o-IRT-o), bilaterale contacten, en incident gedreven samenwerking.

Als algemene verbeterpunten in het ICT veiligheidsbeleid wordt het vergroten van (operationele) samenwerking tussen overheidspartijen genoemd, en informatiebeveiliging van de diverse initiatieven betreffende elektronische dienstverlening van de overheid (elektronische overheid).

2.5.3 Waarschuwingsdienst

[G1] De Waarschuwingsdienst is een initiatief dat in 2003 is gestart en valt onder verantwoordelijkheid van GBO.Overheid. Organisatorisch is de dienst daar ondergebracht omdat de Waarschuwingsdienst grotendeels gebruikmaakt van de faciliteiten en kennis en expertise van GOVCERT. Doel van de Waarschuwingsdienst is computergebruikers en kleinbedrijf te waarschuwen tegen computervirussen en lekken in software. De dienst publiceert en verspreidt de informatie via hun website, via een mailinglist en via sms.

[9] Stichting ICTU is opgericht door het ministerie van BZK en de Vereniging Nederlandse Gemeenten (VNG).

2.5.4 OPTA

De OPTA is in 1997 ingesteld bij de Wet Onafhankelijke post- en telecommunicatieautoriteit.[10] OPTA rapporteert jaarlijks aan de minister van EZ middels een jaarverslag dat ook publiekelijk beschikbaar wordt gesteld. Daarnaast kan de minister beleidsregels stellen met betrekking tot de door het college uit te oefenen taken. Het college wordt gefinancierd door het ministerie van EZ en door partijen die onder toezicht van OPTA staan.

OPTA onderneemt de volgende activiteiten op het gebied van ICT veiligheid:

1. Spambestrijding: Sinds de gewijzigde Telecommunicatiewet (Tw) van mei 2004 ziet OPTA toe op de handhaving van overtredingen van het zogenaamde spamverbod zoals gesteld in art. 11.7 van deze Tw. OPTA inventariseert klachten en geeft op basis daarvan waarschuwingen of boetes aan overtreders. Deze hebben ongevraagde elektronische berichten, d.w.z., via e-mail, sms, automatische oproepen zonder menselijke tussenkomst of per fax, gezonden aan abonnees die geen rechtspersoon zijn. Doelstelling van OPTA is het omlaag brengen van het aantal verzonden spamberichten in en vanuit Nederland door het opleggen van boetes en het geven van waarschuwingen aan spammers, waardoor deze worden gedwongen hun activiteiten te stoppen of te verplaatsen.
2. Autodialers: OPTA verricht onderzoek naar mogelijke overtredingen van artikel 4.1 van het Besluit universele dienstverlening en eindgebruikersbelangen (Bude) bij onverwacht hoge telefoonrekeningen. Deze hoge rekeningen zijn veelal het gevolg van software, die (al dan niet zelfstandig) inbelverbindingen met dure telefoonnummers (0900 nummers of buitenlandse nummers) tot stand brengt (zogenaamde autodialers). Doelstelling van OPTA is het vergroten van de internetveiligheid voor consumenten en het beschermen van consumentenbelangen bij dure telefoonnummers. Dit gebeurt in de vorm van opsporing en eventueel boeteoplegging.
3. Spyware: OPTA is voornemens zich vanaf juli 2006 te richten op de bestrijding van spyware in Nederland. De wettelijke basis hiervoor is artikel 4.1 Bude[11]. Exacte doelstelling is nog niet bekend, maar zal in lijn liggen met het ‘vergroten van de internetveiligheid’. OPTA verwacht met haar activiteiten het groeiende probleem van de verspreiding van schadelijke software buiten medeweten van de gebruiker te reduceren door samen met technische maatregelen en voorlichting, sanctionerend op te treden.

De rol van OPTA inzake bovengenoemde activiteiten is die van toezichthouder, maar ook van aanjager die zijn kennis en deskundigheid gebruikt en deelt in internationale gremia en met iedereen die daarom vraagt.

Op het gebied van spam en autodialers werkt OPTA samen met aanbieders van openbare elektronische communicatiediensten, politie, KLPD, OM, Fiod/ECD, CBP en internationale toezichthouders. Op het gebied van spyware wordt op dit moment samenwerking gezocht met GOVCERT, de KLPD, het bedrijfsleven en diverse private organisaties.

OPTA ziet als belangrijkste verbeterpunt in het ICT-veiligheidsbeleid het verkrijgen van synergie tussen organisaties. OPTA ziet dat diverse instanties bezig zijn met een

[10] Staatsblad 1997, 320. Wet Onafhankelijke post- en telecommunicatieautoriteit.
[11] Besluit universele dienstverlening en eindgebruikersbelangen.

vergelijkbaar probleem, maar niet of nauwelijks van elkaars activiteiten op de hoogte zijn. Door informatiedeling en meer samenwerking (ook internationaal) zou de opsporing volgens OPTA gerichter plaats kunnen vinden.
[A1] Wat consumentenbescherming betreft zijn in art.7.8 Tw verplichtingen gesteld aan de aanbieder van een telecommunicatienetwerk en/of -dienst met betrekking tot o.a. tarieftransparantie, maximale tariefhoogte voor informatienummers en levering of opschorting van dienstverlening. Naast de Telecommunicatiewet zijn de eindgebruikersbelangen nog verder uitgewerkt in het Besluit universele dienstverlening en eindgebruikersbelangen (ministeriële regeling) en in de Regeling universele dienstverlening en eindgebruikersbelangen (Amvb).

Recentelijk zijn aanpassingen in de Telecommunicatiewet en lagere regelingen[12] gedaan die consumentenbescherming moeten bieden bij gebruik van informatienummers (0800, 0900, 0906 en 0909). Hiertoe worden (strengere) verplichtingen aan aanbieders van telecomdiensten en carrierselectiediensten opgelegd en krijgt OPTA uitgebreidere bevoegdheden. Met deze maatregelen legt de wetgever de verantwoordelijkheid bij meerdere partijen in de keten, verwacht hij de consument beter te kunnen beschermen en malafide aanbieders van (dure) informatienummers (autodialers) beter en sneller te kunnen opsporen.

2.5.5 Korps Landelijke Politiedienst (KLPD)

Het KLPD is een agentschap, ressorterend onder DG Veiligheid van het ministerie van BZK en heeft een wettelijke basis voor zijn activiteiten. De KLPD onderneemt de volgende activiteiten op het gebied van ICT-veiligheid:

- Het realiseren van een beveiligingsarchitectuur om een goede en veilige informatie-uitwisseling mogelijk te maken, zowel binnen de KLPD en de politie als met externe partijen (MinJus, MinDef, VROM, VenW etc.).
- Er is een rubriceringsregeling opgesteld waarmee de vertrouwelijkheid van de informatie eenduidig is aan te geven. Dit is een voorwaarde om vertrouwelijke informatie op de juiste en veilige wijze uit te wisselen en vormt de basis voor de beveiligingsarchitectuur.
- Structurele samenwerking tussen de concerndienst informatievoorziening en de diverse diensten van het KLPD. Het doel is om een optimaal beveiligingsniveau te realiseren.
- Onderzoeken en toepassen van cryptografische middelen
- Korpsbreed adviseren met betrekking tot informatiebeveiliging (strategisch)
- Adviseren in relatie tot klantvragen vanuit de diensten (tactisch/operationeel)

Deze activiteiten worden uitgevoerd met als doel een betere informatie-uitwisseling binnen de KLPD en met partnerorganisaties, alsmede een betere informatiepositie voor het KLPD. Er wordt verwacht dat dit leidt tot:

- Betere informatieuitwisseling en informatiepositie
- Optimaal beveiligingsniveau
- Lagere kosten door generieke oplossingen
- Hoge kwaliteit

Als algemene verbeterpunten voor het ICT-veiligheidsbeleid wordt genoemd:

[12] Hiermee worden bedoeld de Regeling Universele Dienstverlening en Eindgebruikersbelangen en het Besluit Universele Dienstverlening en Eindgebruikersbelangen.

- het uitgangspunt zou een optimaal beveiligingsniveau moeten zijn en niet een maximaal beveiligingsniveau
- meer aandacht voor bewustwording
- periodieke aanpassingen aan de hand van trends en nieuwe mogelijkheden
- meer aandacht voor internettechnologie

Daarnaast is men binnen de KLPD bezig met het oprichten van een Team High Tech Crime. Dit is een uitvloeisel van een in 2004/2005 gehouden project dat bekend stond onder de naam NHTCC (National High Tech Crime Centre).

2.5.6 Nationaal Platform Criminaliteitsbeheersing (NPC)

Het Nationaal Platform Criminaliteitsbeheersing (NPC) is een in 1992 opgericht samenwerkingsverband tussen overheid en bedrijfsleven (PPS) gericht op het aanpakken van criminaliteit gericht tegen het bedrijfsleven. Doelgroep is hoofdzakelijk het bedrijfsleven en in mindere mate de overheid. Vertaald naar het domein ICT-veiligheid betreft dit de vitale bedrijven en sectoren. Het NPC is samengesteld uit een ongeveer gelijk aantal vertegenwoordigers van overheid en bedrijfsleven. De Minister van Justitie is voorzitter van het platform, de voorzitter van de VNO-NCW is de vice-voorzitter. Staatssecretaris Van Gennip (EZ) is voorzitter van de Raad van Advies. Alle relevante departementen zijn in het platform vertegenwoordigd, evenals de politie, het openbaar ministerie (OM) en de gemeenten. Namens het bedrijfsleven maken organisaties van werkgevers en werknemers deel uit van het platform en is een groot aantal branches vertegenwoordigd. Onder de vlag van het NPC wordt een groot aantal projecten en programma's uitgevoerd. Het is voor ons niet altijd even duidelijk geworden wie de politieke, organisatorische en financiële verantwoordelijkheid en de risico's draagt voor deze programma's en projecten. Onder de vlag van het NPC is het Nationaal Project Aanpak Cybercrime (NPAC) opgestart in het kader van Actieplan Veilig Ondernemen II (AVO II). Inmiddels geeft NICC (Nationale Infrastructuur Bescherming Cybercrime) invulling aan dit project.

2.5.7 NICC

Het programma Nationale Infrastructuur Bescherming Cybercrime (NICC) dat begin 2006 is gestart, is gericht op zowel het voorkomen (preventie) als het bestrijden van cybercrime (opsporing en vervolging). Het programma heeft het karakter van een publiek-private samenwerking (PPS) met de notie dat Staatssecretaris Van Gennip (ministerie EZ) de politieke verantwoordelijkheid voor dit programma op zich heeft genomen. De uitvoering van het programma is ondergebracht bij de uitvoeringsorganisatie ICTU (dat overigens onder BZK valt).

Het uiteindelijke doel van NICC is een nationale infrastructuur ter bestrijding van cybercrime. Het NICC initieert, ontwikkelt en experimenteert, maar heeft niet tot doel zelf de nationale infrastructuur te worden. NICC fungeert uitsluitend als ontwikkelomgeving en legt verbindingen tussen betrokken partijen. Nadruk bij de ontwikkeling van de nationale infrastructuur ligt op de publiek-private informatie-uitwisseling. De eerste lijn richt zich op de ontwikkeling van experimenten die kennis op het gebied van cybercrime moeten genereren. Een voorbeeld hiervan is het experiment 'Cybercrime en het MKB'. Doel van het experiment is te onderzoeken in welke mate het MKB door cybercrime wordt bedreigd, wat de mate van besmetting is en welke de te nemen maatregelen zijn. Kortom, het gaat om het verkrijgen van inzicht

in de aard en omvang van cybercrime en het reduceren van schade voor het MKB. Aangezien in het kader van het programma Digibewust een soortgelijk experiment ('Pilot onderzoek cybercrime') op de agenda staat, is besloten de krachten te bundelen. Het experiment zal in november 2006 van start gaan en onder de vlag van Digibewust en NICC worden uitgevoerd door ECP.nl.

De tweede lijn richt zich op de realisatie van een nationaal informatieknooppunt Cybercrime. In dit laatste traject zoekt het nog niet officieel opgerichte Nationaal Adviescentrum Vitale Infrastructuren (NAVI), dat zich hoofdzakelijk richt op informatie-uitwisseling tussen vitale sectoren, aansluiting met het NICC. NICC en NAVI zullen op korte termijn beginnen met de vormgeving van het nationale informatieknooppunt Cybercrime voor vitale sectoren. In deze samenwerking zal getracht worden om een overlappende doelstelling, namelijk één nationale infrastructuur, gezamenlijk te realiseren. Op dit project zal hieronder nader worden ingegaan.

Het NICC is zich bewust van bestaande organisaties als het Nationaal Coördinatie Centrum (NCC), die in geval van nationale crises een coördinerende rol heeft, de Nationaal Coördinator Terrorismebestrijding (NCTb), die bij terroristische dreiging de regie heeft, en de Algemene Inlichtingen en Veiligheidsdienst (AIVD) die in haar activiteiten de nadruk legt op cybercrime waarbij de nationale veiligheid in het geding is. Het NICC onderkent dat dit in het begin onduidelijkheid kan opleveren, maar zegt dit probleem te ondervangen door voor iedereen aanspreekbaar te zijn: het NICC kan vervolgens doorverwijzen naar de juiste instantie.

NICC werkt samen met BZK (politie/GOVCERT), Justitie (politie, OM, wet- en regelgeving), OPTA (spam, spyware/handhaving), KLPD (opsporing), AT (kennis en expertise), GOVCERT (kennis en expertise), AIVD (informatie-uitwisseling), bedrijfsleven (koepels, individuele bedrijven en vitale sectoren).

