Cybersecurity (hoofdstuk 13)

van der Meulen, N.S.; Lodder, A.R.

published in
Recht en Computer (6e druk)
2014

1 Cybersecurity

Nicole S. van der Meulen & Arno R. Lodder

1.1 Inleiding

Mede naar aanleiding van incidenten, zoals de hack op DigiNotar in de zomer van 2011, de honderdduizenden patiëntgegevens van het Groene Hart ziekenhuis die in het najaar 2012 benaderbaar bleken en de serie Distributed Denial of Service (DDoS) aanvallen op banken in het voorjaar van 2013, is het onderwerp cybersecurity, oftewel digitale veiligheid,[1] niet meer uit de hedendaagse maatschappij weg te denken.

Veiligheid ofwel security op internet is om meerdere redenen een lastig te realiseren doel. Om te beginnen is internet niet ontworpen om op een veilige manier te gebruiken. Aanvankelijk was de kring van internetgebruikers namelijk beperkt en behoorden daar geen personen of instanties toe van wie criminele of anderszins verstorende activiteiten te verwachten waren. In de tweede plaats is zelfs als technologie ontworpen wordt om veilig te zijn, er nooit een garantie dat misbruik onmogelijk is. Dit is op zich niet typisch voor internet, ook in andere domeinen is geen 100% garantie te geven, maar door de wereldwijde toegang tot het internet is de potentiële groep personen die een gevaar voor de veiligheid vormt groter dan bij aan fysieke objecten of personen gerelateerde veiligheid. Een derde reden is dat bij de ontwikkeling van technologie nog steeds veiligheid veelal een sluitpost is. Doorgaans is het eerste doel om een systeem draaiende te krijgen en, als het zover is, wordt pas naar de veiligheid gekeken. Hierdoor is het lastiger om de veiligheid op orde te krijgen, omdat het uitgangspunt niet een veilig systeem was. Tenslotte kan nog de zwakste schakel worden genoemd, de mens. Hoe goed de beveiliging technisch ook is, als mensen toegang verschaffen of belangrijke gegevens prijsgeven kan een systeem altijd binnengedrongen worden.

Cybersecurity is in de technische praktijk en literatuur een belangrijk onderwerp, maar begint steeds meer aandacht te krijgen vanuit een juridische en beleidsmatige hoek. Dit hoofdstuk richt zich specifiek op de interactie tussen cybersecurity en recht en beleid.

De opbouw van dit hoofdstuk is als volgt. Het begint met een beschrijving van enkele incidenten die het onderwerp cybersecurity en recht en beleid in Nederland duidelijk op de kaart hebben gezet. Vervolgens wordt het fenomeen cybersecurity kort besproken om aan te geven wat ermee bedoeld wordt en hoe het begrip zich verhoudt tot andere gerelateerde begrippen, zoals informatiebeveiliging en cyberwar. In het kader daarvan worden diverse categorieën dreigingen en dreigersgroepen besproken. Daarna ligt de focus op de respons door een bespreking van strategie en actoren op nationaal en Europees niveau.

[1] Security betekent ook beveiliging. De Engelse term security verwijst dus zowel naar het middel (beveiliging) als het doel (veiligheid).

1.2 Incidenten

De afgelopen jaren heeft een groot aantal cybersecurity incidenten plaatsgevonden. Wij beperken ons in dit hoofdstuk tot de meest in het oog springende voorbeelden in Nederland die tevens een grote mate van media-aandacht ontvingen. Tegelijkertijd illustreren deze incidenten het uiteenlopende karakter van cybersecurity.

1.2.1 Diginotar

Als er één incident de geschiedenisboeken in zal gaan als het incident dat cybersecurity in Nederland op de kaart zette, dan is dat zonder enige twijfel DigiNotar. Het relatief onbekende, in Beverwijk gevestigde bedrijf wist de internationale media te halen in de zomer van 2011. DigiNotar was een certificatenleverancier die onder andere PKIoverheid-certificaten leverde voor de Nederlandse overheid. Het DigiNotar-incident kwam in de schijnwerpers, nadat op 29 augustus 2011 bekend werd dat er een frauduleus certificaat van het bedrijf in omloop was. Deze ontdekking werd gedaan nadat een internetgebruiker in Iran probeerde in te loggen op zijn Gmail account, waarna hij een waarschuwing kreeg van zijn internet browser, Google Chrome, over de (on)betrouwbaarheid van het certificaat. Vervolgens werd bekend dat er bij DigiNotar in juli 2011 succesvol was ingebroken, waardoor fraudeleuze certificaten aangemaakt konden worden. Met deze certificaten konden inloggegevens en ander dataverkeer afgetapt worden. Het incident escaleerde tot de eerste digitale crisis, toen de Nederlandse overheid haar vertrouwen in de certificaten van DigiNotar opzegde.[2]

1.2.2 Lektober 2011

In oktober 2011 hield Webwereld de actie Lektober en publiceerde elke dag een beveiligingslek op hun website. Volgens Sander van der Meijs, journalist bij Webwereld, was de Lektober-actie ontstaan uit frustratie.[3] Webwereld krijgt gemiddeld drie lekken per dag gemeld, waaruit Van der Meijs de conclusie trekt dat gegevens over het algemeen onvoldoende beveiligd worden. De focus van Lektober lag vooral bij de overheid en dan in het bijzonder gemeentelijke websites die onvoldoende beveiligd bleken. Op 8 oktober kopte Webwereld: Lektober Superknaller Megalek treft 50 gemeenten.[4] Hierdoor konden DigiD-sessies in theorie door kwaadwillenden overgenomen worden. Het overnemen van een dergelijke sessie of het klonen daarvan geeft kwaadwillenden mogelijkheden om gegevens aan te passen en identiteitsfraude te plegen.[5] Na interventie door de Vereniging Nederlandse Gemeenten (VNG) werden de betreffende sites offline gehaald.

---

[2] Zie uitgebreid Van der Meulen, N.S. (2013). DigiNotar: Dissecting the First Dutch Digital Disaster, *Journal of Strategic Security* Vol. 6, Issue 4.

[3] NOS op 3. (2011). 'Lektober uit frustratie ontstaan', beschikbaar op: http://nos.nl/op3/artikel/278234-lektober-uit-frustratie-ontstaan.html.

[4] De Winter, B. (2011). 'Lektober superknaller: Megalek treft 50 gemeenten', beschikbaar op: http://webwereld.nl/beveiliging/54950-lektober-superknaller-megalek-treft-50-gemeenten.

[5] Zie van der Meulen, N.S. (2011a). *Financial Identity Theft: Context, Challenges and Countermeasures*. The Hague: TMC Asser Press.

