ICT-NOTA SP

KNOOPPUNTEN EN OPLOSSINGEN

Sharon Gesthuizen, SP Tweede Kamerlid
Sjoerd van Dijk, fractiemedewerker SP Tweede Kamer
augustus 2012

Sharon Gesthuizen, SP Tweede Kamerlid
Sjoerd van Dijk, fractiemedewerker SP Tweede Kamer
augustus 2012
Foto's: sxc.hu

ICT-NOTA SP
KNOOPPUNTEN EN OPLOSSINGEN

INLEIDING

Een wereld zonder internet is bijna niet meer voor te stellen. Waar we ook gaan en staan: digitale systemen zijn met ons dagelijks leven verbonden. Of we nu digitaal aangifte doen bij de belastingdienst, de chipkaart gebruiken bij het inchecken in de bus of metro, of actief zijn op een social network, we maken gebruik van het wereldwijde web. Het vrij kunnen gebruiken van internet is een ***basisrecht*** *en behoort daarom ook in de toekomst voor iedereen toegankelijk te blijven. De overheid moet dit dan ook bevorderen.*

Het belang van internet voor onze economie neemt toe. Juist in de informatie- en communicatietechnologie (ICT) ligt een grote kans voor ***innovatie****. Denk bijvoorbeeld aan software die het lokaliseren van voorwerpen vergemakkelijkt of aan het betalen voor producten terwijl je onderweg bent met alleen je telefoon. Met de vlucht die ICT en internet hebben genomen is een platform ontstaan waarbij burgers en bedrijven makkelijk informatie en ideeën kunnen uitwisselen.*

Maar ICT en internet zijn ook voor kwaadwillende personen interessante middelen om criminele activiteiten te ontplooien. Optreden tegen online criminaliteit verdient een prominente plaats bij politie en justitie, zowel in expertise als in aandacht. Helaas staat de aanpak van deze misdrijven op veel plaatsen nog in de kinderschoenen.[1]

De komende jaren zal de invloed van ICT en internet blijven toenemen. Om hun positieve mogelijkheden verder te ontwikkelen en de negatieve effecten aan te pakken moet de overheid duidelijk beleid maken. De SP wil met deze ICT-nota haar ideeën presenteren om een veilige, betrouwbare en gebruikersvriendelijke digitale toekomst zeker te stellen.

1 Artikel Algemeen Dagblad, 29 juni 2012: 'Te weinig kennis en aansturing bij politie over aanpak cybercrime'.
www.ad.nl/ad/nl/5601/TV-Radio/article/detail/3278984/2012/06/29/Te-weinig-kennis-en-aansturing-bij-politie-over-aanpak-cybercrime.dhtml

1 BELANGEN INTERNETGEBRUIKERS

Bij vrijwel alle mensen en ondernemingen die dagelijks gebruik maken van internet bestaat een grote behoefte aan continuïteit van deze dienst. Het is daarom van groot belang dat het netwerk betrouwbaar is. Ook moeten burgers en bedrijven meer grip krijgen op de persoonlijke informatie die van hen opgeslagen of verhandeld wordt. De overheid noch commerciële partijen mogen zomaar een profiel maken of opslaan van iemand die argeloos op het internet surft. Iedereen moet op een simpele manier kunnen aangeven dat hij of zij niet wil worden gevolgd op het net ('do-not-track-me'). Al deze onderwerpen zijn van belang voor de privacy van de internetgebruiker en de kwaliteit en betrouwbaarheid van internetdiensten.

TOEGANG EN NETNEUTRALITEIT

In Nederland is internet vrij en toegankelijk. Het vrij kunnen gebruiken van internet is een recht dat niet zomaar mag worden ingeperkt: voor ieder mens geldt het recht op toegang tot internet.[2] Diensten als email zijn immers cruciaal geworden bij het kunnen werken en studeren in ons land. De overheid moet alles in het werk stellen om privacy en veiligheid bij internetgebruik te waarborgen en dient daartoe dan ook regels op te stellen en te handhaven. Het door bedrijven ongevraagd gebruikmaken van internetgegevens van mensen wordt verboden.

