Project Nationale Veiligheid

Geïntegreerde rapportage interdepartementale zelfevaluatie

Digitale verlamming

Intern werkdocument

Datum: 16-05-2006

Inhoudsopgave

Voorwoord

De status van deze rapportage is een intern werkdocument. De rapportage beschrijft de resultaten van een inventariserend onderzoek naar

1. blinde vlekken in het beleid gericht op het inperken en/of voorkomen van digitale verlamming
2. knelpunten in het interdepartementale beleidsproces dat ten behoeve hiervan wordt ingezet.

De resultaten geven een overzicht van de visies van de betrokken departementen m.b.t. de blinde vlekken en knelpunten. Nadrukkelijk dient hierbij vermeld te worden dat de resultaten soms gebaseerd zijn op de visie van één departement en nog geen gemeenschappelijk beeld weergeven. De rapportage bevat daarom kansen en mogelijkheden voor het versterken van het proactieve beleid.

De komende periode zal in het kader van het project geïnventariseerd worden welke kansen en mogelijkheden voor het versterken van het proactieve beleid opgepakt gaan worden, door wie en hoe. Daarnaast worden de resultaten van het onderzoek gebruikt als bouwstenen bij de ontwikkeling van een strategie voor de Nationale Veiligheid.

De geïntegreerde rapportage is opgesteld op basis van een aantal departementale zelfevaluaties en collegiale toetsen. In bijlage 1 treft u een overzicht welke departementen hebben bijgedragen aan het onderzoek.
De rapportage wordt niet gepubliceerd. Wel kan deze als intern werkdocument worden aangevraagd door de medewerkers van de departementen die betrokken zijn bij dit vervolgtraject en/of hebben bijgedragen aan het onderzoek. Aanvragen kunt u sturen aan het secretariaat van het Project Nationale Veiligheid.

Meer informatie over het onderzoek is opgenomen in een informatiebrochure met als titel: “Project Nationale Veiligheid: Achtergrondinformatie bij de interdepartementale zelfevaluatie en collegiale toets”. Ook deze brochure kunt u aanvragen bij het secretariaat van het Project Nationale Veiligheid.

Secretariaat Project Nationale Veiligheid
Mw. A. de Jong-Tokman
Fluwelen Burgwal 56
Postbus 20011
2500 EA Den Haag

070-426 6699
Anna.Jong@minbzk.nl

1. Inleiding

Tot een paar jaar geleden waren binnenlandse en buitenlandse veiligheid twee heel verschillende dimensies van hetzelfde thema.[1] In de afgelopen periode is ons land echter geconfronteerd met een aantal dreigingen, hetgeen duidelijk heeft gemaakt dat sprake is van een toenemende verwevenheid tussen binnen- en buitenlandse veiligheid. Hierbij kan worden gedacht aan de opkomst van het internationale terrorisme, de verspreiding van CBRN-wapens, pandemieën, klimaatverandering en afnemende energievoorzieningszekerheid. Globalisering – onder andere in de vorm van open grenzen en vervaging van de betekenis van plaats en tijd – heeft ertoe geleid dat buitenlands veiligheidsbeleid meer dan ooit van invloed is op de binnenlandse veiligheid, terwijl het omgekeerde ook het geval is. Tegen deze achtergrond is de begripsvorming rondom 'nationale veiligheid' op gang gekomen.

Naar aanleiding van enkele vooronderzoeken waaruit is gebleken dat het beleid op het gebied van nationale veiligheid te repressief is, ad hoc en gefragmenteerd, heeft een stuurgroep Nationale Veiligheid besloten een vervolgonderzoek in te stellen waarbij interdepartementaal en proactief beleid centraal staan.

Als uitgangspunt voor dit onderzoek (het aggregatieniveau) gelden negen dreigingen met daaraan gekoppelde incidentcategorieën. Hieronder volgt een overzicht van deze dreigingen met bijbehorende incidentcategorieën.

Klassieke dreigingen	**Incidentcategorieën**
1. Aantasting van de internationale vrede en veiligheid	• Falende staten • Risicolanden
2. CBRN	• Verspreiding van CBRN-wapens (proliferatie)
3. Terrorisme	• Catastrofaal terrorisme • Radicalisering
4. Internationaal georganiseerde criminaliteit	• Toenemende verwevenheid onder- en bovenwereld • Wereldwijde handel in drugs
Sociaal-economische dreigingen	**Incidentcategorieën**
5. Sociale kwetsbaarheid	• Toenemende (interetnische) spanningen en afnemend burgerschap
6. Digitale onveiligheid	• Digitale verlamming
7. Economische onveiligheid	• Aantasting van de sociale zekerheid • Extreme schaarste van energiedragers en grondstoffen
Natuurlijke dreigingen	**Incidentcategorieën**
8. Klimaatverandering en natuurrampen	• Toenemend overstromingsrisico • Toenemende kans op extreme droogte/hitte • Plaagorganismen
9. Pandemieën	• Pandemieën van reeds bekende ziekten • Zoönosen

[1] Zie ook de Wijk & Toxopeus, Hoe binnen- en buitenlandse veiligheid verweven zijn, in: *Internationale Spectator*, 2005

Het onderzoek heeft het karakter van een zelfevaluatie met daarop volgend een collegiale toets. Het onderzoek is concreet gericht op:

1. ‘het identificeren van blinde vlekken in het op proactie gerichte beleid ten aanzien van de gekozen incidentcategorieën
2. het achterhalen van knelpunten in het interdepartementale beleidsproces dat ten behoeve hiervan wordt ingezet
3. het creëren van inzicht in de wijze waarop met deze blinde vlekken en knelpunten kan worden omgegaan.

De voorliggende geïntegreerde rapportage heeft betrekking op de incidentcategorie ‘digitale verlamming’ en is het resultaat van drie departementale zelfanalyses en enkele collegiale toetsen. De zelfanalyses zijn verricht door de Ministeries van EZ, Defensie en BZK (zie bijlage 2 voor een totaaloverzicht van zelfevaluaties en collegiale toetsen). Van de departementale zelfanalyses zijn separaat rapportages beschikbaar.

Leeswijzer

De voorliggende rapportage is als volgt opgebouwd:

- in hoofdstuk 2 wordt ingegaan op de omschrijving van de incidentcategorie ‘digitale verlamming’
- in hoofdstuk 3 wordt uiteengezet welke beleidsactiviteiten worden uitgevoerd en welke interdepartementale samenwerkingsrelaties aanwezig zijn
- in hoofdstuk 4 wordt beschreven welke blinde vlekken in het beleid aanwezig zijn, welke knelpunten zich in het beleidsproces voordoen en welke behoeften/ambities de betrokken ministeries hebben als het gaat om deze incidentcategorie
- in hoofdstuk 5 wordt een conclusie gepresenteerd.

De rapportage wordt afgerond met twee bijlagen:

- in bijlage 1 wordt een overzicht weergegeven van de betrokken ministeries en de aard van hun bijdrage aan dit onderzoek
- in bijlage 2 staat een overzicht weergegeven van de activiteiten van de ministeries.

2. Omschrijving incidentcategorie

In dit hoofdstuk wordt aandacht besteed aan de omschrijving van de incidentcategorie ‘digitale verlamming’. Daarnaast wordt stilgestaan bij enkele opmerkingen vooraf. Beide paragrafen kunnen worden gezien als de achtergrond waartegen de resultaten van het onderzoek moeten worden beschouwd.

2.1 Digitale verlamming [2]

Onze samenleving is inmiddels zó afhankelijk geworden van ICT, dat digitale verlamming zou leiden tot maatschappelijke ontwrichting. Het betalingsverkeer, de waterkering, onze strijdkrachten, crisisbeheersing, sociale zekerheid, het openbaar bestuur, dit zijn slechts enkele van de vele mogelijke voorbeelden van sectoren die niet meer zonder ICT zouden kunnen functioneren.
Tegelijk zien we dat onze ICT-huishouding in toenemende mate wordt bedreigd door vormen van cyberterrorisme en cybercriminaliteit. Voor het plegen van deze vormen van criminaliteit kunnen virussen en wormen verspreid worden binnen ICT. Feit is dat ICT als target gebruikt kan worden om criminaliteit te plegen, maar ook als middel om criminaliteit te plegen. Deze ontwikkelingen tezamen maken dat onze maatschappelijke kwetsbaarheid met betrekking tot digitale verlamming vergroot is. Belangrijk is hierbij ook op te merken dat voor feitelijke maatschappelijke ontwrichting het moet gaat om verstoringen door digitale verlamming die een langdurig karakter hebben.

2.2 Opmerkingen vooraf

Het Ministerie van BZK is samen met het Ministerie van Justitie verantwoordelijk voor het veiligheidsbeleid. Dat beleid omvat crises- en rampenbeheersing, waaronder Bescherming vitale infrastructuur (BVI). Het Ministerie van BZK als coördinerend Ministerie op het gebied van BVI is belast met de coördinatie, monitoring en toetsing van het totaal. Ook is het Ministerie aanspreekbaar op de sectoroverstijgende maatregelen en op een blijvende samenhang van het totale pakket van beschermingsmaatregelen.