2.5.8 NICC – Project Informatieknooppunt

Het Project Informatieknooppunt[13] moet de kiem vormen voor de toekomstige informatie-uitwisseling in het kader van de nationale infrastructuur ter bestrijding van cybercrime. Het voornemen is om, gebaseerd op het in Engeland door het National Infrastructure Security Co-ordination Centre (NISCC) ontwikkelde informatiemodel, in september te starten met een experiment in een tweetal vitale sectoren om dit informatiemodel te beproeven. In de loop van de tijd zal het aantal deelnemende vitale sectoren worden uitgebreid. Cybercrime raakt meer partijen dan alleen de vitale sectoren. Het Informatieknooppunt beperkt zich desondanks tot deze groep, omdat het gebruikte Engelse informatiemodel bij uitstek geschikt is voor (zeer) vertrouwelijke informatie-uitwisseling binnen (en tussen) relatief kleine groepen. De werkzaamheden van het Informatieknooppunt zullen zich richten op alle cybercrime waarmee de vitale sectoren worden geconfronteerd (zowel maatschappij ontwrichtende gebeurtenissen als niet-maatschappij ontwrichtende gebeurtenissen).

Het in Engeland ontwikkelde informatiemodel houdt in dat per vitale sector een overlegorgaan wordt opgericht dat door (één of meer) overheidsdiensten wordt ondersteund bij het bepalen van de risico's die cybercrime voor die sector met zich

[13] Mac Gillavry, E.C. (2006), Concept Projectplan Informatieknooppunt, NICC-programma.

meebrengt en de maatregelen die nodig zijn om de risico's te mitigeren. De separate overlegorganen zullen steeds vanuit dezelfde kern worden gefaciliteerd, zodat een informatieknooppunt ontstaat waar kennis wordt opgebouwd. Bovendien kan dit knooppunt de verkregen informatie vanuit de ene sector (geanonimiseerd) beschikbaar maken voor een andere sector.

Uit het projectplan wordt niet duidelijk of in de realisatie van het Informatieknooppunt aansluiting wordt gezocht met BVI, in het kader waarvan al een structureel overleg per vitale sector bestaat, en/of met het Platform Vitaal dat een overeenkomstige doelstelling als het Informatieknooppunt lijkt na te streven, namelijk informatie-uitwisseling tussen vitale sectoren. Platform Vitaal zal hieronder nader worden besproken.

2.5.9 Nationaal Adviescentrum Vitale Infrastructuren (NAVI)

Het NAVI is een organisatie in oprichting met mogelijke taken op het terrein van informatie-uitwisseling, kennis en analyse, en advisering over beschermingsmaatregelen. Als eerste speerpunt is de informatie-uitwisseling met de vitale sectoren aangewezen. Hier ligt, zoals boven beschreven, een raakvlak met het programma NICC (die het accent legt op cybercrime). Er bestaat dan ook het voornemen samen te werken op dit vlak in het Project Informatieknooppunt. Naast bovengenoemde taken en rollen wordt onderzocht in hoeverre het NAVI een toegevoegde waarde kan vervullen als front-office op het gebied van security. Het NAVI is zich bewust dat er vele organisaties op dit gebied actief zijn.

BZK leidt de organisatie van het NAVI vanuit haar coördinerende verantwoordelijkheid van BZK voor veiligheid, crisisbeheersing en de vitale infrastructuur, en werkt in nauwe samenspraak met andere departementen en organisaties. De kans is groot dat wanneer het NAVI daadwerkelijk start, NAVI ook bij BZK wordt gepositioneerd.

NAVI werkt samen met de 12 vitale sectoren, met private en publiek partijen, waaronder verschillende vakdepartementen. Belangrijke stakeholders aan overheidszijde zijn: AIVD, NCTb, KLPD, GOVCERT, bureau's CCB (Conflict en Crisisbeheersing) op regionaal niveau, veiligheidsregio's i.o.

Als verbeterpunt in het ICT veiligheidsbeleid van de overheid noemt NAVI het gebrek aan mechanismen om informatie en kennis te delen en te ontwikkelen, en kennis te benutten uit het bedrijfsleven.

2.5.10 Digibewust - Nationaal Platform Continuïteit Vitale ICT (Platform Vitaal)

[D3] Als een van de maatregelen die zijn voortgekomen uit de kwetsbaarheidsanalyse (BVI-VISTIC) werd genoemd de oprichting van een overlegplatform tussen vitale sectoren en de overheid om informatie, kennis en ervaringen uit te wisselen op het gebied van ICT-veiligheid. Onder de vlag van het programma Digibewust is begin 2006 een dergelijk platform opgericht: het Nationaal Platform Continuïteit Vitale ICT, ook wel kortweg Platform Vitaal genoemd.

De initiatiefnemers voor een eerste verkennende bespreking zijn een aantal bedrijven en instellingen uit verschillende vitale sectoren in Nederland: Gasunie, TenneT, Shell, Urenco, KPN, Interpay, Havenbedrijf Rotterdam, het ministerie van Economische Zaken, de Nederlandse Vereniging van Banken, VNO-NCW en ECP.NL. De uitkomst

van deze bespreking is dat er een duidelijke behoefte bestaat bij vitale bedrijven in verschillende sectoren in Nederland om te komen tot kennisuitwisseling m.b.t. risico's, bedreigingen, maatregelen en best practices, die verband houden met de bescherming van vitale infrastructuren. Daarbij wordt nog opgemerkt dat het geen praatgroep, maar een 'doe'-groep moet zijn, waar informeel gewerkt kan worden.

In de projectbeschrijving worden de volgende doelstellingen genoemd:

1. Het ontwikkelen van een vertrouwde omgeving waar informatie kan worden uitgewisseld tussen degenen die verantwoordelijk zijn voor de bescherming van bepaalde elementen (sector, functie of technologie) van onze kritische nationale infrastructuur;
2. Het bieden van een werkbaar forum waar issues geïdentificeerd worden gerelateerd aan ongeautoriseerde penetratie of manipulatie van netwerken of systemen en hun ondersteunende software, die onze kritische nationale infrastructuur bedreigen;
3. Het identificeren en uitwerken van de mogelijkheden om bepaalde kwetsbaarheden op een veiliger wijze te exploiteren;
4. Het afschrikken van potentiële aanvallen op bepaalde elementen (sector, functie of techniek) van onze kritische nationale infrastructuur door middel van het ontwikkelen en toepassen van best practices en incident response plannen.

Het voornemen is om ongeveer 4 keer per jaar bijeen te komen. Afspraken dienen nog gemaakt te worden over welke bedrijven kunnen/mogen deelnemen, op welke niveau de deelnemende bedrijven vertegenwoordigd zullen zijn (CIO, CEO of Security officer) en hoe omgegaan zal worden met vertrouwelijke informatie.

2.5.11 Programma Digibewust

[G2] Digibewust is een publiekprivate samenwerking (geïnitieerd vanuit EZ, DGET) en is gericht op het vergroten van de bewustwording rondom veiligheid en het gebruik van elektronische communicatiemiddelen. In het programma Digibewust zijn bestaande activiteiten rond bewustwording over veilig Internet gebundeld vanuit de gedachte dat deze activiteiten in samenhang beter tot hun recht komen. Het programma KWINT is beëindigd en Digibewust is de opvolger. De campagne Surf op Safe is ondergebracht in het programma Digibewust. Het programma voldoet aan de wens van de Tweede Kamer om activiteiten in het kader van het veilige gebruik van internet bij burgers en bedrijven te intensiveren.

Digibewust kent 4 pijlers:

1. *Verstevigen publiek-private samenwerking*: goede samenwerking tussen overheid, bedrijfsleven en instellingen is de kern van Digibewust.
2. *Bewustwording en voorlichting*: de publiekscampagne die onderdeel uitmaakt van de pijler zal zich de komende jaren wisselend gaan richten op jongeren, senioren en MKB. In 2006 richt het programma zich vooral op jongeren, hun docenten en ouders. De website van Digibewust (www.digibewust.nl) is voor het programma een centraal communicatiemiddel.
3. *Kwaliteitsbeleid van het MKB*: met name in het midden- en kleinbedrijf wordt het belang van informatiebeveiliging vaak onvoldoende erkend. Het doel van deze pijler is dat het MKB veiligheid van elektronische communicatie als vanzelfsprekend onderdeel behandelt van een goede bedrijfsvoering.

4. *Betere benutting van kennis*: het gaat hier om het beter ontsluiten en uitwisselen van de aanwezige kennis over risico's en veiligheid van elektronische communicatie in begrijpelijke vorm richting de verschillende gebruikers. Daarvoor bestaan platforms als Nationaal Platform Continuïteit Vitale ICT, Platform afstemming ENISA en Platform kennisuitwisseling R&D gebruikers.

Het programma is in januari 2006 gestart en wordt uitgevoerd door ECP.NL. ECP.NL wordt aangestuurd door de stuurgroep Digibewust onder voorzitterschap van EZ. ECP.NL zorgt voor aansluiting van partijen uit de markt. EZ/DGET werkt samen met de ministeries van Justitie, BZK, OCW en daarnaast met GOVCERT, Kennisnet, OPTA en het College Bescherming van Persoongegevens.

DGET heeft verschillende rollen in dit programma, waaronder:
- Borgen beleidswensen
- Aanstuurder/aanjager
- Zorgen aansluiting (inter)departementale diensten
- Liaison naar EU (Safer Internet Plus)

Als verbeterpunten in het ICT veiligheidsbeleid worden genoemd:
- Internationale samenwerking
- Betere kennisontwikkeling (informatiedeling en structurele analyse)
- Eenduidige communicatie naar eindgebruiker

2.5.12 Surf op Safe

[G3] Surf op Safe is in 2001 als publiekprivate samenwerking (ministeries EZ, Justitie, OCW, brancheorganisaties, software aanbieders) gestart als campagne over veilig internetten gericht op consumenten en MKB. Het doel was bewustwording te kweken over de risico's en gevaren van het gebruik op internet. Surf op Safe verschafte informatie via hun website, brochures en flyers. Surf op Safe is nu onderdeel van het programma Digibewust. Tot dit jaar fungeerde Surf op Safe als Awareness Node onder het Europese *Safer Internet Action Plan* en *Safer Internet Plus*. Digibewust neemt die rol over.

2.5.13 ECP.nl

ECP.nl is in 1998 opgericht door het ministerie van Economische Zaken en VNO-NCW. ECP.nl noemt zichzelf het platform voor eNederland. ECP.nl telt 150 deelnemende bedrijven, instellingen, overheden en intermediairen. ECP.nl is een platform waarin verschillende publiek-private samenwerkingsprogramma's en -projecten van de overheid zijn ondergebracht, zoals o.a. de campagne Digibewust, het Nationaal Authenticatieplatform en het experiment Cybercrime (van NICC/ Digibewust). Het platform voert programma's en projecten uit (vaak in opdracht van een ministerie) en brengt partijen samen om kennis en informatie te delen in seminars en werkgroepen.

2.5.14 ECP.nl – Nationaal Authenticatie Platform (NAP)

Het NAP bestaat uit de belangrijkste spelers van nationale authenticatie initiatieven (zoals PKI-overheid, DigiD, e-banking initiatieven), zowel van de kant van de overheid als de kant van het bedrijfsleven en kennisinstellingen. Het doel van het platform is

kennis uitwisselen over nationale en internationale ontwikkelingen rond e-authenticatie en identity management. De activiteiten omvatten het organiseren van seminars, ronde tafels en vergaderingen en verspreiden van brochures. ECP.nl voert het project Nationaal Authenticatie Platform uit in opdracht van EZ.

2.5.15 PKIoverheid, DigiD en eNIK

Een PKI (Public Key Infrastructure) is een samenstel van architectuur, techniek, organisatie, procedures en regels, gebaseerd op asymmetrische encryptie. Het doel is het mogelijk maken van betrouwbare elektronische communicatie en betrouwbare elektronische dienstverlening (elektronische identificatie, elektronische handtekening en versleuteling). Bij de PKI voor de overheid is het oogmerk specifiek het mogelijk maken van betrouwbare communicatie binnen en met de Nederlandse overheid. PKI verkeert sinds enige jaren in de beheerfase. De organisatie maakt deel uit van de beheerorganisatie GBO.Overheid.

DigiD (spreek uit: Diegiedee) staat voor digitale identiteit. Het is een gemeenschappelijk systeem van en voor de overheid. Overheidsinstellingen kunnen met DigiD de identiteit verifiëren van burgers en bedrijven die gebruikmaken van hun elektronische diensten (bijvoorbeeld Belastingdienst). DigiD kent een drietal betrouwbaarheidsniveaus: basis, midden en hoog. DigiD is gestart in 2003/2004. Het basisniveau (gebruikersnaam/wachtwoord) is operationeel en beschikbaar. De doorontwikkeling van DigiD is voorzien tot en met 2007.

eNIK staat voor elektronische Nederlandse identiteitskaart (NIK). De toevoeging van de elektronische functionaliteit op de NIK maakt het mogelijk dat burgers een elektronische handtekening kunnen zetten, zich elektronisch kunnen identificeren (de eNIK geeft binnen DigiD invulling aan het hoogste betrouwbaarheidsniveau) en vertrouwelijk elektronisch kunnen communiceren (versleuteling). De eNIK maakt gebruik van PKIoverheid-standaarden en –techniek. De ontwikkeling van eNIK loopt vanaf 2005 tot de introductie in 2007/2008.

