ICT-kwetsbaarheid en Nationale Veiligheid

NOTITIE Nº 02 | 10 | 10

DENKTANK
NATIONALE
VEILIGHEID

ICT-kwetsbaarheid en Nationale Veiligheid

Notitie N° 02 | 10 | 10
ISBN/EAN: 978-94-91040-17-7

Auteurs: *Aksel Ethembabaoglu, Erik Frinking, Michel Rademaker*

Grafisch ontwerp: *Studio Maartje de Sonnaville, Den Haag*
Drukwerk: *Koninklijke De Swart, Den Haag*

Den Haag Centrum
voor Strategische
Studies

Lange Voorhout 16
2514 EE Den Haag
Nederland

info@hcss.nl
www.hcss.nl

ICT-kwetsbaarheid en Nationale Veiligheid

DENKTANK NATIONALE VEILIGHEID: NOTITIE Nº 02 | 10 | 10

DENKTANK
NATIONALE
VEILIGHEID

De Denktank Nationale Veiligheid heeft als doel het verhelderen van maatschappelijke vraagstukken die samenhangen met en van belang zijn voor de nationale veiligheid in Nederland. De Denktank stimuleert het debat en publiceert nieuwe en vernieuwende inzichten. Hierdoor draagt de Denktank bij aan het verbeteren van het kennisniveau over nationale veiligheid bij publiek, pers, de wetenschappelijke gemeenschap en de beleidswereld. De Denktank doet dit op basis van eigen onderzoek en analyse en in samenwerking met de bestaande kennisbasis in Nederland en Europa. Hierbij betrekt de Denktank actief de netwerken van de deelnemers.

De Denktank Nationale Veiligheid is een initiatief binnen de strategie Nationale Veiligheid. Producten van de Denktank zijn openbaar en worden tevens aangeboden aan de interdepartementale Stuurgroep Nationale Veiligheid.

De Denktank bestaat uit een vast kernteam onder leiding van Prof. Dr. Rob de Wijk (directeur Den Haag Centrum voor Strategische Studies) en een per thema wisselende groep experts uit het bedrijfsleven, de wetenschap en maatschappelijke organisaties.

Inhoudsopgave

1 Introductie

Elektronische aanvallen en digitale spionage vinden wereldwijd in toenemende mate plaats. Ook in Nederland komt dit steeds meer voor.[1] 'De AIVD heeft in Nederland meerdere digitale aanvallen vanuit verschillende landen waargenomen die een steeds gerichter en specifieker karakter hebben gekregen. Vooral overheidssectoren en het bedrijfsleven zijn doelwit van digitale spionage', schrijft de AIVD in het jaarverslag van 2009. De aanval op Google, Adobe en tientallen andere bedrijven van begin 2010 was zo geavanceerd dat diverse getroffen partijen verdenkingen van bemoeienis van de Chinese overheid met de aanvallen uitten. Melissa Hathaway, voormalig senior adviseur cyber security van zowel President Bush als Obama, verklaarde tijdens een recent bezoek aan Nederland dat door deze aanval 2100 bedrijven in Amerika ernstige problemen ondervonden. Bij de aanval werden zwakke plekken in de beveiliging van Internet Explorer gebruikt om op servers informatie uit Google accounts van mensenrechtenactivisten te bekijken en intellectueel eigendom en de broncode van software van bedrijven te stelen. De financiële schade hiervan is moeilijk te bepalen, maar wordt als omvangrijk geschat.

De leden van de Denktank Nationale Veiligheid is verzocht hun oordeel over ICT-kwetsbaarheid te geven door deze te beoordelen in de context van de Strategie Nationale Veiligheid. Op basis van deze analyse is de leden tevens gevraagd mee te denken over mogelijke beleidsimplicaties en handelingsperspectieven. De discussie heeft zich op een aantal vraagstukken gericht:

- Er is vooralsnog beperkte informatie en er zijn beperkte inzichten over de exacte aard en oorsprong van de bedreigingen voor ICT-kwetsbaarheid. Is het onderwerp een hype of niet?
- Brengen maatregelen ter verlaging van ICT-kwetsbaarheid een *return on investment* met zich mee of moeten deze maatregelen voornamelijk als last worden gezien?

1 AIVD, Jaarverslag 2009; GovCert, jaarverslag 2009; Govcert, Trendrapport 2009: Cybercrime in trends en cijfers; KLPD, Dienst Nationale Recherche, 2009.

- Wat kunnen de overheid en het bedrijfsleven hierin betekenen zodat maatschappelijk draagvlak voor de te nemen maatregelen wordt bereikt?
- Zijn traditionele middelen van de overheid zoals marktordening en –regulering in het brede en multinationale domein effectief en welke alternatieven heeft de overheid?
- Welke balans in overkoepelende coördinatie en regie enerzijds en zelfstandige verantwoordelijkheid anderzijds is noodzakelijk?

De verkregen inzichten uit deze discussie zijn in de analyse van deze notitie verwerkt.

2 Hoe kan ICT-kwetsbaarheid worden gekenschetst?

Digitale aanvallen en verstoringen zijn zeker niet nieuw. Een traditioneel voorbeeld van een van de eerste 'hacking' incidenten betreft de vernietiging van een geponste aandrijving van een geautomatiseerde weefmachine in Frankrijk in 1820. Maar de meeste voorbeelden zijn uiteraard van recentere aard. Kevin Mitnick begon in de jaren 80 van de 20ste eeuw computersystemen van Motorola, NEC, Nokia, Sun Microsystems and Fujitsu Siemens te hacken. De omvang, de mate van professionaliteit, het technisch vernuft en de effecten van de aanvallen nemen in de 21ste eeuw echter steeds meer toe. En zoals in het voorbeeld van Google in de introductie van deze notitie al werd geschetst, is de mogelijke betrokkenheid van statelijke actoren een reële mogelijkheid. Daarnaast zijn criminele activiteiten, waarbij geldelijk gewin voorop staat, tegelijk met de toename van digitale economische transacties, al jaren in opgang.

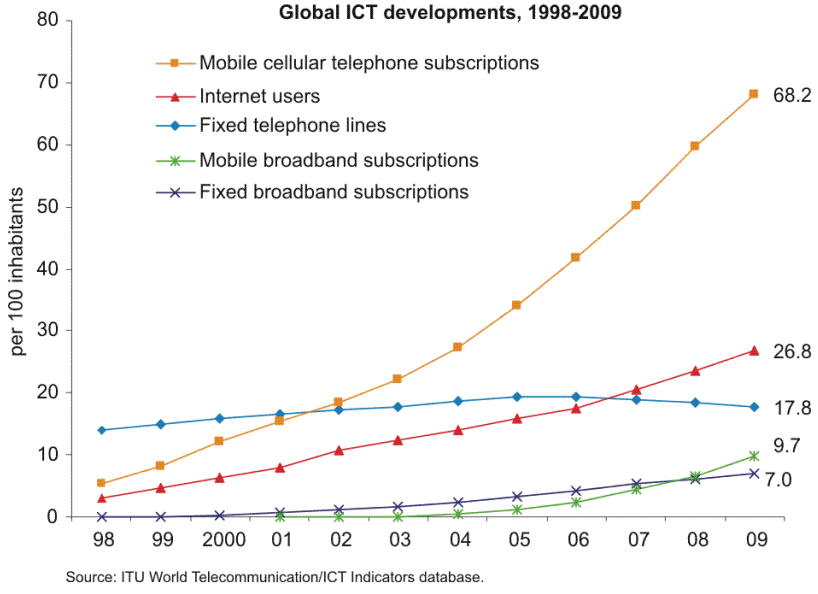
Waar vroeger lokale computers werden geïnfecteerd, worden tegenwoordig volledige systemen van bedrijven besmet. Ook landen als geheel krijgen steeds meer te maken met aspecten van ICT-kwetsbaarheden. Bij deze laatste vorm van kwetsbaarheid is er mogelijk sprake van aantasting van de integriteit van een geheel land en het gebrek aan vermogen om hier tegen op te treden. Zo werden elektronische communicatiemiddelen van de overheid tijdens de Russische inval in Georgië lamgelegd, waardoor de overheid zowel intern als naar de burgers toe nauwelijks meer over de ontwikkelingen kon berichtgeven.

Tegelijkertijd speelt dat onze samenlevingen niet meer zonder de voordelen van ICT kunnen. Het maatschappelijk en economisch belang van het ICT-domein is onbetwist. Het economisch verkeer is er wereldwijd afhankelijk van geworden, sociale netwerken zoals Facebook en Twitter zorgen voor nieuwe verbintenissen binnen de samenleving en naast bedrijven digitaliseert ook de Nederlandse overheid steeds meer functies en gegevens. Veel privacygevoelige gegevens van burgers worden ter bevordering van dienstverlening digitaal opgeslagen. Kort gezegd, het gebruik van ICT is niet terug te draaien.

De groei van het gebruik, de toegevoegde waarde en daarmee de afhankelijkheid van internet en ICT-systemen worden breed ervaren. Van alledaagse activiteiten in het huishouden tot aan gespecialiseerde processen in bedrijven in allerlei verschillende domeinen: chips in het openbaar vervoer, smart grids, betalingsystemen in de financiële sector, voedselproductie, industrie, systemen in de zorg etc. worden in toenemende mate met ICT-systemen verbeterd, gekoppeld of efficiënter ingericht. Ook de activiteiten op sociale netwerken en het gebruik van online diensten worden steeds intensiever. Die groei zal zich blijven doorzetten.

De toenemende kwetsbaarheid loopt hand in hand met groeiende afhankelijkheid. Deze ontwikkeling roept een aantal wezenlijke vragen op:

- Hoe ernstig zijn dreigingen; wat zijn de gevolgen? Hoe gaat zich dit ontwikkelen?
- Zijn de gevolgen in het kader van Nationale Veiligheid relevant en substantieel?
- Hoe kan tegen de negatieve gevolgen worden opgetreden zonder daarbij de positieve aspecten te ondermijnen?



FIGUUR 1 GROEI VAN VERSCHILLENDE ICT TOEPASSINGEN (BRON: ITU)

Voor het beantwoorden van deze vragen schetst deze notitie allereerst een analytisch kader. Dit kader beschouwt naast de bronnen die onze ICT-infrastructuur kunnen aantasten ook de elementen die door bewust handelen van mensen of door natuurlijke omstandigheden en menselijk falen worden getroffen. Het kan om zowel ICT-systemen gaan die onderdeel van grote netwerken zijn en veelal via internet of satellietcommunicatie met elkaar zijn gekoppeld als om zelfstandige systemen die (vooralsnog) eigenstandig opereren en niet met andere ICT-infrastructuren zijn verbonden.