1.2.3 Patiëntgegevens

De invoering van het Elektronisch Patiënten Dossier (EPD) leidt tot veel aandacht voor bescherming van patiëntgegevens, of het gebrek daaraan. In 2006 gaven twee ziekenhuizen toestemming aan Nederlandse publicist Karen Spaink om hun systemen door informatiebeveiligingsexperts te laten testen.[6] Deze experts waren relatief rap in staat om toegang te verwerven tot 1,2 miljoen patiëntgegevens, deels door technische aanvallen (SQL-injecties) en deels door social engineering.[7] Tevens kon Spaink bloedgroepen veranderen of lijsten van mensen met besmettelijke ziekten opvragen. In de loop der jaren vonden meer incidenten plaats waaruit de kwetsbaarheid van patiëntgegevens blijkt. In oktober 2012 werd bekend dat een server bij het Groene Hart ziekenhuis in Gouda gehackt was, waardoor inzage in patiëntgegevens plaats kon vinden. Deze server werd na de ontdekking direct van het internet afgehaald. Desondanks waren de gegevens enige tijd toegankelijk, hetgeen ruime media-aandacht trok.

1.2.4 Aanvallen op banken voorjaar 2013

Distributed Denial of Service (DDoS) aanvallen zijn een bekend fenomeen binnen de cybersecurity-wereld. Een DDoS-aanval zorgt ervoor dat een webdienst, zoals een website, overbelast wordt, waardoor reguliere dienstverlening niet meer kan plaatsvinden. Een DDoS-aanval wordt veelvuldig gebruikt als instrument om partijen te dwarsbomen. Een belangrijk doelwit zijn banken, ook in Nederland. In het voorjaar van 2013 kregen meerdere banken, waaronder de ING en ABN Amro, te maken met dergelijke DDoS-aanvallen. Hoewel deze aanvallen zeker niet de eerste waren, kregen ze wel veel meer media-aandacht dan in voorgaande jaren. Redenen daarvoor waren niet alleen de lange duur van de aanvallen en de opeenvolging van verschillende aanvallen in korte tijd, maar ook het grote ongemak voor consumenten en de economische schade voor winkels, doordat het op een zaterdag geruime tijd onmogelijk was om via IDEAL of met de pinpas te betalen.

De verschillende incidenten hebben meegewerkt aan een gevoel van urgentie, zo blijkt ook uit de *Visiebrief digitale overheid 2017* van 23 mei 2013, waarin de Minister van Binnenlandse Zaken en Koninkrijksrelaties aan de kamer schrijft:

> "De lessen uit het DigiNotarincident, maar ook na Lektober en de recente DDoS-aanvallen op DigiD laten zien dat het beveiligen van informatie en de beschikbaarheid van de digitale dienstverlening urgent en blijvend op de agenda moeten staan."

1.3 Wat is cybersecurity?

Hoewel de term cybersecurity veel gebruikt wordt, ontbreekt een eenduidige definitie. Dit wordt mede veroorzaakt door de betrokkenheid van veel verschillende stakeholders die allen het onderwerp en de daaraan gekoppelde problematiek primair vanuit hun eigen invalshoek benaderen. Volgens Hathaway en Klimburg werd de term cybersecurity breed geadopteerd aan

---

[6] http://lodder.cli.vu/flits/

[7] Door bijvoorbeeld als niet arts in een witte jas binnen te wandelen en aan de receptie inlog gegevens te vragen.

het begin van het nieuwe millennium na de opruiming van de millenniumbug.[8] De term cybersecurity is gerelateerd aan de eveneens veelvuldige gebruikte term informatiebeveiliging. In de Nationale Cybersecuritystrategie wordt cybersecurity als volgt gedefinieerd:[9]

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

In deze definitie komt het verband met informatiebeveiliging nadrukkelijk naar voren door de referentie aan het CIA-principe. CIA staat voor *confidentiality* (vertrouwelijkheid), *integrity* (integriteit) en *availability* (beschikbaarheid). Soms wordt dit palet uitgebreid met de toevoeging van *authenticity* (authenticiteit) en *reliability* (betrouwbaarheid).

Von Solms en Van Niekerk beargumenteren dat cybersecurity breder is dan informatiebeveiliging en geven de volgende voorbeelden om aan te geven op welke vlakken cybersecurity informatiebeveiliging voorbij streeft: cyberbullying, home automation, digital media en cyberterrorism.[10] Deels is deze constatering juist, veiligheid op internet kan ook onveilige situaties omvatten die niet door beveiliging zijn op te lossen. Ook het omgekeerde is echter het geval, op punten is informatiebeveiliging breder dan cybersecurity. Cyber verwijst naar internet en informatiebeveiliging ziet ook op beveiliging buiten een netwerkomgeving.

Wat verder opvalt, is dat de term ICT gebruikt wordt. Cyber als prefix verwijst normaliter naar het internet, denk aan cyberspace, cyberbullying, cybercrime, zie bijvoorbeeld O'Connell (2012):

"the key issue is how to achieve security on the Internet."

ICT omvat echter meer dan het internet en ziet op *alle* informatie– en communicatietechnologiën. De term informatiebeveiliging ligt in combinatie met ICT meer voor de hand. Cybersecurity oprekken tot ook niet aan het internet gerelateerde veiligheid is terminologisch onjuist, maar gezien de populariteit van de term waarschijnlijk niet tegen te gaan. Ook informatiebeveiliging buiten het internet schaart men daarom graag onder cybersecurity.

De nadruk bij cybersecurity ligt op het beveiligen en weerbaarder maken van systemen en netwerken, waarbij het noodzakelijk is om inzicht te krijgen in potentiële kwetsbaarheden, aanvallen en dreigingen. Op basis van een risicoanalyse kunnen vervolgens maatregelen worden bepaald en geïntroduceerd. Cybersecurity onderscheidt zich van bijvoorbeeld terrorisme door de grotere diversiteit aan daders en typen dreigingen. Hoewel daders van

---

[8] Hathaway, M. & A. Klimburg (2012). Preliminary Considerations: On National Cyber Security. National Cyber Security Framework Manual, p. 12.
[9] Nationale cybersecurity strategie, 2011.
[10] R. von Solms & J. van Niekerk (2013). From Information Security to Cyber Security, *Computers & Security*, in press.

cyberdreigingen gebruik kunnen maken van dezelfde technieken, zijn hun beweegredenen divers waardoor eveneens de doelwitten verder uiteenlopen dan die van terrorisme. Een bespreking van cybersecurity moet daarom noodzakelijk ook een bespreking bevatten van de typen dreigingen die de diversiteit van het fenomeen aangeven. De dreigingen zijn immers de input voor het ontwikkelen van cybersecuritymaatregelen om aanvallen te voorkomen of te mitigeren. Daarbij hoort overigens direct een kanttekening. De roep om maatregelen is significant in het bijzonder door een toenemende hoeveelheid van aanvallen waarover in de media gerapporteerd wordt. Desondanks is meer niet altijd beter. Een belangrijke stroming binnen het interdisciplinaire domein van cybersecurity richt zich op de economische kant daarvan. Daarbinnen wordt duidelijk hoe meer maatregelen gezien vanuit een kosten-batenanalyse soms onwenselijk zijn.[11]