Als het gaat om de incidentcategorie ‘digitale verlamming’, dan is het Ministerie van EZ verantwoordelijk voor het treffen van maatregelen ter bescherming van de openbare ICT-infrastructuur. Het Ministerie van BZK is primair verantwoordelijk voor bescherming van de gesloten ICT-infrastructuur van de publieke sector. Het bedrijfsleven is zelf verantwoordelijk voor de gesloten infrastructuur die zij heeft aangelegd. Bedrijven als Shell, KLM, banken laten voor eigen gebruik een infrastructuur aanleggen voor hun eigen systemen. Het Ministerie van EZ heeft wel een verantwoordelijkheid als het gaat om bedrijven die diensten aanbieden aan een ieder, aangezien het dan als de openbare infrastructuur wordt beschouwd (bijvoorbeeld KPN dat diensten aanbiedt aan bedrijven, overheden en consumenten).
Maatregelen die het Ministerie van BZK heeft genomen zijn gericht op de dagelijkse praktijk van veiligheid en de beveiliging van ICT binnen de rijksoverheid en de medeoverheden.

[2] Deze tekst is zowel gebaseerd op het voortraject dat in het kader van het project Nationale Veiligheid is doorlopen als op de sessies (zelfevaluaties) die in het kader van ronde 1 hebben plaatsgevonden.

Het beleid is gericht op het tegengaan van verstoringen van ICT-systemen binnen de overheid, die zowel van binnen als van buiten bedreigd kunnen worden. In het Voorschrift Informatiebeveiliging Rijksdienst (VIR 1994) is geregeld dat departementen zelf integrale verantwoordelijkheid dragen. Dit pakket is niet direct gericht op het tegengaan van ‘digitale verlamming’ op nationale schaal.

Vanzelfsprekend hebben de AIVD en opsporingsinstanties een belangrijke taak om signalen te achterhalen als (groepen van) personen proberen publieke en private organisaties via ICT te treffen.

3. Beleidsproces en beleidsinhoud op hoofdlijnen

In dit hoofdstuk wordt een overzicht gegeven van de interdepartementale samenwerking in het kader van het inperken en/of voorkomen van digitale verlamming. Daarnaast wordt ingegaan op de beleidsactiviteiten die een proactieve uitwerking hebben op het inperken en/of voorkomen van digitale verlamming en op de mate waarin deze activiteiten voortvloeien uit vastgesteld interdepartementaal beleid. De zelfanalyses van de Ministeries van EZ, BZK en Defensie hebben voor deze drie onderdelen als input gediend.

Het hoofdstuk is als volgt opgebouwd:

- in paragraaf 1 wordt een overzicht gegeven van het interdepartementale beleidsnetwerk dat bij het inperken en/of voorkomen van digitale verlamming betrokken is
- in paragraaf 2 wordt op hoofdlijnen ingegaan op de beleidsactiviteiten die proactief uitwerken op het inperken en/of voorkomen van digitale verlamming
- in paragraaf 3 wordt aangegeven in welke mate er vastgesteld interdepartementaal beleid aanwezig is dat richting geeft aan de beleidsactiviteiten en de samenwerking.

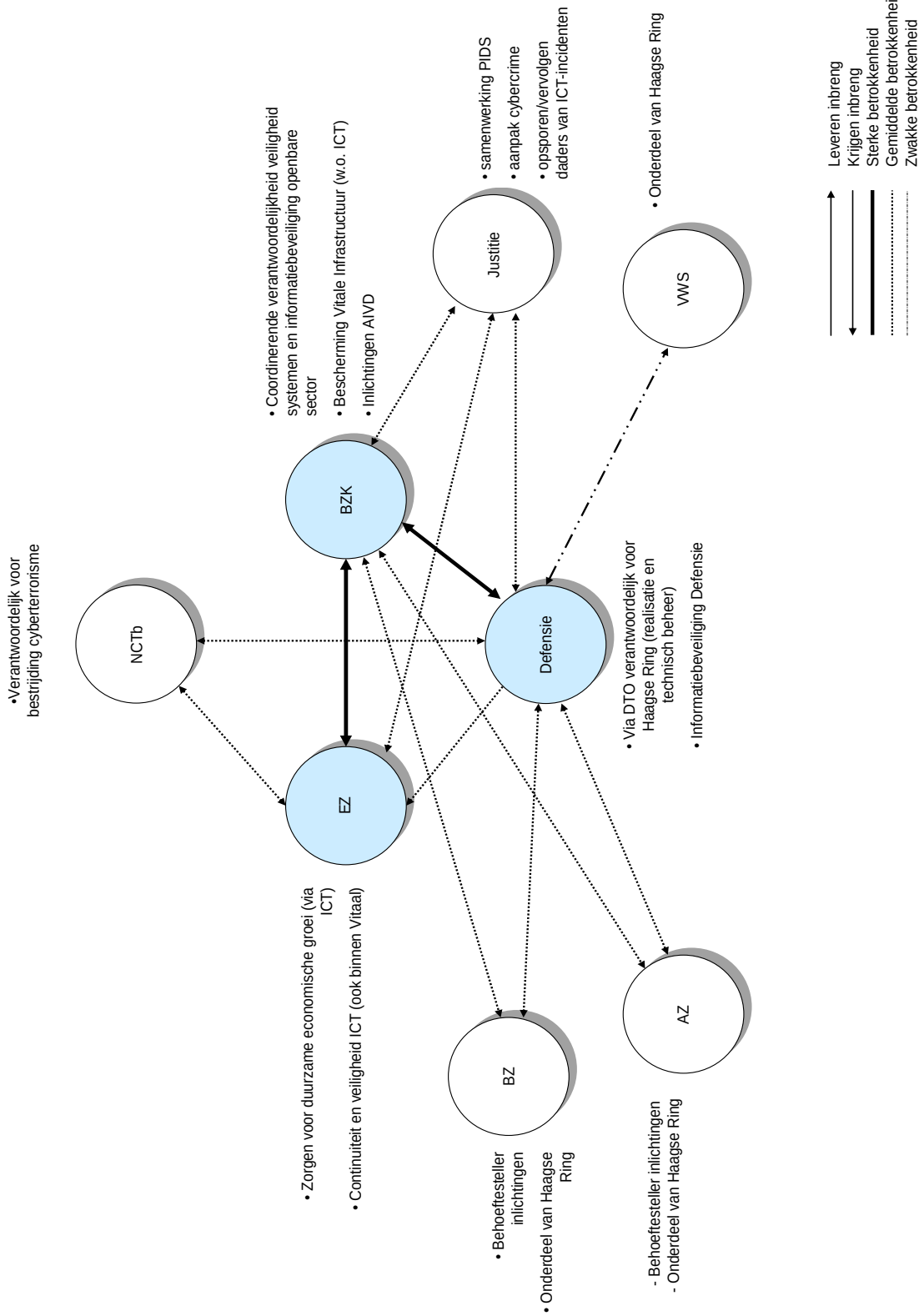
3.1. Beleidsnetwerk (proces) op hoofdlijnen

Het inperken en/of voorkomen van digitale verlamming is geen opgave die door één Ministerie succesvol volbracht kan worden. Er werken daarom verschillende ministeries vanuit uiteenlopende rollen samen aan het proactieve beleid. In deze paragraaf wordt in beeld gebracht hoe deze samenwerking er vanuit het perspectief van de Ministeries van EZ, BZK, Defensie en BZ uitziet. Het gaat dan om de vraag welke ministeries vanuit welke rol betrokken zijn bij het inperken/voorkomen van digitale verlamming.

Rollen in beeld

In figuur 1 wordt weergegeven hoe de ministeries de huidige inter-departementale samenwerking zien. De ‘gekleurde’ ministeries zijn de ministeries die de zelfevaluatie hebben uitgevoerd en dus de kans hebben gehad de interdepartementale samenwerking te beschrijven.

Figuur 1. Interdepartementale samenwerking in het kader van het inperken en/of voorkomen van digitale verlamming



Beschrijving interdepartementale samenwerking

De kern van het beleidsnetwerk rondom het inperken en/of voorkomen van digitale verlamming wordt gevormd door de Ministeries van EZ, Defensie en BZK.

Wanneer wordt gekeken naar de intensiteit en inhoud van de betrekkingen die het Ministerie van EZ onderhoudt rondom het inperken en/of voorkomen van digitale verlamming, dan valt op dat de relatie met het Ministerie van BZK het meest intensief en inhoudelijk van grote betekenis is. Voor een deel is deze samenwerking gericht op het bestrijden van de gevolgen van digitale verlamming (bijvoorbeeld in het kader van het project Vitaal), terwijl een ander deel betrekking heeft op het inperken en/of voorkomen van digitale verlamming. Dit laatste deel komt ook voort uit de verantwoordelijkheid die het Ministerie van BZK heeft ten aanzien van het beschermen van de overheid als gebruiker van ICT. Ook met het Ministerie van Justitie wordt (weliswaar in mindere mate en vooral in het kader van projecten rondom cybercrime en ten behoeve van de Herijking van het ICT-Veiligheidsbeleid) intensief samengewerkt. Met het Ministerie van BZ en (het bureau van) de Nationaal Coördinator Terrorismebestrijding (NCTb) wordt minder frequent en meer ad hoc afgestemd over specifieke onderwerpen die binnen de competentie van het betreffende Ministerie vallen. Met het Ministerie van BZ wordt gesproken over de Nederlandse inbreng in internationaal verband, terwijl de NCTb in beeld komt als het gaat om terroristische daden gericht op digitale verlamming.