Daarmee komt de vraag op welke capaciteiten Nederland nodig heeft om de mogelijke kwetsbaarheden te voorkomen of te herstellen. Moeten deze capaciteiten in handen van de overheid of het bedrijfsleven zijn of internationaal worden belegd. Deze beoordeling moet worden afgezet tegen capaciteiten die al beschikbaar zijn. Deze capaciteiten kunnen worden ingezet om taken langs de gehele veiligheidsketen uit te voeren, variërend van preventie tot respons en vervolging. Belangrijk is te bezien hoe deze verdeling van capaciteiten momenteel is georganiseerd en afgestemd en of dit op een effectieve en efficiënte wijze gebeurd. Kortom, hoe is de regie georganiseerd?

Deze laatste vraag is des te relevanter naar aanleiding van de motie van de Tweede Kamerleden Knops, Voordewind en Eijsink van december 2009 om in interdepartementaal verband een Nederlandse cybersecuritystrategie te ontwikkelen. In de tweede helft van 2010 worden de aanzetten hiertoe afgerond. In deze notitie zijn de bovenstaande elementen als uitgangspunt genomen. Het stuk geeft een overzicht van de gepercipieerde huidige en toekomstige gevaren en dreigingen en hoe deze de nationale veiligheid raken. Het verschaft inzicht in de beleidsontwikkelingen in andere landen en presenteert uitdagingen die op het gebied van ICT-kwetsbaarheid voor een effectiever beleid moeten worden aangepakt. Aansluitend zijn de uitgangspunten besproken voor de keuze van de te nemen maatregelen. Tenslotte zijn de maatregelen benoemd die kunnen worden ondernomen.

3 De kwetsbaarheid van Nederland

3.1 De reikwijdte van ICT-kwetsbaarheid

Er worden diverse begrippen gebruikt om het domein waarin ICT-kwetsbaarheden worden ervaren te duiden zoals cyberspace, internet, en digitale omgeving. Overheden, organisaties, en instituties hanteren hiervoor diverse definities.[2]

Het East West Institute hanteert de volgende definitie voor cyberspace: *'Cyberspace comprises IT networks, computer resources, and all the fixed and mobile devices connected to the global internet. They are connected through undersea cables, satellites in outer space, land lines, and radio links'*.[3]

Uit deze definitie komt helder naar voren dat cyberspace meer is dan alleen dé desktopcomputer of hét internet. Feitelijk gaat deze definitie uit van alle bestaande infrastructuur tussen de computer, het internet, en mobiele applicaties. De gekoppelde infrastructuur en de gedeelde toegang en functionaliteit die dat oplevert, wordt daarbij als een essentieel ingrediënt van cyberspace gezien. Deze koppeling is, naast de waarde die dat oplevert, ook het voornaamste richtpunt van de kwetsbaarheid.

Tegelijkertijd beperkt deze definitie zich tot IT, telecommunicatiediensten en -producten die met elkaar verbonden zijn. In onze beschouwing omvat cyberspace echter meer dan de ICT-systemen die zijn aangesloten op het 'global internet'. Deze conceptie wordt door de volgende definitie het best verwoord:

2 Zie voor een illustratie overzicht van deze definities bijvoorbeeld M. Klaver, H.A.M. Luiijf, Cyberspace als militaire dimensie, TNO Defensie en Veiligheid, Den Haag, 2010 (TNO DV2010 A136), bijlage A, p.1

3 Bajaj K., East West Institute, The Cyber Security Agenda: Mobilizing for International Action, 2010.

'Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunication networks, computer systems, and embedded processors and controllers.'[4]

Chips in bankpassen, medische en huishoudelijke apparatuur en ICT in vervoersmiddelen maken ook deel uit van het ICT-domein, net zoals auto's die communiceren met de buitenwereld. In 2015 moet iedere nieuwe auto bij een crash automatisch 112 bellen en sommige autoverhuurbedrijven in de Verenigde Staten kunnen gestolen auto's op afstand stil zetten en kunnen de claxon laten afgaan. Slechts een klein percentage van deze ICT-systemen is nu nog verbonden met het internet, maar in toenemende mate komen deze ICT-systemen echter ook 'online'. Zo brengt LG een koelkast op de markt met een voedselmanagementsysteem en een internetverbinding. Ook al deze systemen zullen in de discussie in ogenschouw moeten worden genomen. De afhankelijkheid in het gebruik neemt toe en daardoor de kwetsbaarheid voor misbruik en uitval. Hierdoor worden de effecten voor de samenleving gevoeld. Bovendien veranderen de ontwikkelingen in dit gebied razendsnel en vereisen daarom flexibiliteit en aanpassingsvermogen.

De verwachting is dat het te beschouwen domein in omvang en intensiteit alleen maar toeneemt. Wat logischerwijs te beredeneren valt, is dat met steeds meer gebruikers op internet, steeds meer programma's en applicaties (ook voor mobiel internet en telefoon) er ook steeds meer mogelijkheden zijn die uitgebuit of misbruikt kunnen gaan worden.

3.2 Elementen van ICT-kwetsbaarheid

In de discussie rondom ICT-kwetsbaarheid zijn verscheidene dimensies te onderscheiden. De wijze van bedreiging (virus, botnet, inbraak en dergelijke), de motivatie voor bedreiging (zoals geldelijk gewin, grappenmakerij, ideologische dominantie), het effect van de bedreigde kwetsbaarheid (van aantasting integriteit betrouwbaarheid gegevens tot fysiek lijden), de getroffen partijen (individuen, organisaties, overheden, vitale nationale infrastructuren) of de systemen (IT infrastructuur, mobiel dataverkeer, elektriciteitsnetwerken, voor economische transacties) zijn verschillende aspecten van ICT-kwetsbaarheid.

4 Deze definitie is afkomstig uit Amerikaanse Department of Defense (2008)

Er zijn vele verschijningsvormen die de geschetste aspecten van ICT-kwetsbaarheden weergeven. Hoewel voorbeelden van deze verschijningsvormen op zich niet het richtpunt van de identificatie van mogelijke effectieve capaciteiten hoeven te zijn, helpen ze wel om kwetsbaarheden concreet en tastbaar te maken. Een belangrijk onderscheid in verschijningsvorm wordt gegeven door het verschil tussen moedwillige aanvallen en onbedoelde uitval. Cybercriminaliteit, cyberwarfare, cyberspionage en cyberterrorisme zijn vier verschijningsvormen van moedwillige dreigingen.

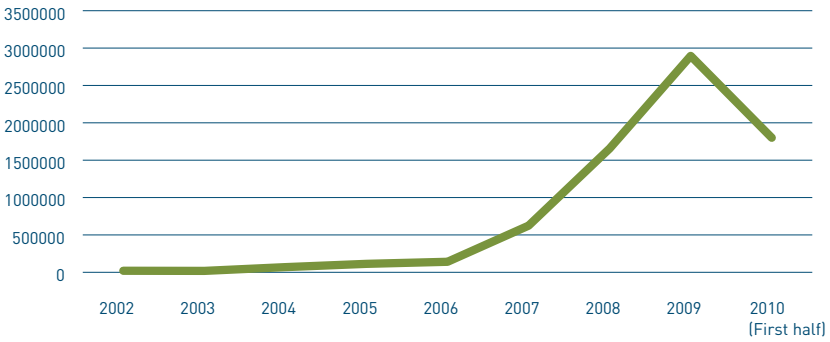
Onder cybercriminaliteit valt enerzijds criminaliteit specifiek gericht op elektronische netwerken, zoals computervredebreuk of spam-aanvallen. Cybercrime kan ook 'traditionele' criminaliteit zijn waarbij digitale instrumenten gebruikt worden, bijvoorbeeld oplichting of smaad.[5] Deze tweedeling kan in feite door alle verschillende verschijningsvormen worden ervaren: cyberspace als middel en tevens als object of terrein van ICT-kwetsbaarheid. Door middel van verspreide malware worden veelal persoonlijke gegevens en bankgegevens van internet gebruikers verzameld. Zo worden gestolen creditcardgegevens misbruikt om illegale aankopen te doen (de kosten van gestolen creditcard informatie ligt tussen de $0,06 -$30) [6] of er wordt fraude gepleegd met gestolen identiteitsgegevens.

Het KLPD heeft recentelijk aangegeven dat cybercriminaliteit een ernstige toename kent en dat deze groei zich vooralsnog zal doorzetten, in sommige deelgebieden tot 100% per jaar. [7] Tevens merkt de dienst op dat de grens tussen high-tech crime en andere vormen van criminaliteit aan het vervagen is. Ook diverse internet security bedrijven nemen een sterke toename in malware waar, die zich zowel op overheden, private organisaties en burgers richt. McAfee gaf aan dat het aantal malware varianten van 1,5 miljoen in 2008 naar 2,7 miljoen in het eerste half jaar van 2009 was gestegen. De ontwikkelingen in malware worden goed geïllustreerd door de onderstaande grafieken, die door twee voorname organisaties die burgers en bedrijven helpen bij het beveiligen van hun IT omgeving zijn geproduceerd.

5 Een samensmelting hiervan is ook mogelijk waarbij het digitaal ontvreemden van on-line gegevens gebruikt wordt voor het doen van illegale digitale transacties

6 Symantec Internet Security Threat Report, april 2009

7 Korps landelijke politiediensten (KLPD), Dienst Nationale Recherche, Overall-beeld Aandachtsgebieden KLPD, Driebergen, juli 2010, p.22



FIGUUR 2 NIEUWE TYPES MALWARE BEDREIGINGEN DIE JAARLIJKSE WORDEN GEDETECTEERD (BRON: SYMANTEC CORP)

Ook de daadwerkelijke effecten van deze malware worden steeds breder gevoeld. In de Verenigde Staten waren er in 2008 al 313.982 klachten bij de Federal Trade Commission ontvangen over identiteitsfraude. [8]

Een belangrijk deel van malware dreigingen wordt gebruikt door criminele organisaties, maar ook individuele actoren doen mee aan deze ontwikkeling. Hackers kunnen personen, organisaties en overheden afpersen of chanteren door het penetreren, manipuleren en controleren van hun ICT-systemen en het compromitteren van computers voor gebruik in grootschalige botnets.[9] Een botnet kan vervolgens gebruikt worden voor een digitale aanval. Zo kan een enkeling met beperkte technische kennis een botnet opzetten om daar vervolgens een zogenaamde distributed *denial of service attack*, mee uit te voeren. Dit type aanval overbelast een computer of server zodanig dat deze niet meer functioneert.

8 Federal Trade Commission, februari 2009, Consumer Sentinel Network Data Book for January – December 2008

9 In deze notitie refereert de term 'Botnets' naar een collectie van aan elkaar gekoppelde computers die op afstand kunnen worden bestuurd met mogelijke kwaadwillige intenties.

