

Marc Kuipers (AIVD): “Intellectueel eigendom is heilig, vaak niet veilig”



■ AIVD, afdeling Communicatie



Dat heel kleine stukje aarde dat Nederland vormt, staat in schril contrast met de plaats die ons land inneemt op het internationale economische speelveld. Nederland is een handels- en doorvoerland over zee, door de lucht en via de digitale snelweg en een plek waar innovatie hoog in het vaandel staat. Keerzijde: ons land is daarmee erg aantrekkelijk voor anderen die een graantje willen meepikken.

Experts aan een Nederlandse universiteit die jaren ploeteren op een belangwekkende uitvinding. Het kan zomaar gebeuren dat in mum van tijd dezelfde ontdekking in een ander land van een lopende band rolt. Gepikt. “En daar gáán al je investeringen, een zeer voorstelbaar scenario,” zegt Marc Kuipers, plaatsvervangend hoofd van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). “Intellectueel eigendom is heilig, maar heel vaak niet veilig. Dat kost miljoenen.”



INTERNET ALS GAME CHANGER

De interesse van andere landen in de opstelling van de Nederlandse overheid ten opzichte van bepaalde (politieke) wereldissues, is er nog altijd. Buitenlandse inlichtingendiensten zoeken fysiek contact met personen, die hen daarbij, al dan niet bewust, kunnen helpen. Deze vorm van spionage is zo oud als de weg naar Rome, net als het doel: wat staat in de verborgen agenda van een land? Maar spionage heeft een ontwikkeling doorgemaakt. Kuipers: “De middelen zijn veranderd door digitale mogelijkheden, maar ook het doel is verbreed met kennis kapen.”

Nederland kent duizenden cyberaanvallen per jaar. Een groot deel is gericht op inbraken in ICT-systemen. “Internet is een *game changer* voor spionage en diefstal,” zegt Kuipers. “Als land steken wij honderden miljoenen euro’s in het ontwikkelen van onze kennis. We willen vooraan lopen als het om innovatie gaat, maar laten we zorgen dat die kennis ook beschermd blijft.” De verantwoordelijkheid ligt bij de partijen zelf, maar de AIVD ziet het als zijn taak om betrokken partijen bewust te maken van de risico’s, vooral omdat er niet zelden buitenlandse overheden achter zitten.

TER ZEE, DOOR DE LUCHT EN VIA DE KABEL

Rotterdam heeft veruit de grootste zeehaven van Europa, Schiphol vormt een *hub* in het internationaal vliegverkeer. De overheid ziet het economisch belang van de Rotterdamse haven en hecht veel waarde aan de beveiliging van Schiphol. Dat zijn de fysieke poorten naar de wereld. Kuipers: “Met de AMS-IX beschikt ons land over een van de grootste internetknooppunten van de wereld. Omdat de economie steeds meer op digitale diensten drijft, is beveiliging van de AMS-IX, als digitale poort, van minstens zo groot belang. In 1953 wisten we dat de dijken niet sterk genoeg zouden zijn bij extreem weer, maar pas na de watersnoodramp zijn de Deltawerken van de grond gekomen. Laten we nu niet wachten op een digitale dijkdoorbraak.”

De AIVD is samen met het Nationaal Cyber Security Center betrokken bij de detectie van verdacht netwerkverkeer, dat kan wijzen op aanvallen. Digitale aanvallers kunnen zich op meerdere doelen richten, bijvoorbeeld overheidsinstellingen. “Vaak met het klassieke doel: politieke inlichtingen,” zegt Kuipers. Daarnaast bestaat een risico dat (terroristische) hackers zich richten op het uitschakelen van vitale sectoren, zoals energievoorziening, waardoor de maatschappij ontwricht raakt. “Maar wij hebben grote zorgen over de topsectoren: hightech bedrijven, de energiesector en de chemische industrie. Aanvallen op onze kroonjuwelen raken direct het verdienvermogen van Nederland en zorgen voor economische terugval, met alle gevolgen van dien. Economische veiligheid raakt de nationale veiligheid.”

Economische veiligheid in Duitsland



■ AIVD, Afdeling Communicatie

Het feit dat de economie in Duitsland relatief goed draait, heeft ook nadelen. Vanuit de gezichtshoek van inlichtingendiensten buiten Duitsland is er veel waardevols te halen. In andere woorden: er is veel te beschermen. Zou de schade van economische spionage niet zo ernstig zijn, zo verklaart het Hoofd van de Duitse veiligheidsdienst op een persconferentie in Berlijn op 12 november, dan zou je in de economische interesse van inlichtingendiensten de erkenning kunnen zien dat Duitsland op innovatief en creatief gebied veel te bieden heeft.