Doelstellingen van PKI, DigiD en eNIK zijn: 1. betrouwbare en vertrouwelijke elektronische communicatie met de overheid, 2. beperken van de “digitale sleutelbossen”. Alle drie de activiteiten vallen onder verantwoordelijkheid van BZK.

2.5.16 Wetgeving

In deze alinea wordt de wetgeving rondom de bescherming persoonlijke levenssfeer besproken en de wetgeving elektronische handtekening. Hoofdstuk 11 van de Telecommunicatiewet (Tw)[14] betreft de bescherming van persoonsgegevens en de persoonlijke levenssfeer. Het gaat hierbij enerzijds om de bescherming van de eindgebruiker tegen ongewenst gebruik van telecommunicatievoorzieningen en diensten, zoals telemarketing activiteiten, ongewenste e-mail (beide vallen onder spam), en anderzijds om bescherming van persoonsgegevens die aanbieders van communicatiediensten beheren. Dit laatste is overigens in algemene zin ook in de Wet bescherming persoonsgegevens (Wbp)[15] geregeld. OPTA houdt als toezichthouder van

[14] Staatsblad (2004), nr. 308, Beschikking van de Minister van Justitie van 30 juni 2004, houdende plaatsing in het Staatsblad van de tekst van de Telecommunicatiewet, zoals deze luidt met ingang van 19 mei 2004.
[15] Staatsblad (2000), nr. 302, Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens).

de telecommunicatiemarkt toezicht op de naleving van de Tw en het College Bescherming Persoonsgegevens (CBP) doet dat voor de Wbp.

Doel van EZ is allereerst adequate en technologie onafhankelijke wet- en regelgeving binnen de kaders van de Europese richtlijnen. Daarnaast het bewaken en bevorderen van de kwaliteit van de wetgeving.

Op dit gebied werkt EZ samen met Justitie, BZK, de toezichthouders OPTA en CBP en de markt, brancheorganisaties (o.a. Vecai) en VNO-NCW.

De Europese richtlijn op het gebied van de elektronische handtekening uit 1999 is in 2003 geïmplementeerd in Nederlandse wetgeving.[16] Doel van de wet is het vertrouwen in de informatiemaatschappij te vergroten. De wetgeving regelt de juridische gelijkstelling van de elektronische handtekening aan de papieren handtekening. Wat betreft de activiteiten rondom de wetgeving elektronische handtekening is EZ de beleidsbepaler en heeft op onderdelen ook een beheersmatige functie. Indien een partij (een zogeheten Trusted Third Party) namelijk een gekwalificeerde elektronische handtekening wil uitgeven, dan kan deze partij ervoor kiezen zich te laten certificeren tegen de eisen die daaraan in de Tw zijn gesteld. EZ is verantwoordelijk voor het aanwijzen van de instanties die een dergelijke certificering mogen doen. Certificerende instanties die deze rol willen vervullen, kunnen hiertoe bij EZ een aanvraag indienen. Daarnaast houdt OPTA toezicht op de TTPs (Trusted Third Parties) die de gekwalificeerde certificaten (kwalitatief hoogwaardige handtekeningen) uitgeven.[17]

[16] Staatsblad 2003, 199, Wet elektronische handtekening.

[17] Terzijde, de eerder beschreven PKIoverheid heeft aansluiting gezocht bij de eisen zoals deze in de Tw zijn gesteld aan deze kwalitatief hoogwaardige handtekeningen.

3 Bevindingen uit resultaten quickscan

3.1 Inleiding

In dit hoofdstuk wordt een eerste beeld geschetst van de bevindingen die volgen uit de resultaten van de quickscan. Een aantal opmerkingen vooraf: belangrijkste bronnen van informatie waren de ingevulde vragenlijsten van de verantwoordelijke dossierhouders bij de ministeries EZ en BZK (helaas zijn geen vragenlijsten van Justitie ontvangen). Deze ingevulde vragenlijsten geven een eerste beeld, maar kunnen niet als compleet worden gezien. Enerzijds zijn de vragenlijsten op zeer uiteenlopende wijze (van zeer summier tot zeer uitgebreid) door de betrokkenen ingevuld, waardoor vergelijken lastig bleek. Daarnaast heeft geen nadere verificatie plaatsgevonden van de ingevulde vragenlijsten door middel van bijvoorbeeld aanvullende interviews met betrokken dossierhouders. Toch is een redelijk betrouwbare indicatie te geven van bestaande initiatieven op het gebied van ICT-veiligheid in Nederland, waarop een aantal bevindingen en gevolgtrekkingen zijn te maken. Reden is dat ook aanvullende documentatie omtrent de initiatieven is geanalyseerd (zie referenties). In de volgende paragrafen wordt ingegaan op de vraag of er sprake is van overlap of witte vlekken in het bestaande beleid (paragraaf 3.2), hoe de rollen, taken en verantwoordelijkheden zijn verdeeld (paragraaf 3.3) en wat de door de dossierhouders zelf genoemde verbeterpunten zijn (paragraaf 3.4).

3.2 Overlap of witte vlekken

In Nederland lopen veel activiteiten op het gebied van ICT-veiligheid. Zowel de initiatieven op het gebied van maatschappij ontwrichtende gebeurtenissen als van niet-maatschappij ontwrichtende gebeurtenissen zijn goed vertegenwoordigd. Daarnaast blijkt uit de actietabel van Annex II dat de activiteiten die zijn geagendeerd in de Rijksbrede ICT-agenda voor het grootste gedeelte zijn opgestart of al enige tijd lopen. In die zin lijken er geen ‘witte vlekken’ te bestaan in het bestaande beleid. Echter, wanneer gerichter naar de doelstellingen, taken en activiteiten van de bestaande initiatieven wordt gekeken, ontstaat het beeld dat aan de ene kant aanzienlijke overlap bestaat in doelstellingen en activiteiten van een aantal initiatieven, maar aan de andere kant een ‘witte vlek’ op een hoger niveau bestaat in het nemen van concrete (veiligheids)maatregelen om het hogere doel, namelijk een veiliger ICT-Nederland te bereiken. Hieronder zal op een aantal initiatieven worden ingezoomd die deze overlap illustreren.

3.2.1 Overlap NAVI, NICC, Platform Vitaal

Op verschillende aspecten kan overlap worden geconstateerd tussen het NAVI, het project Informatieknooppunt (NICC) en Platform Vitaal. Allereerst benoemen alle bovenstaande initiatieven als belangrijkste doelstelling: kennisuitwisseling tussen vitale bedrijven uit verschillende sectoren en de overheid. Ook de invulling ervan lijkt overeen te komen. Zowel het project Informatieknooppunt als Platform Vitaal nemen het Engelse Informatiemodel als uitgangspunt. Het NAVI richt zich in eerste instantie op kennisuitwisseling tussen vitale sectoren, maar heeft inmiddels aansluiting gezocht bij het NICC in het project Informatieknooppunt, die daarnaast nadruk legt op de bestrijding van cybercrime. Gezamenlijk zal nu gewerkt worden aan de totstandkoming

van een informatieknooppunt cybercrime voor vitale sectoren. Ook de doelgroep van alle initiatieven is gelijk, namelijk de vitale bedrijven/sectoren. Bovendien zijn de initiatieven alle drie publiekprivate samenwerkingsverbanden (PPS). Ook de niveaus (strategisch, tactisch, operationeel) waarop de initiatieven zelf aangeven hun activiteiten vorm wensen te geven, komen grotendeels overeen met hier en daar kleine verschillen.

NICC stelt zich het meest strategisch op en wil hoofdzakelijk faciliterend zijn (ontwikkelomgeving, experimenten faciliteren, kennis doorgeven). Het NAVI beoogt een structureel centraal aanspreekpunt/adviescentrum te worden op strategisch niveau. De inzet is meer dan een tijdelijk programma of project. Platform Vitaal heeft aangegeven graag een doe-groep te willen zijn en geen praat-groep, maar in de verdere uitwerking (slechts 4x per jaar bij elkaar komen en twijfel tussen CIO/CEO en Security Officer als deelnemer) lijkt nog onduidelijkheid te bestaan over het niveau waarop het platform actief wil zijn.

Het NICC en NAVI hebben, zoals aangegeven, inmiddels aansluiting bij elkaar gezocht. Uit de ingevulde vragenlijsten blijkt echter niet dat NAVI en/of NICC samenwerken met Platform Vitaal, terwijl ook daar een duidelijke overlap zit in doelstelling en activiteiten. Ook wordt niet duidelijk of voor de invulling van het informatiemodel, de reeds bestaande overlegvormen per vitale sector (zoals bijvoorbeeld NCO-T voor de sector ICT/Telecom) worden benaderd om mee te werken of dat een ‘nieuw’ overleg per sector zal worden opgestart.

Voorts dient opgemerkt te worden dat de doelstelling en activiteiten van het SOVI ook grote overeenkomsten vertonen met bovenstaande platformen. Het grote verschil is echter dat het SOVI zich meer richt op maatschappij ontwrichtende gebeurtenissen en het een strategisch overleg is dat op een vrij (hoog) abstract niveau wordt ingestoken. Dat blijkt met name uit het soort deelnemers van het overleg: DGs van ministeries en leden van de RvB van vitale bedrijven.

Dit bij elkaar opgeteld zou aanleiding kunnen zijn om bovenstaande initiatieven nog eens nader te bekijken, temeer aangezien alle initiatieven nog maar net zijn opgestart (in 2006) of nog opgestart moeten worden (zoals het NAVI).

3.2.2 Overlap Digibewust en NICC

Een ander voorbeeld waarin doel en activiteiten bijna geheel overeen komen is het experiment cybercrime in het MKB. Zowel NICC als het programma Veilige Elektronische Communicatie (VEC), later omgedoopt tot Digibewust, hadden in hun programmabeschrijving een experiment, respectievelijk pilot opgenomen om de mate van cybercrime-incidenten in het MKB in kaart te brengen. Uit de beantwoording van de vragenlijsten komt naar voren dat beide activiteiten nu zijn gebundeld en dat één gezamenlijk experiment zal worden gedaan. De uitvoering ervan is neergelegd bij ECP.nl.

Eenzelfde bundeling van krachten heeft recentelijk plaatsgevonden met een aantal bestaande bewustwording- en voorlichtingscampagnes. Daarvan is besloten deze zoveel mogelijk onder te brengen in de campagne Digibewust (o.a. Surf op Safe). Dit is een goede stap voorwaarts in het structureren van de lappendeken aan initiatieven.

3.2.3 Overlap Herijking ICT-veiligheid en Nationale veiligheid

Niet alleen EZ heeft het initiatief genomen om in samenwerking met BZK en Justitie te komen tot een interdepartementaal ICT-veiligheidsbeleid. Ook onder aanvoering van BZK loopt een programma Nationale Veiligheid, waarin een interdepartementale strategie op het gebied van nationale veiligheid als een van de belangrijkste doelstellingen is geformuleerd. BZK neemt hierin het ICT-veiligheidsbeleid mee als onderdeel van de nationale veiligheid en betrekt hierin ook EZ en Justitie. Een verschil tussen beide programma's is dat Herijking ICT-veiligheid zowel beleidsbepaling rondom niet-maatschappij ontwrichtende gebeurtenissen als maatschappij ontwrichtende gebeurtenissen beoogt, terwijl Nationale veiligheid zich voornamelijk richt op maatschappij ontwrichtende gebeurtenissen (in het programma digitale verlamming genoemd). Een ander verschil is de aanpak / benadering van het programma. Er is (nog) geen concrete samenwerking tot stand gekomen tussen beide programma's, maar er is wel degelijk contact en participatie in elkaars programma's.

3.3 Rollen, taken en verantwoordelijkheden

Het blijkt lastig om helder de rollen, taken en verantwoordelijkheden van de bestaande initiatieven en de ministeries te definiëren. Dit geldt in de eerste plaats zowel voor de dossierhouders zelf, zoals blijkt uit de zeer uiteenlopende beantwoording van de vragen die naar rollen en taken refereren, maar ook voor neutrale derden. De vraag wie de (eind) verantwoordelijkheid heeft in een bepaald initiatief wordt in de enquête niet expliciet gesteld en wordt daarom door slechts enkelen aangestipt. Bovendien blijken ministeries dikwijls samen te werken in gedeelde verantwoordelijkheden, soms onder algehele coördinatie van één ministerie, met uitvoerende bevoegdheden voor en door andere ministeries. Soms blijken uitvoerende taken en verantwoordelijkheden te zijn neergelegd bij non-gouvernementele organisaties of publiek-private samenwerkingsverbanden waar de overheid zorgdraagt voor (een deel van) de financiering en de uitvoering aan marktpartijen wordt overgelaten. Dit maakt het in veel gevallen lastig om helder te krijgen hoe de verdeling van rollen, taken en verantwoordelijkheden in elkaar steekt. Hieronder volgen enkele voorbeelden van deze onduidelijkheden. Deze zijn illustratief, maar niet uitputtend.