Er zijn daarnaast talrijke voorbeelden van individuen die niet noodzakelijkerwijs op geldelijk gewin uit waren, hoewel hun activiteiten wel als illegaal worden beschouwd. In Ohio werd in 2003 het procescontrolesysteem van de nucleaire reactor Davis-Besse geïnfecteerd met de SQL Slammer worm. De beveiligingsparameters voor de weergavesystemen werden geïnfecteerd waardoor het systeem vijf uur lang niet bruikbaar was, inclusief de centrale procescomputer die niet functioneerde en zes uur lang was uitgeschakeld.[10] In 2008 wist een hacker in Polen de tramwissels te manipuleren met een aangepaste afstandsbediening waardoor vier trams ontspoorden en er twaalf gewonden vielen.[11] In 2009 zorgde een medewerker van een Amerikaans olieplatform, die onenigheid had met zijn werkgever, ervoor dat lekkages van olie en gas niet meer in het systeem zichtbaar konden worden gemaakt.[12]

Van geheel andere orde is cyberwarfare. Dit is gerelateerd aan digitale, statelijke capaciteiten die politieke belangen en militaire operaties ondersteunen. Bijvoorbeeld digitale aanvallen om militaire installaties te verstoren. In 2008 viel Rusland buurland Georgië binnen waarbij het, naar verluidt, ondersteunende digitale aanvallen uitvoerde. De aanvallen zouden de C3I (Command, Control, Communications and Intelligence) van Georgië gedurende het begin van de Russische invasie hebben verstoord. Hierdoor was de Georgische overheid niet tot adequaat handelen in staat. Soms worden aanvallen op politieke en militaire belangen ook ondersteund door non-statelijke actoren en capaciteiten.

In het geval van cyberspionage worden overheden en organisaties doelbewust aangevallen om informatie in te winnen voor inlichting en doeleinden. Vanuit een internationaal-politieke context is zowel politieke, (bijvoorbeeld langjarige visies of onderhandelingsstrategieën) als militaire informatie (bijvoorbeeld onderzoeksresultaten of operationele informatie) interessant. Het wereldwijde digitale spionage netwerk GhostNet, vermoedelijk door China opgezet, spioneerde op computers van (politieke) organisaties in meer dan 100 landen.[13] Daarnaast wordt bedrijfsvertrouwelijke informatie op ICT-systemen ontvreemd voor economisch gewin. Zo constateert de AIVD in verscheidene publicaties dat de dreiging van digitale spionage steeds meer toeneemt, waarbij vooral overheidsdiensten en

10 'Toeval speelt vaak een belangrijke rol', Eric Luiijf, TNO Magazine, juli 2010.
11 Ibid., p.8
12 Ibid. 'Toeval speelt vaak een belangrijke rol', Eric Luiijf, TNO Magazine, juli 2010.
13 Zie: http://www.infowar-monitor.net/

het bedrijfsleven doelwit zijn.[14] Hierbij zijn gegevens op gekoppelde computersystemen en de uitbesteding van ICT-gerelateerde activiteiten kwetsbare elementen.

Het begrip cyberterrorisme kent vele verschillende definities. In 2008 omschreef Ir. H.A.M. Luiijf cyberterrorisme als '[...] het - al dan niet in samenspanning – opzettelijk plegen van of dreigen met onrechtmatige acties tegen de integriteit, vertrouwelijkheid en beschikbaarheid van informatie en informatieverwerkende systemen en –netwerken zodat dit leidt tot één of meer van de volgende gevolgen'.[15] De gevolgen die beschreven zijn, hebben stuk voor stuk betrekking op de aantasting van de vitale belangen van de nationale veiligheid.[16] De Nationaal Coördinator Terrorismebestrijding (NCTb) bekeek in het vernieuwde rapport *Jihadisten en het internet* vooral de wijze waarop het internet door Jihadisten voor operationele en ondersteunende doeleinden wordt gebruikt. Daarin werd aangegeven dat Jihadisten het internet vooral als middel voor propaganda en rekrutering benutten. Aanvallen tegen of via het internet zijn wel mogelijk, maar grootschalige aanvallen worden niet als waarschijnlijk beschouwd.[17]

Bij de genoemde verschijningsvormen komt naar voren dat vooral de intentie verschillend van elkaar is. Ook kunnen moedwillige aanvallen aanzienlijk verschillen in hun graad van organisatie. Tegelijkertijd vindt de manier waarop de kwetsbaarheid aan het licht komt op gelijke wijze plaats; via het plaatsen van virussen, botnets of simpelweg via inbraak van systemen. Het falen van systemen kan moedwillig of door menselijke fouten hebben plaatsgevonden. Attributie van dergelijke incidenten is daarom niet altijd eenvoudig.

14 'Digitale Spionage, wat is het risico?', Algemene Inlichtingen en Veiligheidsdienst, Den Haag, januari 2010; Kwetsbaarheidsanalyse spionage: spionagerisico's en de nationale veiligheid, Algemene Inlichtingen en Veiligheidsdienst, Den Haag, februari 2010

15 H.A.M. Luiijf, 'Cyberterrorisme', in E.R. Muller, U. Rosenthal, R. de Wijk (red), Studies over terrorisme en terrorismebestrijding, 2008, Deventer, Kluwer.

16 Ook de FBI gebruikt een definitie die intentie, middel en beoogd effect met elkaar combineert: 'According to the U.S. Federal Bureau of Investigation, cyberterrorism is any 'premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents. Unlike a nuisance virus or computer attack that results in a denial of service, a cyberterrorist attack is designed to cause physical violence or extreme financial harm.'

17 Nationaal Coördinator Terrorismebestrijding, Jihadisten en het internet, 2009

Moedwillige aanvallen krijgen vaak grote aandacht en kunnen voor publieke onrust zorgen. Toch is de inschatting dat de waarschijnlijkheid van ICT-gerelateerde incidenten van menselijk falen en systeemfalen groter is. De kwetsbaarheden voor menselijke fouten of voor ICT-systeemfalen komen minder voor het voetlicht en worden wellicht als minder ernstig gepercipieerd. Maar een onderhoudsmonteur die met een virus besmette laptop inplugt op het netwerk van een raffinaderij, drinkwaterbedrijf, elektriciteitsproducent of de flesafvulinstallatie van een grote bierbrouwer kan ernstig de werkzaamheden schaden, een situatie die met regelmaat kan voorkomen.[18]

Incidenten ontstaan veelal door natuurlijke rampen, ongelukken, het falen van systemen of het onbewust handelen van mensen. In 2005 vernielde de orkaan Katrina in New Orleans een groot aantal ICT-systemen waardoor de federale en regionale overheden het zicht op de situatie na de ramp kwijt waren. In hetzelfde jaar vond in het Verenigd Koninkrijk een grote explosie bij de Buncefield raffinaderij plaats waarbij de computersystemen van het nabijgelegen ICT-bedrijf Northgate Information Solutions werden vernietigd. Hierdoor konden zij geen diensten aan hun cliënten leveren, waaronder ziekenhuizen.

Een vergelijkbaar ongeluk vond plaats aan de kust voor Egypte waar twee schepen in een storm terecht kwamen en hun ankers over de zeebodem lieten slepen. Hierdoor werden twee communicatiekabels stukgetrokken wat tot een daling van 75% van de Internetcapaciteit in het Midden-Oosten en India leidde.[19] Storingen in de procescontrolesystemen voor de drinkwatervoorziening in het oosten van Nederland leidden tot gebroken leidingen en uitval van de watervoorziening.[20] Ook het uitbrengen van een verkeerde upgrade van het antivirus programma van McAfee in april 2010 leidde tot grootschalige en langdurige uitval van computers over de gehele wereld.

18 'Toeval speelt vaak een belangrijke rol', Eric Luiijf, TNO Magazine, juli 2010.

19 House of Lords report, Protecting Europe against large-scale cyber-attacks, 2010, pp.12-13

20 NICC, Process Control Security in het Informatieknooppunt Cybercrime, november 2009, p.12

Een samenvattend overzicht van typen moedwillige en niet moedwillige bronnen en de effecten die zij kunnen veroorzaken, is in de onderstaande tabel geschetst. Daarbij zijn een aantal bekende en wellicht minder bekende 'cases' genoemd.

MOEDWILLIGE HANDELEN	VOORBEELDEN	VOORNAAMSTE ACTIVITEITEN EN EFFECTEN
Hackers en hacktivisten	Kevin Mitnick, 'Kaas', the Hacktivismo group, Young hackers against Terrorism (Yihat)	Illegale aanpassingen op websites, verlies van persoonsgegevens, ongewenste propaganda, spionage bij overheid en bedrijfsleven (cybercriminaliteit en cyberspionage)
Criminelen	Shadowcrew, Carderplanet	Fraude, identiteitsdiefstal, diefstal van persoons- en bankgegevens, aanvallen op financiële instituties (cybercriminaliteit)
Terroristen	Al-Qaeda (voor rekrutering en communicatie, niet voor gecoördineerde aanvallen)	Onderlinge communicatie, ongewenste propaganda, fraude ter ondersteuning van terroristische activiteiten (Cyber terrorisme)
Staten	Verenigde Staten, China, Rusland	Spionage bij overheid en bedrijfsleven, digitale aanvallen op landen en organisaties (Cyber warfare en cyberspionage)
SYSTEEMFALEN EN ONBEWUST HANDELEN	**VOORBEELDEN**	**VOORNAAMSTE EFFECTEN**
Natuurgeweld	Onweer, hoosbuien, stormen, sneeuw, hitte	Grootschalige uitval van systemen, cascade effecten en maatschappelijke onrust
Techniek	Defecte hardware, softwarefout • gebrek aan technologische vernieuwing • complexiteit	Willekeurige uitval met zeer uiteenlopende vormen van effecten
Menselijke fouten	Bedieningsfout, menselijke slordigheid	Identiek aan technisch falen

De bescherming tegen deze dreigingen wordt steeds vaker omvat door de term cyber security. Er speelt daarbij een paradox: hoe betrouwbaarder onze vitale digitale/ICT-infrastructuur is, des te groter de impact van verstoringen.[21]

De toenemende groei van ICT-systemen in organisatorische processen en in de samenleving zorgen ervoor dat de waarschijnlijkheid en impact van incidenten zal toenemen. Grote groepen mensen maken gebruik van sociale netwerken waar zij vrijelijk persoonlijke gegevens delen. LinkedIn, Facebook en Hyves zijn rijke bronnen van persoonlijke informatie die gebruikt kunnen worden voor digitale aanvallen. Bedrijfsprocessen maken steeds vaker gebruik van 'cloud computing' diensten waarbij informatie opgeslagen wordt op de 'cloud', een centraal, maar fysiek gedecentraliseerd verzamelpunt. Daarnaast wordt steeds vaker van voice-over-IP (VOIP) telefonie gebruik gemaakt. Dit bespaart kosten in de ICT-infrastructuur van bedrijven maar brengt nieuwe risico's met zich mee omdat de eigen controle over gegevens en systemen wordt verminderd. Tot slot zal de toenemende integratie van online ICT-systemen in nieuwe en alledaagse systemen en objecten, bijvoorbeeld in kleding, auto's of huizen, nieuwe mogelijkheden bieden om de nationale veiligheid te bedreigen. Medische ICT-systemen kunnen worden aangevallen, bijvoorbeeld door alle pacemakers te hacken en massaal hartaanvallen te veroorzaken.[22]

21 'Toeval speelt vaak een belangrijke rol', Eric Luiijf, TNO Magazine, juli 2010.