Vanuit het Ministerie van BZK geldt dat waar het digitale verlamming in algemene zin betreft, vooral het Ministerie van EZ een belangrijke samenwerkingspartner is van het Ministerie van BZK. Het Ministerie van EZ heeft een zelfstandige verantwoordelijkheid wanneer het gaat om het inperken en/of voorkomen van digitale verlamming. De laatste jaren is het Ministerie van BZK hier in toenemende mate betrokken bij geraakt, mede als gevolg van het beleidsplan Crisisbeheersing en het project Vitaal. De samenwerkingsrelatie tussen beide ministeries is dan ook vrij intensief en inhoudelijk van relatief grote betekenis. Alle ministeries zijn betrokken bij het overleg over informatie- en ICT-beveiliging op het niveau van de rijksoverheid. De Ministeries van BZK en Defensie, in het kader van het realiseren van de ‘Haagse Ring’, hebben hierin een belangrijke rol, mede omdat ook de AIVD een rol speelt in het kader van de zogenaamde beveiligingsbevordering bij andere ministeries.

Wanneer wordt gekeken naar de intensiteit en inhoud van de betrekkingen die het Ministerie van Defensie onderhoudt rondom het inperken en/of voorkomen van digitale verlamming, dan valt op dat er vooral intensief wordt samengewerkt met het Ministerie van BZK. Een aantal departementen hebben een meer algemene betekenis (Ministeries van AZ, BZ en EZ) voor het Ministerie van Defensie en een aantal departementen hebben een meer specifieke betekenis voor bepaalde deelaspecten rondom digitale verlamming (Ministeries van Justitie, VROM en het NCTb).

3.2 Beleidsactiviteiten op hoofdlijnen

In deze paragraaf wordt ingegaan op de verhouding tussen internationaal en nationaal beleid (paragraaf 3.2.1) en op de beleidsactiviteiten die door de ministeries van namen ministeries worden verricht in het kader van het inperken en/of voorkomen van digitale verlamming (paragraaf 3.2.2).

3.2.1 Verhouding internationaal - nationaal

ICT kan worden gezien als een belangrijk middel om duurzame economische groei te bereiken. Het woord duurzaam verwijst naar de borging van ecologische en sociale aspecten. In het kader van ICT is vooral het vertrouwen dat gebruikers hebben in de technologie essentieel. Dit maakt dat continuïteit en veiligheid van ICT van groot belang zijn. Het Ministerie van EZ is verantwoordelijk voor het (zoveel als mogelijk) garanderen van continuïteit en veiligheid. Vanuit Europa wordt binnen het 2010-programma een klein deel gericht op veilig ICT-gebruik. Op 1 juni 2005 heeft de Commissie het initiatief 2010 (de Europese informatiemaatschappij van 2010) goedgekeurd, dat gericht is op ondersteuning van groei en werkgelegenheid in de informatiemaatschappij en de media. Het gaat om een algemene strategie voor modernisering en toepassing van alle instrumenten die de Europese Unie ter beschikking staan om de ontwikkeling van de digitale economie te stimuleren: regelgeving, onderzoek en partnerschappen met de particuliere sector. De Commissie zal daarbij ook met name de ontwikkeling van veilige breedbandnetwerken met rijke en gevarieerde inhoud in Europa ondersteunen. De veiligheid van ICT kan niet alleen binnen de landsgrenzen worden opgelost. Derhalve is de EC gestart met het agentschap voor netwerk- en informatiebeveiliging (ENISA). Daarnaast wordt ook in internationaal verband gewerkt aan veiligheid van ICT via ondermeer het Safer Internet Program. [3]

Het voorkomen en/of tegengaan van digitale verlamming is door het karakter van internet bij uitstek een domein dat in internationaal verband aandacht behoeft. Door defensie is opgemerkt dat zowel de noodzakelijke infrastructuur om digitale verlamming te veroorzaken overal ter wereld kan staan en makkelijk vervangbaar is en bovendien ook groepen/individuen die digitale verlamming willen veroorzaken zich snel kunnen verplaatsen in diverse landen. Op international vlak hebben diverse landen afspraken gemaakt over wederzijdse juridische steunverdragen, uitlevering, het delen van inlichtingen en de uniformering van de wetten op computercriminaliteit. Deze afspraken moeten het mogelijk maken cybercriminelen op te sporen en te vervolgen zelfs wanneer hun misdaden internationale grenzen overschrijden.

3.2.2 Beleidsactiviteiten [4]

Om de beleidsactiviteiten inzichtelijk te maken, is een indeling gemaakt in verschillende fasen van het beleidsproces:

- de fase van beleidsvoorbereiding waarin kennis en informatie over de achtergronden bij digitale verlamming wordt verzameld (onderzoek) en de fase waar in kaart wordt gebracht wat de aard en de omvang van digitale verlamming is (risicoanalyses)
- de fase beleidsontwikkeling die gericht op het ontwikkelen van acties, standpunten, e.a. die bijdragen aan het inperken en/of voorkomen van digitale verlamming
- de fase beleidsuitvoering waarin uitvoering wordt gegeven aan wat ontwikkeld is in het kader van het inperken en/of voorkomen van digitale verlamming
- de fase beleidsevaluatie waarin wordt gekeken naar de resultaten/effecten van het beleid met betrekking tot het inperken en/of voorkomen van digitale verlamming.

---

[3] zie www.minez.nl

[4] In bijlage 2 vindt u een opsomming van de beleidsactiviteiten die door de Ministeries van EZ, BZK en Defensie worden uitgevoerd in het kader van het inperken en/of voorkomen van digitale verlamming.

Onderzoek en risicoanalyses

Het Ministerie van EZ geeft aan dat TNO een doelfinanciering ontvangt voor het verrichten van onderzoek. Een van de onderdelen uit het onderzoeksprogramma is gericht op aspecten van digitale verlamming. Daarnaast heeft TNO onderzoek gedaan naar de kwetsbaarheden van het internet en zijn ze betrokken geweest bij een quick scan naar vitale, afhankelijke infrastructuren in Nederland. Daarnaast ondersteunt Het Ministerie van EZ (financieel) het Sentinels-onderzoeksprogramma. Het doel van het Sentinels-onderzoeksprogramma is om alle soorten informatiesystemen en netwerken veiliger te maken. Hieronder vallen zowel de standaard systemen zoals pc's en netwerken, alsook hand-held-devices, embedded systemen en draadloze en on-chip netwerken.

Het Ministerie van Defensie doet in het kader van uiteenlopende taken (beheersen zeegebied/grondgebied, commandovoeringsoperaties) onderzoek naar de mogelijkheden om de informatie zo goed als mogelijk te beveiligen en tools beschikbaar te hebben voor detectie. Voor defensie is het voor het eigen optreden belangrijk dat de afhankelijkheden van de informatievoorziening (en de onderliggende structuur) zoveel als mogelijk verspreid worden. Met behulp van TNO wordt via onderzoek de robuustheid ICT-infrastructuur van Defensie getoetst.

In het kader van het project Vitaal (bescherming van de vitale infrastructuur) en het Nationaal Continuïteitsplan Telecommunicatie (NACOTEL) worden analyses verricht naar kwetsbaarheden van ICT. Dit vormt ook een belangrijke basis voor het uitvoeren van beschermende maatregelen. Voor wat betreft het project Vitaal bevordert het Ministerie van BZK de interdepartementale afstemming en het Ministerie van EZ verricht de inhoudelijke analyse van ICT-kwetsbaarheid. Binnen de VIR (Voorschrift Informatiebeveiliging Rijksoverheid) is het voor de departementen een verplichting om afhankelijks- en kwetsbaarheidsanalyses uit te voeren.
Door de AIVD en de MIVD worden risicoanalyses verricht ten aanzien van personen/groepen en objecten, die eventueel digitale verlamming willen veroorzaken. De activiteiten van de beide inlichtingendiensten zijn wel afhankelijk van de prioriteiten die door de behoeftestellers in het kader van het Inlichtingenbesluit worden aangedragen.

Beleidsontwikkeling

In het kader van 'Telecommunicatie en veiligheid' zijn verschillende onderwerpen die in het kader van beleidsontwikkeling door het Ministerie van EZ zijn opgepakt voor het voorkomen en/of tegengaan van digitale verlamming. Te denken valt hierbij aan onderwerpen als nationaal continuïteitsbeleid (vanaf 2001), vitale infrastructuur (vanaf 2001) en het nationaal noodnet (vanaf 1991). Het is beleid waar nog steeds veranderingen, aanvullingen en verbeteringen in plaatsvinden. Het Ministerie van EZ stimuleert in dit kader dat er regelgeving wordt ontwikkeld die expliciet gericht is op het voorkomen en/of tegengaan van digitale verlamming. In dit kader wordt ook in internationaal verband met belanghebbenden overleg gevoerd.

Daarnaast werkt het Ministerie van EZ in het kader van beleidsontwikkeling aan een ketengerichte aanpak van cybercrime. In dit verband wordt geïnvesteerd in het bewust maken van burgers en bedrijven van de gevolgen van cybercrime en er wordt beleid ontwikkeld ten behoeve van het repressief opgetreden tegen daders. Dit heeft allebei een proactieve werking op digitale verlamming.

In meer algemene zin geeft het Ministerie van EZ aan dat er thans een herijking plaatsvindt op de belegde verantwoordelijkheden tussen de verschillende departementen in het kader van ICT-veiligheid. Daarin wordt ook aandacht besteed aan de samenhang van de diverse projecten en trajecten. Dit wordt door het Ministerie van EZ gezamenlijk met de departementen van de Ministeries van BZK en Justitie uitgevoerd.