3.3.1 NCTb, NCC/DCC en AIVD

Op papier heeft het Nationaal Coördinatie Centrum (NCC) in geval van nationale crises een coördinerende rol en de Nationaal Coördinator Terrorismebestrijding (NCTb) de regie bij terroristische dreiging. De Algemene Inlichtingen en Veiligheidsdienst (AIVD) legt in haar activiteiten de nadruk sterk op cybercrime waarbij de nationale veiligheid in het geding is. Hierin lijkt een rolverdeling te zitten, maar bij een crisis op het gebied van ICT-veiligheid kan zowel sprake zijn van een nationale crisis, een terroristische dreiging en een geval van cybercrime. In zo'n geval kan snel onduidelijkheid ontstaan over wie de algehele regie heeft, wie informatie doorspeelt aan wie, etc. Uit de beantwoording van de vragenlijsten wordt niet duidelijk in hoeverre deze drie organisaties deze noodzakelijke afstemming hebben gedefinieerd. De AIVD noemt het ministerie van BZK en GOVCERT, maar niet het NCC of de NCTb. Laatste twee hebben geen vragenlijst ingevuld, dus daarvan ontbreekt deze informatie. Uit het programmavoorstel van NICC blijkt dat NICC onderkent dat er onduidelijkheid zou kunnen bestaan wie van de bovenstaande organisaties in welke gevallen het beste aanspreekpunt is. NICC werpt zich in het programmavoorstel op als coördinerende instantie die doorverwijst naar de juiste instantie. Het is echter wenselijk dat alle

betrokkenen, zowel de organisaties zelf, de overheid en andere partijen, zicht hebben op een duidelijke en heldere onderlinge rol-, taak- en verantwoordelijkheidsverdeling.

3.3.2 Publiekprivate samenwerking favoriet

In vele initiatieven is de PPS-constructie als overlegvorm favoriet, waarbij in zeer veel gevallen de kennis- en informatie-uitwisseling de belangrijkste doelstelling is. Dit betekent twee dingen. In de eerste plaats bestaan natuurlijk verschillende vormen van publiekprivate samenwerking, maar een van de kenmerken is de (gewenste) gedeelde verantwoordelijkheid voor een bepaald onderwerp of probleem. Hierin schuilt het gevaar dat onvoldoende duidelijk is wie uiteindelijk de (eind)verantwoordelijkheid heeft in een bepaald initiatief. De onduidelijke beantwoording van de vragenlijsten op dit vlak bevestigen dit beeld. In veel initiatieven komt niet duidelijk naar voren wie de organisatorische, financiële en eindverantwoordelijkheid draagt, wie de risico's op zich neemt en wie welke maatregelen neemt als zaken in een project dreigen mis te gaan.

In de tweede plaats betekent de veelvuldig voorkomende doelstelling van kennis- en informatiedeling dat overheid en bedrijven vooral veel met elkaar blijken te *praten* over mogelijke risico's en dreigingen van de ICT-veiligheid. De discussies blijken in zeer veel gevallen te blijven hangen op strategisch / tactisch niveau. Er worden weinig concrete acties en maatregelen geformuleerd en getroffen om het uiteindelijke doel, een veiliger ICT-Nederland, zowel geheel als op onderdelen ook daadwerkelijk te bereiken. Opmerkelijk is dat uit de beantwoording van de vragenlijsten blijkt dat in veel gevallen de doelstelling, het probleem en de activiteiten van het overleg nog bepaald moeten worden, in plaats van dat naar aanleiding van een geconstateerd probleem gericht aan de slag wordt gegaan in een bepaald project. Zo zijn bijvoorbeeld het NAVI, maar ook NICC, Platform Vitaal en Digibewust nog zoekende naar een juiste invulling en besteding van de reeds toegewezen middelen.

3.4 Genoemde verbeterpunten door initiatieven zelf

In de vragenlijst werden de partijen gevraagd mogelijke verbeterpunten te noemen in het ICT-veiligheidsbeleid. Hieronder worden de meest genoemde verbeterpunten besproken.

1. Kennis- en informatiedeling plus analyse

De betrokken dossierhouders blijken grote behoefte te hebben aan kennis- en informatiedeling. Dat is hoogstwaarschijnlijk ook de reden dat dit punt in zeer veel platforms en andere overlegstructuren als (een van de) belangrijkste doelstelling is geformuleerd. Genoemd wordt kennisdeling tussen initiatieven, tussen ministeries en departementen, tussen overheid en bedrijfsleven en tussen overheid en wetenschap.

2. Samenwerking, nationaal en internationaal

Wat betreft de samenwerking tussen de bestaande initiatieven: er wordt al veel samengewerkt op een aantal vlakken, maar in nog veel meer gevallen lijken partijen niet op de hoogte te zijn van de activiteiten of gedeelde doelstelling van een andere partij of initiatief. Uit de beantwoorde vragenlijsten worden wel vaak partijen waarmee wordt samengewerkt benoemd, maar er wordt niet concreet aangegeven waaruit die samenwerking dan bestaat. Dat maakt het lastig te beoordelen in welke mate en op welke vlakken constructief aan maatregelen of oplossingen of kennisdeling wordt samengewerkt. Als samenwerkingsvormen worden genoemd: internationale

samenwerking (afstemming op Europees beleid), operationele samenwerking, samenwerking tussen de verschillende niveaus (pro-actie, preventie etc.) en interdepartementale samenwerking.

3. Governance: samenhang, coördinatie en rolverdeling
Door verschillende dossierhouders wordt een gebrek aan governance onderkend en benoemd als verbeterpunt in het ICT-veiligheidsbeleid. Genoemd worden het verbeteren van de samenhang en coördinatie tussen bestaande initiatieven en een betere rolverdeling tussen de verschillende departementen en organisaties.

Annex I: Overzicht ICT-veiligheidsbeleid (beleidsdocumenten)[18]

Inleiding

Drie ministeries, te weten de ministeries van BZK, EZ en Justitie spelen een kernrol in de ontwikkeling en uitvoering van het ICT-veiligheidsbeleid. In diverse beleidsdossiers wordt uitgebreid aandacht geschonken aan ICT-veiligheid. Zo zijn er diverse actieprogramma's, nota's en visies waarin ICT-veiligheid soms in een hoofdrol, en soms in een (belangrijke) bijrol ten tonele wordt gevoerd. Een overkoepelend beleidsdocument waarin 'het' ICT-veiligheidsbeleid kernachtig staat omschreven ontbreekt echter tot op heden.

In deze bijlage wordt op basis van nota's, visies, agenda's en correspondentie met de Tweede Kamer een beeld geschetst van het huidige beleid en het recente beleidsverleden. Een belangrijk aspect in dit veiligheidsbeleid, namelijk grensoverschrijdende ofwel internationale samenwerking inzake ICT-veiligheid wordt slechts summier aangestipt in deze rapportage.

De volgende beleidsdossiers worden in de volgende paragrafen besproken:
- Bescherming Vitale Infrastructuur (sinds 2002, doorlopend)
- Visie SPAM en uitvoering (sinds 2004, doorlopend)
- Beleidsplan Crisisbeheersing 2004-2007
- Rijksbrede ICT agenda (2004) en haar vervolg Beter Presteren met ICT (2005)
- Actieprogramma Maatschappelijke sectoren en ICT 2005-2009
- Terrorismebestrijding (sinds ?, doorlopend)
- Internationaal

Bescherming Vitale Infrastructuur – BZK[19] (start april 2002, doorlopend)

Op grond van een motie van Tweede Kamerlid Wijn[20] heeft de regering een sectoroverschrijdend plan van aanpak inzake de bescherming van de vitale infrastructuur opgesteld. In april 2002 is het project Bescherming Vitale Infrastructuur (BVI), kortweg aangeduid als Vitaal, ingesteld, onder algemene coördinatie, monitoring en toetsing van BZK. Binnen BVI wordt nauw samengewerkt met alle departementen, het bedrijfsleven en de medeoverheden. BVI omvat:

3. De ontwikkeling van een samenhangend pakket maatregelen ter bescherming vitale infrastructuur, waaronder ICT;
4. De verankering van maatregelen binnen bedrijfsvoering overheid en bedrijfsleven.

[18] Opgesteld op basis van openbare beleidsdossiers en correspondentie Tweede Kamer der Staten-Generaal.
[19] TK 2003-2004, 26 643 nr. 43 en TK 26 643 nr. 56., Rapportage Bescherming Vitale Infrastructuur, 9 juli 2004
[20] TK 2000-2001, 26 643 nr. 20, maart 2001.

Vitaal heeft tot doel de kwetsbaarheid van de vitale infrastructuur in Nederland in kaart te brengen en door het treffen van beschermende maatregelen waar nodig deze te verminderen. Vitaal genereert kennis over kwetsbaarheden, risico's en daarop toegesneden maatregelen. Vitaal heeft betrekking op macroverstoringen; verstoring of uitval van een vitale sector, een dienst of product wat economische of maatschappelijke ontwrichting op (inter)nationale schaal kan veroorzaken en direct of indirect tot veel slachtoffers kan leiden. Het gaat hierbij om ontwrichting die van lange duur is en waarvan het herstel relatief veel tijd kost en gedurende het herstel vooralsnog geen reële alternatieven voorhanden zijn.

Per mei 2004 is het project Vitaal omgevormd tot een structureel beleidsdossier dat verankerd ligt binnen overheden en sectoren, met een coördinerende rol voor BZK. De minister van BZK rapporteert de Tweede Kamer periodiek over de bescherming van de vitale infrastructuur als onderdeel van vierjaarlijkse rapportagecyclus met betrekking tot crisisbeheersing.

In de structurele samenwerking tussen overheid en bedrijfsleven met het oog op bescherming van de vitale infrastructuur staan de volgende uitgangspunten centraal:
1. Hoe grootschalige uitval of verstoring van de vitale infrastructuur beter kan worden voorkomen (pro-actie en preventie);
2. Of overheid en bedrijfsleven zich adequaat hebben voorbereid op de gevolgen van uitval of verstoring (preparatie); en
3. Hoe effectieve maatregelen kunnen worden genomen om schade van uitval of verstoring zo veel mogelijk te minimaliseren (repressie).

Dossier Vitaal bestaat uit een inmiddels afgeronde quickscanfase[21] en een vervolgfase. De quickscan heeft geleid tot een inventarisatie van vitale sectoren, vitale producten en diensten en knooppunten[22]. Er zijn onder meer knooppuntanalyses gemaakt per vitale sector, uitgevoerd onder leiding van het primair verantwoordelijke ministerie in overleg met de betrokken bedrijfssector en andere beheerders van infrastructuur. De zeven gedefinieerde vitale elektronische diensten zijn:

- vaste telecommunicatie
- mobiele telecommunicatie
- satellietcommunicatie
- post- en koeriersdiensten
- radiocommunicatie en -navigatie
- omroep
- toegang tot het internet

Er is onderscheid gemaakt tussen directe en indirecte knooppunten. De directe knooppunten zijn de knooppunten binnen de vitale sector Telecommunicatie/ICT (zoals antennevoorzieningen t.b.v. mobiele communicatienetwerken). Onder de indirecte knooppunten worden knooppunten tussen de vitale sector Telecommunicatie/ICT met andere vitale sectoren verstaan. Deze zijn:

- Drinkwater (VROM);
- Voedsel (LNV);
- Gezondheidszorg (WVS);
- Financiële sector (Financiën). Bij haar dienstverlening is de financiële sector vooral afhankelijk van elektriciteit en ICT/communicatie-infrastructuur.

[21] TK 2002-2003, 26 643 Nr. 39; TK 26 643 Nr. 48; TK 2004-2005, 26 643, nr. 75
[22] Zie TK 26 643 Nr. 48.

- Energie (EZ);
- Keren en beheren oppervlaktewater (VWS);
- Openbare orde en veiligheid (BZK);
- Rechtsorde (Justitie);
- Openbaar bestuur (BZK);
- Diplomatie (BuZa);
- Krijgsmacht (Defensie);
- Transport (VWS).

De vervolgfase BVI loopt vanaf 2004 en kent twee stappen, onder verantwoordelijkheid van de vakdepartementen, met een uitwisseling van ervaringen elk kwartaal middels toetsingsbijeenkomsten:

- Het in kaart brengen van kwetsbaarheden en risico's van sectoren, waarin onder meer gebruik wordt gemaakt van scenarioanalyses; de departementen hebben zich gecommitteerd aan strikte aanleverdata.
- Het ontwikkelen van samenhangend pakket aan beschermingsmaatregelen op basis van de quickscan en in kaart gebrachte kwetsbaarheden en risico's, waaronder het leggen van structurele verbanden tussen de vitale infrastructuur, de zgn. *soft targets* en de concrete invulling van het te implementeren alerteringssysteem.

Voor de beveiliging van de vitale infrastructuur worden primair de betreffende eigenaar en beheerder verantwoordelijk geacht. De overheid is verantwoordelijk voor maatregelen die noodzakelijk zijn als de dreiging de beschermingsmogelijkheden van het bedrijfsleven overtreffen. In het geval dat de overheid zelf eigenaar van vitale infrastructuur is worden in die hoedanigheid extra maatregelen getroffen, te financieren uit 30 miljoen euro incidenteel hiervoor uitgetrokken FES-gelden. In een rapportage aan de Tweede Kamer in 2005 is gesteld dat een gezamenlijk en eenduidig kader voor afstemming tussen private en publieke partijen ontbreekt. Ook geven partijen die bij de analyses van de vitale infrastructuur zijn betrokken aan behoefte te hebben aan meer kennis en kunde op het gebied van beveiligen.[23] Het beleidspakket Bescherming Vitale Infrastructuur omvat:

1. Het intensiveren van het securitybeleid vitale infrastructuur, waaronder begrepen:
- het in versneld tempo ontwikkelen van (innovatief) beleid en eventuele maatregelen ten aanzien van de security van vitale infrastructuur,
- het verzamelen en delen van kennis in samenwerking met andere kennisleveranciers
- het opzetten van een «front-office» (één-loketgedachte) ten behoeve van vragen van lokale overheden en bedrijven op het gebied van security, en een Taskforce Security.