22 KLPD High Tech Crime, Criminaliteitsbeeldanalyse 2009, p. 145

4 ICT-kwetsbaarheid en Nationale Veiligheid

4.1 De effecten van ICT-kwetsbaarheid

De waarschijnlijkheid en consequenties van ICT-kwetsbaarheid kunnen groot zijn en door integratie van systemen in verschillende domeinen verder toenemen. De Strategie Nationale Veiligheid definieert dreigingen voor de nationale veiligheid als dreigingen die de vitale belangen van Nederland in gevaar brengen en er sprake is van potentiële maatschappelijke ontwrichting.[23] De vitale belangen omvatten de volgende elementen:

- territoriale veiligheid
- fysieke veiligheid
- economische veiligheid
- ecologische veiligheid
- sociale en politieke stabiliteit.

De dreigingen in het ICT-domein kunnen een gevaar vormen voor de nationale veiligheid. ICT-kwetsbaarheid kan voor elk van de vitale belangen gevolgen hebben. Hieronder worden in het kort mogelijke effecten omschreven, aangevuld met relevante voorvallen die hebben plaatsgevonden.

Territoriale en Fysieke Veiligheid

Digitale aanvallen die een militaire operatie ondersteunen of waarbij vitale infrastructuur verstoord wordt, tasten de integriteit van het grondgebied en het internationaal aanzien van Nederland aan. Zo kunnen digitale aanvallen de Nederlandse militaire (C4ISR) processen verstoren.[24] Daarnaast kunnen levens verloren gaan en gewonden vallen als vitale infrastructuur, zoals elektriciteitsvoorziening, wordt getroffen. Tijdens de Russische inval in Georgië in 2008 werden ter ondersteuning van de militaire operaties vermoedelijk digitale aanvallen

23 Strategie Nationale Veiligheid, Den Haag, mei 2007, p.4

24 Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

uitgevoerd. Hoewel het onduidelijk was wie deze aanvallen uitvoerde, werden Georgische strijdkrachten hierdoor ernstig gehinderd.

Digitale spionage (cyberspionage) van de Nederlandse overheid en het bedrijfsleven ondermijnt de Nederlandse soevereiniteit. Hoewel er in open bronnen weinig voorbeelden zijn van digitale spionage in Nederland waarschuwt de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) al enige tijd voor deze dreiging. In het AIVD jaarrapport van 2009 wordt met name China als belangrijk risico-land beschouwd. Maar ook door de ontvreemding van persoonsgegevens van ICT-systemen van overheidsinstanties wordt de Nederlandse soevereiniteit ondermijnd. Daarbij maakt het niet uit of dit nu gebeurt om geldelijk gewin of om personen te chanteren.

Fysieke en economische Veiligheid

Digitale kwetsbaarheid van bijvoorbeeld procescontrolesystemen (PCS) van de vitale infrastructuur heeft consequenties voor de veiligheid van burgers. Het is mogelijk om PCS van buitenaf te manipuleren waardoor zij buiten werking worden gesteld of worden verstoord. In een Europese bankinstelling manipuleerde een hacker in het gebouwbeheersysteem de airconditioning waardoor de servers door oververhitting buiten werking werden gesteld.[25] Hierbij wordt 'cyberspace' zowel middel als doelwit.

In een niet-moedwillig incident in Finland kwam in 2007 de fysieke veiligheid in het geding toen een verbinding tussen een afvalwaterleiding en drinkwaterleiding werd opengezet. Door drukverschil vloeide afvalwater de drinkwaterleiding in waardoor het schone water werd verontreinigd. Ruim 12.500 inwoners kregen als gevolg van het verontreinigde drinkwater last van maag- en darmklachten, waaraan drie personen overleden. Herstel van de situatie duurde geruime tijd en leidde tot aanzienlijke kosten.[26]

Economische Veiligheid

De economische impact van digitale aanvallen of systeemfalen, ontstaat vooral door verstoring van bedrijfsprocessen en de daarbij veroorzaakte financiële schade en de oplopende kosten van bestrijding en herstel.

25 NICC - Process Control Security in het Informatieknooppunt Cybercrime, p.27
26 Ibid., p.34

In Nederland zijn er weinig gegevens over de verliezen van bijvoorbeeld internetbankieren. In het Verenigd Koninkrijk bestaan er wel cijfers. Het Britse APACS meldde dat de verliezen in 2008 naar £52.5 miljoen stegen, een toename van 132% ten opzichte van 2007.[27] Deze cijfers beschrijven slechts de financiële verliezen door individuele eindgebruikers, maar niet de kosten van verliezen door spionage, directe diefstal (bijvoorbeeld door hacken), bedrijfsverlamming of het herstel van schade.

Ook de verstoring van (bedrijfs)processen, zoals productie en de levering van diensten, heeft vergaande economische gevolgen. Volgens een onderzoek van PricewaterhouseCoopers is de impact van verstoringen door digitale aanvallen bij de 1000 grootste bedrijven in de wereld op $45 miljard per jaar geschat.[28] In een onderzoek van McAfee bleek dat voor 26% van de Amerikaanse kleine en middelgrote bedrijven een week nodig was om van een digitale aanval te herstellen. Hierbij zijn ICT-systemen offline waardoor er geen productie of levering van diensten plaatsvindt.[29] Vooral voor de kleine tot middelgrote bedrijven zijn de financiële consequenties desastreus. Als voorbeeld van onbewust menselijk handelen dient het helikopterincident in de Bommelerwaard in 2007. Doordat de piloot een elektriciteitskabel stukvloog, werd de elektriciteitsvoorziening getroffen, waardoor bedrijven en instellingen gedurende meer dan 4 dagen geen of beperkte voorzieningen hadden. De ICT-systemen bij de organisaties die geen noodvoorziening hadden, werden hierdoor ernstig verstoord.

Naar mate meer economische activiteiten gebruik maken van ICT-systemen is de verwachting dat de absolute schade zal toenemen. Of dit per definitie leidt tot een relatief groter aandeel van de schade in verhouding tot de opbrengsten, is echter de vraag. Zo meldde APACS namelijk dat financieel verlies door 'card-not-present' fraude (veelal ongeautoriseerde aankopen via internet, telefoon en mail order met gestolen creditcard informatie) van 2000 tot 2008 steeg met 350%, maar dat de totale waarde van aankopen door middel van online winkelen met 1077% steeg.[30]

27 Govcert Trendrapport 2009, p. 26

28 Zie: http://www.zdnet.co.uk/news/it-strategy/2008/03/12/corporate-espionage-not-if-but-when-39365959/

29 McAfee - Does Size Matter?

30 APACS, Fraud, The Facts 2009, 2009, p.8, From 2000 to 2008 card-not-present fraud losses rose by 350 per cent; over the same time period, the total value of online shopping alone increased by 1077 per cent (up from £3.5 billion in 2000 to £41.2 billion in 2008).

Sociale en Politieke Stabiliteit

Een mogelijk tweede orde effect van digitale kwetsbaarheid is de aantasting van de sociale en politieke stabiliteit als gevolg van de verminderde economische positie en de psychologische impact bij de verstoring van vitale infrastructuur. Belangrijke criteria voor sociale en politieke stabiliteit zijn verstoring van het dagelijks leven, sociaal psychologisch impact (onzekerheid over oorzaak of oplossing) en aantasting van de democratische rechtstaat.

Burgers en bedrijven kunnen het vertrouwen in de overheid en andere bedrijven verliezen als de veiligheid van gegevens niet wordt gewaarborgd. Hierdoor zullen burgers en bedrijven terughoudend zijn met het delen van gegevens. Dit wantrouwen van burgers voor ICT-diensten in de publieke sector, die beschouwd wordt als een vitale infrastructuur, kan daarmee financiële gevolgen hebben. Tenslotte kan het vertrouwen in elektronische systemen als geheel verminderen.

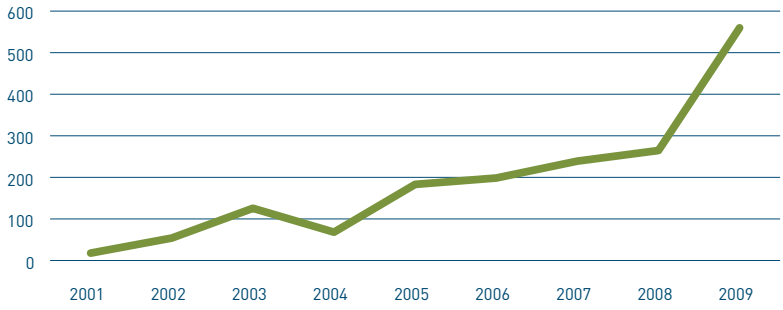
Maatschappelijke ontwrichting of niet

Hoewel de effecten op elk van de belangen van nationale veiligheid eenvoudig te concretiseren zijn, blijft de vraag of de effecten van deze mogelijke aanvallen of onbedoelde uitval of verstoring ernstig zijn of dat het meevalt. Kunnen deze effecten een maatschappelijk ontwrichtend karakter hebben? Ontwrichtende factoren komen vooral voort uit de effecten voor de politieke en sociale stabiliteit. Het wegvallen van ICT-diensten kan bij langdurige uitval of ernstige verstoring het dagelijks leven ernstig ontwrichten. Naar mate de afhankelijkheid van ICT verder toeneemt en de alternatieve middelen steeds minder voorhanden zijn, wordt de maatschappij steeds kwetsbaarder. Als daarboven ook de zelfredzaamheid onvoldoende is ontwikkeld, kan een situatie ontstaan waarin maatschappelijke ontwrichting een kans maakt.

4.2 Beoordeling van de risicofactoren van ICT-kwetsbaarheid

Hoewel er talloze voorbeelden van moedwillige bedreiging zijn, ontbreekt in Nederland een systematisch overzicht van aard, omvang, schade, doelwit en herkomst. Ook de gegevens over de risico's van onbewust menselijk handelen en systeemfalen zijn beperkt beschikbaar. Hierdoor is de exacte omvang van het probleem moeilijk in kaart te brengen, zeker in vergelijking met sommige andere incidentscenario's die in het kader van de nationale risicobeoordeling zijn opgesteld.

De oorzaken voor het ontbreken van gegevens zijn zowel sociaalorganisatorisch van aard (bedrijven zijn bang voor imagoschade als zijn hun kwetsbaarheden melden ongeacht of er sprake is van moedwillig handelen dan wel falen van ICT-systemen) als technisch van aard (aanvallen worden niet altijd gedetecteerd). Daarnaast wordt menselijke fouten en systeemfalen niet openbaar gemaakt. Al eerder is geconstateerd dat er sprake lijkt te zijn van een aanzienlijke stijging in het aantal dreigingen. Ook de economische kosten van diverse vormen van cybercriminaliteit en cyberspionage zijn hier en daar aangegeven. In een anonieme inventarisatie onder 800 Chief Information Officers (CIO's) uitgevoerd door Purdue University gaven 119 respondenten aan dat zij in 2008 waren geconfronteerd met diefstal van R&D gegevens of strategische informatie. De economische schade werd geschat op $4.6 miljoen per bedrijf.[31] In onderstaande figuur wordt de groei van het economisch verlies in de Verenigde Staten als gevolg van cybercriminaliteit aangegeven.



