Aan

De Voorzitter van de Tweede Kamer der
Staten-Generaal
Binnenhof 4
2513 AA ‘s-GRAVENHAGE

Datum	Uw kenmerk	Ons kenmerk	Bijlage(n)
17 december 2007		ET/TM / 7144426	1

Onderwerp

Agenda ICT en veiligheid

Op 16 juli jongstleden zijn u de rapporten Herijking Veiligheidsbeleid ICT aangeboden (Tweede Kamer, vergaderjaar 2006-2007, 26649 nr 96). Daarbij is u een nadere agenda toegezegd. Met deze brief wordt u deze agenda aangeboden.
Voorts heeft de Tweede Kamer met de motie Gerkens (Tweede Kamer, vergaderjaar 2006-2007, 28 684, nr 94) gevraagd om versterking van de coördinatie en aansturing: de in deze brief beschreven aanpak kan als een reactie op deze motie worden gezien.

Achtereenvolgens zullen in deze brief aan de orde komen: Aanleiding en reikwijdte, de belangrijkste bevindingen uit het rapport, de inzet van het kabinet en de agenda.

1. Aanleiding en reikwijdte

ICT Veiligheid is een beleidsterrein, waarvoor meerdere departementen een verantwoordelijkheid kennen. Onder ICT veiligheid wordt hier verstaan zowel de continuïteit van de ICT/telecom dienstverlening, de borging van de mogelijkheid om daar veilig gebruik van te maken, als de opsporing en vervolging ingeval deze veiligheid op strafbare wijze is aangetast. Het inzetten van elektronische middelen ten behoeve van veiligheidsmaatregelen wordt niet tot de reikwijdte van deze brief gerekend.

Coördinatie vanuit de betrokken departementen richting uitvoerende organisaties en samenleving is belangrijk om samenhang en richting in de aanpak van ICT veiligheid te bevorderen.

De rapporten van het project Herijking ICT Veiligheidsbeleid zijn opgesteld om intern richting te geven aan het verbeteren van de interdepartementale samenwerking tussen Justitie, BZK en EZ op het terrein van het ICT veiligheidsbeleid. De departementen hadden behoefte aan meer

Bezoekadres		Doorkiesnummer	Telefax
Hoofdkantoor	Telefoon 070-379 6106	Behandeld door	
Bezuidenhoutseweg 30	Telefax 070-379 6154	Ed Buddenbaum	
Postbus 20101	Email f.heemskerk@minez.nl		
2500 EC 's-Gravenhage	Website www.minez.nl	*Verzoeke bij beantwoording van deze brief ons kenmerk te vermelden*	

gezamenlijk inzicht, waar de coördinatie en samenhang in alle activiteiten op dit terrein noodzakelijk en mogelijk is. Deze rapporten zijn niet opgesteld met het oogmerk van externe verspreiding. De status van de rapporten moet in dat licht worden bezien. Inmiddels hebben de drie departementen goede stappen gezet op weg naar structurele borging van de coördinatie en samenhang in al deze activiteiten.

2. Bevindingen van het rapport

In algemene zin heeft het rapport het beeld opgeleverd dat weliswaar alle bekende bedreigingen actief worden bestreden, maar dat daarbij de beschikbare mix aan (beleids)instrumenten niet ten volle wordt benut. Daarnaast bleek een grote behoefte aan meer regie en minder versnippering op dit terrein.

De belangrijkste aanbevelingen uit het rapport zijn:

- groepering van gerelateerde beleidsonderwerpen in arena's en een gezamenlijke agenda op de punten waar de arena's elkaar raken; in de uitwerking van de gezamenlijke agenda zal worden gezorgd voor een betere sturing en een betere samenwerking.
- verbetering van de governance; professionalisering door bewuster andere beleidsinstrumenten mee te wegen en aandacht voor internationale samenwerking.
- zoeken naar en borgen van een goede samenwerking met het bedrijfsleven: effectiviteit van het beleid wordt alleen bereikt als overheid en bedrijfsleven in deze agenda gezamenlijk optrekken.

Het rapport constateert een verdeling in de volgende drie arena's:

- maatschappij ontwrichtende gebeurtenissen,
- niet-maatschappij ontwrichtende gebeurtenissen,
- opsporing en vervolging.