1.3.1 Bescherming vitale infrastructuur

Naast cybersecurity komt de term critical infrastructure protection, oftewel vitale infrastructuur-bescherming, veelvuldig voorbij. Vitale infrastructuur-bescherming betreft een gespecialiseerder aspect van cybersecurity. De veiligheid van sectoren binnen de vitale infrastructuur geniet een andere status, mede omdat onveiligheid daarbinnen grote (fysieke) schade kan opleveren. Welke sectoren specifiek aangeduid worden als vitale infrastructuur verschilt per land, maar voor Nederland betreft het:

- Energie: elektriciteit, aardgas en olie;
- Telecommunicatie en ICT: vaste en mobiele telefonie, radio, omroep en internet;
- Drinkwater: het leveren van drinkwater;
- Voedsel: voedselvoorziening (onder andere supermarkten) en voedselveiligheid;
- Gezondheid: spoedeisende hulp en andere ziekenhuiszorg, geneesmiddelen en vaccins;
- Financiële sector: betalingen en financiële overdracht overheid;
- Beheer oppervlaktewater: waterkwaliteit en waterkwantiteit (‘keren en beheren’);
- Openbare orde en veiligheid;
- Rechtsorde: rechtspraak en detentie, rechtshandhaving;
- Openbaar bestuur: diplomatie, informatieverstrekking overheid, krijgsmacht en besluitvorming;
- Transport: vliegveld Schiphol, haven Rotterdam, hoofdwegen en hoofdvaarwegennet en spoor;
- Chemische en nucleaire industrie: vervoer, opslag, productie en verwerking van stoffen.

1.3.2 Cyberwar

Cyberwar is een bijzonder onderdeel van Cybersecurity. Internetoorlogsvoering betreft het inzetten van internettoepassingen om oorlogshandelingen te verrichten of om via het internet bijvoorbeeld door het storen van de communicatie van de tegenstander ondersteuning te bieden bij een aanval met klassieke wapens. Cyberwar is een bredere term, want betreft niet alleen cyberaanvallen maar ook cyberverdediging. Dit laatste maakt cyberwar een diffuus en complex

[11] Voor de oorsprong van deze benadering, zie: Anderson, R. (2001), "Why information security is hard – an economic perspective", *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, IEEE Computer Society, Washington, DC.

concept, omdat bij verdediging tegen aanvallen het lang niet altijd duidelijk is wie achter de aanval zit of wat de motieven van de dader zijn. Er zitten veel interessante juridische kanten aan het onderwerp,[12] maar we zullen ons hier tot twee aspecten beperken.

Voor de kwalificatie als oorlogshandeling zijn het motief en de dader van belang.[13] Een aanval van een staat op het elektriciteitsnetwerk van een andere staat kan als een oorlogshandeling worden gezien en een reactie hierop is in beginsel onder het volkenrecht gelegitimeerd. Precies dezelfde handeling van een baldadige puber, een cybercrimineel of een terrorist is zeker wat de eerste twee betreft geen oorlogshandeling.[14] Dit levert juridische problemen op, omdat afhankelijk van wie achter een daad zit een andere instantie (leger, openbaar ministerie, veiligheidsdienst, etc.) met andere bevoegdheden en vanuit andere beweegredenen bevoegd is. Het NCSC of ENISA[15] vervult vooralsnog een coördinerende rol, maar zal mogelijk op termijn ook de verschillende bevoegdheden in zich moeten gaan verenigen om snel en adequaat te kunnen reageren.

Cyberspionage wordt zowel door staten als bedrijven gebruikt vanuit politieke of economische motieven. Landen gebruiken bedrijfs- en overheidsinformatie over andere staten om een strategisch voordeel te verkrijgen. Binnen het internationale recht is spionage toegestaan, maar cyberspionnen kunnen op grond van het strafrecht worden vervolgd. De scheidslijn tussen wat nog spionage is en wat in de buurt komt van een oorlogshandeling is op het internet dun. Als ten gevolge van het plaatsen van aftap- of afluistersoftware in de computers van Defensie de computers die wapens aansturen worden beïnvloed, wordt de grens tussen spionage en oorlogshandeling overschreden. Of zoals Clark & Knake zeggen:[16]

“These military and intelligence organizations are preparing the cyber battlefield with things called logic bombs and trapdoors, placing virtual explosives in other countries in peacetime.”

Tenslotte wordt er ook wel gesproken over de hype die cyberwar omgeeft,[17] vooral ingegeven door boeken die geschreven zijn door consultants van het leger en beangstigende scenario's schetsen.[18] Wat verder het realisme van dergelijke toekomstperspectieven ook moge zijn, zeker is wel dat het internet ook binnen de oorlogsvoering een steeds belangrijker rol zal gaan innemen.

---

[12] Boer, L.J.M. & A.R. Lodder (2012), Chapter 10 Cyberwar (Cyberwar: What Law to Apply? And to Whom?), in: Leukfeldt/Stol (eds.), *Cyber Safety: An Introduction*, Eleven Publishing, zie ook http://ssrn.com/id=2039220.

[13] Er is veel literatuur over de toepasselijkheid van art. 2(4) Handvest van de Verenigde Naties. Ook moet de Talinn manual van Schmidt et. al. (2013) genoemd worden.

[14] Terroristische activiteiten worden sinds 9/11, aanvallen op WTC in New York, onder omstandigheden als oorlogshandeling gezien.

[15] Zie hierna voor toelichting over deze organisaties.

[16] R.A. Clark & R.K. Knake (2010), Cyber War: The Next Threat to National Security and What to Do About It, Harper Collins.

[17] T. Rid (2013), *Cyber War Will Not Take Place*, C Hurst & Co Publishers Ltd.

[18] Clark & Knake (2010).

1.4 Dreigingen

Over welke dreigingen spreken wij binnen het brede domein van cybersecurity. Het Cybersecuritybeeld Nederland (CSBN) geeft daarvoor een bruikbare uiteenzetting, waarin de verscheidenheid aan aanvallen te classificeren zijn. Sinds eind 2011 wordt in Nederland voor het in kaart brengen van cybersecurity-dreigingen het CSBN opgesteld. Dit document hanteert de volgende categorisering voor dreigingen:

- Informatiegerelateerde dreigingen,
- Systeemgerelateerde dreigingen, en
- Indirecte dreigingen.

Bij informatiegerelateerde dreigingen is de primaire intentie van de dader om informatie te verkrijgen, te misbruiken, te publiceren of te veranderen. Bij systeemgerelateerde dreigingen is de intentie van de daders om de dienstverlening of de bedrijfsvoering van een organisatie te verstoren. Beide categorieën sluiten elkaar niet per se uit. Daders kunnen namelijk middels het verwijderen van informatie de bedrijfsvoering verstoren. Het onderscheid zit primair in de intentie van de dader en in tweede instantie in de hulpmiddelen die daarvoor gebruikt worden. De indirecte dreiging is een categorie waarin de neveneffecten van de twee voorgaande categorieën worden samengebracht. Dit is een soort spill-over effect, waarbij ook organisaties en andere gebruikers getroffen kunnen worden zelfs als zij geen primair doelwit zijn van een aanval maar toch de gevolgen ervaren.