Internetproviders mogen zich niet inlaten met de inhoud van het verkeer van hun internetgebruikers, net zoals post- en telefoniebedrijven zich niet mogen inlaten met de inhoud van brieven of telefoongesprekken van hun klanten. Er mag door providers geen onderscheid gemaakt worden in de kostenberekening voor verschillende soorten data.

PROFILING, DEVICE FINGERPRINTING EN SPYWARE

Voor internetbedrijven is het economisch interessant om te weten welke websites een internetgebruiker zoal bezoekt. Op deze wijze kunnen deze belanghebbende partijen gericht advertenties plaatsen die passen bij de interesse van de internetgebruiker. Het verzamelen van informatie over het internetgedrag wordt gedragsprofilering genoemd.
Een bekende manier van gedragsprofilering is 'device fingerprinting'. Door onder meer de karakteristieken van de door de consument gebruikte apparatuur en applicaties te analyseren ontstaat er een interesseprofiel dat door internetbedrijven gebruikt kan worden om gericht te adverteren.

De SP pleit voor een verbod op ongevraagde gedragsprofilering. De internetgebruiker moet kunnen beslissen of een bedrijf wel of niet gegevens mag verzamelen voor commerciële doeleinden. Niemand mag ongevraagd gegevens van anderen verzamelen om deze te verkopen of er gedragsprofielen mee te creëren. Hetzelfde geldt

2 Hierbij dient wel te worden opgemerkt dat gedetineerden dit recht in bepaalde gevallen verliezen of beperkt zullen zien zoals ook het geval is met telefoneren in de gevangenis.

voor spyware: het zonder medeweten van de gebruiker installeren van software wordt verboden, net als het ongevraagd verzamelen en doorgeven van data over personen. Mensen hebben voorts zelf zeggenschap over hun gegevens.

COOKIEVERBOD EN SUPERCOOKIES

Het is van groot belang dat internetbedrijven expliciet toestemming vragen aan internetgebruikers om cookies te mogen plaatsen. De wet die voorkomt dat internetgebruikers automatisch via de standaardinstellingen van hun webbrowser toestemming geven om third part cookies te plaatsen draagt bij aan de bescherming van privacy van internetgebruikers.
De SP is voor het verbod op 'supercookies'. Deze vernieuwde versies van cookies zijn moeilijk te vinden en herstellen zich bovendien nadat ze door de gebruiker zijn verwijderd.

Door de snel veranderende techniek is het onmogelijk om per specifieke techniek beleid op te stellen. De SP pleit dan ook voor duidelijke algemene regels die gericht zijn op beveiliging van privacygevoelige gegevens in de digitale wereld. Met het aannemen van de motie Gesthuizen/Verhoeven[3] is de basis gelegd om te komen tot regels die algemeen gelden voor iedereen, ongeacht welke (nieuwe) techniek er wordt gebruikt om informatie over internetgebruikers te achterhalen of op te slaan.

GARANTIE SNELHEID INTERNET

Consumenten sluiten abonnementen af met internetproviders waarin onder andere de snelheid van het internet is opgenomen. Een internetprovider is verplicht de snelheid te leveren waarvoor de consument betaalt. Indien de snelheid lager is dan de snelheid die is vastgelegd in het contract beschikt de consument over de mogelijkheid om direct het contract te beëindigen. Hierbij is het van belang dat de consument kan zien wat de geleverde snelheid op een specifiek moment is.

2 INTERNETCRIMINALITEIT

De voortrazende ontwikkeling van ICT brengt vele voordelen met zich mee. Helaas vinden er ook allerlei criminele activiteiten plaats op of middels het internet. De aanpak hiervan loopt echter achter en dat is kwalijk voor een land waarin we in grote mate afhankelijk zijn van ICT.