- *Voorkomen van maatschappij ontwrichtende gebeurtenissen*: hier worden vraagstukken omtrent maatschappijontwrichtende risico's en nationale veiligheid behandeld. Het betreft gebeurtenissen die ten koste van bijna alles moeten worden voorkomen. Daar treedt de overheid sturend op, opdat de overheid de zekerheid heeft dat partijen doen wat vanuit publiek belang noodzakelijk is. BZK is in deze arena de belangrijkste portefeuillehouder; EZ is op grond van hoofdstuk 14 Telecommunicatiewet (buitengewone omstandigheden) betrokken.
- *Beperken van niet maatschappij ontwrichtende gebeurtenissen*: vraagstukken omtrent risico's waar de maatschappij last van heeft, maar die niet maatschappijontwrichtend zijn. De overheid tracht hier d.m.v. interventies organisaties te beïnvloeden het gewenste gedrag te vertonen. Vanuit haar rol op gebied van duurzaam ondernemen is EZ hier een belangrijke portefeuillehouder. Waar het goed huisvaderschap van de eigen overheidssystemen betreft, is dit BZK als beleidscoördinator binnen de overheid.
- *Opsporen en vervolgen cybercriminelen*: vraagstukken die te maken hebben met opsporing en vervolging van cybercriminelen. Het betreft hier reguliere overheidstaken van het OM, politie en opsporingsdiensten; Justitie is in deze arena de belangrijkste portefeuillehouder.

De drie voorgestelde arena's overlappen elkaar op sommige onderwerpen, daarnaast zijn veel dreigingsbeelden of kwetsbaarheidrisico's niet eenduidig aan één bepaalde arena gebonden. Soms kunnen dreigingen door toename of verandering van kenmerken verschuiven naar een andere arena.

De aanbevelingen uit de rapporten 'Herijking ICT Veiligheidsbeleid' zijn als volgt opgepakt:

- interdepartementale afstemming en coördinatie, waartoe ook een geregeld overleg tussen de drie meest betrokken directeuren-generaal wordt gerekend.
- de gezamenlijke agenda, die u in de bijlage aantreft en die gerelateerd is aan de twee grotere beleidsprogramma's: Nationale Veiligheid en Veiligheid begint bij voorkomen.
- het streven naar een goede samenwerking met bedrijfsleven en betrokken sectoren, zoals uit de agenda naar voren komt.

Zo werken de departementen in samenhang aan reeds eerder ingezette maatregelen zoals de diverse pilots binnen de ontwikkelomgeving van de Nationale Infrastructuur Cybercrime (NICC) en de ondersteuning van de vitale sectoren door het Nationaal Adviescentrum Vitale Infrastructuur (NAVI).

3. Inzet van het kabinet

ICT levert een belangrijke bijdrage aan het innovatieve vermogen van de samenleving. Borging van een veilig en vertrouwd gebruik van ICT is derhalve van groot belang.
Kijkend naar de toekomst is het kabinet dan ook van mening dat onze samenleving weerbaar dient te zijn tegen dreigingen: tegen fysieke maar ook tegen digitale dreigingen, zoals ICT-verstoring of cybercrime.
Deze weerbaarheid geldt niet alleen voor burgers en bedrijven maar ook voor de overheid. Daarnaast dient de veiligheidsketen optimaal te functioneren indien een dreiging toch tot een gebeurtenis heeft geleid.

Het kabinetsbeleid krijgt vorm in twee grote beleidsvelden waarbinnen de borging van de veiligheid van ICT en veiligheid een belangrijke rol vervult:

- De strategie Nationale Veiligheid, die zich richt op de bescherming van de samenleving en bevolking op eigen grondgebied tegen interne en externe dreigingen en het project Bescherming Vitale Infrastructuur, gericht op continuïteit van de voor onze samenleving vitale sectoren, inclusief ICT.
- Binnen het project "Veiligheid begint bij Voorkomen" (VbbV, zie Tweede Kamer, vergaderjaar 2007-2008, 28 684, nr 119) neemt cybercrime een belangrijke plaats in: naast de aangekondigde intensivering van de opsporing en vervolging van cybercrime zijn preventie en onderzoek belangrijk. Het op cybercrime gerichte beleid in deze pijler is met name gericht op het bevorderen van de werkende veiligheidsketen.

Bij beide beleidsvelden speelt de inbreng van bedrijfsleven en consumenten in het kader van preventie, handhaving en toezicht een belangrijke rol.