Om de informatiepositie van bedrijven te borgen zal de AIVD met de sectoren afspraken maken over onder andere de frequentie van de te leveren dreigingsinformatie.

2. Het nemen van het initiatief voor een gebiedgerichte benadering

3. Activiteiten in het kader van het Alerteringssysteem Terrorismebestrijding waarop aangesloten:
– Luchthaven Schiphol (zowel land- als airside);
– Drinkwater (waterleidingbedrijven);
– Spoor (personenvervoer en stations);
– Haven Rotterdam en de petrochemische industrie aldaar.

Alerteringssysteem zal naar verwachting worden uitgebreid naar andere sectoren in de toekomst.

4. Oefenen op basis van verdelingsplannen in geval van schaarste

[23] TK 2004-2005, 26 643, nr. 75 ICT. Brief betreffende inhoudelijke analyse van de bescherming van de vitale infrastructuur in Nederland (project BVI, BZK).

5. Het verbeteren van de middelen voor noodcommunicatie. Tijdens crises kan het openbaar bestuur gebruikmaken van het Nationaal Noodnet. Het contract met KPN omtrent het huidige noodnet loopt eind 2008 af. Noodnet biedt nu alleen telefoniediensten en fax. Bekeken wordt of ook datadiensten via dit net kunnen lopen en in hoeverre behoefte is aan een mobiel noodnet.
6. Oprichting Strategisch Overleg Vitale Infrastructuur (SOVI). In het overleg zijn zowel de overheid als het bedrijfsleven vertegenwoordigd (intersectoraal).
7. Intensivering communicatie tussen sectoren. Belangrijke vragen: 'Wat is de ernst van de situatie?', maar vooral ook op de vraag 'Hoe lang zal deze crisis duren?' Het antwoord op deze laatste vraag bepaalt namelijk of de getroffen vitale sectoren verdere maatregelen zouden moeten treffen om de continuïteit te blijven garanderen. Het sinds mei 2005 bestaande Expertisecentrum Risico- en Crisiscommunicatie (ERC) zal in de verdere uitwerking van Vitaal een ondersteunende rol vervullen. Ook medeoverheden kunnen in deze een beroep doen op het ERC.
8. Het opzetten van een visitatieprogramma 2006–2009; ondermeer om de kwaliteit van de maatregelen ter bescherming van de vitale infrastructuur te toetsen.
9. Evaluatie; Het beleidsdossier Bescherming Vitale Infrastructuur is in het eerste kwartaal van 2006 geëvalueerd.[24]

Visie SPAM[25] en uitvoering – EZ (start begin 2004, doorlopend)

In een brief aan de Tweede Kamer schetst de minister EZ zijn beleidsvisie inzake de aanpak van spam. Daarin wordt gesteld dat private partijen de primaire verantwoordelijkheid worden geacht te dragen voor het beveiligen en betrouwbaar maken van internet. De rol van de overheid ligt in het creëren van de juiste randvoorwaarden. Regelgeving is beperkt effectief, omdat het internet geen geografische grenzen kent. Het is daarom van belang om, naast regelgeving, tevens te zoeken naar oplossingen waarmee de eigen verantwoordelijkheid van de gebruikers en marktpartijen wordt ingevuld. Het opstellen van wetten en regelgeving kan beter in internationaal verband gebeuren. De minister zal onderzoeken welke mogelijkheden er zijn om de spamproblematiek en de kosten van spam in kaart te brengen en de ontwikkelingen en initiatieven op het gebied van spambestrijding op de voet volgen en waar nodig stimuleren.

Regelgeving. Juridische maatregelen om spam te beperken, richten zich op het aan banden leggen van de verzending van ongevraagde commerciële e-mail. In het voorstel van Wet implementatie Europees regelgevingkader voor de elektronische communicatiesector 2002 (28 851) wordt onder artikel 11.7 van de Telecommunicatiewet een opt-in regime ingevoerd voor het gebruik van elektronische berichten (zoals e-mail) voor het overbrengen van communicatie met onder meer commerciële doelstelling. Het opt-in regime zal worden gehandhaafd door toezichthouder OPTA. Het opt-in regime zal naar verwachting een effectief middel zijn om spam van afzenders binnen de Europese Unie tegen te gaan en is een goede aanzet voor de verdere bestrijding van spam in breder internationaal verband.

Met betrekking tot één enkel element is voorzien in een strafbaarstelling in de Wet op de economische delicten. Het betreft hier de verplichting om in (ongevraagde) commerciële elektronische berichten te vermelden: (a) de werkelijke identiteit van

[24] TK 26 643, Nr. 75. (16 september 2005).
[25] TK26643, Nr. 46. Zie ook Verslag van algemeen overleg, idem, Nr. 52.

degene namens wie de communicatie wordt overgebracht en (b) een geldig postadres of nummer waaraan de ontvanger een verzoek tot beëindiging van dergelijke communicatie kan richten. FIOD/ECD is belast met de handhaving hiervan.

Bewustwording en voorlichting (preventie). Gebruikers moeten nog bewuster worden van de gevaren en hun eigen verantwoordelijkheden. Zowel nationaal als internationaal wordt daarom geïnvesteerd in awareness programma's voor een veiliger gebruik van internet en *empowerment* van de individuele gebruiker (zoals Surf op Safe). Ook het bedrijfsleven moet goed geïnformeerd worden over de nieuwe regels voor het verzenden van commerciële e-mail.

Monitoring. Naast de implementatie van het opt-in regime wordt bekeken welke knelpunten er in de praktijk blijven. De minister is van plan dit actief te monitoren. Ook wordt Europese wetgeving afgewacht voordat verdere maatregelen worden genomen. Daarnaast wordt onderzocht of (en hoe) de omvang en kosten van de spamproblematiek in kaart kunnen worden gebracht. Ook worden nieuwe technische mogelijkheden om spam te bestrijden vanuit de industrie ontwikkeld, gevolgd. De minister acht een meldpunt niet wenselijk, omdat dit onjuiste verwachtingen zou wekken bij de consument.

Zelf-regulering/overleg/private initiatieven. In Nederland wordt gewerkt aan een gedragscode voor direct marketing waarin, voortbordurend op de wettelijke bepalingen, aanvullende gedragsregels worden afgesproken over bijvoorbeeld de maximale omvang van een commercieel bericht, het meezenden van bijlagen, etc.

Gewijzigde Telecommunicatiewet en beleidsvisie SPAM[26]- EZ (betreft follow-up)

Regelgeving. Wijziging Telecommunicatiewet - Het op 19 mei 2004 ingestelde opt-in regime (OPTA) gaat ook gelden voor zakelijke gebruikers. Klachten kunnen worden ingediend op www.spamklacht.nl. Tijdens de behandeling van de Telecommunicatiewet is de motie Van Dam/Atsma aangenomen om initiatieven te nemen waardoor ook voor bedrijven ten aanzien van spam het opt-in regime zal gelden. Dit is conform de Europese e-Privacy richtlijn, die met dit wetsvoorstel werd geïmplementeerd.
Coördinatie. Periodiek overleg nationale partijen (ISP's, kabelaanbieders, mobiele providers), daarnaast VNO-NCW, Consumentenbond, Stichting SPAMvrij
Bewustwording en voorlichting. Voorlichtingscampagne Surf op Safe gaat optreden als National Awareness Node op het gebied van veilig internetten, in het kader van het Europese Safer Internet Actieplan. Dit betekent een verdere intensivering van de voorlichtingscampagne met onder andere de volgende acties: vernieuwing website, nieuwe brochure veilig internetten met uitgebreide informatie over spam, phishing en computer hijacking (januari 2005), speciale flyer over spam, en uitbreiding informatie via websites Postbus 51, staiksterk. In 2005 zijn nieuwe projecten opgestart, gericht op doelgroepen MKB en senioren. In 2005 gaat een pilot van start op 20 scholen in het kader van 'Diploma Veilig Internetten'.

Onderzoek & analyse. EZ heeft een onderzoek laten uitvoeren naar de diverse aspecten van spam.

[26] TK 26 643 Nr. 61 Informatie- en communicatietechnologie (ICT) – EZ (20 december 2004).

R&D. EZ heeft gesproken met diverse partijen in Nederland die bezig zijn met het bedenken van nieuwe, technische oplossingen voor het spamprobleem.
Internationaal. Handhaving (Europese samenwerking uitwisseling gegevens), sluiten van global alliances, voorlichting en bewustwording (uitwisseling tussen lidstaten van ervaringen en best practices), R&D gericht op spam.

De Rijksbrede ICT agenda en haar vervolg Beter Presteren met ICT

Het vergroten van de ICT veiligheid is één van de zes speerpunten in de Rijksbrede ICT agenda (2004): beter presteren met ICT die is opgesteld door de ministeries EZ, BZK en OC&W. In deze Rijksbrede ICT agenda wordt veiligheid in een adem genoemd met betrouwbaarheid van en vertrouwen in het gebruik van ICT-voorzieningen en internet. Veiligheid en vertrouwen worden door het Rijk gezien als noodzakelijke randvoorwaarden om de ICT kennisbasis te versterken en te exploiteren, het overkoepelende doel van de Rijksbrede ICT agenda. De Rijksbrede ICT agenda is tevens bedoeld een impuls aan de Europese agenda eEurope 2005 te geven.

Kernpunten ICT veiligheid in de Rijksbrede ICT agenda:
Communicatie-infrastructuren moeten ongestoord kunnen functioneren, privacy wordt beschermd en cybercrime wordt voorkomen en bestreden. Dit wordt bereikt door:
(A) Een veiligheidsbeleid dat is gedifferentieerd naar vitale en minder vitale domeinen, met een scherpe afbakening van publieke belangen
(B) Blijvende aandacht in het onderwijs voor het bijbrengen van ICT vaardigheden.

Veiligheid. Burgers en bedrijven in Europa hebben te weinig vertrouwen in internet, waardoor eCommerce en gebruik van elektronische diensten achterblijft. Veiligheid en vertrouwen zijn een absolute voorwaarde voor de verdere ontwikkeling van de informatiemaatschappij. De oprichting van het Europese Agentschap voor Netwerk en Informatiebeveiliging (ENISA) illustreert het belang dat Europa hieraan hecht.

Vaardigheden. Het Europese beleid op gebied van ICT-vaardigheden en eLearning is gericht op benchmarking van breedbandtoegang bij onderwijsinstellingen en universiteiten; onderzoek naar computerondersteunde netwerken en platforms; lancering van opleidingen voor eSkills. Voor ondersteuning van regionale en nationale acties maakt de Commissie gebruik van een aantal instrumenten en programma’s (waaronder eTEN, de Kaderprogramma's, ESF-gelden, de eLearning faciliteit).

Meer specifiek is er aandacht voor:
- Voorkomen verstoringen in netwerken: de overheid zal samen met netwerkaanbieders bezien hoe ernstige verstoringen kunnen worden voorkomen en zo nodig zo snel mogelijk kunnen worden hersteld.
- Betrouwbaarheid van vitale ICT diensten: de overheid moet de betrouwbaarheid van vitale ICT diensten garanderen en creëert randvoorwaarden opdat gebruikers en dienstverleners hun eigen verantwoordelijkheid kunnen oppakken om hun eigen systemen te beschermen. In sommige gevallen zal de overheid dat doen.
- Bewustwording gebruikers
- Bescherming gebruikers
- Voorkomen en bestrijden van cybercrime.

De Rijksbrede ICT agenda is vertaald in een lijst van concrete actiepunten (zie verder hoofdstuk 3). De uitvoering van hiervan ligt primair bij drie departementen: EZ, BZK en Justitie. Deze dragen al naar gelang het actiepunt een gezamenlijke dan wel eigen verantwoordelijkheid voor het realiseren van de actiepunten.

In juni 2005 verscheen het vervolg op deze agenda onder de titel Beter presteren met ICT – Vervolg rijksbrede ICT agenda 2005-2006.[27] De Europese agenda blijft het uitgangspunt voor het Nederlandse beleid. In i2010, de nieuwe Europese ICT-agenda, zijn de volgende zes speerpunten van belang:
(1) een excellente ICT-sector en innovatieve bedrijvigheid; (2) beter gebruik van ICT door burgers en betere ICT-vaardigheden; (3) beter ICT-gebruik in publieke dienstverlening; (4) ontwikkeling van content en nieuwe producten en diensten; (5) ontwikkeling van netwerken en communicatie infrastructuur en (6) voldoende vertrouwen en veiligheid in gebruik van ICT. Het Nederlandse Kabinet geeft prioriteit aan de volgende vier aandachtsgebieden: Standaardisatie; Veiligheid en vertrouwen; ICT-gebruik in het publieke domein; en Ontwikkeling breedbandige netwerken.