FIGUUR 3 GESCHATTE JAARLIJKSE FINANCIËLE SCHADE DOOR CYBER CRIME IN DE VERENIGDE STATEN (BRON: US INTERNET CYBER CRIME COMPLAINT CENTER (IC3))

31 Forbes, 29 January 2009

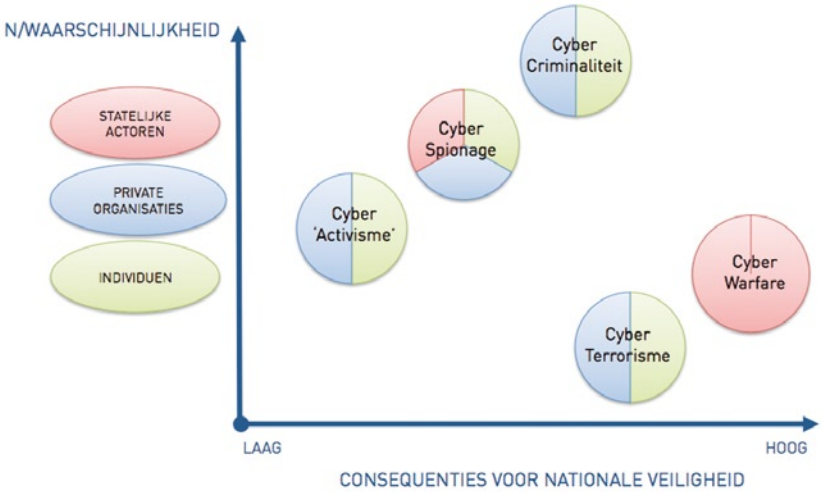
Al eerder zijn verschillende ICT-gerelateerde scenario's in het kader van de nationale risicobeoordeling (NRB) van het Programma Nationale Veiligheid op ernst en waarschijnlijkheid gescoord.[32] Volgens de methodiek van de NRB hebben deze scenario's zich op specifieke incidenten gericht die met ICT-kwetsbaarheid te maken hebben, te weten een moedwillige verstoring van de ICT-sector door milieuactivisten die procescontrolesystemen van energiebedrijven verstoren en een verstoring van het IP-netwerk (internet, telefoon, tv etc.) waarbij een antiglobaliseringsgroep het netwerk manipuleerde. De gevolgen van ICT-kwetsbaarheid voor de nationale veiligheid worden door de nationale risicobeoordeling ingeschat als hoog, waarbij de waarschijnlijkheid dat dit gebeurd, wordt ingeschat als 'geen concrete aanwijzingen, gebeurtenis is voorstelbaar'. Daarbij wordt in acht genomen dat veel van de mogelijke incidenten individueel niet altijd veel grootschalige gevolgen hebben, maar dat de potentie daarvan wel zeer reëel is.

Een gebrekkig zicht op de dreigingen door de afwezigheid van systematische gegevens bemoeilijkt een inschatting van de waarschijnlijkheid en impact van risico's. In grote lijnen is echter een verontrustend beeld geschetst van de (potentiële) dreigingen voor de nationale veiligheid. Dit beeld suggereert dat ICT-kwetsbaarheid vanuit het oogpunt van nationale veiligheid een hoge prioriteit vraagt. Op basis van beschikbare gegevens en een eerste illustratieve inschatting, kan een beeld van de verdeling van risicofactoren worden aangegeven.[33]

Uit figuur 4 komt een tweedeling naar voren. Allereerst zijn er gebeurtenissen die vaak voorkomen, (cybercrime, cyberspionage) maar relatief geringe effecten hebben op de nationale veiligheid, Daarnaast zijn er gebeurtenissen die tot nu toe sporadisch voorkomen, maar grote consequenties voor de nationale veiligheid hebben. Het is daarbij de vraag of de incidenten leidend moet zijn voor de afbakening van een Nederlandse cybersecuritystrategie of dat die op andere uitgangspunten gebaseerd moet zijn.

32 Scenario's Nationale Risicobeoordeling 2008/2009, Den Haag, Directie Nationale Veiligheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2009.

33 Bij deze inschatting is geen expliciet gebruik gemaakt van de indicatoren van de Nationale Risicobeoordeling.



FIGUUR 4 RISK ASSESMENT IN CYBERSPACE IN PREPARATION FOR WCIT 2010 (BRON HCSS, TER VOORBEREIDING VAN WCIT 2010, AMSTERDAM)

5 Knelpunten voor effectief beleid

De voorgaande analyse toont aan dat het vraagstuk van ICT-kwetsbaarheid zich kenmerkt door een aantal aspecten. ICT-kwetsbaarheid:

- strekt zich uit over verschillende beleidsterreinen
- kent gedeelde verantwoordelijkheden van verschillende actoren, binnen en buiten de overheid
- vraagt om de inzet van capaciteiten van juridische, technologische en organisatorische aard
- vindt plaats in een technologische omgeving die zeer dynamisch is.

Vanuit dit perspectief zijn de volgende knelpunten van belang:

5.1 Lastig te duiden dreigingen en doelwitten

Inherent aan het ICT-domein is het gebrek aan *situational awareness*. Dit heeft diverse redenen. Allereerst is het technisch zeer moeilijk om het gehele internet (en offline systemen) te monitoren. Ten tweede delen betrokken partijen informatie over ICT-incidenten niet. Aan de ene kant vrezen private partijen voor imagoschade die de bedrijfsbelangen kan schaden. Aan de andere kant zijn ook overheidsinstanties, in het bijzonder organisaties met een heimelijke component, terughoudend met het delen van informatie onder het mom van nationale veiligheid.

De rol van eindgebruikers in ICT-kwetsbaarheid is zeer groot. Computers van individuele gebruikers kunnen een grote dreiging vormen indien zij door kwaadwillende actoren zijn gecompromitteerd.

Landen hanteren verschillende definities van onwetmatige activiteiten in cyberspace. Een eenduidig wetgevend kader over wat nu onder de verschillende verschijningsvormen van criminaliteit en warfare wordt verstaan is niet beschikbaar. Dit verhindert een eenduidige aanpak van de problematiek.

5.2 Diversiteit van spelers en belangen

Het ICT-domein kent niet dezelfde territoriale grenzen als de fysieke wereld. Digitale actoren opereren overal ter wereld. De noodzaak tot samenwerking genereert tegelijkertijd spanningen voor de soevereiniteit en het vertrouwen tussen actoren, zeker wanneer het de nationale veiligheid betreft.

Verminderen van de ICT-kwetsbaarheid kan niet door een enkele partij bewerkstelligd worden. De overheid heeft geen volledige controle over het ICT-domein. ICT-netwerken zijn gedecentraliseerd en veelal in handen van de private sector. De private sector moet veiligheid echter afwegen tegen winstgevendheid. Return on investment in veiligheidsmaatregelen is vooralsnog moeilijk aan te tonen. Daarnaast zijn veel private organisaties huiverig voor de inmenging van de overheid in de markt. Het opleggen van minimale standaarden of het publiceren van performance management praktijken kan als concurrentievervalsende praktijk worden beschouwd.

Parallel hieraan kan het bevorderen van de ICT-veiligheid op gespannen voet staan met privacybelangen. De keuze voor het monitoren van ICT-systemen ten behoeve van veiligheid kan inbreuk maken op de privacy van burgers.

De grote rol van de internationale private sector in de levering en productie van hard- en software maakt de integriteit van de nationale ICT-infrastructuur tot een belangrijk aandachtspunt. In het buitenland geproduceerde producten kunnen aangetast zijn voordat zij geleverd zijn, waardoor de integriteit van de apparatuur of software niet gegarandeerd kan worden.

5.3 Technologische dynamiek en complexiteit

Het ICT-domein is constant in ontwikkeling. Nieuwe technologieën volgen elkaar in hoog tempo op, waarbij beleidsmaatregelen regelmatig achterblijven. Ook dreigingen, regelgeving en preventieve maatregelen verouderen hierdoor snel. Het ICT-domein is een dynamisch speelveld wat ervoor zorgt dat nieuwe ontwikkelingen lastig bij te houden zijn.

Daarnaast bevat het vraagstuk van ICT-kwetsbaarheid een sterk technische component. De technische aard van digitale dreigingen zorgt voor een grote afstand tussen de belevingswerelden van zowel experts en beleidsmakers. ICT-systemen en de netwerken waar zij deel van uitmaken zijn sterk met elkaar verweven en als zodanig lastig te doorgronden.

De verscheidenheid aan betrokken partijen, het gebrek aan zicht op dreigingen en de afhankelijkheid van de private sector zorgen voor grote uitdagingen voor effectief en slagvaardig beleid. De private sector speelt een grote rol omdat het zowel delen van netwerken controleert en de gebruikte software en hardware produceert. In het digitale domein is de rol van overheden minder vanzelfsprekend dan in andere strategische domeinen. Hierdoor lijkt de rol van de overheid betreffende ICT-kwetsbaarheid in eerste instantie beperkt, terwijl de zorg om de vitale infrastructuren wel degelijk een aandachtspunt van de (rijks)overheid is. ICT is echter een steeds belangrijkere factor in onze samenleving en het gebruik van ICT kent steeds meer gevolgen die aan vitale nationale belangen raken.

6 Huidige beleidsrespons op ICT-kwetsbaarheid

6.1 Beleidsontwikkeling in andere landen

Het *Den Haag* Centrum voor Strategische Studies (HCSS) heeft een onderzoek uitgevoerd naar hoe in andere landen tegen het vraagstuk 'cybersecurity' wordt aangekeken.[34] De resultaten van deze analyse zijn in deze paragraaf weergegeven.[35] De focus van dit onderzoek is hierbij op de meest essentiële vraagstukken van strategievorming, organisatorische aansturing, publiekprivate samenwerking en civiel-militaire afstemming gericht. In de onderliggende studie zijn de volledige analyses te vinden. Deze studie is als bijlage toegevoegd.

Strategievorming

Een aantal landen met een hoge ICT-afhankelijkheid heeft beleidsprioriteit gegeven aan ICT-kwetsbaarheid of cyber security. De Verenigde Staten, het Verenigd Koninkrijk en Australië hebben National Cybersecurity-strategies ontwikkeld.[36] Het Verenigd Koninkrijk heeft haar strategie ontwikkeld als uitvloeisel van de Nationale Veiligheidsstrategie terwijl de VS een aparte cybersecuritystrategie heeft. Tegelijkertijd wordt ook in de meest recente uitgave van de US National Security Strategy weer aparte aandacht aan cyberdreigingen besteed.