Het kabinet is van mening dat, gezien het bovenstaande, verder voortgebouwd moet en kan worden op de bevindingen uit het rapport "Herijking ICT en Veiligheid" en dat de beoogde versterking van de samenhang in de inzet van de departementen het beste bereikt wordt door

waar mogelijk op deze twee beleidsvelden gezamenlijk op te trekken. Dit wordt mogelijk gemaakt door de gezamenlijke agenda, die in deze brief wordt gepresenteerd.

4. Agenda

Deze agenda zal onlosmakelijk deel uitmaken van deze beleidsvelden, waarover u via de periodieke rapportages geïnformeerd wordt:
* de rapportages in het kader van Nationale Veiligheid en Bescherming Vitale Infrastructuur (over de voortgang van dit laatste onderwerp wordt u parallel aan deze brief geïnformeerd door de Minister van BZK)
* en de rapportage in het kader van het programma 'Veiligheid begint bij Voorkomen'.
Gelet op deze borging zal niet in een zelfstandige rapportagecyclus over deze bijgevoegde agenda worden voorzien.

Voor zover het de continuïteit van de ICT betreft en de weerbaarheid van de sector tegen diverse dreigingen zal de aanpak passen binnen het bredere kader van Nationale Veiligheid en Bescherming Vitale Infrastructuur. Eén van de rode draden in dit verband betreft 'ICT als doorsnijdend thema', omdat vrijwel alle (al dan niet vitale) sectoren in belangrijke mate van eigen ICT én openbare netwerken afhankelijk zijn.
Binnen dit kader wordt nauw samengewerkt met het bedrijfsleven, vanwege het feit dat het merendeel van de vitale infrastructuur in beheer is bij private bedrijven. In diverse PPS gelijkende samenwerkingsvormen is het bedrijfsleven betrokken bij de uitwerking en implementatie van de diverse beleidvelden rond ICT veiligheid. Waar nodig zal de samenwerking verder verdiept worden. In de agenda in de bijlage bij deze brief wordt dit nader aangegeven.

Preventie en bestrijding van cybercrime is een belangrijk thema in het programma Veiligheid begint bij Voorkomen, dat de invulling geeft aan de vijfde pijler van het kabinetsbeleid. Cybercrime is een breed begrip en omvat diverse vormen van criminaliteit: diverse vormen van fraude, verspreiding van illegale content, terrorisme, bedreiging, oplichting tot phishing. Elke vorm heeft zijn eigen bijzonderheden en aandachtspunten, dus een effectieve bestrijding van cybercrime vergt een gedifferentieerde aanpak.
Evenals bij andere vormen van criminaliteit begint een effectieve aanpak van cybercrime bij preventie. Hiertoe dienen kennis, kunde en middelen op orde te zijn. Daarnaast is vooral ook een goede samenwerking tussen burger, bedrijfsleven en opsporingsinstanties gewenst. In de voortgangsrapportages over Pijler V zal worden ingegaan op de voortgang van de preventie en bestrijding van cybercrime. Daarnaast zal de opsporing en vervolging van cybercrime geïntensiveerd worden door een betere toerusting van de opsporings- en vervolgingsinstanties.

Het verstevigen van de aanpak en het gezamenlijk optrekken leidt intrinsiek tot een professionaliseringsslag op de diverse onderwerpen en in de benodigde middelen. Er wordt niet ingezet op een apart traject hiervoor, de aandacht voor governance zal onderdeel zijn van de aanpak van de diverse onderwerpen op de agenda en daardoor effectiever zijn.

De gezamenlijke agenda voor ICT veiligheid volgt op de gebieden nationale veiligheid en bescherming vitale infrastructuur de elementen, die in de General Assembly van de Verenigde

Naties (30-01-2004: A/RES/58/199) genoemd zijn voor de bescherming van vitale informatie-infrastructuren. Ook voor de opsporing en vervolging kunnen deze elementen tot voorbeeld dienen voor een soortgelijke aanpak (voor zover relevant). In de bijlage wordt ingegaan op lopende en nieuwe activiteiten, die voor de komende periode onderdeel uitmaken van deze agenda.

Minister van Justitie,

(w.g.) dr. E.M.H. Hirsch Ballin

Minister van Binnenlandse Zaken en Koninkrijkrelaties,

(w.g.) dr. G. ter Horst

Staatssecretaris van Economische Zaken,

(w.g.) drs. F. Heemskerk

BIJLAGE

Gezamenlijke agenda op het gebied van ICT veiligheidsbeleid.