De Duitse veiligheidsdienst is slechts één van de spelers in een samenwerkingsverband van ministeries, werkgeversverbanden, veiligheidsdiensten, kamers van koophandel en veiligheidskoepels die in Berlijn hun samenwerking bevestigen. De Staatssecretaris van het *Bundesministerium des Innern*, Emily Haber, verklaart dat bescherming van de wetenschap een aanpak vereist waarbij publieke en private partijen samenwerken én waarbij internationaal wordt samengewerkt. Ervaringen, best practices en beschermingsstrategieën moeten worden uitgewisseld, want de belangen van de economie eindigen niet bij de landsgrenzen. Hoge publieke gezagsdragers uit Oostenrijk, Zwitserland en Liechtenstein sluiten zich bij deze boodschap aan.

De ruggengraat van de welvaart in Duitsland wordt gedragen door kleine en middelgrote bedrijven. Bedrijfjes dus vaak, die vooral bezig zijn met innovatie en geen tijd, geld of aandacht hebben om een bewustzijn te ontwikkelen van hun aantrekkelijkheid voor inlichtingendiensten. Laat staan zich tegen deze diensten te beschermen. De helft van de bedrijven is direct of indirect al betrokken geraakt in deze asymmetrische strijd. Een kwart heeft er rechtstreeks schade door geleden. Maar slechts één vijfde van alle incidenten bereikt een overheidsdienst. Het gaat bij deze incidenten allang niet meer om uitsluitend "harde" know how: ook prijscalculaties, profielen van medewerkers en strategische marktplanning zijn doelwit. Schade vertaalt zich als oneerlijke achterstand ten opzicht van concurrentie, politieke en economische schade en verlies van arbeidsplaatsen. Een relatief nieuwe vorm van spionage is onzichtbare sabotage van technische specificaties, waarbij producten op termijn defect raken, met alle (imago)schade van dien. De Staatssecretaris wijst er op, dat in de nauw aansluitende en verweven productieketens aanvallen op kleine bedrijfjes uitstralings-effecten op de gehele keten kunnen hebben. Ze gebruikt hiervoor het woord "metastaseren", waarmee direct duidelijk wordt hoe de Duitse overheid over spionage denkt.

Centraal uitgangspunt van de Duitse strategie is: preventie door informatie. Daarbij heeft de Duitse overheid niet de bedoeling om in elk bedrijf een economische politieagent te plaatsen. De staat moet, in een vroeg stadium, actief faciliteren bij de totstandkoming



van initiatieven waarbij informatie-uitwisseling, sensibilisering en gekwalificeerde opleidingen worden gerealiseerd. In bedrijven moet een vertrouwenscultuur ontstaan, waardoor veel meer incidenten gemeld worden. Informatie-uitwisseling moet normaal worden en schroom van bedrijven moet overwonnen worden. Van alle partners wordt een actieve bijdragen gevraagd en de overheidsrol wordt omschreven met de woorden: "hulp tot zelfhulp". Het gaat daarbij niet alleen om de digitale wereld maar ook om de ouderwetse – maar actuele – menselijke spion.

Een deel van de initiatieven is al in gang gezet. De veiligheidsdienst verricht onderzoek, duidt dreigingen en biedt lezingen en folders aan om het bewustzijn te vergroten. Een verbond van werkgevers en veiligheidsbedrijven werkt aan een toolbox voor preventieve beveiliging van economische informatie. Overheidsdiensten werken aan accreditatie van ICT-bedrijven die mogen worden ingezet bij het adviseren over gevoelige economische infrastructuur. Ook in andere Duitstalige landen lopen grensoverschrijdende initiatieven. De Duitse, Oostenrijkse, Zwitserse en Liechtensteinse veiligheidsdiensten werken op dit thema al samen.

Succes kan alleen verkregen worden als niet alleen de uitvoerende partners maar ook het politieke hoogste niveau doordrongen is van het nationale belang van een gesloten beschermingscirkel. In het *Koalitionsverdrag* van de regering is vastgelegd dat ondernemingen in Duitsland beschermd worden tegen statelijk georganiseerde spionage en criminaliteit. Een convenant tussen werkgevers, Binnenlandse Zaken en de Kamers van Koophandel werkt de samenwerking verder uit. Aan het einde van 2015 is de nationale strategie voor bescherming van de Duitse industrie gereed: *Nationale Strategie zum Wirtschaftsschutz 2015*.

Meer informatie: www.verfassungsschutz.de