Ook andere landen, zoals Frankrijk en Zweden, zijn bezig met nationale ICT-veiligheid. In afwezigheid van een nationale strategie hebben zij diverse richtlijnen voor ICT-securitybeleid ontwikkeld.[37]

34 Deze studie is ondernomen voor de Denktank alsmede het Strategy & Change programma van HCSS en heeft zich gericht op Frankrijk, Nederland, Verenigd Koninkrijk, Verenigde Staten en Zweden.

35 Voor een uitgebreide vergelijking van de behandeling van ICT -kwetsbaarheid in de Verenigde Staten, Verenigd Koninkrijk, Frankrijk, Zweden en Nederland, zie 'International comparison of national cyber security policies' (concept), HCSS, augustus 2010.

36 Ook Canada heeft in oktober 2010 een strategie uitgebracht.

37 Zie 'International comparison of national cyber security policies'.

COUNTRY	STRATEGY NAME	NATIONAL CYBER SECURITY STRATEGY?	YEAR
FRANCE	The White Book on National Security and Defence	No (due 2010)	2008
THE NETHERLANDS	National ICT Agenda	No (due 2010)	2008
UNITED KINGDOM	Cyber Security Strategy	Yes	2009
UNITED STATES	The National Strategy to Secure Cyberspace	Yes	2003
SWEDEN	Strategy for Improved Security on the Internet	Yes	2006

FIGUUR 5 CYBERSECURITYSTRATEGIEËN EN ANDERE RELEVANTE BELEIDSDOCUMENTEN

De focus in deze benaderingen verschilt per land. Zo schenken de Verenigde Staten veel aandacht aan het militaire aspect van ICT-kwetsbaarheid en aan de ontwikkeling van capaciteiten voor het voeren van 'cyber war'. Het Verenigd Koninkrijk legt hier minder nadruk op en benadrukt juist de noodzaak tot de publiekprivate samenwerking in het beschermen van ICT-infrastructuur, en vitale infrastructuur in het bijzonder. Frankrijk heeft vooralsnog geen nationale cyberstrategie maar zet met het bestaande ICT-veiligheidsbeleid een zeer breed vraagstuk neer, dat zowel nationale en internationale aspecten kent en waarbij alle capaciteiten van de overheid en het bedrijfsleven moeten worden betrokken. De Fransen zullen overigens binnenkort hun eigen cyberstrategie presenteren. Zweden hanteert een zogenaamd 'Total Defence Concept'. Militaire en civiele belangen worden in de huidige samenleving als ondeelbaar van elkaar gezien.

FIGUUR 6 VERGELIJKENDE ANALYSE VAN DE ONDERZOCHTE LANDEN

Organisatorische aansturing

Naast het al dan niet hebben van een overkoepelende (cyber)security strategie, verschilt ook de organisatorische aansturing van overheidsactiviteiten tussen de landen. In de Verenigde Staten is de CyberCzar binnen het Witte Huis de leidende regeringsfunctionaris.. Die ultieme verantwoordelijkheid is niet onbetwist en wordt bovendien bemoeilijkt door het feit dat zowel vanuit de civiele- als de defensiehoek twee andere belangrijke personen voor cybersecurity zijn aangesteld. Centrale aansturing wordt derhalve door een sterk gefragmenteerde bureaucratie gehinderd. Aan de andere kant van het spectrum van organisatorische aansturing ligt Zweden. Hier is elk ministerie verantwoordelijk voor de opbouw van expertise en de uitvoering voor het specifieke beleid. Tussen de twee uitersten bevinden zich het Verenigd Koninkrijk en Frankrijk met geïnstitutionaliseerde, coördinerende organisaties en Nederland waarin een coördinatiemechanisme van de direct betrokken ministeries bestaat (EZ, BZK, Justitie). Deze instanties van geformaliseerde coördinatie laten niet onverlet de verschillende informele vormen van samenwerking en afstemming die op nationaal niveau (bijvoorbeeld het operational Incident Response Teams-overleg (o-IRT-o)) en op internationaal niveau (bijvoorbeeld de European Cert group (ECG)) bestaan.

Publiek-private samenwerking

Het belang van publiekprivate samenwerking wordt in de meeste landen erkend. Het succes van de samenwerking is echter bij de meeste landen beperkt. Nederland wordt daarbij, ook in andere landen, als voorbeeld gebruikt (zoals de Nationale Infrastructuur Cyber Crime (NICC)). De informele verbanden die hier zijn opgezet om op basis van gelijke voet, vertrouwelijk informatie uit te wisselen, kennen geen gelijkwaardig voorbeeld in andere landen. Het Britse model waarop dit was gebaseerd, werkt in de praktijk veel minder goed omdat de informatiestroom vooral eenrichtingsverkeer is en de samenwerkingsverbanden als oppervlakkig worden beschouwd. In de Verenigde Staten is er nauwelijks sprake van een vertrouwensrelatie waardoor private partijen schuchter zijn in het delen van specifieke bedrijfsvertrouwelijke informatie uit angst dat dit vanuit wetgeving op het gebied van openbaar bestuur publiek moet worden gemaakt. De traditioneel meer statelijk gedreven bedrijven in Frankrijk hebben van nature een hechtere relatie met de Franse overheid gehad. Hoewel dit duidelijk de samenwerking tussen overheid en bedrijfsleven heeft gefaciliteerd, is dit model minder eenvoudig overdraagbaar.

Op operationeel en uitvoeringsniveau zijn verschillende samenwerkingsverbanden opgezet die wellicht niet perfect verlopen, maar wel een belangrijke voorwaarde voor uitwisseling en samenwerking vervullen. Op strategisch niveau hebben we deze vormen van samenwerking niet kunnen identificeren.

Defensie en cybersecurity

In de vergelijkende studie is vooral gekeken naar de mate waarop cyberdefense wordt gepositioneerd. Naast de bescherming van de eigen defensiesystemen tegen aanvallen van buitenaf, komt de ontwikkeling van offensieve capaciteiten steeds verder. Die inzet kan verschillen tussen soft power (Frankrijk) aan de ene kant en de proactieve verstoring van buitenlandse exploitatie van netwerken (Verenigde Staten) aan de andere kant. De afstemming van capaciteiten tussen civiele en militaire spelers lijkt nog niet vergevorderd. Er vindt naast samenwerking in oefeningen weinig andere gedeelde coördinatie of activiteiten plaats. Het Amerikaanse detectie- en waarschuwingscentrum NICC is een van de weinige voorbeelden waarin diverse civiele departementen en het Department of Defense een gecoördineerde monitoring van en verdediging tegen digitale aanvallen uitvoeren.

6.2 Multinationale ontwikkelingen

Europese Unie

In 2002 werd het eEurope Action plan gepresenteerd met de ICT-ambities voor Europa.[38] Europa moet op het gebied van ICT en dienstverlening wereldwijd een leidende rol gaan spelen. ICT-veiligheid kreeg echter pas later meer aandacht. In 2006 nam de Europese Commissie de Communicatie 'Dialogue, partnership and empowerment: 'A Strategy for a Secure Information Society' aan,' die in het teken stond van veiligheid.[39] De focus hierbij is echter op algemene kwetsbaarheden en minder op bewuste ondermijning of het misbruik van ICT. De Commissie oordeelde dat te weinig partijen iets voelden voor de uitvoering van deze strategie. In maart 2009 werd derhalve in de Communicatie *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience* verdere nadruk gelegd op de noodzaak tot een meer geharmoniseerde Europese aanpak, de ontwikkeling van monitoringmechanismes en informatie-uitwisseling tussen lidstaten en een betere publiekprivate samenwerking.

38 Council of the European Union, eEurope 2002 Action Plan.

39 A strategy for a Secure Information Society – 'Dialogue, partnership and empowerment', COM(2006) 251, Brussels, 2006.

De Europese Veiligheidstrategie geeft eveneens aandacht voor cybersecurity. In een document van EU-voorzitter Spanje en de komende voorzitters België en Hongarije, wordt cybercrime een van de vijf dreigingen voor de interne veiligheid van Europa genoemd. Als uitvloeisel daarvan sprak de Nederlandse Minister van Justitie (Hirsch Ballin) de wens uit voor de oprichting van een Europese Cyber Autoriteit, die zich speciaal richt op de aanpak van internetcriminaliteit.[40]

NAVO

De NAVO heeft recentelijk een belangrijke impuls gegeven aan de agendering van cybersecurity. Op 17 mei 2010 verscheen het expertrapport *NATO 2020: assured security; dynamic engagement* waarin analyse en aanbevelingen voor een nieuw NAVO strategisch concept werden gepresenteerd.[41] De analyse geeft grote prioriteit aan onconventionele dreigingen, waaronder cyberaanvallen op moderne communicatiesystemen en vitale aanvoerlijnen. Het rapport geeft aan dat er al talloze inbreuken op NAVO systemen plaatsvinden op een betrekkelijk laag niveau. Maar er wordt in de analyse aangegeven dat deze aanvallen, bijvoorbeeld op 'command and control' systemen of energiegrids, zelfs het niveau van een Artikel 5 aanval kunnen bereiken, waarop een gemeenschappelijk antwoord van de NAVO bondgenoten zal moeten volgen.[42] 'The next significant attack on the Alliance may well come down a fibre optic cable.[43]'

Deze gepercipieerde dreiging noodzaakt de NAVO volgens het rapport tot de ontwikkeling van nieuwe capaciteiten die zowel op preventie, detectie, respons als herstel gericht moeten zijn. Hoewel de NAVO al diverse organen heeft opgericht (Cyber Defence Management Authority, de Cooperative Cyber Defence Centre of Excellence, en een Computer Incident Response Capability), zijn er aanzienlijke gaten in de cyberdefensiecapaciteiten. Deze capaciteiten moeten zich richten op het verhogen van het training- en kennisniveau, het verbeteren van het monitoren van NAVO netwerken en zich op termijn richten op het ontwikkelen van passieve en actieve defensiecapaciteiten.

40 Zie: http://www.ad.nl/ad/nl/1005/Digitaal/article/detail/487905/2010/06/03/Hirsch-Ballin-wil-besmette-computers-uitschakelen.dhtml

41 NATO 2020: assured security; dynamic engagement, analysis and recommendations of the group of experts on a new strategic concept for NATO, 17 mei 2010.

42 Voordat overigens sprake is van het in werking stellen van Artikel 5, zal eerst eerst onder artikel 4 overleg over de gestelde bedreiging of aanval moeten plaatsvinden.

43 Ibid. p. 45

Verenigde Naties

Via de Verenigde Naties worden ook pogingen ondernomen om op mondiaal niveau cybercriminaliteit te bestrijden. Hoewel de ambitie om cyberfraude, vervalsing en misbruik van informatie te verminderen breed wordt gedeeld, kon in een recente VN-conferentie over criminaliteitsbestrijding in Brazilië geen overeenstemming worden bereikt over hoe deze problemen moesten worden aangepakt. De doelstelling om voort te bouwen op de Boedapest conventie, die een gezamenlijke aanpak tegen cybercriminaliteit voorstond, werd hierbij vooralsnog niet bereikt. Geconstateerd kan worden dat initiatieven vanuit de VN vooralsnog niet op een breed gedeeld perspectief van de problematiek steunen.