De gezamenlijke agenda is nooit af. Dit komt deels door het dynamische karakter van de ICT sector, waarin markt- en technologische ontwikkelingen zich in een hoog tempo opvolgen. Deels komt dit door het in elkaar overlopen van lopende activiteiten en de ambitie om met nieuwe activiteiten een antwoord te hebben op de snel veranderende ICT ontwikkelingen.

De agenda is derhalve een mengsel van lopende activiteiten en een vooruitblik naar verdere ambities, die zich nog niet in concrete activiteiten hebben vertaald. Het jaar 2007 was het jaar van de opbouw van de samenwerking en coördinatie en was tevens het jaar, waarin het kabinet heeft geïnventariseerd, waar aanvullende ambities en activiteiten zijn gewenst. Het jaar 2008 wordt het jaar van de inhoudelijke synergie. Justitie, BZK en EZ willen niet alleen onderling gezamenlijk optrekken, maar dat ook graag doen met het bedrijfsleven en andere betrokkenen.

Samenwerking betekent open staan voor een aanpak die ook de partners aanspreekt. Bij ICT veiligheidsbeleid is dat onontbeerlijk, omdat die partners grotendeels zélf de verantwoordelijkheid hebben om de preventieve maatregelen te treffen, die de veiligheid en de weerbaarheid rond ICT kunnen vergroten. De overheid stimuleert, ondersteunt en moet in de respons en bestrijdingsfase naadloos aansluiten bij hetgeen de partners reeds aan preventie hebben gerealiseerd. De ambitie is om in het jaar 2008 beter grip te krijgen, waar die aansluiting verbetering behoeft en dat zal zich in een zich verder ontwikkelende agenda vertalen.

De agenda kent een tweedeling, die aansluit bij de rapportagecycli van:
- Nationale Veiligheid en Bescherming Vitale Infrastructuur, respectievelijk
- Het kabinetsbeleid in pijler V: Veiligheid begint bij voorkomen.

Vervolgens worden de kopjes gebruikt, die aansluiten bij de indeling van maatregelen, zoals internationaal is geaccepteerd (indeling volgens structuur van de Genera Assembly van de Verenigde Naties).

Weerbare samenleving en continuïteit

Publiek-private samenwerking

In de vitale sectoren wordt de publiek-private samenwerking gestimuleerd teneinde ICT-verstoringen te voorkomen dan wel een voorspoedig herstel na uitval te bevorderen. Continuïteit van de dienstverlening vormt daarbij het uitgangspunt.
- Samenwerking overheid en aanbieders in Nationaal Continuïteitsoverleg Telecom (op basis van H14 TW)
- Samenwerking overheid en vitale sectoren in Strategisch Overleg Vitale Infrastructuren en Nationaal Adviescentrum Vitale Infrastructuren
- Samenwerking overheid en bedrijfsleven in het programma Nationale Infrastructuur Cybercrime (informatieknooppunten) gericht op ICT aspecten in de diverse aangesloten sectoren (waaronder SCADA systemen)

Voorlichting, bewustwording en ketensamenwerking
Op dit terrein zijn de beleidsinspanningen zowel gericht op voorlichting en bewustwording (bewust en veilig gebruik van ICT door het bedrijfsleven in de vitale sectoren) als op informatiedeling (o.a. via samenwerking in de keten) en preventie, gericht op het tegengaan van cybercrime. Tot de veiligheidsketen behoren de private partijen die ICT en telecommunicatiediensten leveren (alsmede hun belangrijkste leveranciers), de vitale gebruikers van ICT en telecom en de (overheids)partijen die vanuit inlichtingensfeer of in beleidsmatige zin een bijdrage kunnen leveren aan een optimaal presteren van deze keten. Hieronder volgt een opsomming van lopende en afgeronde activiteiten op dit vlak.

- Voorlichting in het kader van Nationale Veiligheid: gericht op burger, veiligheidsregio's en vitale bedrijfsleven
- Versterken informatieknooppunten rond ICT en vitale sectoren
- De in juni 2007 gehouden Oefening Shift Control was gericht op bewustwording en crisisbeheersing, de evaluatie ervan geeft o.a. aan dat communicatie en samenwerking in tijden van crisis verbeterd kunnen worden, wat zal leiden tot een intensievere oefenagenda.
- Binnen het programma DigiBewust wordt onder meer gerichte voorlichting over veilig gebruik van ICT gegeven aan de partners in de veiligheidsketen: particuliere gebruikers, MKB, onderwijs, e.a.
- De telecommunicatiesector is v.w.b. de openbaar aangeboden diensten voor een groot deel op (inter)nationale schaal georganiseerd en ook de ketensamenwerking houdt met deze schaal rekening. Hierbij worden alle partners in de veiligheidsketen betrokken.
- Binnen de landelijke crisisorganisatiestructuur wordt samen met LOCC en NCC gewerkt aan een nationaal responsplan gericht op een adequate respons bij grote ICT verstoringen.