Er wordt verder gewerkt aan het verder verbeteren van de veiligheid van de elektronische communicatiesystemen. Op basis van het programma Kwetsbaarheid op Internet (KWINT) is actie ondernomen met de campagne Surf op Safe en door het instellen van een Waarschuwingsdienst (onderdeel van GOVCERT). Samen met de grote landelijke aanbieders van (vaste en mobiele) telecommunicatie wordt gewerkt aan het zekerstellen van de beschikbaarheid van de vitale telecommunicatiediensten (NCO-T). Bescherming van vitale infrastructuren (BVI) is onderdeel van het Actieplan terrorismebestrijding. Tevens zijn er diverse programma's voor de aanpak van computercriminaliteit gedefinieerd en zijn/worden diverse acties gepleegd die de ICT veiligheid moeten versterken, waaronder:

- bewustwording ten aanzien van beveiliging bij zowel de burger als zakelijke gebruiker van elektronische communicatiesystemen (Digibewust en Surf op Safe).
- Inzicht verkrijgen in de kwetsbaarheid van de telecom/ICT-sector.
- Borging van de beschikbaarheid van vitale telecommunicatiediensten in wet- en regelgeving als uitwerking van het beleid inzake NACOTEL (nu NCO-T).
- Onderzoek naar Cybercrime: voorstel door het National High Tech Crime Center voor inhoudelijke en organisatorische aanpak
- Bevoegdheden voor politie en justitie om computercriminaliteit op te sporen en feiten strafbaar gesteld worden die dat eerder niet waren (zoals grootschalige SPAM gericht op verstoring van ICT-systemen).
- Activiteiten voor en met bedrijven voor het bestrijden van de kwetsbaarheid van het internet.
- Onderzoek naar de gevolgen van nieuwe technologieën als VOIP en RFID voor de continuïteit, kwetsbaarheid en betrouwbaarheid van ICT.
- Internationale samenwerking en kennisverhoging is verbeterd met de start van ENISA en de samenwerking binnen Europa is tot stand gekomen inzake het European Program on Critical Infrastructure Protection (EPCIP).
- Het Kabinet streeft naar internationale afspraken over spam.
- Mondiaal - in het kader van de WSIS35 - zal het Kabinet een actieve rol spelen voor beheer van internet (o.a.. Internet Governance)

[27] EZ, BZK, OCW (2005) Beter presteren met ICT – Vervolg rijksbrede ICT agenda 2005-2006

- In 2005 – 2006 wordt het project Aanpak Cybercrime uitgevoerd als onderdeel van het Actieplan Veilig Ondernemen II en wetgeving wordt toegespitst op de eisen van de digitale omgeving.
- Er komt een centraal meldpunt voor de overheid voor cybercrime
- Het opt-in regime inzake SPAM geldt ook voor zakelijke gebruikers.

Actieprogramma Maatschappelijke sectoren en ICT 2005-2009[28]

Het Actieprogramma Maatschappelijke sectoren en ICT 2005-2009 heeft als doelstelling: "Het helpen oplossen van maatschappelijke vraagstukken in de sectoren mobiliteit, onderwijs, veiligheid en zorg, door het wegnemen van belemmeringen zodat doorbraken kunnen worden gerealiseerd in de ontwikkeling en de implementatie van innovatieve ICT-toepassingen en -diensten."

ICT-toepassingen in de sector veiligheid hebben betrekking op de preventie en bestrijding van criminaliteit en overlast in de publieke ruimte, de bestrijding en het voorkomen van rampen, en de communicatie en informatievoorziening tussen hulpdiensten. Het Kabinet heeft tevens een veiligheidsprogramma opgesteld om de sociale onveiligheid in Nederland terug te dringen. Het Actieprogramma Maatschappelijke sectoren en ICT 2005-2009 is een aanvulling op dat programma en andere activiteiten. Doelstelling is het verbeteren van het (gevoel van) veiligheid in de samenleving door het breder gebruik maken van innovatieve ICT-toepassingen en –diensten, met drie actielijnen:

1. Effectiever gebruik van sensoren voor veiligheid en opsporing;
2. Informatie-uitwisseling in veiligheidsketens: uitbreiding CIOT en online beschikbaar maken van gegevens bestanden, Informatie Basisvoorziening Veiligheid (IBV) en P-info[29]
3. Verhogen van veiligheid door innoverende technologieën.

Tevens worden een aantal verkenningen uitgevoerd:
- Uitwerken van scenario's met als doel doorzicht te geven naar een toekomstige ICT-samenleving als er grootschalig gebruik wordt gemaakt van RFID, Ambient Intelligence, mobiel breedband e.d. vanuit een veiligheidsperspectief
- Mogelijkheden voor datamining in open bronnen om te komen tot inlichtingen over criminele of terroristische organisaties en activiteiten;
- Uitwerken van de mogelijkheden die virtual reality simulaties en space synax software bieden om al bij het ontwerp van nieuwe woon-, werk- en winkelgebieden rekening te houden met de veiligheidsconsequenties van ontwerpkeuzen.

Behalve actielijn 2 die raakt aan crisisbeheersing en de informatie-uitwisseling tussen veiligheidsketens, gaat dit actieprogramma voor het grootste deel in op het bereiken van (het gevoel van) veiligheid met behulp van ICT-toepassingen. Dit laatste gebied valt verder buiten de scope van dit onderzoek.

[28] EZ, BZK, Justitie, OCW, VenW, VWS (2005) Actieprogramma maatschappelijke sectoren & ICT; beter benutten van ICT, meer kwaliteit in maatschappelijke sectoren
[29] Ibid, blz. 96, 97, 98

Beleidsplan Crisisbeheersing 2004-2007[31] - BZK

Beleidsplan Crisisbeheersing 2004-2007 richt zich op risicobeleid in het algemeen; ICT veiligheid is hiervan een onderdeel/aspect. Zelfredzaamheid van burgers bij crisisrespons is en blijft uitgangspunt van beleid. Hier wordt verder de nadruk op gelegd met de ontwikkeling van een meetinstrument voor het veiligheidsbewustzijn van burgers; ook wordt ingezet op het bevorderen van de crisisbestendigheid (o.a. ontwikkeling crisisbestendigheidstoets). Beleidsacties op nationaal niveau omvatten:

- Online risicokaart - alle provincies moeten in 2006 beschikken over deze risicokaart.
- Actualisering Handboek Crisisbesluitvorming. Begin 2006 is door de minister van Justitie en BZK het handboek Terrorismebestrijding op lokaal niveau verspreid onder openbaar bestuur en hulpverleningsdiensten.
- Wetgeving: De regeling met betrekking tot de veiligheidsregio wordt in 2006 als wetsvoorstel aan de Tweede Kamer voorgelegd. Regelingen omtrent de bijstandsverlening en de interventiemogelijkheden van de minister van BZK in fasen van preventie, preparatie en respons worden tegen het licht gehouden. Ook zal op nationaal niveau de specifieke departementale (nood)wetgeving op het terrein van crisisbeheersing worden bezien, hetgeen moet uitmonden in voorstellen tot aanpassing van de (nood)wetgeving.
- Alerteringssysteem 2005: opgeleverd 1 april 2005
- Shared Services Crisisbeheersing (SSCB)
- Intensivering civiel-militaire samenwerking (ICMS)
- Opleiden en oefenen op national niveau: Bonfire, NSOn. In 2006 staan twee oefeningen gepland, het eerste scenario' is een terroristische aanslag, het tweede een grootschalige uitval van ICT.
- Kwaliteitszorgcrisisbeheersing: vaststellen en toetsing van kwaliteitsniveau en –eisen, evaluaties van crises, landelijk operationeel coördinatiecentrum (LOCC)
- Het Beleidsplan Crisisbeheersing omvat een jaarlijkse voortgangsrapportage waarin ook het beleidsdossier Bescherming Vitale Infrastructuur wordt betrokken.

Terrorismebestrijding - Justitie, BZK - doorlopend

Het antiterrorismebeleid kent drie onderdelen: 1) tegengaan van radicalisering, 2) het creëren van een slagvaardige organisatie en instrumenten en 3) het voorbereid zijn op (de gevolgen van) een mogelijke aanslag. Tevens wordt gekeken naar verschillende veiligheidsmaatregelen, communicatie en internationale ontwikkelingen. ICT, waaronder zeer expliciet ook het gebruik van internet en satellietzenders, behoort tot de aandachtvelden van de terrorismebestrijding.

Het huidige Dreigingsbeeld Terrorisme Nederland (DTN) laat duidelijk het belang zien van het vroegtijdig signaleren en tegengaan van radicaliseringsprocessen. Daarbij wordt een driesporenbeleid gehanteerd, waarin naast versterken van de binding aan de samenleving en vergroting van de weerbaarheid van de samenleving, ook actief ingrijpen centraal staat. Internet en satellietzenders kunnen hierbij een rol spelen.

Op vele wijzen wordt verder vorm gegeven aan een het creëren van een slagvaardige organisatie en instrumenten. Van specifiek belang voor ICT-veiligheid zijn daarbij

[31] TK 29 668 Nr. 8 Beleidsplan Crisisbeheersing 2004-2007 – BZK (30 januari 2006) (eerste voortgangsrapportage).

CBRN-terrorisme; wetgeving inzake bestuurlijke maatregelen nationale veiligheid; strafrechterlijke handhaving, en informatievoorziening: in samenwerking met diverse organisaties op het gebied van terrorismebestrijding, crisisbeheersing en criminaliteitsbestrijding werkt de NCTb aan concrete projecten op het gebied van de toepassing van informatievoorziening, zoals het programma Veiligheidsverbetering door Information Awareness (VIA).

Concrete veiligheidsmaatregelen betreffen onder meer het Alerteringssysteem Terrorismebestrijding: naast het aansluiten van twee nieuwe sectoren op het systeem, en het uitbreiden van de reeds aangesloten sectoren Schiphol en Rotterdam worden oefeningen gehouden en is gestart met het maken van een ontwerp voor een ICT-ondersteund en snel communicatiesysteem ten behoeve van de gebruikers van het alerteringssysteem.

Onder reageren op crises vallen de volgende zaken: crisesbeheersing; Crisismanagement bij terroristische aanslagen; oefeningen; en civiel-militaire samenwerking.

Aanpak gebruik internet en satellietzenders radicale en terroristische doeleinden

Deze aanpak is in 2005 in gang gezet ter bestrijding van radicale en terroristische uitingen op het internet. De essentie bestaat uit het verkrijgen van inzicht in de problematiek en het gelijktijdig ondernemen van verschillende activiteiten ter bestrijding. Samenwerking tussen overheid en private partners is daarbij het uitgangspunt. De aanpak richt zich op monitoring, het vormgeven en versterken van surveillance, en opsporing op het internet. Ter versterking hiervan lopen diverse pilot-projecten bij politie, OM en private partijen. In het voorjaar is het Meldpunt Cybercrime gestart. Meldingen worden beoordeeld door medewerkers van de politie en wordt al dan niet doorgestuurd naar de participerende organisaties.

Daarnaast vormt de totstandbrenging van een aanpak binnen Europees verband op het terrein van internet en terrorisme een van de voornaamste aandachtsvelden. Het Commissariaat voor de Media heeft in kaart gebracht in hoeverre Nederland buitenlandse (satelliet) zenders zijn te ontvangen die zich mogelijk schuldig maken aan haat zaaien en geweldsoproepen. Op 26 januari 2006 is in overleg met de Kamer geconcludeerd dat er 1) geen indicaties zijn dat buitenlandse zenders die aan Nederlands toezicht zijn onderwerpen, zich schuldig maken aan bovengenoemde uitingen, maar dat
2) er enkele andere zenders in Nederland te ontvangen zijn die zich hier mogelijk wel schuldig aan maken. Satelliettelevisie heeft een internationaal karakter. Dat raakt de kern van het probleem van de aanpak van zenders die worden gebruikt voor radicale en terroristische uitingen. Binnen de EU bestaan voornemens tot ontwikkeling van gemeenschappelijk buitenlands beleid tegenover derde landen die doorgifte van extremistische uitzendingen naar Europa blijven faciliteren. Bezien wordt in hoeverre Nederland hierin een aanjagende rol kan vervullen. Naast deze inventarisatie van satellietzenders is onderzocht met behulp van welk instrumentarium doorgifte van dergelijke zender in zijn algemeenheid kan worden beëindigd. Besloten is tot aanpassing van de Mediawet.

Internationaal

Het ICT-veiligheidsbeleid kan niet los worden gezien van de internationale context. Het is een aandachtsgebied dat ook in Europa en daarbuiten hoog op de agenda staat. Dit blijkt o.a. uit de volgende activiteiten:
- International Forum Critical Infrastructure Information Protection (CIIP)
- European Programme on Critical Infrastructure Protection (EPCIP)
- European Network Information Security Agency (ENISA)
- EU Safer Internet Plus Programme 2005-2008
- EU project National Awareness Node (veilig internetten)
- Groenboek Europees Programma voor de bescherming van vitale infrastructuur (2005)
- Diverse mededelingen van de Europese Commissie, zoals de onlangs uitgekomen COM(2006)251 '*Een strategie voor een veilige informatiemaatschappij'*.

Op het terrein van terrorismebestrijding bestaat er uitgebreide samenwerking, zowel tussen Nederland en andere landen (bilateraal) als met de volgende supranationale/internationale organisaties: EU (vgl EU Strategie en Actieplan Terrorismebestrijding: Radicalisering en rekrutering, Richtlijn dataretentie, Crisisbeheersing); NAVO; VN.

In hoofdstuk 2 komt een aantal van deze initiatieven terug, maar het voert te ver om daar in deze rapportage uitgebreid op in te gaan.