INZET POLITIE EN JUSTITIE

Om te kunnen inspelen op de snelle technologische ontwikkelingen en het groeiend aantal criminele activiteiten moet de kennisachterstand bij politie en justitie worden weggewerkt. Er dienen voldoende mensen met technische kennis bij politie

3 Motie Gesthuizen/Verhoeven (24095-294) over privacybeleid.

en justitie te zijn om grote bendes, die burgers en bedrijven via het net oplichten, op te kunnen rollen. Daarvoor zijn investeringen nodig.

Tegelijkertijd hangt juist op dit terrein veel af van goede internationale samenwerking. Daarom moet Nederland zowel in Europees verband als daarbuiten partners zoeken in landen waarmee samengewerkt kan worden in deze strijd.

Meer prioriteit is nodig voor de opsporing, vervolging en aanpak van de verspreiding van afbeeldingen van kindermisbruik op het internet. Kinderpornografie is een term die de lading van dit misdrijf niet dekt. Het maken, verspreiden en bekijken van kinderverkrachtingen of andere vormen van misbruik is strafbaar, maar de problemen op dit terrein nemen eerder toe dan af. Het internet heeft het voor mensen die kwade intenties hebben met kinderen gemakkelijker gemaakt om contacten te leggen en beelden van misbruik te verspreiden of ontvangen.
In de eerste plaats is het zaak het kindermisbruik zelf én de criminele winsten die daardoor worden geboekt veel meer aandacht te geven, nationaal en internationaal. Daarnaast moet worden geïnvesteerd in voorlichting aan kinderen, ouders en potentiële daders. Daarbij kan het internet juist een belangrijke rol spelen.
Goede methodes bij politie die werken om misbruikers of verzamelaars op te sporen moeten in alle districten de norm worden.

INZET SLACHTOFFERHULP

Steeds vaker komt in het nieuws dat mensen slachtoffer worden van webcamafpersingen en ongewenste webcamseks. Hulpverleningsdiensten zoals de Kinderchat en Sensoor moeten in staat gesteld worden om hun hulpverlening op het net 24 uur per dag live te kunnen onderhouden. Ook in geval van internetverslaving moet hulpverlening snel en adequaat beschikbaar zijn.

Omdat problemen rond internetgebruik veel onder jongeren voorkomen moeten privacy en internetveiligheid vaste aandacht krijgen op school. Door kinderen op jonge leeftijd bewust te maken van de gevaren van onder meer spelletjes op de computer en het gebruik van sociale media kan veel leed worden voorkomen. Daarnaast worden scholen en ouders informatie en ondersteuning aangeboden bij opvoedingsvragen rond het gebruik van internet.

In het geval van verslaving is het belangrijk dat mensen, die iets willen doen aan hun verslaving, direct ergens terecht kunnen. Het moet daarbij niet uitmaken of het gaat om een drank-, drugs- of gameverslaving. Het verslaafd zijn aan games of spelletjes is nog een betrekkelijk nieuwe aandoening. De hulpverlening moet erop zijn ingericht om jongeren of volwassenen te kunnen helpen.

VOORLICHTING INTERNETCRIMINALITEIT

Voor internetcriminaliteit geldt dat voorkomen beter is dan genezen; voorlichting aan burgers en bedrijven over criminelen die op slinkse wijze proberen gegevens te bemachtigen of mensen op te lichten werpt haar vruchten af. We moeten blijven investeren in goede voorlichting. Een goed voorbeeld hiervan is het Steunpunt Acquisitiefraude dat burgers en bedrijven onder meer waarschuwt voor spooknota's of andere vormen van fraude die veelal via het internet plaatsheeft.[4]

MELDPLICHT DATALEKKEN

Er dient een meldplicht te komen voor alle situaties waarbij sprake is van verlies van persoonsgegevens uit datasystemen. De meldplicht moet gelden voor zowel Internet Service Providers als voor alle andere bedrijven en organisaties die persoonsgegevens beheren.
Elke partij die persoonsgegevens verwerkt en deze verliest, bijvoorbeeld door een hack, dient dit direct aan het College Bescherming Persoonsgegevens (CBP) te melden.
Door de meldplicht bij het CBP zal de hoeveelheid onderzoeken naar datalekken toenemen. Om deze onderzoeken te kunnen uitvoeren zal de overheid budget beschikbaar moeten stellen om voldoende mankracht bij het CBP in te kunnen zetten.