Onderzoek en kennis
Om onderzoek en kennis op het gebied van ICT veiligheid te bevorderen zijn de banden met kennisinstellingen aangehaald en worden de mogelijkheden voor een gezamenlijke onderzoeksagenda onderzocht.

- Op basis van een inventarisatie van reeds lopende onderzoeken zal worden bezien welke aanvullende onderzoeksactiviteiten hiervoor benodigd zijn

Juridische randvoorwaarden
Binnen de maatschappijontwrichtende arena lijkt het juridisch kader toereikend voor alle partners in de veiligheidsketen om de maatregelen in preventieve en preparatiesfeer te treffen die nodig zijn. Dit laat onverlet dat lopende programma's gericht op het identificeren van keteneffecten en intersectorale afhankelijkheden nieuwe inzichten kunnen genereren, met inbegrip van juridische implicaties.

Intersectorale aanpak
De introductie van nieuwe technologieën (en daarmee afhankelijkheden) maakt structurele aandacht binnen de vitale infrastructuur voor de weerbaarheid en betrouwbaarheid van telecommunicatie/ICT noodzakelijk. Op basis ervan worden veel processen aangestuurd, en ook de afhankelijkheden tussen sectoren zijn in belangrijke mate telecommunicatie/ICT gerelateerd.

- Binnen het programma Bescherming Vitale Infrastructuur worden de intersectorale afhankelijkheden in 2008 op basis van scenario-ontwikkeling nader verkend, opdat een (nationale) risicobeoordeling mogelijk wordt. Op voorhand is duidelijk, dat telecommunicatie/ICT op vrijwel alle andere sectoren een belangrijke invloed heeft.
- Omgekeerd zal ook worden bezien wat de telecommunicatie/ICT-sector aanvullend kan doen om geprepareerd te zijn op dreigingen als overstromingen en pandemieën.

Internationaal
De internationale agenda met betrekking tot continuïteit omvat de bescherming van de vitale (informatie) infrastructuur (cybersecurity) en de weerbaarheid van ICT en telecommunicatie als sector.

- De Europese Commissie overweegt een richtlijn (EPCIP) omtrent de Europese samenwerking en afstemming rond ‘Critical Infrastructure Protection’. Deze richtlijn is gericht op grensoverschrijdende gebruik van vitale infrastructuren (waaronder ICT en telecom) en vormt het kader waarbinnen lidstaten de onderlinge (grensoverschrijdende) samenwerking vorm kunnen geven.
- Rond SCADA-systemen (regel- en meetsystemen op afstand), die bij veel vitale infrastructuren worden toegepast, wordt in Europees verband kennis uitgewisseld, waarbij Engeland, Nederland en Zweden een trekkende rol vervullen.
- In diverse internationale gremia komt bescherming en weerbaarheid van ICT en telecommunicatie aan de orde: civiele NAVO; Europese Commissie, OESO, VN
- De samenwerkende Europese lidstaten ontwikkelen samen met de Europese Commissie een uitwerking van ‘best practices’ met betrekking tot de weerbaarheid van telecomdiensten. DG Information Society heeft hiertoe enkele studies laten verrichten. Het uitwisselen van best practices helpt om de aanpak internationaal op elkaar afgestemd te krijgen. Bovendien helpt het internationaal opererende telecombedrijven om de maatregelen generiek te implementeren en niet per lidstaat een andere aanpak te hoeven volgen.

Preventie en bestrijding cybercrime
Publiek-private samenwerking
Aanbieders en gebruikers van ICT en telecommunicatie maken deel uit van de veiligheidsketen, waarvan de ambitie is deze goed werkend te krijgen. Vooral op het gebied van preventie ligt de sleutel bij bewuste en alerte gebruikers.

- het programma NICC (Nationale Infrastructuur Cybercrime) is een tijdelijk programma om de bestaande partners in de veiligheidsketen (OM, politie, OPTA, GovCert, Consumentenautoriteit, CBP, e.d.) te ondersteunen en samen met de private sector instrumenten te ontwikkelen voor een effectieve preventie en samenwerking, bijvoorbeeld de ontwikkeling van een modelontwerp gericht op Notice & Takedown (dat wil zeggen filtering of blokkering van buitenlandse websites).