Het Ministerie van Defensie heeft aangegeven dat er met name beleid wordt ontwikkeld voor de bescherming van de eigen ICT-infrastructuur en dat wordt ook toegesneden op een aantal specifieke defensietaken, zoals bijvoorbeeld ‘command and control’ en de ‘inlichtingenfunctie’. Voor de inlichtingenfunctie wordt in dit kader ook samengewerkt met de Beveiligingsautoriteit van Defensie.

Het Ministerie van Justitie heeft in het kader van het tegengaan van cybercrime verschillende wetgeving in de afgelopen jaren ontwikkeld. Te denken valt aan de Wet Computer-criminaliteit I, Wet Computercriminaliteit II en de uitvoering van de Dataretentierichtlijn van de EU. Voortdurend wordt door Justitie voeling gehouden met de ontwikkelingen en (inter)nationale omgeving, dan wel wordt daar input aan geleverd.

Beleidsuitvoering

In het kader van beleidsuitvoering geeft het Ministerie van EZ aan dat het organiseren van publiek-private samenwerking ten behoeve van het voorkomen van cybercrime (en daarmee het inperken van het gevaar van digitale verlamming) een belangrijk onderdeel is dat proactief kan doorwerken. Er worden in dit kader diverse pilots en activiteiten uitgevoerd, ondermeer gericht op het vergroten van het bewustzijn van burgers en bedrijven. Dit staat onder meer onder regie van het National High Tech Crime Center (NHTCC). Het NHTCC in Nederland sluit aan bij mondiale ontwikkelingen om te komen tot een internationale aanpak van technisch complexe vormen van zware georganiseerde criminaliteit en terrorisme. Hierbij wordt specifiek gekeken naar de consequenties die dit kan hebben voor de Nederlandse samenleving in het algemeen en voor de zogenaamde vitale informatie infrastructuren in het bijzonder. Bij vitale informatie infrastructuren kan worden gedacht aan de computersystemen op bijvoorbeeld de luchthaven Schiphol, de computernetwerken van grote financiële instellingen of de energiesector. Als het gaat om het NHTCC geldt dat dit initiatief als project wordt beëindigd. Er wordt gewerkt aan het ontwikkelen van nieuwe ambities met betrekking tot de bestrijding van cybercrime in de vorm van de ‘Nationale Infrastructuur Bestrijding Cybercrime’ (NIBC).

Het automatiseringsbeleid (de techniek) van de rijksoverheid en de uitvoering hiervan draagt bij aan het inperken en/of voorkomen van digitale verlamming, omdat dit beleid van invloed is op de kwaliteit van de voorzieningen en de getroffen voorzorgsmaatregelen.

Met andere woorden: een robuuste en veerkrachtige ICT-infrastructuur, die wordt ondersteund door een effectief beveiligingsbeleid en beveiligingsstandaarden, verkleint de kans op digitale verlamming. BZK heeft hierin een activerende rol in de richting van de overige departementen. De geformuleerde kaders binnen GOVCERT spelen hierbij een belangrijke rol.

Door overheidsdiensten op toenemende schaal op basis van ICT-toepassingen aan te bieden, maakt zij zichzelf in toenemende mate afhankelijk van ICT en daarmee kwetsbaar voor digitale verlamming. Door bij het aanbieden van overheidsdiensten goed stil te staan (aansluitvoorwaarden, stimulerend gebruik Public Key Infrastructure, etc.) bij het gevaar van digitale verlamming om daarmee de kwetsbaarheid te verminderen. De Ministeries van BZK en EZ toetsen ook de geformuleerde kwaliteitseisen, richtlijnen en standaarden (ondermeer ten aanzien van de beveiliging) om daarmee de kwetsbaarheid van de overheid voor digitale verlamming te verminderen.

Het Ministerie van Justitie is qua beleidsuitvoering in het kader van het tegengaan en/of voorkomen van digitale verlamming verantwoordelijk voor de aansturing van Platform Interceptie, Decryptie en Signaalanalyse (PIDS) en het Centraal Informatiepunt Telecommunicatiegegevens (CIOT). Het PIDS is een coördinerend platform voor het Nederlandse aftapbeleid. Het CIOT zal het vragen van informatie door politie en inlichtingendiensten binnen de telecommunicatiesector stroomlijnen en bijdragen aan de beveiliging van de gegevensuitwisseling.

De Ministeries van Defensie en BZK geven ook aan dat er oefeningen worden gehouden om de ICT-infrastructuur op haar kwetsbaarheden te toetsen in het licht van digitale verlamming. De gegevens uit de oefeningen geven vervolgens ook weer richting aan de te nemen maatregelen in de hiervoor genoemde categorieën.

Beleidsevaluatie

In evaluatieve zin – specifiek gericht op het voorkomen en/of tegengaan van digitale verlamming – worden op dit moment weinig activiteiten verricht. Wel worden er volgens het Ministerie van EZ specifieke programma’s en projecten geëvalueerd (bijvoorbeeld binnen de kaders van de Telecommunicatiewet) waar digitale verlamming een klein onderdeel van uitmaakt, maar hierop ligt niet het hoofdaccent. Ditzelfde geldt ook voor de activiteiten van de Ministeries van Defensie en BZK. Er wordt vanuit verschillende beleidsterreinen informatie verkregen, dit levert uiteindelijk weer input voor nader te ontwikkelen beleid in het kader van het voorkomen en/of tegengaan van digitale verlamming. Het Ministerie van Justitie geeft aan dat er voortdurend de uitkomsten van maatregelen tegen het licht worden gehouden om ervoor te zorgen dat - indien nodig - zo adequaat mogelijk nieuwe technieken of mogelijkheden worden gecreëerd om cybercriminaliteit te kunnen pareren.

3.3 Aanwezigheid interdepartementaal beleid

De interdepartementale samenwerking gericht op het inperken en/of voorkomen van digitale verlamming kent volgens de departementen van de Ministeries van EZ, BZK en Defensie geen algemene beleidsmatige basis, bijvoorbeeld in de vorm van een beleidsnota. Wel wordt er op basis van het project Vitaal, Beleidsplan Crisisbeheersing, een rijksbrede ICT-agenda en de Telecommunicatiewet samengewerkt tussen de departementen. Toch dient benadrukt te worden volgens het Ministerie van Defensie dat er nog geen interdepartementaal beleid en samenwerking is met als doel het leveren van een proactieve bijdrage ten opzichte van digitale verlamming.

Voor de informatiebeveiliging van de ICT-infrastructuur van de rijksoverheid is er wel interdepartementaal beleid aanwezig. In het Voorschrift Informatiebeveiliging Rijksoverheid (VIR) zijn regels opgenomen die voor alle ministeries gelden. Er bestaan aanvullende regels met betrekking tot bijzondere informatie (VIR-BI 2004) en het Beveiligingsvoorschrift 2005.

Een ander punt hierbij is het doel om voor de rijksoverheid een ICT-infrastructuur te volbrengen, de zogenaamde Haagse Ring. De Haagse Ring is een glasvezelnetwerk in de Haagse regio dat alle afzonderlijke netwerken van de departementen met elkaar verbindt. De stichting ICTU heeft namens de ministeries de gemeenschappelijke eisen en wensen gebundeld. DTO verzorgt de realisatie en het technisch beheer.
Een belangrijke voorwaarde voor het verbeteren van de samenwerking tussen de departementen – en daarmee de dienstbaarheid aan de burger – is het beschikken over moderne elektronische communicatie. Deze communicatie is daarmee een van de bouwstenen van Andere Overheid; het programma dat met name de dienstverlening aan de burger en bedrijfsleven moet verbeteren. De zogenoemde ‘Haagse Ring’ legt de basis voor die communicatie.
Bij de realisatie van de Haagse Ring wordt gebruik gemaakt van de bestaande voorzieningen van het ‘Netherlands Armed Forces Integrated Network’ (NAFIN), het bestaande netwerk van het Ministerie van Defensie. Zo wordt de controle uitgevoerd vanaf de commandobrug van NAFIN in Soesterberg. Vanzelfsprekend is goed onderzocht hoe de beveiliging van het NAFIN gewaarborgd blijft. Daarnaast zijn aanvullende (glasvezel)voorzieningen nodig. Na realisatie van de Haagse Ring hebben alle partijen bij de ICTU één aanspreekpunt voor veilig, snel en goedkoop onderling datatransport, waarvan de beschikbaarheid en continuïteit maximaal zijn gegarandeerd.

4. Knelpunten, blinde vlekken en behoeften

Na in het vorige hoofdstuk een zo compleet mogelijk beeld van de huidige stand te hebben gegeven, staan in dit hoofdstuk de knelpunten in het beleidsproces, de blinde vlekken in het beleid en de behoeften die de betrokken ministeries hebben centraal. Het identificeren van deze onderdelen maakt het mogelijk de proactieve kracht van het beleid te versterken.

Het hoofdstuk is als volgt opgebouwd:
- in paragraaf 1 wordt aandacht besteed aan de knelpunten in het interdepartementale beleidsproces, die in dit kader gezien kunnen worden als verbetermogelijkheden
- in paragraaf 2 wordt stilgestaan bij de blinde vlekken in het beleid, die in dit kader kunnen worden gezien als kansen
- in paragraaf 3 wordt aangegeven welke behoeften de betrokken ministeries hebben geformuleerd om de proactieve kracht van het beleid te versterken.