De classificatie van dreigingen vindt grotendeels plaats op basis van de onderliggende principes van informatiebeveiliging, welteverstaan: confidentiality, integrity and availability. Voor informatiegerelateerde dreigingen ligt de nadruk op vertrouwelijkheid en integriteit van de informatie; terwijl voor de systeemgerelateerde dreigingen beschikbaarheid centraal staat. Op deze wijze weten deze twee typen dreigingen een grote lading te dekken.

Het in kaart brengen van dreigingen en daaraan gekoppeld de kwetsbaarheden en hulpmiddelen waarvan misbruik gemaakt wordt om aanvallen uit te voeren, is van belang voor het vervolgens inschalen van de mogelijkheden tot maatregelen. In het kader van dit hoofdstuk ligt de focus uiteraard vooral op de mogelijkheden voor juridische maatregelen om de staat van digitale veiligheid te bevorderen.

1.4.1 Informatiegerelateerde dreigingen

Bij digitale aanvallen kunnen daders geïnteresseerd zijn in verschillende typen informatie. Een belangrijk voorbeeld is de interesse van criminelen in het verkrijgen van financieel gewin middels persoonsgegevens, in het bijzonder log-in credentials, geboortedata, burgerservicenummers, etc. Deze persoonsgegevens zijn het doelwit van aanvallers omdat wij, als gebruikers, deze gegevens inzetten voor identificatie- en authenticatie-doeleinden. Onze gebruikersnaam en wachtwoord geeft ons toegang tot een email-account, een bankrekening of kan worden gebruikt om in te loggen op ons werk. Voor criminelen zijn deze gegevens dus een sleutel om de deur te openen. Er is daarom ook voorgesteld om het helen van (digitale)

gegevens strafbaar te stellen.[19] Het is immers een voorbereidende actie om vervolgens bijvoorbeeld identiteitsfraude te plegen.

Een belangrijk voorbeeld van hoe criminelen tot hun financieel gewin kunnen komen is fraude met internetbankieren, waarbij zij middels het afvangen van de communicatie tussen de cliënt en de banktransacties kunnen initialiseren en veranderen. De schade door fraude met internetbankieren vertoonde de afgelopen jaren een stijgende lijn, ondanks het gebruik van het twee factor authenticatie-systeem.[20] Criminelen zijn namelijk alsnog in staat om tussen de cliënt en de bank in te gaan staan. Dit komt door middel van een Man-in-the-middle of een Man-in-the-Browser-aanval, waarbij de computer van de cliënt geïnfecteerd wordt en vervolgens de communicatie afgevangen en gemanipuleerd kan worden. Dit jaar constateerde de Nederlandse Vereniging van Banken (NVB) echter voor het eerst een daling. Volgens de NVB is deze daling mede tot stand gekomen door het gebruik van verbeterde detectiesoftware en de inzet van publiekscampagnes, waardoor gebruikers beter op de hoogte zijn van de risico's en daarom de nodige voorzorgsmaatregelen nemen. Dit is van buitenaf lastig empirisch vast te stellen, aangezien meer gedetailleerde informatie over aanvalsmanieren en de misbruikte kwetsbaarheden ontbreken. Criminelen kunnen immers middels verschillende methoden fraude plegen. De graad van de betrokkenheid van het individuele slachtoffer is gezien de diversiteit van methoden uiteenlopend.[21] Zo kan een consument volledig buitenspel gezet zijn als zij slachtoffer is geworden van een drive-by download, waardoor alleen het bezoeken van een geïnfecteerde site al kan leiden tot een geïnfecteerde computer. Echter, kan een consument ook een actievere rol spelen door een phishing email te openen en vervolgens op een link te klikken om in-log credentals af te geven.

Een van de juridische maatregelen die relevant is voor dit type dreiging is de introductie van een meldplicht voor datalekken. Een dergelijke meldplicht werd voor het eerst in de staat Californië in de Verenigde Staten ingevoerd. Het idee achter een meldplicht naar aanleiding van een datalek is dat slachtoffers of een organisatie op de hoogte worden gebracht van het feit dat (hun) (persoons)gegevens gecompromitteerd zijn. Deze maatregel heeft in theorie bepaalde voordelen. Ten eerste kunnen slachtoffers actie ondernemen om de gevolgen van het datalek te beperken. Zij kunnen wachtwoorden veranderen, creditcards blokkeren of beter in de gaten houden of verdachte transacties plaatsvinden. De mogelijkheden voor slachtoffers om misbruik te voorkomen zijn nagenoeg afwezig. De gegevens zijn immers al potentieel in criminele handen. Het enige wat slachtoffers kunnen doen is vroegtijdige detectie van fraude. Ten tweede zorgt een meldplicht voor de introductie van een bepaalde prikkel voor organisaties om meer prioriteit te geven aan informatiebeveiliging. Het moeten melden van een datalek kan leiden tot reputatieschade, aangezien het vertrouwen in de organisatie daalt door een dergelijk incident.

---

[19] Zie wetsvoorstel versterking bestrijding computercriminaliteit, https://www.internetconsultatie.nl/wetsvoorstel_versterking_bestrijding_computercriminaliteit.

[20] Bij een twee factor authenticatie systeem wordt gebruik gemaakt van een gebruikersnaam en een wachtwoord (something you know) en een andere authenticatievorm, zoals een randomizer of een sms bericht (something you have).

[21] Zie voor een uitgebreide bespreking Van der Meulen (2011b). Between Awareness and Ability: Consumers and Financial Identity Theft. *Communications & Strategies*, No. 81: 23-44.

Ten derde biedt een meldplicht tevens de gelegenheid om data te vergaren over de aard en omvang van het datalekken-probleem.

In Nederland is op 21 juni 2013 een wetsvoorstel geïntroduceerd om een meldplicht te introduceren in de Wet bescherming persoonsgegevens (Wbp). Dit voorstel voor een meldplicht is specifiek gericht op verantwoordelijken voor de verwerking van persoonsgegevens, wanneer gebleken is dat getroffen beveiligingsmaatregelen zijn doorbroken en indien "redelijkerwijs kan worden aangenomen dat die leidt tot een aanmerkelijke kans op nadelige gevolgen voor de bescherming van de persoonsgegevens die door de desbetreffende verantwoordelijke worden verwerkt" (nieuw art. 34a lid 1 Wbp). Op basis van het wetsvoorstel ontvangt het CBP de bevoegdheid om een boete van 450.000 euro op te leggen indien er geen (tijdige) melding plaatsvindt.