Ook is de SP een groot voorstander van een digitaal crashteam dat bij grote ICT-debacles direct in actie kan komen (zie hoofdstuk 'ICT bij de overheid').

3 AUTEURSRECHTEN EN DOWNLOADVERBOD

Auteursrechten zijn door de komst van internet onder druk komen te staan. De SP wil terug naar het oorspronkelijke idee van het auteursrecht dat de makers (bijvoorbeeld muzikanten en componisten) beloond worden voor hun creatieve uitingen. De commercialisering is doorgeslagen en zorgt ervoor dat het geld niet of nauwelijks bij de makers terecht komt. Wij willen het auteursrecht moderniseren zonder dat consumenten op onnodig hoge kosten worden gejaagd.

Veel auteursrechtelijk materiaal wordt gekopieerd. Om er toch voor te zorgen dat de makers van dit materiaal een vergoeding krijgen is de thuiskopieheffing in het leven geroepen. Deze heffing wordt geheven op blanco dragers (bijvoorbeeld lege CD's). De heffing wordt vervolgens naar rato verdeeld onder de makers van het product.

De komst van het internet heeft met zich meegebracht dat mensen auteursrechtelijk materiaal als muziek en film kunnen downloaden. De makers van het materiaal

4 www.fraudemeldpunt.nl/home

5 In internationale verdragen bestaat de keuze uit de volgende twee opties: downloaden verbieden of downloaden uitzonderen van het auteursrecht met in plaats daarvan een vergoeding voor de auteur (in de praktijk is dit laatste een vorm van thuiskopieheffing).

lopen hierdoor veel inkomsten mis, omdat de consument bijvoorbeeld niet eerst een blanco CD hoeft te kopen om iets te kopiëren. Hierdoor wordt er geen thuiskopieheffing afgedragen.
Om de creatieve makers toch een eerlijke vergoeding te geven, dient er een oplossing gevonden te worden voor het downloaden van auteursrechtelijk materiaal.[5]

Er zijn betere oplossingen dan een downloadverbod. Het handhaven van zo'n verbod is immers feitelijk niet te doen. De SP wil dat een voorlopige oplossing wordt gevonden in een uitbreiding van de huidige thuiskopieheffing. Door ook te heffen op apparatuur die muziek en films kan opnemen en afspelen (zoals harddiskrecorders, MP3- en MP4-spelers en mobiele telefoons met geïntegreerde MP3-speler) kunnen internetgebruikers legaal blijven downloaden en ontvangen makers een eerlijke vergoeding.

Er moet verdere uitwerking gegeven worden aan de plannen van onder andere de Consumentenbond[6] om apparatenvergoeding over te laten gaan in een bredere internetvergoeding zodra meer dan 70 procent van de thuiskopieën van internet afkomstig is.

Op de lange termijn zal de toekomst voor makers van muziek en film meer liggen in op een slimme manier gebruik maken van de mogelijkheden die internet en ICT in het algemeen bieden. Voor veel makers is het net nu al een prachtig platform dat hen juist geld oplevert.

4 ICT BIJ DE OVERHEID

Op zowel lokaal, regionaal als landelijk niveau wordt er bij de overheid veel gebruik gemaakt van ICT-toepassingen. Het is daarom belangrijk dat de overheid een IT-governance code heeft en zich daaraan houdt. Ondanks de recent verscherpte aandacht en verbeteringen doemen er nog steeds ICT-projecten op die problematisch zijn of uiteindelijk te duur uitpakken. Bovendien hebben zich recentelijk problemen voorgedaan op het gebied van veiligheid en privacy bij ICT-projecten. Hiermee is nogmaals de noodzaak aangetoond dit goed te organiseren. Het debacle rond onveilige certificaten van DigiNotar (het bedrijf achter DigiD) maakte duidelijk dat de overheid eigenlijk al te lang achter de feiten aanliep.