4.1. Knelpunten in het beleidsproces

In het vorige hoofdstuk is duidelijk geworden dat de Ministeries van EZ, BZK en Defensie de primair betrokken departementen zijn in het kader van het inperken en/of voorkomen van digitale verlamming. Niettemin is er een groot aantal departementen betrokken bij dit onderwerp. Het Ministerie van EZ is in het algemeen tevreden over de wijze waarop de interdepartementale samenwerking verloopt. Ditzelfde geldt voor het Ministerie van BZK als het gaat om de huidige verantwoordelijkheidsverdeling om digitale verlamming te voorkomen en/of tegen te gaan.

In het totale interdepartementale beleidsproces doet zich wel een aantal specifieke knelpunten voor, dat hieronder wordt behandeld.

Het Ministerie van EZ: samenhang initiatieven Ministeries van EZ en BZK soms afwezig
Door het Ministerie van EZ wordt evenwel aangegeven dat de samenhang in de verschillende initiatieven - gericht op cybercrime, terrorismebestrijding of de bescherming van de vitale sectoren in algemene zin - soms beperkt is. Een duidelijke scheiding tussen cybercrime en terrorisme is wat het Ministerie van EZ betreft bijvoorbeeld noodzakelijk.

Het Ministerie van EZ: rollen soms onvoldoende helder en daardoor te weinig begrip voor rol van de overheid in geliberaliseerde markten
De rolinvulling van de betrokken Ministeries is volgens het Ministerie van EZ niet altijd duidelijk. Dit geldt met name voor de Ministeries van BZK en Justitie en de NCTb. Er wordt nogal eens over het hoofd gezien dat de zeggenschap van de overheid in de telecommarkt beperkt is en dat een aangepaste wijze van benaderen en betrekken van deze markt gehanteerd moet worden. Meer begrip hiervoor is noodzakelijk.

Ten aanzien van de onduidelijke rolinvulling tussen de betrokken Ministeries en de NCTb kan worden gesteld dat meer duidelijkheid gewenst is ten aanzien van wie waarvoor verantwoordelijk is en hoe deze verantwoordelijkheden op elkaar aansluiten. Dit wordt momenteel opgepakt in het kader van het traject Herijking Veiligheidsbeleid.

De bewering van het Ministerie van EZ dat er nogal eens over het hoofd wordt gezien dat er een aangepaste wijze van benaderen en betrekken van de telecommarkt nodig is, wordt door het Ministerie van Justitie niet onderschreven. Dat er soms sprake lijkt te zijn van een beperkte samenhang, ligt volgens het Ministerie van Justitie aan het feit dat er verschillende departementen betrokken zijn en in een veld opereren vanuit verschillende verantwoordelijkheden en bijbehorende taken. In die zin zijn volgens het Ministerie van Justitie de aangegeven knelpunten herkenbaar en verklaarbaar. Dat geldt volgens het Ministerie van Justitie dan ook voor de verantwoordelijkheid die het Ministerie van EZ voor de telecommarkt heeft. Aanvullend daarop is nog door Justitie opgemerkt dat 'begrip' in de telecommarkt vaak wordt 'ingevuld' door financiële middelen.

Het Ministerie van BZK: vergroten wederzijdse afhankelijkheid kan tot afstemmingsproblemen leiden met het Ministerie van EZ
Zoals aangegeven ervaart het Ministerie van BZK in de huidige rolverdeling tussen de Ministeries van EZ en BZK geen knelpunten. Niettemin kan het Ministerie van BZK zich voorstellen als er meer focus wordt gelegd op het voorkomen van digitale verlamming in het perspectief van maatschappelijke ontwrichting, er door de toenemende afstemmingsbehoefte en de verschillende verantwoordelijkheden samenwerkingsproblemen kunnen ontstaan. Het Ministerie van EZ heeft in reactie hierop aangegeven zich niet te herkennen in de bovenstaande opmerking van het Ministerie van BZK.

Het Ministerie van Defensie: samenwerking met het Ministerie van BZK kan versterkt worden
Volgens het Ministerie van Defensie verloopt de samenwerking met het Ministerie van BZK niet altijd even voorspoedig. Dit is volgens het Ministerie van Defensie het gevolg van het feit dat er binnen het Ministerie van BZK verschillende afdelingen betrokken zijn bij dit onderwerp en de interne afstemming moeizaam verloopt, en de bestuurbaarheid van de sector blijkbaar beperkt is hetgeen de daadkracht van het Ministerie van BZK niet ten goede komt.

4.2. Blinde vlekken in het beleid

In het vorige hoofdstuk is beschreven welke beleidsactiviteiten op hoofdlijnen en in de verschillende fasen worden uitgevoerd ten behoeve van het inperken en/of voorkomen van digitale verlamming. Binnen het kader van het totale onderzoek is ook ingegaan op de mate waarin er zich blinde vlekken in het beleid voordoen, die in dit kader ook 'kansen' genoemd kunnen worden.

Het Ministerie van EZ: geen blinde vlekken ten aanzien van voorkomen digitale verlamming
Volgens het Ministerie van EZ doen zich echte blinde vlekken niet voor in het beleid van het Ministerie van EZ, dat gericht is op het inperken en/of voorkomen van digitale verlamming. Er is een tweetal beleidsterreinen dat specifiek gericht is op veiligheidsaspecten (Telecommunicatie/veiligheid en cybercrime), terwijl de veiligheidsaspecten bij andere beleidsterreinen een bijproduct zijn. In algemene zin is volgens het Ministerie van EZ het bewustzijn ten aanzien van veiligheid in relatie tot ICT groot.

Het Ministerie van BZK: doordenken rol van het Ministerie van BZK voor openbare sector
De ICT-infrastructuur voor de openbare sector is in grote mate afhankelijk van de landelijke ICT-infrastructuur. Er is weliswaar een basis gelegd voor bescherming van de ICT-infrastructuur voor de openbare sector, maar goed huisvaderschap vanuit het Ministerie van BZK voor die infrastructuur is niet voldoende om ontwrichting van de samenleving ten gevolge van digitale verlamming te voorkomen.

Het Ministerie van BZK: analyse kwetsbaarheden digitale verlamming
Het Ministerie van BZK heeft aangegeven dat het inzicht in de kwetsbaarheden - die kunnen leiden tot digitale verlamming - niet volledig is afgedekt voor de landelijke ICT-infrastructuur en de wijze waarop de overheid daarvan gebruik maakt (vergelijk ook project Vitaal en kwetsbaarheid Telecomvoorzieningen). Hieraan zou meer aandacht besteed moeten worden. Het Ministerie van EZ gaat er hierbij vanuit dat het Ministerie van BZK niet de openbare infrastructuur bedoelt, maar dat de opmerking betrekking heeft op de ‘gesloten’ infrastructuur van de publieke sector.

Het Ministerie van Defensie: meer focus op digitale verlamming in beleids-doelstellingen
Het voorkomen en/of tegengaan van digitale verlamming heeft bij het Ministerie van Defensie zeker aandacht, maar wordt niet voor iedere defensietaak als afzonderlijke doelstelling benoemd. Het Ministerie van Defensie besteedt expliciet aandacht aan dit thema als het gaat om de ICT-infrastructuur van het Ministerie van Defensie en de (rijks)overheid. Verder wordt digitale verlamming expliciet benoemd bij rampenbestrijding/noodhulp, inlichtingen en nationale operaties/ informatiebeveiliging. De focus binnen het Ministerie van Defensie op deze incidentcategorie zou nog meer aandacht kunnen krijgen door het bestrijden van digitale verlamming meer expliciet als beleidsdoelstellingen op te nemen voor andere beleidsterreinen (bijvoorbeeld op terrein van inlichtingen en commandovoering).

Het Ministerie van Defensie: meer aandacht voor cyberterrorisme
Het Ministerie van Defensie geeft aan dat de samenwerking met de NCTb de afgelopen periode is versterkt. Er was al langere tijd aandacht voor het bestrijden van cybercriminaliteit, maar het fenomeen cyberterrorisme is een relatief nieuw verschijnsel. Het Ministerie van Defensie vindt dat de NCTb en het Ministerie van Defensie de inspanningen voor het bestrijden van cyberterrorisme nog kunnen intensiveren.

Het Ministerie van BZK/het Ministerie van BZ: meer beleidsmatige aandacht voor digitale verlamming
Volgens het Ministerie van BZK ontbreekt een stevige beleidsmatige basis voor de samenwerking op het gebied van tegengaan van ICT-verstoring die leidt tot maatschappelijke ontwrichting. Wanneer de focus verschuift van invulling van het goede huisvaderschap naar het voorkomen van maatschappelijke ontwrichting, is het verbreden van de interdepartementale beleidsmatige basis van belang.

Dit onderwerp heeft volgens het Ministerie van BZ aan de technische kant weliswaar de aandacht die zij behoeft, maar is aan de beleidsmatige kant (als erkend probleem van wereldomvang en van nationale veiligheid) nog relatief nieuw. Het Ministerie van BZ wil op dit terrein de samenwerking met o.a. Het Ministerie van EZ intensiveren.

4.3. Ambities/behoeften van de betrokken ministeries

Zoals in de inleiding van deze rapportage is aangegeven, hebben de betrokken ministeries allemaal de kans gekregen hun behoeften/ambities ten aanzien van het inperken en/of voorkomen van digitale verlamming aan te geven. In deze paragraaf worden deze beschreven.