Andere informatie waarvoor daders interesse hebben, zijn vertrouwelijke gegevens van publieke en private organisaties. Digitale spionage staat sinds enkele jaren op de kaart. Voor private organisaties is de zorg vooral het beschermen van bedrijfsgeheimen over producten, terwijl publieke organisaties vooral vertrouwelijke inlichtingen en defensie-informatie beschermen.

1.4.2 Systeemgerelateerde dreigingen

Systeemgerelateerde dreigingen zijn vooral gericht op het verstoren van de dienstverlening of de bedrijfsvoering. In 2013 lijkt de hoeveelheid Distributed Denial of Service (DDoS)-aanvallen toe te nemen. Een DDoS-aanval kan uitgevoerd worden door een te grote hoeveelheid verzoeken naar de website te sturen, waardoor deze wordt overbelast. Hierdoor kan legitiem dataverkeer, denk aan de internetgebruiker die een website wil bezoeken, geen gebruik meer maken van de dienst. Een veelgebruikt voorbeeld om het probleem beter te visualiseren is om het te vergelijken met een file. Iedereen wil tegelijkertijd naar dezelfde locatie toegaan, waardoor de plek onbereikbaar wordt omdat de wegen vol zitten. Sinds het begin van 2013 zijn onder andere verschillende Nederlandse banken, iDeal, de belastingdienst, DigiD, de douane en de Telegraaf het doelwit geworden van DDoS-aanvallen. Vanuit welke hoek deze dreiging komt, is lastig vast te stellen. De aanvallen in combinatie met de berichtgeving hebben er wel voor gezorgd dat er een roep om meer actie is gekomen. De beschikbaarheid en effectiviteit van maatregelen lijkt momenteel echter beperkt. Zodoende werd de ING zelfs na het implementeren van maatregelen getroffen door aanvallen.[22] Voorkomen lijkt daarom slechts een illusie. Over de maatregelen wordt relatief weinig informatie verstrekt; de bank deelde slechts mee dat het maatregelen waren om onderscheid te maken tussen goed en kwaadaardig dataverkeer.[23] Op deze manier kan een aanval in een vroeg stadium herkend worden en kan de duur van het succes van de aanval beperkt worden.

[22] Zie "ING ondanks maatregelen getroffen door nieuwe DDos-aanval" http://www.nrc.nl/nieuws/2013/04/10/ing-nieuwe-cyberaanval-sneller-afgeslagen-door-maatregelen/.

[23]0 Zie "ING nieuwe cyberaanval sneller afgeslagen door maatregelen." http://www.nrc.nl/nieuws/2013/04/10/ing-nieuwe-cyberaanval-sneller-afgeslagen-door-maatregelen/.

Het Nationaal Cybersecurity Centrum (NCSC) geeft in haar Factsheet Continuïteit van online diensten aan welke maatregelen getroffen kunnen worden. Deze hebben vooral een organisatorisch of technisch karakter, zoals “stel een strategie en plan van aanpak vast”, “monitor uw infrastructuur”, en “instrueer uw communicatieadviseur”.[24] Een uitgebreide bespreking van juridische maatregelen blijft veelal buiten beschouwing. Boele Staal van de NVB meent dat mogelijkheden voor compensatie niet aan de orde zijn, omdat de aanvallen en de daaraan gekoppelde schade een kwestie van overmacht zijn. De banken stellen regelmatig dat ze er alles aan doen om DDoS-aanvallen te beperken. Prins vraagt zich daarentegen af:[25]

> “[w]aren de genomen maatregelen – binnen de grenzen van het redelijke – wel ‘voldoende’? Dat verlangt een discussie over de vraag welke risico’s bij een DDoS-aanval de aanbieder van online diensten vallen toe te rekenen en dus wanprestatie oplevert (art 6:74 BW) en in welke situaties de omstandigheden zodanig zijn dat ze een overmachtsituatie rechtvaardigen (artikel 6:75 BW)?”

Prins gaat specifiek in op de banken en meent dat zij een grotere mate van zorgvuldigheid dan andere organisaties dienen na te leven. Vervolgens trekt zij het idee van overmacht deels in twijfel en stelt dat bij een grotere mate van alertheid overmacht niet meer aangedragen kan worden als reden. Dit is een punt van discussie aangezien het voorkomen van DDoS-aanvallen zelfs als ‘onmogelijk’ bestempeld wordt. Engelfriet schrijft:[26]

“[e]en DDOS aanval zou ik eerder als iets van buitenaf zien, net zoals een hagelstorm. Je kunt het niet voorkomen, je kunt alleen de impact beperken.”

Bij overmacht is de vraag naar het al dan niet kunnen voorkomen relevant. Hoe vervolgens omgegaan wordt met de aanval als die zich voordoet, zou de focus moeten zijn van het debat rondom verantwoordelijkheden van schadebeperking en eventuele aansprakelijkheid. De suggestie van Prins om “[d]e juridische praktijk en het maatschappelijke en politieke debat om cyberveiligheid niet langer uitsluitend vanuit strafrechtelijke opsporing van daders te benaderen” zou zeker ter harte genomen dienen te worden. Volgens haar zouden “[c]ivielrechtelijke zorgplichten voor dienstenaanbieders, de rol van zelfregulering daarbij en wellicht zelfs de implicaties van een en ander voor strafrechtelijke aansprakelijkheid” ook bediscussieerd moeten worden. Hetgeen tot op heden onvoldoende gedaan wordt.

1.4.3 Dreigersgroepen

Vooral de diversiteit aan daders onderscheidt cybersecurity van andere veiligheidsdomeinen, zoals de bestrijding van terrorisme. Het Cybersecuritybeeld Nederland (CSBN) geeft een overzicht van relevante dreigersgroepen. De pure dreigersgroepen zijn hacktivisten,

---

[24] NCSC (2013). Continuiteit van Onlinediensten, FS 2013-01.
[25] Prins, C. (2013). Zorgplichten en cybercrime, http://njblog.nl/2013/05/01/zorgplichten-en-cybercrime/.
[26] Engelfriet, A. (2011). Wat moet een provider doen bij een DDoS-aanval op de server van een klant? http://blog.iusmentis.com/2011/08/26/wat-moet-een-provider-doen-bij-een-ddos-aanval-op-de-server-van-een-klant/.

beroepscriminelen, terroristen en scriptkiddies. Dit zijn pure dreigersgroepen aangezien zij zich onderscheiden doordat ze een dreiging vormen en niet tevens doelwit zijn, dit in tegenstelling tot staten en private organisaties. Zij kunnen zowel dreigersgroep als doelwit zijn. Zoals in het CSBN beschreven:

> "[h]et ontwikkelen van een model dat alle actoren goed weergeeft, blijft een uitdaging. Omdat de dreigersgroepen op intentie zijn ingedeeld, is het goed denkbaar dat een persoon of groep in meerdere dreigersgroepen past."