Annex II: Actietabel 2005-2006 Rijksbrede ICT agenda

(Legenda N = nieuwe activiteit; C1 = gecontinueerd, ongewijzigd; C2 = gecontinueerd, gewijzigd)

Wat willen we bereiken	*Wat beloven we en wat gaan we doen*	*Huidige stand van zaken*		*Departement*
		Volgens Rijksbrede ICT agenda 2005-2006	Bevindingen TNO	
Communicatie-infrastructuren				
(A) Versterking positie gebruikers (bedrijven en consumenten) tegenover aanbieders van informatie- en communicatiediensten	1. 2005: Wijziging van de Telecommunicatiewet om de huidige consumentenbescherming uit te breiden van telefoniediensten naar andere elektronische communicatiediensten. (C1) - De wijziging biedt de mogelijkheid om additionele wettelijke garanties toe te voegen, onder meer inzake de mogelijkheid om aanbieders van elektronische communicatiediensten te verplichten zich te laten onderwerpen aan onafhankelijke geschillenbeslechting.		Zie onder 'OPTA', **[A1]**	EZ
(B) Overheid is voorbereid op de toenemende bedreigingen rond netwerken voor elektronische	1. 2005: verlenging van de noodvoorziening: in noodsituaties kan de overheid blijven communiceren (C1)	1. Er is werk gemaakt van de noodvoorziening, waardoor de overheid kan blijven communiceren in noodsituaties. In 2005 wordt deze voorziening	Op KPN rust de verplichting om het (gesloten) Nationale Noodnet tot 1 januari 2009 operationeel te houden. **[B1]**	EZ

communicatie		verlengd.		
(C) Ongewenste effecten bij faillissementen van telecomaanbieders of vitale dienstverlening voorkomen.		1. Er is een beleidsvoorstel geformuleerd om bij faillissement rond vitale infrastructuren ongewenste effecten voor gebruikers te voorkomen. 2. De beschikbaarheid van vitale telecommunicatie-diensten is geborgd in wet- en regelgeving als uitwerking van het beleid inzake NACOTEL.		EZ
De randvoorwaarden				
(D) De overheid is voorbereid op EZ de toenemende bedreigingen rond netwerken voor elektronische communicatie	1. 2005: presentatie actieplan terrorismebestrijding met maatregelen voor een betere bescherming van vitale communicatie-infrastructuren en -diensten. (C1) 2. 2005: afronding project bescherming vitale infrastructuren ICT-deel (C2) Borging in de reguliere organisatie: de vitale	2. Er is gewerkt aan het project bescherming vitale infrastructuren, ICT-deel	1. TK 29 754, nr. 5, 24, 60, 73: samenhangend stelsel maatregelen en beleid + halfjaarlijkse voortgangsrapportages 2. Het project Bescherming Vitale infrastructuren (BVI) is beëindigd met een	EZ

	ICT-sector is optimaal beschermd tegen bedreigingen 3. 2005: platform vitale ICT-bedrijven opgericht informatie-uitwisseling wordt geregeld (C2) 4. 2005: oprichting internationaal forum Critical Infrastructure Information Protection (CIIP) (N) Verbetering internationale afstemming op gebied van bescherming ICT		eindrapportage over alle 12 vitale sectoren. Het project is een structureel beleidsdossier geworden. **[D2]** 3. In 2006 is het Nationaal Platform Continuïteit Vitale ICT (kortweg Platform Vitaal) gestart in het kader van het Digibewust-programma. **[D3]** 4. TK 22112, nr. 422: Op 17 november 2005 is een Groenboek voor EPCIP (European Programme Critical Information Protection) gepubliceerd. Daarin wordt ook de oprichting van CIWIN (Critical Warning Information Network) voorgesteld	
(E) Continuïteit van vitale dienstverlening	1. 2005: actieve deelname aan European Network en Security Agency (ENISA) (C2)		1. Nederland levert actieve bijdrage in ENISA. Afgevaardigde van DGET is	EZ

	2. 2005: uitbreiden van de PPS Nationaal Continuïteitsplan Telecommunicatie (NACOTEL) in nationaal en in Europees verband: oefenen van gemaakte afspraken. (C2)		vertegenwoordigd in de Managementboard van ENISA. Daarnaast participeert Nederland in diverse werkgroepen 2. NACOTEL is geformaliseerd in het Nationaal Continuïeitsoverleg Telecommunicatie (NCO-T). Een van de doelen is om meer aanbieders bij het overleg te betrekken. Dat loopt nog. **[E2]**	
(F) Er is een voldoende basis voor vertrouwd en betrouwbaar elektronisch handelen		1. De Richtlijn Elektronische handel is geïmplementeerd. - Voorlichting aan consumenten via consumentenportaal www.staiksterk.nl: e-commerce vragen zijn hieraan toegevoegd. - Bij ECP.nl is een contactpunt ingericht voor	1. De Richtlijn is geïmplementeerd in mei 2004: Staatsblad 2004, nr. 210, Aanpassingswet richtlijn inzake elektronische handel - Sta Ik Sterk voor consumenten is opgegaan in de website www.consuwijzer.nl, het Gemeenschappelijk Informatieloket van de Consumentenautoriteit, NMA en OPTA.	EZ/Justitie

		vragen van burgers en bedrijven.	ConsuWijzer is het informatieloket voor consumenten van de overheid. Het is ontstaan uit een samenwerking tussen drie toezichthouders die onder het Ministerie van Economische Zaken vallen; de Consumentenautoriteit, de Nederlandse Mededingingsautoriteit (NMa) en de Onafhankelijke Post en Telecommunicatie Autoriteit (Opta).	
(G) Gebruikers moeten internet veilig en betrouwbaar vinden	1. 2005: continueren waarschuwingsdienst als onderdeel van GOVCERT, voor o.m. virussen (C1) 2. 2005: stimuleren beschikbaarheid beveiligingsproducten (project KWINT) (C1) 3. 2005: intensivering voorlichtingsprogramma	1. De Waarschuwingsdienst voor ondermeer virussen is gecontinueerd. 2. Programma KWINT is gecontinueerd en heeft producten opgeleverd over continuïteit en transparantie van internet. 3. Het programma ‘Surf	1. Waarschuwingsdienst is gecontinueerd. **[G1]** 2. Programma KWINT is eind 2005 beëindigd en voortgegaan in het programma Digibewust.**[G2]** 3. Surf op Safe heeft een	EZ

	Surf op Safe (C1)	op Safe' is bezig met een nieuwe brochure en andere voorlichtings-activiteiten. De activiteiten worden uitgebreid en er wordt meer eenheid aangebracht in de communicatie van 'Surf op Safe' en de Waarschuwingsdienst	aantal nieuwe brochures gepubliceerd over o.a. spam, dialers, phishing, spyware en zal binnenkort ook bij Digibewust worden ondergebracht. **[G3]**	
	4. 2005: actieve betrokkenheid bij het EU Safer Internet Plus programma (2005 – 2008) (N)		4. TK 30 303, nr. 1, TK 29 361, nr. 12: Onder Nederlands voorzitterschap van EU is verder politiek akkoord bereikt over Safer Internet Plus programma	
	5. 2005: uitvoeren lopend EU-project National Awareness Node op het gebeid van veilig internetten (C2)		5. In november 2004 heeft SurfopSafe een contract gesloten met de Europese Commissie voor een project onder het 'Safer Internet Action Plan'. Surf op Safe treedt op als 'National Awareness Node' op het gebied van veilig	

	6. 2005: Pilot en ontwikkeling Diploma Veilig Internet voor lagere scholen i.s.m. marktpartijen; afronding en borging (C1)	6. Het programma 'Surf op Safe' is bezig met een Diploma Internet Veilig Internetten	internetten. Het EU-project beoogt een betere coördinatie op het gebied van voorlichting over veilig internet, zowel binnen als tussen landen. Het coördinerende netwerk heet Insafe (www.saferinternet.org) 6. Diploma Veilig Internet is ontwikkeld door Technika 10 i.s.m. De Kinderconsument, Stichting ICT op school en Kennisnet in opdracht van EZ.	
(H) Elektronische communicatienetwerken vormen geen veilig domein voor activiteiten van criminelen	1. 2005: oprichten van een meldpunt voor o.a. e-fraude en cybercrime (N) 2. 2005: Project Cybercrime inbrengen in Actieplan veilig ondernemen II. 3. 2005: in het kader van nationaal Platform Criminaliteitsbeheersing (NPC) uitvoeren van het project Cybercrime (C2)	3. Inmiddels is voor de aanpak van cybercrime een publiekprivaat project gestart onder het Nationaal	1. Meldpunt Cybercrime is opgericht. 2. Het Project Cybercrime is ondergebracht bij AVO II. Doel is te komen tot een nationale infrastructuur ter bestrijding van cybercrime (NICC) **[H3]** 3. Nationaal Project Aanpak Cybercrime	EZ/Justitie/BZK

	4. 2005: project National High Tech Crime Centre (NHTCC) en besluitvorming rondom opzet (N)	Platform Criminaliteitsbestrijding.	(NPAC) is ondergebracht bij het Nationaal Platform Criminaliteitsbestrijding. Het project gaat over in het programma NICC **[H3]** 4. Het NHTCC is eind 2005 geëindigd. Het eindadvies over NPAC en het NHTCC hebben geresulteerd in het programma Nationale Infrastructuur Cybercrime (NICC). KLPD is bezig met het opzetten van een Team High Tech Crime **[H3]**	
(I) Criminelen kunnen elektronische communicatienetwerken niet misbruiken voor hun activiteiten	1. 2005: in de TK wordt een nota voor wijziging van het wetsvoorstel ingediend om het Wetboek van Strafrecht en het Wetboek van Strafvordering in overeenstemming te brengen met het Cybercrime Verdrag van de Europese Raad, evenals een wetsvoorstel voor goedkeuring van dat verdrag. (N)		1. Deze nota is ingediend. In 1999 werd het wetsvoorstel Computercriminaliteit II bij de Tweede Kamer ingediend, wat wijziging betekende voor het Wetboek van Strafrecht,	

			het Wetboek van Strafvordering, de Telecommunicatiewet en andere wetten. Het wetsvoorstel is tot op heden nog niet in werking getreden. Gewacht is op het Verdrag Cybercrime van de Raad van Europa. Recentelijk is een definitief voorstel van wet behandeld door de Eerste Kamer, waarin zowel aanpassingen van de wet als gevolg van het Cybercrime Verdrag als het wetsvoorstel Computercriminaliteit II zijn opgenomen.32 Hiermee zullen het Wetboek van Strafrecht, het Wetboek van Strafvordering, de Telecommunicatiewet en enige andere wetten worden gewijzigd.	

[32] Eerste Kamer, vergaderjaar 2005-2006, 26 671, A.

(J) Geen ongewenste commerciële communicatie op internet	1. 2005: wetswijziging opt-in regime ook voor zakelijke gebruikers (motie van Dam / Atsma) (C2) 2. 2005: nadere internationale afspraken (EU, VS, ITU, OESO etc.) (C2) 3. 2005: WSIS: inbreng Spam onder internet governance (C2) 4. 2005: voorlichting over spam en bescherming van de consument: (C2) - Uitgave spamfolder, website (zie ook 'Surf op Safe')	1. Besloten is dat het opt-in regime inzake SPAM ook gaat gelden voor zakelijke gebruikers. 2 en 3. Internationaal heeft de Nederlandse bijdrage in de strijd tegen SPAM verder vorm gekregen (EU, VS, ITU, OESO, WSIS) 4. Samen met ECP.NL is een gedragscode ontwikkeld die consumenten beschermt en bedrijven de mogelijkheid biedt om elektronische handelsreclame legaal te blijven gebruiken	Zie stuk 'OPTA'**[A1]**	
Inzet van ICT in semi-publieke domein				
(K) Betere publieke dienstverlening en beter presterende overheid met gebruik van ICT (Rijk, gemeente, provincies).	1. 2005-2007: uitbreiden van gemeenschappelijke authenticatievoorziening (DigiD)		1. DigiD heeft inmiddels 1.000.000 gebruikers. Met één authenticatiesysteem (inlognaam en password) kan van verschillende	BZK (i.s.m. EZ)

			overheidsdiensten gebruik worden gemaakt bij meer dan 60 gemeenten, Belastingdienst, Sociale Verzekeringsbank (SVB), Kadaster, UWV en Centrum voor Werk en Inkomen (CWI). DigiD is ondergebracht bij GBO.overheid.	

Annex III: Vragenlijst

VRAGEN

1. Welke activiteiten[33] op het gebied van ICT veiligheid onderneemt uw organisatie(onderdeel)? N.B. geef s.v.p. niet alleen een opsomming maar geef een korte omschrijving; uiteraard kan u ook een reeds bestaande omschrijving toevoegen.

2. Wat is globaal de omvang (in fte en budget) van deze activiteiten?

3. Wat is de geplande start en einddatum van deze activiteiten?

4. Wat is de rol (beleidsbepaler, toezichthouder, uitvoerder, aanjager, deskundige, interveniërend vanuit belang, …) van uw organisatie in deze activiteiten?

5. Waarom vervult uw organisatie deze rol (wettelijke basis, omdat we beleidsverantwoordelijk zijn voor…, in opdracht van…, …)?

6. Onder welke processtappen (zie bijlage) zou u deze activiteiten scharen?

7. Welke doelstellingen streeft uw organisatie met deze activiteiten na?

8. Welke problemen verwacht uw organisatie daarmee op te lossen of welke kansen verwacht uw organisatie te benutten?

9. Met wie (zowel binnen overheid als met intermediaire en private organisaties) werkt uw organisatie bij voorgaande activiteiten samen, of verwacht uw organisatie te gaan samenwerken? Geef hierbij s.v.p. ook de reden van samenwerking aan die u ziet.