4.3.1. Departementale ambities/behoeften

De departementale behoeften hebben betrekking op behoeften/ambities die te realiseren zijn zonder dat intensieve samenwerking met andere ministeries noodzakelijk is. Hieronder worden de behoeften per Ministerie uitgewerkt.

Het Ministerie van EZ: kennisontwikkeling en R&D
Het Ministerie van EZ is van mening dat er vooral aan kennisontwikkeling en R&D meer aandacht moet worden besteed. Dit is volgens het Ministerie van belang, omdat de snelheid van ontwikkelingen in de ICT-sector en het belang van de ICT-sector voor de samenleving maken dat het kennisniveau ten behoeve van bedrijfszekerheid in de ICT-sector op een hoog niveau moet zijn. De betrokkenheid van het bedrijfsleven en onderzoeksinstellingen zijn hierbij essentieel.

Het Ministerie van BZK: meer focus op digitale verlamming vanuit gedachte van maatschappelijke ontwrichting
Vanuit het Ministerie van BZK is aangegeven dat een aantal beleidsterreinen van het Ministerie van BZK in zeer beperkte mate proactief kan doorwerken op het voorkomen en tegengaan van digitale verlamming. De beleidsterreinen van het Ministerie van BZK die genoemd zijn in de zelfanalyse van het Ministerie van BZK, kunnen een bijdrage leveren, maar het heeft een beperkte betekenis als het gaat om het tegengaan van maatschappelijke ontwrichting als gevolg van digitale verlamming.

In de afgelopen periode is gebleken dat er een sterkere onderlinge afhankelijkheid is tussen de ICT-Infrastructuur voor de openbare sector en de landelijke ICT-infrastructuur en dat betekent ook dat het de samenwerking tussen het Ministerie van BZK met voornamelijk het Ministerie van EZ meer raakt. Dit zal in de nabije toekomst meer aandacht moeten krijgen door de onderlinge rolverdeling scherper te krijgen. De focus zou daarbij moeten liggen op het in beeld brengen van kwetsbaarheden en het beleggen van verantwoordelijkheden om digitale verlamming tegen te gaan.

Het Ministerie van Defensie: meer focus op de inlichtingenfunctie ten aanzien van digitale verlamming
Vooral het lokaliseren van organisaties en individuen die zich richten op digitale verlamming, verdient meer aandacht. Het ministerie van Defensie kan hierin van betekenis zijn door haar informatiepositie op dit gebied te verbeteren. Dit kan intensiever worden met een samenwerkingsverband als het NHTCC (of later het NIBC). De samenwerking is gericht op het vroegtijdig signaleren en zo snel mogelijk tegengaan van ernstige misdaden met of tegen ICT. Specifieke aandacht heeft het NHTCC gegeven aan High Tech Crime die vergaande consequenties kunnen hebben voor de Nederlandse samenleving en in het bijzonder voor de vitale informatie-infrastructuren.

Het Ministerie van Defensie: meer aandacht voor interdepartementale risicoanalyse en beleidsontwikkeling op het gebied van cyberterrorisme
Naast militaire operaties op het land, in de lucht en op zee worden ook operaties in de digitale ruimte steeds belangrijker. Er is in deze zin sprake van een nieuwe dimensie van militair optreden. Het Ministerie van Defensie wordt zich steeds meer bewust van het belang van deze nieuwe dimensie. Samen met het Ministerie van BZK en de NCTb kan worden gewerkt aan een interdepartementale risicoanalyse en verdere beleidsontwikkeling op het gebied van cyberterrorisme. Hierbij moet specifiek aandacht worden besteed aan de (toekomstige) rol van GOVCERT (waarschuwingsdienst binnen de Rijksoverheid).

Het Ministerie van Defensie: meer aandacht voor Informatiebeveiliging
Informatiebeveiliging is van belang om departementen in staat te stellen veilig gebruik te maken van openbare ICT-infrastructuur, om te voorkomen dat informatie kan worden misbruikt en om een efficiënte benutting van bronsystemen mogelijk te maken. Er zijn veel departementen betrokken bij het thema informatiebeveiliging. Er zal beleid ontwikkeld moeten worden voor de gewenste eenduidigheid en beveiliging van informatie. Hierbij zal aandacht besteed moeten worden aan de Persoonlijke elektronische identiteit en de mogelijkheid om de betrouwbaarheid van een digitale ‘gesprekspartner’ te kunnen vaststellen. Het Ministerie van BZK kan hierin een belangrijke rol vervullen.

4.3.2 Rijksbrede behoeften/ambities

De rijksbrede behoeften/ambities hebben betrekking op behoeften/ambities die alleen te realiseren zijn door middel van intensieve samenwerking met andere ministeries. Hieronder worden de behoeften per Ministerie uitgewerkt. [5]

Het Ministerie van EZ: ontwikkelen van een visie op noodcommunicatie
Rijksbreed gezien heeft het Ministerie van EZ behoefte aan een visie op noodcommunicatie. Gezien de resultaten in het kader van het interdepartementale project bescherming vitale infrastructuur - waaruit blijkt dat voor wat betreft de nood- en crisiscommunicatie het ontbreekt aan duidelijkheid over taken, rollen, bevoegdheden, e.a.- is een visie op crisis- of noodcommunicatie voor het bestuurlijk niveau noodzakelijk.

[5] Het Ministerie van BZK heeft in de zelfevaluatie aangegeven geen rijksbrede behoeften/ ambities te hebben.

Dit is een beleidsverantwoordelijkheid i voor het Ministerie van BZK. Hierbij dient goed te worden stilgestaan bij de voorzieningen (gewenste functionaliteiten) die op het bestuurlijk niveau nodig zijn, om in een situatie van digitale verlamming, enerzijds onderling te kunnen communiceren en anderzijds ook burgers te kunnen bereiken.

De Ministeries van Defensie en Justitie: gezamenlijk invulling geven aan verschillende initiatieven voor voorkomen en tegengaan van digitale verlamming
Het Ministerie van Defensie heeft verschillende behoeften die rijksbreed uitgewerkt kunnen worden voor het proactief omgaan met digitale verlamming. Door het Ministerie van Defensie zijn in dit kader de volgende elementen benoemd:

- het stimuleren van wetenschappelijk onderzoek naar maatregelen tegen digitale verlamming
- het stimuleren van de bewustwording van overheidspersoneel voor de risico's van digitale verlamming
- het normeren en toetsen van de informatiebeveiliging van digitale systemen en het ontwikkelen van tegenmaatregelen
- het verbreden van het aandachtsgebied van het NHTCC (of later het NIBC) tot het tegengaan van cyberterrorisme en –criminaliteit
- het intensiveren van Govcert
- het leren van voorbeelden uit het buitenland voor het proactief omgaan met digitale verlamming.

Het Ministerie van Justitie heeft in het verlengde hiervan ook aangegeven dat we ons bewust moeten zijn dat Nederland onderdeel van de internationale (digitale) samenleving is. Internationale samenwerking en ontwikkelingen en (on)mogelijkheden spelen dus steeds een rol bij het ontwikkelen adequate tegenmaatregelen.

5. Conclusies

In dit laatste hoofdstuk worden de conclusies weergegeven die op basis van voorgaande hoofdstukken kunnen worden getrokken.

Het hoofdstuk is als volgt opgebouwd:
- in paragraaf 1 wordt het huidige proactieve beleid en de interdepartementale samenwerking kort besproken aan de hand van centrale beleidslijnen
- in paragraaf 2 worden de ‘kansen’ en ‘mogelijkheden’ besproken om de proactieve kracht van het beleid te versterken. Deze kansen en mogelijkheden zijn afgeleid van de blinde vlekken, knelpunten en behoeften, die in het vorige hoofdstuk zijn besproken
- in paragraaf 3 wordt aangegeven aan welke kansen en mogelijkheden prioriteit kan/moet worden gegeven.

5.1 Beleid en interdepartementale samenwerking

Het proactieve beleid en de interdepartementale samenwerking ten behoeve hiervan concentreren zich in essentie op twee strategieën gericht op het inperken en/of voorkomen van digitale verlamming. Deze twee strategieën zijn (gedeeltelijk) gericht op:
- digitale verlamming als gevolg van technisch falen
- digitale verlamming als gevolg van bewust menselijk handelen.

Digitale verlamming als gevolg van technisch falen
Als het gaat om de incidentcategorie ‘digitale verlamming’, dan is het Ministerie van EZ verantwoordelijk voor het treffen van maatregelen ter bescherming van de openbare ICT-infrastructuur. Het Ministerie van BZK is primair verantwoordelijk voor bescherming van de gesloten ICT-infrastructuur van de publieke sector. Het bedrijfsleven is zelf verantwoordelijk voor de gesloten infrastructuur die zij heeft aangelegd.

Er worden zowel binnen de overheid als in het bedrijfsleven maatregelen getroffen om de ICT-infrastructuur te beschermen tegen technisch falen. In het kader van Vitaal (bescherming van de vitale infrastructuur) en het Nationaal Continuïteitsplan Telecommunicatie (NACOTEL) worden analyses verricht naar kwetsbaarheden van ICT. Dit vormt ook een belangrijke basis voor het uitvoeren van beschermende maatregelen.