6.3 Nederlandse politiek-bestuurlijke context

In Nederland staat het onderwerp ICT-kwetsbaarheid al geruime tijd op de politieke en bestuurlijke agenda. Zo presenteerde de overheid al in 2001 in de nota *Kwetsbaarheid op Internet (KWINT)*, de resultaten van een toekomstverkenning naar de kwetsbaarheden en zwakheden in ICT-infrastructuren.[44] De nota richtte zich vooral op (risico's van) het internet en voorzag slechts een bescheiden rol voor de overheid.[45] Eerder dat jaar vroeg de motie Wijn om een brede aanpak van de bescherming van vitale infrastructuren.[46] Mede op basis van de motie en vooral vanwege de veranderde veiligheidsopvattingen na 9/11 werd een jaar later het project Bescherming Vitale Infrastructuren opgezet. In die periode werd het verlagen van de kwetsbaarheid van de rijksoverheid zelf ook als cruciaal gezien, zoals de oprichting van CERT-RO (dat later tot Govcert heeft geleid) aangaf.

In 2004 startte het kabinet de ICT-agenda onder leiding van de ministeries van Economische Zaken (EZ) en Onderwijs, Cultuur en Wetenschap (OCW).[47] De agenda had de betere benutting van ICT-mogelijkheden tot doel door de kennis, infrastructuur en randvoorwaarden hierover te verstevigen. Veiligheid en betrouwbaarheid spelen daarin een belangrijke rol. In 2008 presenteerde EZ de vernieuwde ICT-agenda. Deze ICT-agenda loopt voor een periode van drie jaar en richt zich op het optimaliseren van de productiviteit en efficiëntie van

44 Kamerstukken II 2000/01, 26 643, nr. 30.

45 B.J. Koops, S. van der Hof & V. Bekkers (2005), 'Risico's in de netwerksamenleving: over vervlochten netwerken en kwetsbare overheden', in: Lips, Bekkers & Zuurmond (red.), ICT en openbaar bestuur, Utrecht: Lemma 2005, p. 671-706.

46 Kamerstukken II 2000/01, 26 643, nr. 20.

47 Kamerstukken II 2003/2004, 26 643, nr. 47.

ICT-dienstverlening aan de burger. Harde speer- of actiepunten om de veiligheid te bevorderen, ontbreken.

De risico's van ICT-kwetsbaarheid in de Nederlandse netwerksamenleving zijn echter door de overheid erkend en hebben geleidelijk meer aandacht gekregen. In een kamerbrief van december 2007 beschreven de Ministers van Binnenlandse Zaken en Koninkrijksrelaties (BZK) en die van Justitie alsmede de staatssecretaris van Economische Zaken, de coördinatie en samenhang van het Nederlandse ICT-veiligheidsbeleid. Deze moest grotendeels plaatsvinden in het door BZK gecoördineerde Programma Nationale Veiligheid.[48] In het interdepartementaal overleg op DG-niveau komen de verscheidene perspectieven rondom ICT-kwetsbaarheid bij elkaar.

De bovenstaande ontwikkelingen zijn een greep uit initiatieven en beleidsontwikkelingen die de afgelopen 10 jaar hebben plaatsgevonden. Er is veel gebeurd rondom ICT-kwetsbaarheid. De activiteiten bouwen echter niet altijd voort op elkaar of worden verkokerd opgepakt. Dit heeft ervoor gezorgd dat coherentie en overzicht van strategisch beleid tot nu toe hebben ontbroken, ondanks het regelmatig overleg op interdepartementaal niveau.

In de motie van de Kamerleden Knops (CDA), Voordewind (CU) en Eijsink (PvdA) van december 2009, werd daarom de Minister van Defensie verzocht een cybersecuritystrategie te ontwikkelen en actief bij te dragen aan de gedachtevorming over cyberwarfare binnen de NAVO. In de voortgang hierover deelde de Minister van Defensie aan de Tweede Kamer mee dat Defensie aan de ontwikkeling van een beleidsvisie op dit terrein werkt in samenwerking met andere betrokken departementen. Dit zijn in het bijzonder BZK (samen met Defensie leidend voor digitale verdediging), EZ (leidend voor de nationale informatie-infrastructuren), Justitie (leidend voor digitale criminaliteit) en de Nationaal Coördinator Terrorismebestrijding (NCTb), die leidend is voor digitaal terrorisme.[49]

48 Kamerstukken II 2007/2008, 26 643, nr. 103

49 Voortgangsbrief Motie Knops c.s. inzake Digitale Verdediging, Kamerstukken II 2009/2010, 26 643, nr. 164.

FIGUUR 7 EEN BEKNOPTE WEERGAVE VAN DE ACTIVITEITEN DIE TOE NU TOE IN NEDERLAND EN OP EU NIVEAU ZIJN ONDERNOMEN.

ICT-kwetsbaarheid werd zo internationaal een beleidsprioriteit. De invulling die landen hieraan geven, is echter verschillend. Sommige landenkiezen voor een aparte strategie, terwijl andere landen het als onderdeel van hun nationale veiligheidsstrategie zien.

APARTE CYBER SECURITY STRATEGIE	CYBER SECURITY ONDERDEEL VAN NATIONALE VEILIGHEIDSSTRATEGIE	
	JA	NEE
JA	V.S. / V.K.	Zweden
NEE	Frankrijk	NL

Waar Nederland nog geen geformaliseerde strategische benadering voor cybersecurity heeft ontwikkeld, zijn diverse elementen rondom ICT-kwetsbaarheid al wel onder het mom van nationale veiligheid aan ontwikkeld. Het lijkt er in 2010 op dat Nederland ook een verdere strategische ontwikkeling doormaakt die vergelijkbaar is met de Verenigde Staten en het Verenigd Koninkrijk, zonder dat de inhoudelijke overeenstemming compleet is.

7 Richtpunten voor strategie en beleid

In opvolging van de motie Knops c.s. is de Nederlandse overheid nu bezig aan de ontwikkeling van een nationale cybersecuritystrategie. Daarmee is de vraag of Nederland een dergelijke strategie moet ontwikkelen in de praktijk niet meer relevant. Hiermee wordt tevens aangegeven dat de mogelijke dreigingen en kwetsbaarheden van dien aard zijn dat cybersecurity een strategische prioriteit krijgt.

De urgentie om als overheid en bedrijfsleven in onderlinge afstemming extra maatregelen te nemen ter bescherming van ICT-kwetsbaarheden neemt toe. Deze ICT-kwetsbaarheden kunnen immers leiden tot mogelijke aantasting van de vitale belangen van de nationale veiligheid. Die urgentie wordt echter niet door alle betrokken of getroffen partijen onderkend. Buiten de expertgroepen is de ernst en waarschijnlijkheid van mogelijke aantasting van de nationale veiligheid onvoldoende duidelijk. Het voortdurend zicht krijgen en houden op de dreigingen en kwetsbaarheden blijft hierdoor een belangrijke randvoorwaarde voor deze prioriteitsstelling.

De cybersecuritystrategie zal in elk geval een aanzet moeten geven tot de oplossing van de knelpunten die in dit rapport zijn geconstateerd en zal tenminste de volgende elementen moeten bevatten:
- Een uiteenzetting van wat cybersecurity behelst
- Principes voor toewijzing van organisatorische verantwoordelijkheden en coördinatie en het toebedelen van middelen
- Een koppeling van risico's en benodigde capaciteiten/beleidsopties
- Principes voor integratie en implementatie van de beleidsopties
- Juridische randvoorwaarden: wat is mogelijk en wat is onmogelijk.

7.1 Visie en reikwijdte van de strategie

Het is allereerst essentieel dat naast de mogelijke voordelen van ICT ook de kwetsbaarheden helder worden neergezet in de strategie. Een belangrijk aan-

dachtspunt binnen de visie is hoe ver de strategie zich dient uit te strekken. Een heldere indeling van het cyberdomein zowel op gebied van dreiging ((systeem) falen, rampen, moedwillige activiteiten) als op het gebied van maatregelen (bewustzijn, inlichtingen, safety, security, defensief, offensief) is nodig. Gegeven de dynamiek van de ontwikkelingen binnen het ICT-gebied en de verwevenheid van verschijningsvormen, kwetsbaarheden, actoren en gevolgen, lijkt het niet effectief een knip te leggen in welke bedreigingen of verschijningsvormen wel of niet moeten worden meegenomen. Zo is het argument dat cybercrime niet direct een bedreiging is voor de nationale veiligheid wellicht valide, maar is de verbinding van cybercriminaliteit met andere bedreigingen, zoals cyberwarfare, wel degelijk te maken. Een holistische en adaptieve benadering van cybersecurity is daarmee te prefereren. De strategie moet daarmee vooral kaderstellend zijn; het gaat immers om een omvangrijk, deels onbekend en jong terrein.

Het is zinvol deze strategie nauw aan te laten sluiten bij de uitgangspunten zoals die ook bij het bredere nationale veiligheidsperspectief worden gehanteerd. Hierbij wordt geborgd dat de 'all hazard' (moedwillig en niet-moedwillig) en 'whole of government' benadering die ook voor cybersecurity van belang is vanuit verschillende disciplines en departementen wordt ondersteund. Tevens is het zoeken van de verbinding met andere dreigingen en gevaren die in de strategie nationale veiligheid worden beschouwd van belang gezien de 'enabling' functie die ICT heeft. Tot slot kan door de aansluiting met nationale veiligheid de bestaande structuur, werkwijze en besluitvorming worden gebruikt.

7.2 Sturingsprincipes

Er bestaat bij geen enkele partij een overkoepelend en sluitend beeld van de situatie. Dit beeld ontbreekt zowel voor dreigingen als kwetsbaarheden, mogelijkheden en capaciteiten van de verschillende partijen alsook voor de wetgevende kaders waarbinnen kan en mag worden geopereerd.

In een dergelijke situatie zal specifiek aandacht moeten worden gegeven aan het invullen van een regiefunctie. De vele spelers, taken en verantwoordelijkheden die zowel internationaal, nationaal als lokaal een rol spelen bij de overheid, het bedrijfsleven en de burger vragen om regie. De coördinatie en regiefunctie rondom de bestijding van de ICT-kwetsbaarheid is in Nederland nog onvoldoende ontwikkeld, zowel ten aanzien van beleid rondom preventie als respons. Dit laat niet onverlet de verscheidene informele vormen van samenwerking en afstemming die nationaal en internaal al bestaan.

De denktank is van mening dat er, gezien de fragmentatie en het onoverzichtelijke domein, een actieve én centrale regie op zijn plaats is. Hiervoor is een ambitieuze strategie noodzakelijk waarin een duidelijk aanpak en rolverdeling wordt genoemd met in achtname van de staande bevoegdheden en verantwoordelijkheden. Die aanpak zal de al bestaande activiteiten van verschillende organisaties en invalshoeken goed bij elkaar moeten brengen, waardoor afstemming en versterking van de inzet van de middelen en beleidsopties gekoppeld kunnen worden aan de gepercipieerde risicofactoren die dwars door alle terreinen heengaan.