Intentie staat dus voorop als onderscheidende karakteristiek. Dit kan gepaard gaan met een bepaalde methodiek en een bepaald doelwit. De intentie voor beroepscriminelen is financieel gewin, terwijl het doel voor terroristen is om angst te zaaien. Hacktivisten lijken vooral uit op het inzetten van digitale middelen voor ideologische en activistische doeleinden, alhoewel aandacht trekken soms ook een rol lijkt te spelen. Verder is er een categorie scriptkiddies, die slechts een uitvoerende groep is en verder weinig kennis heeft van de technische kant van aanvallen.

1.5 Strategie & organisaties

Gezien het groeiende belang van cybersecurity hebben al meerdere landen een cybersecurity-strategie gelanceerd. Door de toenemende betrokkenheid van de 'natiestaat' zijn nationale veiligheid en cybersecurity steeds meer met elkaar verweven geraakt. Volgens het NAVO Center of Excellence hebben 24 landen een cybersecurity-strategie gepubliceerd.[27] Volgens Klimburg hebben meer dan vijftig landen een officieel strategiedocument gepubliceerd met daarin hun positie ten aanzien van cyberspace, cybercrime en/of cybersecurity.[28] Daarnaast heeft de Europese Unie eveneens een strategie uitgegeven (zie 1.5.3).

Ondanks onderlinge verschillen tussen de strategieën heeft de OESO op basis van een analyse van 12 leden ook de nodige overeenkomsten geconstateerd. Het eerste terugkerende aspect in de meeste strategieën is de noodzaak voor de bevordering van meer coördinatie binnen de overheid op beleids- en operationeel niveau. Zoals de OESO aangeeft in haar rapport:[29]

> "As cybersecurity becomes an issue of national priority, responsibility for cybersecurity policy making and implementation is being clearly assigned within the government. However, no single existing vertical agency can claim a comprehensive understanding and a sufficiently wide authority to manage all facets of cybersecurity."

Dit wordt ook evident in de volgende paragraaf die specifiek in gaat op de betrokken organisaties. Een tweede aspect dat benadrukt wordt, is de noodzaak voor het versterken van publieke-private samenwerking. Cybersecurity is een gedeelde verantwoordelijkheid, mede omdat geen enkele organisatie alleen de verantwoordelijkheid kan dragen. De publieke sector

---

[27] Op de website heeft het COE de strategieën tot 21 november 2012 bijgehouden.
[28] Klimburg, A (2012). National cyber security framework manual, NAVO CCD COE.
[29] OECD 2012, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy*, p. 13.
[29] OECD 2012.

erkent de urgentie om met private partners samen te werken aangezien zij een essentiële rol spelen binnen het veld.

Naast het betrekken van verscheidene organisaties binnen de publieke en de private sector is het bevorderen van internationale samenwerking eveneens een terugkerend thema. Het internationale of transnationale karakter van het internet vereist dat partners over de gehele wereld toenadering zoeken. Hoewel deze ambitie zeker bewonderenswaardig is, erkent de OESO dat het merendeel van de strategieën weinig detail geeft over hoe landen dit in de praktijk willen brengen. Uitzonderingen zijn de Verenigde Staten en het Verenigd Koninkrijk. De Verenigde Staten heeft specifiek een internationale strategie opgesteld.[30] Het Verenigd Koninkrijk is expliciet op zoek gegaan naar de mogelijkheden om de internationale dialoog te bevorderen middels een conferentie in London in 2011.[31] De noodzaak van een grotere mate van harmonisatie van internationale wetgeving op het gebied van cybercrime wordt veelvuldig benadrukt, in het bijzonder ter ondersteuning van het Cybercrime-verdrag.[32]

Het vierde en laatste aspect dat terugkeert in alle strategieën is respect voor fundamentele rechten. Alle strategieën benadrukken het belang om binnen cybersecurity-beleid privacy, vrijheid van meningsuiting en vrijheid van informatie te respecteren. Het open karakter van het internet moet behouden blijven en voor sommige landen geldt deze openheid als kernvoorwaarde voor de verdere ontwikkeling van de *internet economy*, aangezien vooral innovatie gebaad is bij een dergelijk open karakter.

1.5.1 Nationale cybersecurity Strategie

De Nationale cybersecurity Strategie (NCSS) met als titel *Slagkracht door Samenwerking* werd in februari 2011 gepubliceerd. De inleiding geeft aan dat de strategie uit twee delen bestaat. Het eerste deel legt primair de focus op de analyse van het probleem en het uiteindelijke doel van de strategie. Het tweede deel zet een aantal actielijnen uiteen en geeft aan waar de prioriteiten op het gebied van cybersecurity moeten liggen. Het uiteindelijke doel van de strategie is de versterking van de digitale veiligheid in Nederland om tevens het vertrouwen in het internet te bevorderen. Ook de Nederlandse strategie benadrukt de in de vorige paragraaf genoemde punten uit de OESO analyse.

De actielijnen die de strategie heeft uitgezet, beginnen met het inrichten van een cybersecurity Raad en een Nationaal cybersecurity Centrum. Volgens de strategie:

> "[is] [d]e zorg voor digitale veiligheid […] in Nederland belegd bij veel verschillende partijen. Op dit moment is er nog onvoldoende samenhang tussen het geheel van goede beleidsinitiatieven, voorlichting en operationele samenwerking."

---

[30] White House (2011). International Strategy for Cyberspace, beschikbaar op: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
[31] The London Conference on Cyberspace, 1 – 2 November 2011.
[32] Council of Europe. Convention on Cybercrime. ETS 185.

In de strategie wordt dus onderkend dat er een potentie voor problemen is door een gebrek aan samenhang tussen een diverse groep van betrokken partijen (zie 1.5.2). Middels de Cybersecurity Raad en het Nationaal Cybersecurity Centrum (zie 1.5.2) hoopt de strategie dit gebrek weg te nemen, zowel op beleids- en strategisch als op operationeel niveau. De Raad is op 1 juli 2011 van start gegaan en het Centrum op 1 januari 2012.
De tweede actielijn valt samen met de eerdere bespreking van het Cybersecuritybeeld Nederland. Dit rapport kent haar oorsprong in de strategie aangezien deze specifiek vraagt om het opstellen van dreigings- en risicoanalyses. Volgens de strategie is het doel:

> "…risico's in kaart brengen en capaciteiten identificeren die versterkt moeten worden om dreigingen te voorkomen en op verstoringen te kunnen reageren. Met deze kennis kunnen alle doelgroepen maatregelen treffen in de gehele keten van preventie tot respons en opsporing en vervolging."

Het terrein dat het Cybersecuritybeeld bestrijkt, is dus breed, gezien het feit dat de strategie refereert aan de gehele keten waarin tevens opsporing en vervolging zijn meegenomen.

De derde actielijn is gericht op het vergroten van de weerbaarheid van de vitale infrastructuur. Zoals eerder aangegeven tijdens de bespreking van de definitie is bescherming van de vitale infrastructuur inmiddels een nagenoeg onlosmakelijk aspect geworden van cybersecurity.