Een robuuste en veerkrachtige ICT-infrastructuur, dat wordt ondersteund door een effectief beveiligingsbeleid en beveiligingsstandaarden, verkleint de kans op digitale verlamming. Het Ministerie van BZK heeft hierin een activerende rol in de richting van de overige departementen. Door overheidsdiensten op toenemende schaal op basis van ICT-toepassingen aan te bieden, maakt zij zichzelf in toenemende mate afhankelijk van ICT en daarmee kwetsbaar voor digitale verlamming. Door bij het aanbieden van overheidsdiensten goed stil te staan (aansluitvoorwaarden, stimulerend gebruik Public Key Infrastructure, etc.) bij het gevaar van digitale verlamming, kan de kwetsbaarheid verminderd worden. De Ministeries van BZK en EZ toetsen ook de geformuleerde kwaliteitseisen, richtlijnen en standaarden (ondermeer ten aanzien van de beveiliging) om daarmee de kwetsbaarheid van de overheid voor digitale verlamming te verminderen.

Digitale verlamming als gevolg van bewust menselijk handelen
Cybercrime en cyberterrorisme zijn twee vormen waarop door bewust crimineel handelen er inbreuk wordt gemaakt op de ICT-infrastructuur. Cybercrime wordt gezien als ‘elke strafbare en strafwaardige gedraging voor de uitvoering waarvan het gebruik van geautomatiseerde werken bij de verwerking en overdracht van gegevens van overwegende betekenis is. Onder computercriminaliteit worden zowel verschijningsvormen verstaan waarbij de computer het doel is van strafbare gedragingen (bijvoorbeeld hacking, virusverspreiding) als verschijningsvormen waarbij de computer als middel wordt gebruikt (bijvoorbeeld fraude, verspreiding van kinderpornografie, schendingen van het auteursrecht etc).

Cyberterrorism is een vooropgezette - vanuit politieke motieven - aanval tegen informatie, computersystemen en computerprogramma’s om overheden, maatschappelijke organisaties en burgers bewust te beschadigen. Politiek gemotiveerde aanslagen die serieuze schade veroorzaken, zoals zware economische crisis of duurzaam verlies van energie of water, kunnen eveneens als cyberterrorisme worden aangeduid.

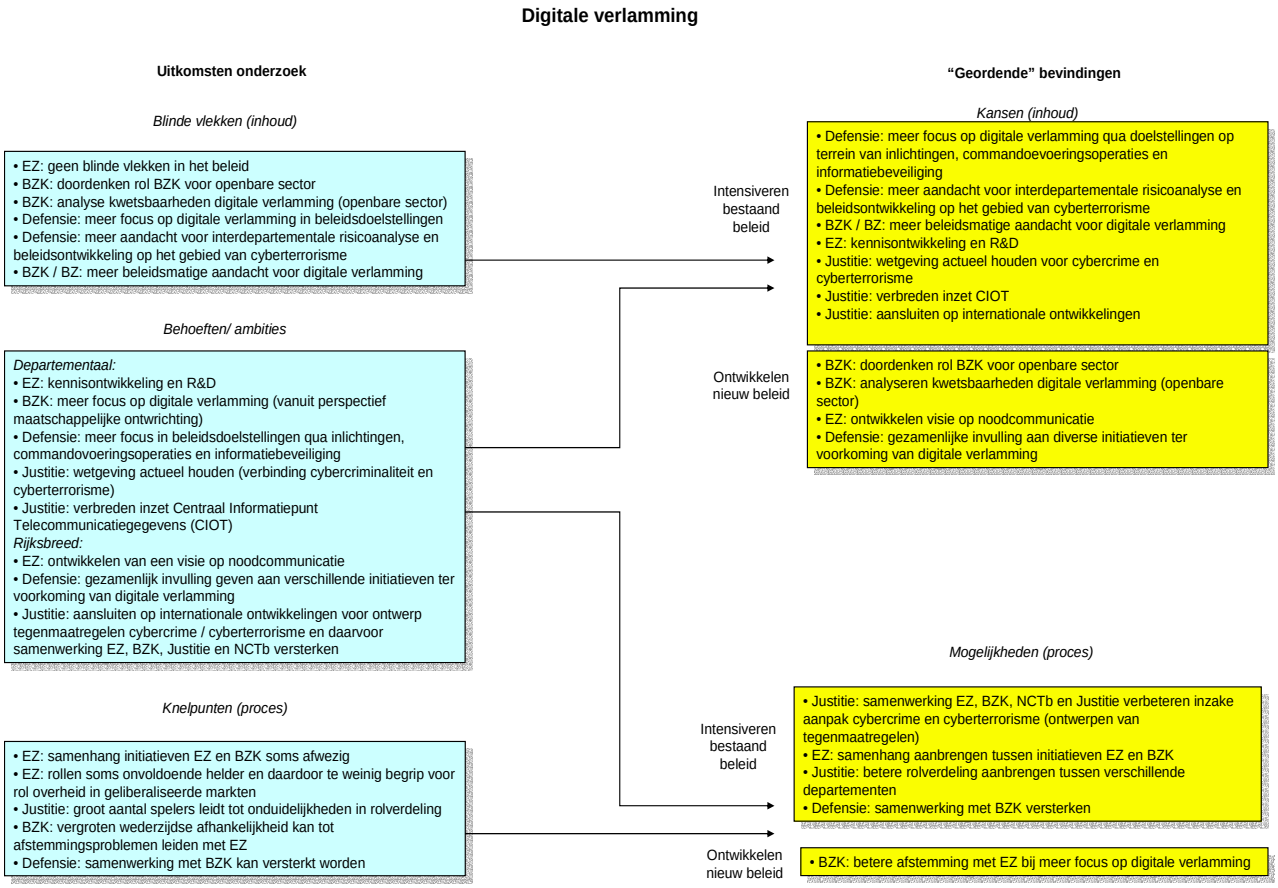
Als het gaat om digitale verlamming kan met name de impact van cyberterrorisme groot zijn. Cyberterrorisme is nog een relatief nieuw beleidsonderwerp, dat vanuit de NCTb wordt opgepakt, in gezamenlijkheid met het Ministerie van Justitie.

5.2 Kansen en mogelijkheden

Op basis van het huidige proactieve beleid – waarvan de kern in de vorige paragraaf is behandeld – is in het onderzoek gekeken naar:
- blinde vlekken in de inhoud van het beleid
- knelpunten in het interdepartementale beleidsproces
- behoeften, zowel inhoudelijk als procesmatig.

In figuur 2 (volgende pagina) staan de blinde vlekken, knelpunten en behoeften weergegeven. Deze zijn vertaald naar ‘kansen’ (inhoud) en ‘mogelijkheden’ (proces), waarbij een onderscheid is gemaakt tussen het intensiveren van het bestaande beleid en het ontwikkelen van nieuw beleid.

Figuur 2: van blinde vlekken, knelpunten en behoeften naar kansen en mogelijkheden



De verantwoordelijkheden met betrekking tot digitale verlamming zijn verschillend belegd. Als het gaat om 'digitale verlamming als gevolg van technisch falen' dan zijn met name de departementen van het Ministerie van EZ (voor de openbare ICT-infrastructuur) en het Ministerie van BZK (voor de gesloten ICT-infrastructuur van de overheid) belangrijke spelers. Vooral vanuit Vitaal zijn de kwetsbaarheden in kaart gebracht. De deskundigen hebben aangegeven dat Vitaal veel omvat, maar het de moeite waard is om nader te onderzoeken of Vitaal de kwetsbaarheden rondom digitale verlamming in de volle breedte heeft opgepakt.

Voor wat betreft de aanpak van cyberterrorisme (digitale verlamming als gevolg van bewust menselijk handelen) geven verschillende departementen (Ministerie van Defensie en BZ) aan dat hier meer prioriteit aan moet worden gegeven. Er overheerst bij verschillende departementen – zo bleek uit het onderzoek - het gevoel dat er op dit onderwerp niet voldoende grip aanwezig is. De kennis en ervaring die is opgedaan rondom de aanpak van cybercrime kan meer gebruikt worden om ook de aanpak van cyberterrorisme vorm te geven. Op dit moment is het met name de NCTb, die deze aanpak vormgeeft. De aanpak heeft een structurele karakter nodig en er zal een verdedigingsstrategie gecreëerd moeten worden tegen het gevaar van cyberterrorisme, waarbij het belangrijk is dat deze ook in de systemen een uitwerking krijgt en daarover actief gecommuniceerd wordt door de verschillende betrokken departementen. Het laatste vindt vooralsnog niet in voldoende mate plaats, blijkens de genoemde kansen en mogelijkheden van de verschillende departementen.

Het is vanuit de gehouden analyse – mede ook door het ontbreken van gegevens van de NCTb – niet duidelijk of er in het kader van cyberterrorisme gewerkt wordt aan verschillende elementen binnen een verdedigingsstrategie, als:

- identificatie van meest kritieke veiligheidsproblemen op het internet (daar ook lerende van de ervaringen in het buitenland)
- internationale samenwerking tussen inlichtingen- en veiligheidsdiensten op dit aandachtsgebied
- uitbouw van cyber- strategische, tactische en operationele competenties
- detectie van terroristische bronnen
- ondersteuning van systeembeheerders en vergroten van de bewustwording.