- Binnen het programma DigiBewust wordt samengewerkt tussen overheid en bedrijfsleven (aanbieders, softwareleveranciers) om de programma-activiteiten in te richten en inhoudelijk vorm te geven.
- Vertegenwoordigers van NL bedrijfsleven en kennisinstellingen zijn lid van of betrokken bij de permanent stakeholdersgroup van ENISA, het Europese agentschap dat programma's ontwikkelt voor een versterking van de bestrijding van Cybercrime.

Voorlichting, bewustwording en ketensamenwerking

Cruciaal voor het tegengaan van cybercrime is samenwerking tussen de bestaande partijen in de veiligheidsketen, waaronder het bedrijfsleven: aanbieders en gebruikers hebben daarin een rol. Preventie van cybercrime kan alleen als alle partijen in de veiligheidsketen (waaronder nadrukkelijk ook aanbieders en gebruikers) bewust omgaan met hun eigen veiligheid.

- Het programma DigiBewust richt zich onder meer op voorlichting, kennisuitwisseling en bewustwording bij (groot)gebruikers. De afgelopen periode is gewerkt met specifieke doelgroepen, waaronder de jeugd (onder in samenwerking met scholen), MKB en komend jaar zal de focus op senioren liggen.
- Via de service 'Waarschuwingsdienst' kan iedere Nederlander zich gratis abonneren op de door GovCERT afgegeven waarschuwingen rond kwetsbaarheden in systemen en virusdreigingen. De website van GovCERT geeft aan gebruikers allerlei tips.
- Op www.samentegencybercrime.nl is informatie te vinden over het programma NICC en de wijze waarop geïnteresseerden zich daarbij kunnen aansluiten. Het (tijdelijke) programma NICC is erop gericht de werkwijzen te ontwikkelen, waarop de partners in de veiligheidsketen hun rol optimaal kunnen vervullen. Het programma heeft daartoe PPS hoog in het vaandel staan.
- De VbbV brief over Pijler V besteed aandacht aan verdere toerusting en professionalisering van OM en politie
- Als onderdeel van de informatie uitwisseling tussen de ketenpartners, wordt onderzocht in welke mate tot een gezamenlijke trendrapportage gekomen kan worden

Onderzoek en kennis

Om onderzoek en kennis op het gebied van ICT veiligheid te bevorderen zijn de banden met kennisinstellingen aangehaald en wordt de wenselijkheid van een gezamenlijke onderzoeksagenda onderzocht.

- Via de informatieknooppunten en het programma DigiBewust vindt tussen private en publieke organisaties uit de vitale sectoren kennisuitwisseling plaats rond dreigingen en oplossingen met betrekking tot ICT verstoringen
- In OESO verband is een studie van de TU Delft vrijwel afgerond inzake 'economische incentives rond voorkomen en bestrijden cybercrime'

Juridische randvoorwaarden
Mogelijk vergt en effectief beleid van preventie en bestrijding van cybercrime nadere wet- en regelgeving. Waar in de praktijk tegen een dergelijke noodzaak wordt aangelopen, zal het kabinet adequaat reageren.

- Het uitwerken van de juridische randvoorwaarden met betrekking tot Notice & Takedown voor diverse vormen van criminaliteit (phishing, kinderporno, haatzaaien)

Intersectorale aanpak
Preventie en bestrijding van cybercrime vergt een gedifferentieerde aanpak, omdat diverse soorten van cybercrime andere partijen en andere omstandigheden betreffen. Dit neemt niet weg, dat in een praktische aanpak leerervaringen uitgewisseld kunnen worden om te bezien of deze toepasbaar kunnen zijn in een andere situatie.

- Uitwisseling ervaringen tussen sectorale informatieknooppunten onderling en met de overheidsdiensten (AIVD, GOVCERT, OM)

Internationaal
Cyberspace kent geen grenzen. Het internationale en dynamische karakter van cybercrime noodzaakt tot internationale samenwerking.

- In Europees, Civiel NAVO en OESO verband zal samenwerking met de internationale gemeenschap versterkt worden, waar dat passend en mogelijk is zal bij activiteiten of projecten kennis en ervaring ingebracht worden.
- Internationale samenwerking tussen CERTs en ISP’s zal meer gestimuleerd worden.