De overige drie actielijnen zijn:

- Versterken van de responscapaciteit om ICT-verstoringen en cyberaanvallen te pareren;
- Intensiveren van opsporing en vervolging van cybercrime;
- Stimuleren van onderzoek en onderwijs op het terrein van cybersecurity.

Ten tijde van dit schrijven zijn de voorbereidingen al begonnen voor de tweede versie van de Nederlandse Cybersecurity Strategie, maar het is te vroeg om daar nu al op in te kunnen gaan.

1.5.2 Organisaties

Het speelveld van cybersecurity wordt steeds breder. Dit is grotendeels het gevolg van de integratie van 'cyber' in nagenoeg alle aspecten van de maatschappij. Hierdoor zijn sommige organisaties zijdelings bij het onderwerp betrokken, terwijl anderen cybersecurity als hun 'core business' beschouwen. De betrokkenheid van diverse spelers heeft echter wel geleid tot de uitdaging om verantwoordelijkheden, bevoegdheden en verplichtingen op de juiste manier te beleggen en coördineren. Mede door het introduceren van 'nieuwe' organisaties ontstaat het risico van een *crowded policy space*.[33] In deze context vertoont cybersecurity overeenkomsten met de oorlog tegen terrorisme, waarin ook 'nieuwe' actoren werden geïntroduceerd waardoor het speelveld nog drukker werd en overlap ontstond. Voor cybersecurity bestaat dat gevaar ook zolang partijen onvoldoende met elkaar afstemmen. Duidelijkheid over verantwoordelijkheden

[33] Van der Meulen, N.S. (2013a). Following in the Footsteps of Terrorism, *Canadian Journal of Foreign Policy*, Vol. 19 (2), p. 123 – 126.

en bevoegdheden zijn bovenal essentieel in het geval van incidenten, waarbij een snelle reactie vereist is. Zoals eerder aangegeven bij de dreigingen is het classificeren van aanvallen een complex geheel omdat verschillende daders dezelfde technieken gebruiken. Het classificeren van een aanval gebeurt daarom veelal op basis van subjectieve indicatoren, zoals doelwit, investeringsvereiste van de aanval, moeilijkheidsgraad en gerichtheid. De herkomst van een aanval is door de technische mogelijkheden over het algemeen onvoldoende te herleiden en kan daarom slechts zelden fungeren als betrouwbare indicator. De uiteindelijke respons is daarom overgeleverd aan *circumstantial evidence*.

Als wij ons beperken tot een bespreking van de organisaties in Nederland liggen de verhoudingen als volgt.[34] De minister van Veiligheid en Justitie is coördinerend bewindspersoon voor cybersecurity en de nationale veiligheid. De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), een organisatie die onder de verantwoordelijkheid van de minister van Veiligheid en Justitie valt, richt zich op de bescherming van vitale belangen en de weerbaarheid van vitale sectoren. Binnen de NCTV fungeert het Nationaal Cyber Security Centrum (NCSC) als informatieknooppunt en expertisecentrum voor cybersecurity. Het NCSC is sinds januari 2012 operationeel, maar kent haar wortels in een eerdere organisatie GOVCERT.NL. GOVCERT.NL was het Computer Emergency Response Team van de Nederlandse overheid en maakte deel uit van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. In 2011 maakte de organisatie de overstap naar het Ministerie van Veiligheid en Justitie, alvorens het zich ontplooide tot het huidige NCSC. Het NCSC brengt betrokken partijen bij elkaar en deelt actief kennis binnen haar nationale en internationale netwerk. Daarnaast levert het NCSC ondersteuning en advies aan getroffen partijen. De primaire doelgroepen voor het NCSC zijn de Rijksoverheid en de vitale sectoren. Verder fungeert het NCSC tevens als informatiepunt voor de overige sectoren in Nederland.[35]

Het NCSC heeft cybersecurity als haar core business, net zoals de Cyber Security Raad. Zoals eerder vermeld zijn beide een voortvloeisel uit de strategie. De Cyber Security Raad (CSR) “stelt prioriteiten in de aanpak van ICT-bedreigingen, bekijkt de behoefte aan nadere research & development en kijkt hoe deze kennis vervolgens het beste kan worden gedeeld met de samenwerkende publieke en private partijen.”[36] De taak voor de Cybersecurity Raad is om gevraagd en ongevraagd advies te geven aan zowel de regering als private partijen over ontwikkelingen op het gebied van cyber security. De raad zelf is samengesteld uit vertegenwoordigers vanuit overheidspartijen, de wetenschap en private partijen.

Naast het NCSC en de CSR is er een verscheidenheid aan partijen die op een of meer manieren zijdelings bij het onderwerp betrokken zijn, zowel binnen als buiten de overheid. Als de bancaire sector doelwit is van aanvallen, zoals in het voorjaar 2013, dan komt het Ministerie

---

[34] Zoals aangegeven in een brief van 14 mei 2013 in reactie op DDoS-aanvallen bij de rijksoverheid, aan de Tweede Kamer.
[35] Brief aan de Tweede Kamer, 14 mei 2013, Reactie op DDoS aanvallen bij de rijksoverheid.
[36] Persbericht ‘Cyber Security Raad geinstalleerd’, 2011, beschikbaar op: http://www.rijksoverheid.nl/documenten-en-publicaties/persberichten/2011/06/30/cyber-security-raad-geinstalleerd.html

van Financiën in de schijnwerpers, terwijl veiligheidsaangelegenheden bij de overheid zelf, zoals DigiD-kwetsbaarheden, binnen het domein van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties vallen. Daarnaast zijn andere ministeries, zoals het minsterie voor Defensie, ook bezig met het bouwen van cybercapaciteiten.

1.5.3 EU-initiatieven

Het grensoverschrijdende karakter van internet en de globaliserende samenleving zijn van invloed op cybersecurity, ziet ook de Europese Unie in:

> "Vanwege dat transnationale karakter kan een ernstige verstoring van die systemen in een lidstaat ook andere lidstaten en de Unie als geheel treffen. De veerkracht en stabiliteit van netwerk- en informatiesystemen is daarom essentieel voor de soepele werking van de eengemaakte markt."[37]

Sinds 2004 is ENISA, het Europees Agentschap voor netwerk- en informatiebeveiliging, actief op het terrein van digitale veiligheid.[38] ENISA moet er op toezien dat binnen de EU problemen rond netwerkveiligheid worden voorkomen, beheerst en opgelost. Om dit te realiseren bevordert ENISA de samenwerking binnen de beveiligingsmarkt en wordt bijstand en advies verleend aan de EU alsmede de lidstaten. Kort na de oprichting van ENISA is in 2005 een kaderbesluit inzake aanvallen op informatiesystemen gepubliceerd dat ten doel had computercriminaliteit te bestrijden en de beveiliging van informatie te bevorderen.[39] In juni 2013 is een verordening gepubliceerd die ten doel heeft ENISA te moderniseren en versterken.[40]