PARLEMENTAIR ONDERZOEK

Op voorstel van de SP onderzoekt de Tweede Kamer het komend jaar ICT-projecten bij de overheid. Hierbij zal een aantal grote projecten onder de loep worden geno-

6 Consumentenbond, FNV Kiem en Ntb Vakbond voor Musici en Acteurs hebben op 24 november 2010 hun plan gelanceerd voor een nieuw thuiskopiestelsel en legalisering van zowel up- en downloaden door consumenten.


Firefox

men en geanalyseerd. Er zijn nog vele lessen te leren over het kunnen garanderen van veiligheid en kostenbeheersbaarheid. Met de kennis uit het onderzoek kan de overheid in de toekomst beter aan de slag. Hieronder staat echter een aantal maatregelen dat volgens de SP zonder meer en direct moet worden genomen.

INVESTEREN IN ICT-KENNIS

ICT speelt een steeds grotere rol in de overheidsdienstverlening. De overheid moet dan ook alles op alles te zetten om de veiligheid en privacy van de gebruikers van deze diensten te garanderen. Daarvoor zal meer specialistische kennis bij de overheid opgebouwd moeten worden. Op dit moment kampt de overheid met een groot tekort aan ICT-specialisten.[7] Maar opvallend genoeg wordt ook steeds weer duidelijk dat juist de mensen die de beslissingen nemen bij de overheid – bijvoorbeeld de ministers en de topambtenaren – te weinig kennis van zaken hebben. Zelfs als er wel voldoende mensen voor de overheid werken die verstand hebben van ICT dan wordt daar te weinig naar geluisterd. Dat moet dus anders.

CRASHTEAM

Voor grote en acute dreigingen op het gebied van ICT veiligheid is het nodig om een team paraat te hebben dat razendsnel in actie kan komen. De SP is groot voorstander van een dergelijke 'digitale brandweer'. Dit team van ICT-experts moet dag en nacht in staat zijn om eventuele veiligheidsproblemen op het gebied van ICT (bijvoorbeeld ten gevolge van een hack) bij de overheid of bij vitale infrastructuren direct aan te pakken. Daarnaast moet het Nationaal Cyber Security Centre dat zich juist richt op de langetermijnvisie voor overheids-ICT zo snel mogelijk op sterkte zijn.

GEORGANISEERDE SAMENWERKING HACKERSGEMEENSCHAP

Veel kennis over internetbeveiliging is te vinden binnen de hackersgemeenschap. Om te kunnen hacken dien je immers kennis te hebben van de beveiliging van systemen. Hier ligt een grote kans voor de overheid. De veiligheid van ICT-systemen kan alleen optimaal getest worden door cyberaanvallen te plegen binnen de reële, werkende internetomgeving. De overheid zou dan ook samenwerking met de hackersgemeenschap moeten organiseren, waarbij hackers op een door de overheid gecontroleerde wijze ICT-diensten van de overheid aanvallen. Op die manier blijkt of deze diensten voldoende veilig zijn en worden zwaktes blootgelegd.

VEILIGHEID OVERHEIDSWEBSITES

De overheid hoort het goede voorbeeld te geven voor wat betreft de veiligheid van websites. Bij nieuwe projecten dient veiligheid en privacy van de gebruikers centraal te staan. De bestaande websites van de overheid dienen voor het eind van 2012

7 NRC, zaterdag 9 juni 2012: 'Wanted: soldaten tegen cybercrime – Tekort van honderden specialisten'.

getest te worden op veiligheid. Zo kunnen problemen, zoals die zich recentelijk voordeden, deels voorkomen worden.

ADVIES NATIONAAL CYBER SECURITY CENTRE

De richtlijnen voor beveiliging en privacy van websites die het Nationaal Cyber Security Centre (NCSC) uitbrengt, moeten bij het aanbesteden van overheidsopdrachten betrokken worden. Daardoor wordt de kennis van het NCSC beter benut en wordt er een goede basis voor veiligheid gelegd.