10. Op welke wijze is (wil uw organisatie) deze samenwerking vorm gegeven?

11. Wat zou kunnen verbeteren bij uw eigen organisatie?

12. Wat zouden in het algemeen verbeterpunten kunnen zijn in het ICT veiligheidsbeleid van de overheid?

13. Welke andere voor ICT veiligheid relevante projecten lopen binnen uw organisatie die u hiervoor niet heeft benoemd, en wie is daarvan contactpersoon?

14. Wat wilt u verder nog kwijt dat niet bij de vorige vragen aan bod kwam?

[33] Dit kunnen zowel structurele activiteiten zijn als kortlopende projecten

BIJLAGE De volgende processtappen kunnen als onderdeel van het totale ICT veiligheidsproces worden onderscheiden[34].

1. *Proactie*
   Deze schakel bestaat enerzijds uit het bij de basis onderwijzen van gebruikers van ICT en internet over risico's en anderzijds bij de ontwikkeling en productie van hard- en software in voldoende mate rekening houden met het potentiële misbruik ervan.
2. *Preventie*
   Het gaat hierbij om de zorg voor adequate bescherming, middels virusbeschermers, firewalls, product-updates e.d.
3. *Preparatie*
   Ondanks de toepassing van proactie en preventie moet men wel voorbereid zijn op een mogelijke aanvallen. Preparatieactiviteiten voorzien daarin.
4. *Signalering*
   Er worden drie vormen van signalering onderscheiden:
   a. melding: iemand belt, mailt of anderszins en geeft aan de ontvangende instantie aan wat het probleem is (een melding kan uit het buitenland komen, van een bank, een bedrijf etc.);
   b. aangifte: iemand heeft schade geleden en doet aangifte bij de politie;
   c. detectie: er is geen melding noch een aangifte, maar er wordt via monitoringssystemen vastgesteld dat er iets aan de hand is.
5. *Opvolging*
   De verschillende manieren waarop een signaal binnenkomt, zijn ook bepalend voor de opvolging. Zes verschillende opvolgingsvarianten worden onderscheiden:
   a. opsporing/vervolging/berechting: een aangifte is al een opsporingsverzoek, maar ook een melding kan een aangifte worden, en politie/OM kunnen besluiten om ambtshalve op te sporen;
   b. stop-actie: het signaal kan aanleiding zijn voor het ondernemen van een stop-actie als samenwerkingsactie van verschillende nationale en/of internationale partijen;
   c. civiele actie: er kan een civiele claim worden gelegd;
   d. waarschuwing: het signaal kan in de vorm van een voorlichtingsproduct worden rond gestuurd;
   e. advies: er kunnen preventie- en (p)reparatie adviezen worden uitgebracht aan bijvoorbeeld netwerkbeheerders en het grote publiek, maar ook beleidsadviezen aan departementen;
   f. ontwikkeling: het signaal kan aanleiding zijn voor het ontwikkelen van bepaalde producten, procedures of organisatievormen.
6. *Terugkoppeling*
   Iedere opvolging kan een terugkoppeling inhouden naar de oorspronkelijke melder/aangever of anderen, opdat zij gemotiveerd blijven om meldingen door te geven. Terugkoppeling is eigenlijk geen afzonderlijke stap, maar loopt dwars door alle stappen heen. Niet alleen het kunnen volgen van de voortgang van een proces is van belang, maar vooral ook wat het tot dan heeft opgeleverd.
7. *Resultaat*

[34] Uit: Ontwerp 'Nationale Infrastructuur Bestrijding Cybercrime', januari 2006

Het resultaat bestaat uit hetgeen de keten uiteindelijk oplevert in termen van: schadevoorkoming of schadereductie, de mate waarin een doelgroep is bereikt, of een site uit de lucht gehaald, of daders zijn veroordeeld, of er door anti-virussoftware leveranciers een instrument is ontwikkeld, of er gaten in software zijn gedicht etc.

8. *Evaluatie*
   In feite is dit een bijzondere vorm van terugkoppeling. Er wordt niet alleen vastgesteld wat er is bereikt maar ook of dat op de juiste wijze is geschiedt. Heeft het proces efficiënt plaatsgevonden, is het resultaat duurzaam, en of het resultaat voldoende is in het licht van generale- of specifieke preventie.
9. *Nazorg*
   Het resultaat wordt tijdens de nazorg in het perspectief van de toekomst geplaatst. Aan de orde is hoe belangrijke zaken onder de aandacht kunnen blijven, de herhalingsfrequentie van bepaalde activiteiten, en hoe men zaken voor kan zijn.
10. *Toezicht*
    De uiteindelijke nacontrole van alle activiteiten vormt het sluitstuk, zodat betrokken partijen er op kunnen vertrouwen dat een ieder zijn of haar steentje bijdraagt. Te denken valt hierbij aan visitaties, audits, en scans.

Referenties

Dossier ICT, 26 643
TK 2000-2001 26 643, Nr. 26 Brief van de minister voor Grote Steden- en Integratiebeleid aan de Voorzitter van de Tweede Kamer der Staten-Generaal (23 maart 2001). Inhoud: over plan van aanpak virusproblematiek & informatiebeveiliging overheid

TK 2000-2001 26643, Nr 30, brief van de Staatssecretaris van Verkeer en Waterstaat aan de Voorzitter van de Tweede Kamer der Staten-Generaal (9 juli 2001). Inhoud: over Nota Kwetsbaarheid op internet (KWINT), de uitwerking van een in De Digitale Delta toegezegde verkenning naar de kwetsbaarheden op internet.

TK 2003-2004, 26 643, Nr. 46. Brief van de minister van EZ aan de Voorzitter van de Tweede Kamer der Staten-Generaal (2 februari 2004). Inhoud: visie spamproblematiek 2004-2005

TK 2003-2004, 26 643, Nr. 47 brief van de ministers van EZ en voor BZK en de staatssecretaris van OC&W aan de Voorzitter van de Tweede Kamer der Staten-Generaal (23 februari 2004). Inhoud: nieuwe ICT-agenda

TK 2003-2004, 26 643, Nr. 48 Brief van de minister van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal (19 maart 2004). Inhoud: rapportage stand van zaken en vervolg project Bescherming Vitale Infrastructuur

TK 2003-2004, 26 643 Nr. 52. Verslag van een algemeen overleg, vastgesteld 9 april 2004 (vaste commissie voor Economische Zaken over beleidsvisie SPAM

TK 2003-2004, 26 643 Nr. 56.Brief van de minister van BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal (9 juli 2004). Inhoud: rapportage Bescherming Vitale Infrastructuur

TK 2003-2004, 26 643, Nr. 61. Brief van de minister van EZ aan de Voorzitter van de Tweede Kamer der Staten-Generaal (20 december 2004). Inhoud: rapportage handhaving opt-in regime voor ongevraagde communicatie

TK 2004-2005, 26 643, Nr. 75. Brief betreffende inhoudelijke analyse van de bescherming van de vitale infrastructuur in Nederland (project BVI, BZK)

Dossier Beleidsplan Crisisbeheersing 2004–2007, 29 668
TK 2003–2004, 29 668, nr. 1. Uitvoering van het beleidsplan Crisisbeheersing

TK 2005-2006, 29 668 Nr. 8. Beleidsplan Crisisbeheersing 2004–2007. Brief van de minister van BZK aan de voorzitter van de Tweede Kamer der Staten-Generaal (30 januari 2006). Inhoud: eerste voortgangsrapportage

Dossier Terrorismebestrijding, 29 754
TK 2004-2005 29 754 Nr. 5 Brief van de ministers van Justitie en BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal (24 januari)

TK 2004-2005 29 754 Nr. 24 Brief van de ministers van Justitie en BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal. Inhoud: Tweede voortgangsrapportage (10 juni)

TK 2004-2005, Nr. 60. Brief van de ministers van Justitie en BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal (5 december 2005)

TK 2005-2006, Nr. 73. Brief van de ministers van Justitie en BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal (7 juni 2006). Inhoud: vierde voortgangsrapportage terrorismebestrijding.

Dossier Beheersing informatiebeveiliging, 24 175
TK 1994-1995, 24 175, Nr. 1. Beheersing informatiebeveiliging. Brief van de Algemene Rekenkamer aan de Voorzitter van de Tweede Kamer der Staten-Generaal (23 mei 1995)

Dossier Computer criminaliteit II, 26 671
TK 1998-1999, 26 671 Nr.3. Memorie van Toelichting. Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II)

TK 2004-2005, 26 671, Nr. 7. Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en de Telecommunicatiewet in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) Tweede nota van wijziging (ontvangen 22 maart 2005)

TK 2005-2006, 26 671 Nr. 24. Wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II). Brief van de staatssecretaris van EZ aan de Voorzitter van de Tweede Kamer der Staten-Generaal (18 mei 2006). Inhoud: eindadvies project National High Tech Crime Center (NHTCC) en het NPC project Aanpak Cybercrime (NPAC)

Dossier Nieuwe Commissievoorstellen en initiatieven van de lidstaten van de Europese Unie, 22 112
Groenboek Europees Programma voor de bescherming van vitale infrastructuur

TK 2005-2006, 22 112, Nr. 422. Brief Minister BZK aan de Voorzitter van de Tweede Kamer der Staten-Generaal betreffende een Europees Programma voor de bescherming van vitale infradtructuur (EPCIP) (7 februari 2006)

TK 2005-2006, 22 112, Nr. 435. Verslag schriftelijk overleg Vaste commissie BZK (vastgesteld 26 april 2006). Inhoud: kabinetsstandpunt op het groenboek van de Europese Commissie inzake een Europees Programma voor de bescherming van de vitale infrastructuur (EPCIP)

Dossier Deelnemingenbeleid Rijksoverheid, 28 165
TK 2003-2004 28 165 Nr. 14 Brief over rol overheid bij faillissement telecommicatieaanbieder (12 maart)

Dossier Staat van de Europese Unie 2005-2006, 30 303
TK 2005-2006 30 303 Nr. 1 Brief minister en staatssecretaris Buitenlandse Zaken met de 'Staat van de Europese Unie 2005-2006' (20 september)

Dossier Nederlands EU-voorzitterschap 2004, 29 361
TK 2004-2005 29 361 Nr. 12 Brief minister en staatssecretaris Economische Zaken over wat er in de tweede helft van 2004 is bereikt op het terrein van Economische Zaken (19 januari)

Overige
Besluit voorschrift informatiebeveiliging rijksdienst – bijzondere Informatie, 24 februari 2004/Nr. 04M464166

Dutch Ministry of Economic Affairs (2004) Dutch answers to the OECD Questionnaire on Practical initiatives to promote a culture of security As called for in the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. DSTI/ICCP/REG(2004)4/FINAL. (Prepared by TNO)

KWINT (2004) Veilig zakelijk internetten: Hoe help ik mijn organisatie verbeteren?

KWINT (2004) Veilig internetten voor iedereen

Mac Gillavry, E.C. (2006), Concept Projectplan informatieknooppunt, NICC-Programma, Ministerie van Economische Zaken (DGET).

Minister van Binnenlandse Zaken en Koninkrijksrelaties (2006), Besluit instelling van het Strategisch Overleg Vitale Infrastructuur (SOVI, Staatscourant 19 april 2006.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2006), Ontwikkeling profiel Nationaal Adviescentrum Vitale Infrastructuren (NAVI) - Voor de bescherming tegen moedwillige verstoring – Projectplan.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2006), Algemene toelichting op de capaciteitenbenadering (capabilities based planning –CBP).

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2005), Rapport bescherming vitale infrastructuren.

Ministerie van Economische Zaken (2006), NICC - Nationale Infrastructuur Cybercrime, programmaplan.

Ministerie van Economische Zaken (2004) Telecomraad wil veiliger internet en minder spam: URL: http://www.ez.nl/content.jsp?objectid=28656

Project Nationale Veiligheid (2006), Geïntegreerde rapportage interdepartementale zelfevaluatie – Digitale veralmming (intern werkdocument).

Staatsblad van het Koninkrijk der Nederlanden Jaargang 2004, 210. Inwerkingtreding Aanpassingswet richtlijn inzake elektronische handel (13 mei), geïmplementeerd in Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten.

Staatsblad van het Koninkrijk der Nederlanden Jaargang 2004, 308. Beschikking van de Minister van Justitie van 30 juni 2004, houdende plaatsing in het Staatsblad van de tekst van de Telecommunicatiewet, zoals deze luidt met ingang van 19 mei 2004

Ministerie van Economische Zaken (2005), Veilige Elektronische Communicatie (VEC) – Digibewust.

Ingevulde vragenlijsten

Agentschap Telecom
AIVD
BZK/DGMOS/IIOS
BZK/DGV/S
BZK/DGV/POL
BVI
BVI/VISTIC
Digibewust
DigiD, PKI, eNIK
ECP.nl
EZ/DGET
GOVCERT.nl
H11 Telecomwet
Nationale Veiligheid
NAVI
NCO-T
NICC
OPTA
TTP-beleid
Waarschuwingsdienst

Websites

www.digibewust.nl
www.ecp.nl – Platform voor e-Nederland
www.gbo.overheid.nl
www.govcert.nl
www.minbzk.nl – Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
www.minez.nl – Ministerie van Economische Zaken
www.minjus.nl – Ministerie van Justitie
www.nctb.nl
www.opta.nl
www.waarschuwingsdienst.nl