7.3 Benodigde capaciteiten

Bij het bepalen van de beschikbare en benodigde capaciteiten voor cybersecurity in Nederland moet er zowel naar de capaciteiten voor preventie (analyse, bescherming, preparatie) als naar respons (herstel, nazorg) worden gekeken.

In het verlengde van de werkwijze nationale veiligheid moet worden bepaald welke capaciteiten voor het voorkomen en bestrijden van ICT-kwetsbaarheid en het herstellen van schade als gevolg van ICT-kwetsbaarheid extra benodigd zijn. Die capaciteiten kunnen op verschillende niveaus verder verfijnd en ingeschaald worden: internationaal, nationaal, regionaal, bedrijfsleven en burger.

Als handvat voor de verdere analyse van prioriteiten voor cybersecuritybeleid kunnen capaciteiten worden geformuleerd om bepaalde taken in de verschillende fasen uit te voeren. Hieronder zijn de capaciteiten, die moeten worden ontwikkeld, verder beschreven. Bij elk van de te ontwikkelen capaciteiten zijn ter illustratie praktijkvoorbeelden uit andere landen aangehaald.

Preventie

Verbeteren van de gedeelde situational awareness

Zoals uit de analyses blijkt, is er een onvolledig beeld van de dreigingen en kwetsbaarheden van het ICT-domein en de capaciteiten die daarbij benodigd en beschikbaar zijn. Het verkrijgen van een betrouwbare en functionele *situational awareness* is zeer lastig.[50] Een verbetering in deze situatie is echter noodzakelijk omdat dit kan leiden tot verbeterde strategische planning en efficiëntere aanpak van incidenten. Daarnaast helpt het ook om een breder bewustzijn over kwets-

50 Zie ook TNO rapport 'CDAG Cyber Operations, Verslag Workshop 14-15 september 2010', Den Haag, september 2010

baarheden bij private organisaties en het breder publiek te stimuleren en om de economische consequenties van deze kwetsbaarheden aan te geven.

- Frankrijk en het Verenigd Koninkrijk hebben organisaties die statistieken bijhouden over digitale dreigingen.
- Veel landen hebben centra die internetdreigingen monitoren in aanvulling op de Computer Emergency Response Teams (CERTs).
- In het Verenigd Koninkrijk zijn er vier monitoring centra: bij het ministerie van Defensie, het Joint Terrorism Analysis Centre, the Combined Security Incident Response Team en bij het Cyber Security Operations Centre.

Verminderen van dreigingen

Een andere doelstelling is het verminderen van dreigingen. Kwaadwillende actoren worden hierbij actief gehinderd in het uitvoeren van digitale aanvallen. Om dit te realiseren moet de overheid een goed zicht hebben op dreigingen en offensieve ICT-capaciteiten ontwikkelen.

- In de Verenigde Staten hebben het Department of Defense en de National Security Agency eigen monitoring capaciteiten. Het meeste werk wordt echter verricht door het National Cyber Security Center, wat onderdeel is van het Department of Homeland Security.
- Frankrijk heeft de monitoring taken gecentraliseerd bij de PHAROS organisatie, die onder leiding staat van de politie, die weer valt onder het ministerie van Binnenlandse Zaken.
- In de Verenigde Staten zijn de National Cyber Investigative Joint Taskforce and the U.S. Cyber Command actief voor offensieve capaciteiten. In het Verenigd Koninkrijk verzorgt het Cyber Security Operations Centre de Britse offensieve capaciteiten.

Verheldering van de juridische kaders en de wetgevingsmogelijkheden

Veel van de capaciteiten die noodzakelijk zijn voor het realiseren van de doelstellingen die hierboven zijn benoemd vragen om een helder en volledig uitgerust wettelijk kader. De juridische domeinen die in Nederland beschikbaar zijn onderscheiden verantwoordelijkheden die sterk georganiseerd zijn naar de diverse rollen van de Nederlandse departementen. Ook internationale juridische ontwikkelingen en standaarden moeten daarin worden meegewogen.

- Frankrijk was een van de eerste landen die de Europese Cyber Crime Conventie ratificeerde. Hiermee wil men orde scheppen in het ICT-domein om ook na incidenten dreigingen te kunnen aanpakken. Zweden is echter huiverig om op

internationaal niveau afspraken te maken die de nationale wetgeving beïnvloeden. Dit land wilde regie over de eigen ICT-infrastructuren houden.

Respons

Verhogen van weerbaarheid bij potentiële doelen

Bij het verhogen van weerbaarheid van potentiële doelen worden maatregelen genomen om de integriteit van ICT-systemen te waarborgen. Het identificeren van potentiële doelen en het beveiligen van deze doelen heeft prioriteit. Investeringen in technologische- en organisatorische veiligheidsmaatregelen moeten er voor zorgen dat potentiële doelen minder kwetsbaar worden. Een zeker niveau van kwetsbaarheid zal, ondanks investeringen in veiligheidsmaatregelen, altijd blijven bestaan. De ernst van de dreiging wordt niet voldoende onderkend; er is behoefte aan een beter verhaal waardoor politieke en economische belangen helder worden. Ook zal moeten worden aangetoond dat investeren in veiligheid een *return on investment* geeft.

- In Zweden brengt de Collaborative Group for Information Security (SAMFI) diverse organisaties samen en fungeert de organisatie als interdepartementaal leider om kwetsbaarheden in de diverse sectoren te reduceren. In Nederland en het Verenigd Koninkrijk wordt door middel van publiekprivate samenwerking extra aandacht besteedt aan het verminderen van kwetsbaarheden in de Nederlandse vitale infrastructuur. In de Verenigde Staten is de federale overheid hierbij het meest bij betrokken.
- In Frankrijk wordt er veel aandacht besteed aan het verminderen van kwetsbaarheden binnen de overheid, bijvoorbeeld door het trainen van ambtenaren.
- De Verenigde Staten houdt in samenwerking met de private sector oefeningen waarbij digitale aanvallen worden gesimuleerd. In Nederland vinden op nationaal niveau oefeningen plaats in samenwerking met onder andere de financiële sector. Het Verenigd Koninkrijk heeft eveneens oefeningen waarbij zowel de publieke als de private sector samenwerken.
- Met name de Verenigde Staten, het Verenigd Koninkrijk en Nederland delen via hun Combined Security Incident Response Teams (CSIRTs) *good practices* met hun omgeving. Nederland neemt deel aan internationale oefeningen, zoals Cyberstorm III, waaraan ook een nationale component zit. De politie in het Verenigd Koninkrijk biedt tevens op maat gemaakte tips aan voor de industrie, wetenschappelijke instellingen en overheid om elektronische criminaliteit te bestrijden.

Verhogen van weerbaarheid van eindgebruikers

Verder bestaat de mogelijkheid om de weerbaarheid van eindgebruikers te verhogen. Veel digitale aanvallen worden uitgevoerd met gecompromitteerde computers van eindgebruikers. Door de weerstand van computers van eindgebruikers te verhogen worden de digitale middelen voor hackers om aanvallen uit te voeren verlaagd. Bij een verhoogde weerstand van de eindgebruiker wordt ook computercriminaliteit teruggedrongen door een verhoogd bewustzijn op de mogelijkheden van digitale criminaliteit. Er is duidelijke behoefte aan training en kennis over mogelijke dreigingen en effecten.

- In veel landen worden bewustzijncampagnes georganiseerd om de veiligheid van eindgebruikers te verbeteren.
- De Europese Unie heeft het EU Safer Internet Plus programma om individuele gebruikers verantwoordelijk gebruik te laten maken van het internet.

Verhogen van herstelcapaciteit van ICT-infrastructuren

Ook kan de herstelcapaciteit verhoogd worden in ICT-infrastructuren. Door investeringen in herstelcapaciteit wordt de kwetsbaarheid niet alleen aanzienlijk verminderd maar kunnen ICT-systemen digitale aanvallen ook relatief snel afslaan of kunnen ICT-systemen weer snel worden opgepakt. Hierdoor vermindert de impact van digitale aanvallen.

- Veel landen hebben diverse Computer Security Incident Response Teams (CSIRTs). Deze zijn opgericht in verschillende sectoren, bij de overheid, in de private sector en bij universiteiten.
- Veel CERTs en CSIRTs onderhouden internationale contacten om informatie uit te wisselen.

Offensieve capaciteiten?

De motie Knops van december 2009 heeft naast de ontwikkeling van een cybersecuritystrategie ook de gedachtevorming over cyberwarfare binnen de NAVO op de agenda geplaatst. Hierbij past ook het denken over het ontwikkelen van offensieve capaciteiten.

Hoewel de ontwikkeling van deze capaciteiten al in verschillende landen is opgepakt, blijft de inzet hiervan nog een wezenlijk probleem. Immers, het blijft (nog) moeilijk te achterhalen welke partijen als agressor optreden en wanneer. Concepten als vergelding, die de inzet van offensieve capaciteiten kunnen legitimeren, blijven hierdoor lastig toepasbaar. Offensieve capaciteiten blijven in deze notitie vooralsnog onbenoemd.

Appendix A

De volgende personen waren aanwezig bij de bijeenkomst over ICT-kwetsbaarheid en Nationale Veiligheid op 22 juni 2010 van de Denktank Nationale Veiligheid.

Dhr. mr. G.P. van de Beek
Arrondissementsparket Dordrecht, Hoofdofficier van Justitie

Bennie (B.P.M.) Bloemberg
RIVM, Hoofd ICT

Mw. drs. E. de Kleuver
Ministerie van Binnenlandse Zaken en Kon. Relaties, Programmamanager PNV

Dhr. dr. M.M. Kommer
Ministerie van Justitie, Coördinator strategieontwikkeling/Dir. AJS

Dhr. H.W.M. Schoof
Ministerie van Binnenlandse Zaken en Kon. Relaties, Directeur-Generaal Veiligheid

Dhr. prof. dr. R. de Wijk
Den Haag Centrum voor Strategische Studies, Directeur

Adhoc leden
Ton Bijl
Ministerie van Defensie, Senior Beleidsmedewerker

Marc Bökkerink
Min BZK, Afd. Dreigingen en Capaciteiten

Drs. H.A.M. (Hellen) van Dongen
MinEZ, plv. directeur Directie Telecommarkt

Erik Frinking
HCSS, Programmadirecteur NV & Intell

Elly van den Heuvel
Govcert, General Manager

Kees d'Huy
TNO Defence and Security and Safety, Expert

Eric Luiijf
TNO Defence and Security and Safety, Expert

Matthijs Veenendaal
Ministerie van Defensie, Senior Beleidsmedewerker

Jeroen van Vugt
NCTb, Programmamanager Internet & Terrorisme en Cybersecurity

Annemarie Zielstra
NICC, Programmamanager

Foto: TNO

Den Haag Centrum voor Strategische Studies

Lange Voorhout 16
2514 EE Den Haag
Nederland

info@hcss.nl
www.hcss.nl