AANBESTEDEN ICT-PROJECTEN BIJ DE OVERHEID

Bij ingewikkelde ICT-projecten zijn aanbestedingen vaak een verkeerd middel om een goede partner te vinden. De overheid doet er goed aan in open overleg met het bedrijfsleven te werken aan goede ICT-oplossingen die technisch kloppen en binnen het budget blijven. Er moet meer aandacht zijn voor de dienstverlening en de garanties die de leverancier biedt. Anders is goedkoop achteraf duurkoop.

MAXIMAAL HALF JAAR OPSLAAN INTERNETVERKEER

Op grond van een Europese richtlijn is de Nederlandse staat verplicht het telefoon- en internetverkeer minimaal 6 en maximaal 24 maanden te bewaren. De SP vindt de minimale verplichting van 6 maanden ruim voldoende. De noodzaak van het langdurig bewaren van gegevens is niet aangetoond. Als binnen de 6 maanden blijkt dat iemand mogelijk heeft deelgenomen aan criminele activiteiten biedt de huidige wet- en regelgeving de mogelijkheid om de gegevens langer te bewaren. Als er geen aanleiding is gegevens te bewaren voor verder onderzoek, dan dienen deze na 6 maanden te worden vernietigd.

INVESTEREN IN ICT-ONDERWIJS

Om de mogelijkheden van innovatie voor de economie te versterken dient de ICT-kennis op peil te zijn. Kennis over en gebruik van ICT is van groot belang in het onderwijs. Hier kan een grote inhaalslag gemaakt worden.

OPEN SOURCE EN OPEN STANDAARDEN

Het business-model van grote commerciële bedrijven in de technologiesector is vaak gebaseerd op licenties, abonnementen en gebruiksrechten. Daarbovenop komen nog eens de kosten voor uitbreidingen aan software- of hardwareproducten en de kosten voor helpdesks en andere vormen van technische ondersteuning. Open Source software biedt aan eindgebruikers dezelfde functionaliteit als commerciële oplossingen, maar zonder de bijkomende kosten. Open Source-software is vrij te gebruiken en belangrijker nog: de programmeercode mag vrijelijk en gratis worden ingezien en uitgebreid, wat gebruikers in staat stelt om de veiligheid van het product te verifiëren. De overheid gaat waar mogelijk gebruik maken van Open Source.

Het gebruik van Open Standaarden dient altijd leidend te zijn. Dit bespaart geld en zorgt voor economische groei. De SP wil de ontwikkeling en het gebruik van

gratis en (platform)vrij te gebruiken, te delen en te exploiteren software-applicaties en bestandsformaten stimuleren, zowel aan de kant van consumenten als aan de zijde van bedrijfsleven en overheden. Ook moeten alle werken die op kosten van de gemeenschap vervaardigd zijn, zonder auteursrechtbeperking ter beschikking komen van de gemeenschap.

5 INTERNATIONAAL

Het 'wereldwijde web' – de term zegt genoeg. Het internet kent nauwelijks betekenis toe aan landgrenzen. Dit biedt naast veel voordelen ook nadelen. Internet is voor grote delen van het recht ongrijpbaar en het maken van nationale regelgeving blijft in sommige gevallen moeilijk. Onze regelgeving voor bijvoorbeeld privacybescherming kan ten opzichte van een ander land sterk verschillen. Door op internationaal niveau goede afspraken te maken kunnen problemen verholpen worden. De SP vindt dat het publieke belang hierbij leidend dient te zijn.

RISICO'S GEBRUIKERS INTERNET

Veel mensen zijn zich er nauwelijks van bewust dat wat ze hier in Nederland doen achter hun computer strafbaar kan zijn in andere landen. Dat brengt risico's met zich mee als mensen vervolgens – al dan niet met hun laptop, tablet of smartphone – gaan reizen. Er zijn landen met minder democratische regimes waar reizigers in de cel belanden als zij gegevens en afbeeldingen van bijvoorbeeld Google Maps Streetview op hun laptop hebben staan. Daarop stonden de locaties van overheidsgebouwen waarvan je in dat land geen afbeeldingen in je bezit mag hebben. De overheid heeft een taak in het zo goed mogelijk informeren van burgers zodat deze zo min mogelijk voor onaangename verrassingen komen te staan.