Eerder in 2010, is door de Europese Commissie een Richtlijn voorgesteld dat eerder genoemd kaderbesluit vervangt[41] om Europa beter te beschermen tegen cyberaanvallen.[42] In 2013 was deze richtlijn nog niet definitief vastgesteld en er wordt naar de nog lopende onderhandelingen daarover binnen de Europese Unie verwezen in een in februari 2013 nieuw voorgestelde richtlijn.[43] Deze nieuwe Richtlijn maakt onderdeel uit van het nieuwste EU-initiatief dat ook een strategie voor cyberbeveiliging omvat. De richtlijn streeft er naar binnen de Europese Unie een hoog niveau van NIB (Netwerk- en InformatieBeveiliging) te realiseren langs drie lijnen:[44]

---

[37] Overweging 3 voorstel Richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en informatiebeveiliging in de Unie te waarborgen, 7 februari 2013, COM(2013) 48 final.
[38] Verordening 460/2004 van het Europees Parlement en de Raad van 10 maart 2004 tot oprichting van het Europees Agentschap voor netwerk- en informatiebeveiliging, *PbEG* L77 13.03.2004, p. 1 -11.
[39] Kaderbesluit 2005/222/JBZ over aanvallen op informatiesystemen, *PbEG L69,* 16.03.2005, p. 67-71.
[40] Voorstel voor een Verordening Inzake het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA), 30.9.2010, COM(2010) 521 def.
[41] Voorstel Richtlijn over aanvallen op informatiesystemen en tot intrekking van Kaderbesluit 2005/222/JBZ, Brussel, 30.9.2010 COM(2010) 517 def.
[42] Commissie wil Europa beter beschermen tegen cyberaanvallen, 30.09.2010, IP/10/1239
[43]Voorstel Richtlijn houdende maatregelen om een hoog gemeenschappelijk niveau van netwerk- en
[43]informatiebeveiliging in de Unie te waarborgen, 7.2.2013, COM(2013) 48 final. Over de verordening COM(2010) 521 def op p. 6, voetnoot 13. Over de Richtlijn COM(2010) 517 def. p. 6, voetnoot 19.
[44] Art. 1 lid 2 van Voorstel Richtlijn Informatiebeveiliging.

1. De vaststelling van verplichtingen voor alle lidstaten met betrekking tot de preventie en behandeling van en de reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;
2. De oprichting van een mechanisme voor samenwerking tussen de lidstaten met het oog op een uniforme toepassing van deze richtlijn in de Unie en, waar nodig, een gecoördineerde en doeltreffende behandeling van en reactie op risico's en incidenten met betrekking tot netwerken en informatiesystemen;
3. De vaststelling van beveiligingseisen voor marktdeelnemers en overheden.

Er zijn kritische kanttekeningen te plaatsen bij de gekozen richting.[45] De komende jaren zullen uitwijzen in hoeverre de EU succesvol blijkt om binnen de gehele Europese Unie een veilig en betrouwbaar internet te garanderen.

1.6 Conclusie

Gaandeweg wordt er meer duidelijk over het complexe landschap waarin het onderwerp cybersecurity zich bevindt. Met de introductie van een nationale strategie beogen landen tenminste voor henzelf helder te krijgen wat het probleem is en hoe zij daarmee om moeten gaan. Cybersecurity kent haar wortels grotendeels in de informatiebeveiliging, dat zelfs voor het digitale tijdperk al relevant was. Cybersecurity is echter een breder en omvattender terrein dan informatiebeveiliging. In het bijzonder aangezien het fenomeen zich uitstrekt over meerdere belangen en domeinen, waaronder eventuele conflicten tussen staten in de vorm van cyberwar. Deze diversiteit wordt weergegeven in het palet aan dreigingen, waarmee verschillende partijen, van individuele gebruikers tot aan overheidsinstanties en vitale bedrijven, worden geconfronteerd. Het is daarom van essentieel belang om na te gaan welke dreiging het meest van toepassing is op welke partij, zodat daarvoor de juiste middelen ingeschakeld kunnen worden om schade te voorkomen dan wel te beperken. Incidenten, van DigiNotar tot de aanvallen op de dienstverlening van banken, hebben de dreiging concreet gemaakt en tevens de urgentie voor actie op het gebied van recht en beleid vergroot.

Geraadpleegde en aanbevolen literatuur

Anderson, R. (2001), "Why information security is hard – an economic perspective", *ACSAC '01: Proceedings of the 17th Annual Computer Security Applications Conference*, IEEE Computer Society, Washington, DC.

Boer, L.J.M. & A.R. Lodder (2012), Chapter 10 Cyberwar (Cyberwar: What Law to Apply? And to Whom?), in: Leukfeldt/Stol (eds.), *Cyber Safety: An Introduction*, Eleven Publishing, zie ook http://ssrn.com/id=2039220.

Clark, R.A. & R.K. Knake (2010), *Cyber War: The Next Threat to National Security and What to Do About It*, Harper Collins.

[45] W. van Holst (2013), Richtlijn cybersecurity: Gemiste kans. Het voorstel van Kroes roept veel vragen op, *Automatiseringsgids* 7 mei 2013.

Feiler, L. (2012), *Information Security Law in the EU and the U.S. A Risk-Based Assessment of Regulatory Policies*, Springer.

Graham R.A., R. Olson & R. Howard (2013), *Cyber Security Essentials*, Auerbach Publications.

Hathaway, M. & A. Klimburg (2012). Preliminary Considerations: On National Cyber Security. National Cyber Security Framework Manual.

Klimburg, A (2012). National cyber security framework manual, NAVO CCD COE.

Leukfeldt, R. & W. Stol (2012)(eds.), Cyber Safety: an Introduction, Eleven publishers international

Meulen, N.S. van der (2011a). *Financial Identity Theft: Context, Challenges and Countermeasures*. The Hague: TMC Asser Press.

Meulen, N.S. van der (2011b), Between Awareness and Ability: Consumers and Financial Identity Theft. *Communications & Strategies*, No. 81: 23 – 44.

Meulen, N.S. van der (2013a), Following in the Footsteps of Terrorism, *Canadian Journal of Foreign Policy, Vol. 19 (2), p. 123- 126*.

Meulen, N.S. van der (2013b),DigiNotar: Dissecting the First Dutch Digital Disaster, Journal of Strategic Security Vol. 6, Issue 4.

NCSC (2013). Continuiteit van Onlinediensten, FS 2013-01.

O'Connell, M.E. (2012), Cybersecurity without Cyberwar, *J Conflict Security Law* (Summer 2012) 17 (2): 187-209.

OECD 2012, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.*

Rid, T. (2013), Cyber War Will Not Take Place, C Hurst & Co Publishers Ltd.

Schmidt, M.N. (ed.)(2013), *Tallinn Manual on the International Law Applicable to Cyber Warfare* Cambridge University Press.

Solms, R. von & J. van Niekerk (2013). From Information Security to Cyber Security, *Computers & Security*, in press.

White House (2011). International Strategy for Cyberspace, beschikbaar op: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.