5.3 Prioritering

Een aantal departementen (Ministeries van BZK, Defensie en BZ) hebben in het onderzoek aangegeven dat digitale verlamming meer aandacht moet krijgen vanuit het perspectief van maatschappelijke ontwrichting. Het Ministerie van EZ daarentegen vindt dat de huidige verbanden prima functioneren en dat daar geen extra impuls hoeft te worden gegeven. Belangrijk is in ieder geval de samenhang tussen de verschillende onderwerpen (een voldoende beveiligde en weerbare ICT-infrastructuur en aandacht voor bewust menselijk handelen om de ICT-infrastructuur te ondermijnen) te borgen. Op basis van deze evaluatie blijkt dat de verantwoordelijkheden bij verschillende organisaties belegd zijn en er meer samenhang en samenwerking gerealiseerd kan worden.

Bijlagen

Bijlage 1: betrokken ministeries

De ministeries die in het kader van het inperken en/of voorkomen van digitale verlamming zijn betrokken, staan in tabel 1 weergegeven. Hierbij geldt dat de mate c.q. vorm van betrokkenheid kan verschillen:

- een *zelfevaluatie* betekent dat er een volledige vragenlijst bij het betreffende Ministerie is afgenomen waarin zowel is ingegaan op het beleid als op het beleidsproces
- een *collegiale toets 1* wil zeggen dat een Ministerie dat een zelfevaluatie heeft uitgevoerd de kans krijgt om op basis van de conceptrapportage te reageren op wat andere ministeries hebben aangegeven in het kader van het beleid en beleidsproces
- een *collegiale toets 2* wil zeggen dat de ministeries die geen zelfevaluatie hebben uitgevoerd de kans krijgt te reageren op de onderdelen die betrekking hebben op de omschreven rol in het kader van het inperken en/of voorkomen van aantasting van digitale verlamming. Daarnaast hebben deze ministeries de kans gekregen aanvullende informatie te geven over hun ervaringen en ambities op dit gebied.

Tabel 1. Aard van betrokkenheid ministeries

Ministerie	**Vorm van betrokkenheid**
Ministerie van Defensie	Zelfevaluatie, collegiale toets 1
Ministerie van BZK	Zelfevaluatie, collegiale toets 1
Ministerie van EZ	Zelfevaluatie, collegiale toets 1
Ministerie van BZ	Collegiale toets 2
Ministerie van Justitie	Collegiale toets 2

Bijlage 2: overzicht van activiteiten ministeries

De Ministeries van BZ en Defensie hebben op dit moment een zelfevaluatie afgerond. In de onderstaande tabellen wordt op hoofdlijnen aangegeven welke beleidsactiviteiten in het kader van het inperken en/of voorkomen van digitale verlamming worden verricht.

Tabel 1. Beleidsactiviteiten van het Ministerie van EZ die bijdragen aan het inperken en/of voorkomen van digitale verlamming

Beleidsactiviteiten	**Beschrijving van de inhoud**
Onderzoek	• TNO ontvangt doelfinanciering en een deel van het onderzoek dat zij verricht, is gericht op aspecten van digitale verlamming. • Het zogenaamde 'Sentinels-onderzoeksprogramma' wordt (financieel) ondersteund en een deel van dit programma is gericht op aspecten van digitale verlamming. • Deelname in het 6e kaderprogramma van de EU waarvan een klein onderdeel gericht is op ICT en de bescherming daarvan. • Ten behoeve van beleid wordt specifiek beleidsondersteunend onderzoek verricht (dan wel uitbesteed).
Risicoanalyses	• Ten behoeve van 'bescherming van de vitale infrastructuur' (project Vitaal) en het Nationaal Continuïteitsplan Telecommunicatie worden analyses verricht naar kwetsbaarheid, oorzaken, e.a. van digitale verlamming.
Beleidsontwikkeling	• Ontwikkelen en monitoren van regelgeving gericht op het inperken en/of voorkomen van digitale verlamming. • Delen van informatie op (inter)nationale schaal ten behoeve van eigen beleid. • Deelname in en organiseren van (internationaal) overleg met de sector en belanghebbenden mede gericht op het inperken en/of voorkomen van digitale verlamming. • Ontwikkelen van een ketengerichte aanpak gericht op cybercrime. • Herijking ICT-veiligheid waarin wordt gekeken naar de logica van de huidige verantwoordelijkheden, bevoegdheden, en activiteiten/projecten, e.a. op het gebied van ICT en veiligheid (samen met BZK en Justitie).
Beleidsuitvoering	• Toezicht op naleving regelgeving. • Organiseren van crisismanagement en oefeningen. • Versterken publiek-private samenwerking ten behoeve van de aanpak van cybercrime. • Diverse activiteiten, pilots en projecten zowel gericht op het verhogen van het bewustzijn van burgers en ondernemers ten aanzien van cybercrime als gericht op repressie.
Beleidsevaluatie	• Evaluatie van specifieke projecten en programma's. • Jaarlijkse rapportages in het kader van de Telecommunicatiewet.

Tabel 2. Beleidsactiviteiten van het Ministerie van BZK die bijdragen aan het inperken en/of voorkomen van digitale verlamming

Beleidsterreinen	Beleidsactiviteiten	Beschrijving van de inhoud
• Automatisering overheid • Datacommunicatie overheid • Elektronische overheid • Informatiebeleid openbare sector • Informatiebeveiliging rijksdienst	Risicoanalyses	• In het Voorschrift Informatie beveiliging Rijksdienst (VIR) uit 1994 is het door de departementen uitvoeren van risicoanalyses (afhankelijkheidsanalyses op procesniveau en kwetsbaarheid-analyses) verplicht gesteld. • Dreigingsanalyses van de AIVD.
	Beleidsuitvoering	• Integrale lijnmanagementtaak (voor wat betreft automatisering en informatiebeleid, beveiliging, e.a.). • Opleggen van regelgeving die digitale verlamming helpt te voorkomen (regels om in aanmerking te komen voor gebruik van systemen - zie aansluit-voorwaarden, etc). • Govcert (Computer Emergency Response Team van de overheid) ondersteunt de aangesloten overheidsorganisaties waaronder alle ministeries, bij het voorkomen van ICT-incidenten (door onder andere adviezen te verstrekken over onderkende kwetsbaarheden).
	Beleidsevaluatie	• In het VIR is periodieke evaluatie verplicht gesteld.
• Vitaal	Risicoanalyses	• Binnen Vitaal bevordert BZK de inter-departementale afstemming rondom risicoanalyses (EZ verricht inhoudelijke analyse van ICT-kwetsbaarheid).

Tabel 3. Beleidsactiviteiten van het Ministerie van Defensie die bijdragen aan het inperken en/of voorkomen van digitale verlamming

Beleidsterreinen	Beleidsactiviteiten	Beschrijving van de inhoud
Beheersing zeegebied, grondgebied	Onderzoek	• Informatiebeveiliging. • Informatieassurance. • Intrusion detection.
	Risicoanalyses	• Op ICT-infrastructuur en informatievoorziening.
	Beleidsontwikkeling	• Alleen voor ICT-infrastructuur als informatievoorziening van Defensie.
	Beleidsuitvoering	• Voorzieningen treffen voor bescherming ICT-infrastructuur en informatievoorziening van Defensie.
	Beleidsevaluatie	• Nagaan of voorzieningen de ICT-infrastructuur en informatievoorziening van Defensie borgen.
Commandovoerings-operatie	Onderzoek	• Gericht op informatiebeveiliging en tools voor detectie. • Start van een R&D programma met BZK.
	Beleidsontwikkeling	• Inrichten van processen Command en Control (C2).
	Beleidsuitvoering	• Trainen en opleiden van functionarissen.
	Beleidsevaluatie	• Evalueren van operaties.
Evacuatie en persoonsbeveiliging	Beleidsuitvoering	• Beperkt ondersteunen van civiele autoriteiten (maar niet direct voor tegengaan en/of voorkomen van digitale verlamming).
Rampenbestrijding en noodhulp	Onderzoek	• TNO-onderzoek met scenario-analyses, waarvan digitale verlamming onderdeel uitmaakt.
	Risicoanalyses	• Beperkt werken aan ontwikkelen van uiteenlopende scenario's.
	Beleidsontwikkeling	• Opzetten van traject Intensivering Civiel Militaire Samenwerking (ICMS).
	Beleidsuitvoering	• Oefeningen met civiele autoriteiten en uitvoering ICMS.
	Beleidsevaluatie	• Vanuit de bevindingen van de oefening Bonfire nadenken over het onderwerp digitale verlamming.
Inlichtingen	Onderzoek	• In eigen beheer en in samenwerking met TNO onderzoeken van robuustheid van eigen ICT-infrastructuur.
	Risicoanalyses	• MIVD informeert en adviseert behoeftestellers van diverse departementen op basis van risico-analyses.
	Beleidsontwikkeling	• De MIVD werkt in deze samen met de beveiligingsautoriteit.

Beleidsterreinen	Beleidsactiviteiten	Beschrijving van de inhoud
Nationale operaties/ informatiebeveiliging	Risicoanalyses	• Opstellen informatiebeveiligingsplannen (afhankelijkheid en kwetsbaarheid).
	Beleidsuitvoering	• Implementeren maatregelen uit informatiebeveiligingsplannen en controle op uitvoering en toepassing Voorschrift Informatiebeveiliging Rijksdienst (VIR) • Specifiek onderbrengen van vitale applicaties/ICT infradiensten bij Defensie Telematica Organisatie (DTO).