Ook bij het internationaal zakendoen krijgen Nederlandse bedrijven te maken met regels die anders zijn dan de regels die gelden in Nederland. De SP vindt het een overheidstaak om bedrijven te informeren en voor te lichten over buitenlandse regelgeving die invloed heeft op zakenactiviteiten van Nederlandse bedrijven. Denk hier bijvoorbeeld aan garantieregelingen.

ACTA

De SP verwerpt in het geheim gesloten verdragen zoals bijvoorbeeld het ACTA-verdrag. ACTA (Anti-Counterfeiting Trade Agreement) was bedoeld om intellectuele eigendomsrechten te beschermen. De SP wil dat er in zulke internationale verdragen veel meer oog is voor de publieke belangen van velen en niet, zoals nu, alleen voor de economische belangen van weinigen. Transparantie over de totstandkoming van de bepalingen en de deelnemers aan de besprekingen die tot de bepalingen hebben geleid is van het grootste belang.

Volgens de SP was er in het ACTA-verdrag geen goede balans tussen aan de ene kant de economische belangen die met intellectuele eigendomsrechten samenhangen

en aan de andere kant de publieke belangen als vrijheid van meningsuiting en internetvrijheid. Gelukkig verwierp het Europees Parlement ook om die reden dit verdrag.[8] Want met afspraken zoals in ACTA worden internetgebruikers volgens de SP veel te snel gecriminaliseerd voor bijvoorbeeld het plaatsen van filmpjes of geluidsfragmenten op het internet.

SPIONAGE EN CYBERWARFARE

Beveiligingsexperts waarschuwen steeds luider en vaker voor de risico's die Nederland neemt als het op spionage en cyberwarfare aankomt. In de politiek bestaat echter te weinig besef van de dreiging die internationaal bestaat op het gebied van virussen en schadelijke computerprogramma's. De SP vindt dat de regering deze dreiging serieus dient te nemen. Ook in Nederland zijn wel degelijk virussen en andere vijandige computerprogramma's aanwezig.

Gezien de risico's die cyberaanvallen met zich meebrengen (bijvoorbeeld het stilvallen van het Nederlandse telefoon- en internetverkeer) moet er bij het ministerie van Defensie snel werk worden gemaakt van de opbouw van een cyberleger. Nederland moet haast maken met het opbouwen van kennis en capaciteit om te kunnen optreden tegen spionage en cyberaanvallen.

INTERNATIONALE AFSPRAKEN

De SP hecht als het gaat over cyberwarfare grote waarde aan diplomatie. Er is dringend behoefte aan internationale verdragen waarin staat welk recht geldt op het moment van een aanval van het ene land op het andere. Dergelijke afspraken tussen landen zijn ook van belang als het gaat om het aanpakken van internationale cybercrime. Op dit moment heeft alleen het land waar een door criminelen gebruikte server staat het recht deze server stil te leggen. Het land dat slachtoffer is van een aanval heeft niet het recht om in te grijpen. Dat zorgt soms voor een onacceptabele vertraging.

Als een cyberaanval een dusdanig grote dreiging vormt dat de nationale veiligheid in gedrang komt, kan niet altijd gewacht worden op toestemming vanuit het buitenland. Het moet dan voor de overheid mogelijk zijn om eigenhandig in te grijpen; bijvoorbeeld door een tegenoffensief waarbij de vijandige server wordt platgelegd. Om zorgvuldige besluitvorming te waarborgen is parlementaire controle hierbij van groot belang. Daarnaast moeten zulke handelingen niet zonder een melding aan het desbetreffende land worden uitgevoerd. Daarmee worden de risico's op ongelukken of repercussie verkleind.

8 Artikel in Trouw, 4 juli 2012: 'Anti-piraterijverdrag ACTA massaal verworpen in Europarlement' www.trouw.nl/tr/nl/5133/Media-technologie/article/detail/3281602/2012/07/04/Anti-piraterijverdrag-ACTA-massaal-verworpen-in-europarlement.dhtml

15

SP

WWW.SP.NL