De informatierevolutie

De informatierevolutie

Het Digitale Paard van Troje ?

"Een inventarisatie van trends, bedreigingen en risicoperceptie voor bedrijfseconomische informatie"

Doctoraalscriptie Communicatiewetenschap
Universiteit van Amsterdam
Faculteit der PSCW

Naam:	**Marcel van Oers**
Studentnummer:	**9654577**
Registratienummer:	**2680**
Adres:	**Bonnikestraat 72**
	1222 EM Hilversum
Telefoonnummer:	**0616 496 032**
Scriptiebegeleider:	**Prof. dr. C.J. Hamelink**
Scriptiecoördinatrice:	**Dr. I.C. Meijer**
Datum:	**Juni 2001**

Inhoudsopgave

Voorwoord

De laatste maanden bereiken ons steeds meer berichten over veiligheids-issues rondom de digitalisering van de economie. Zo was er afgelopen najaar een artikel in een dagblad te lezen over zelfvernietigende e-mail. Het handelde over een nieuw softwareproduct ter voorkoming van het 'meelezen' van e-mail van instanties als de FBI. Maar ook artikelen over lekken in websites en netwerken waren te vinden, evenals berichten dat er kapers op de kust waren als het gaat om modern berichtenverkeer. Sommige artikelen refereerden aan hackers als de kapers, echter was de verbazing bij mij groot dat er minstens zovaak gewezen werd naar overheidsinstanties. Dezen zouden inlichtingen- en veiligheidsdiensten inzetten om economische belangen van het land te dienen. Dit kwam zeer vreemd op mij over, aangezien dit haaks staat op de westerse ideeën over democratie en vrijheid. Daarom besloot ik enige maanden intensief de reguliere media te monitoren over deze issues. Daarbij ben ik me verder gaan verdiepen in mijn interessegebied 'Internationale Communicatie'. Hierdoor kreeg ik een scherper beeld van bedreigingen voor economische informatie in de, in toenemende mate, digitale ruimte. Eén van de meest opvallende internationale bedreigingen van vrije communicatie en informatie die ik tegen ben gekomen, is het Amerikaanse spionagenetwerk Echelon.

Al met al heeft alle informatie en daarmee samenhangende research naar deze fenomenen mij een dieper inzicht gegeven in de situatie. Voor mij was dit nieuwe bewustzijn alarmerend. Tevens riep dit bij mij de vraag op hoe het bewustzijn hierover is bij het bedrijfsleven dat slachtoffer kan worden van zaken zoals bedrijfseconomische spionage. De interesse om hier dieper in te duiken, tezamen met de nieuwsgierigheid naar de perceptie van belanghebbende partijen ten opzichte van dit fenomeen hebben bij mij de basis gelegd voor het schrijven van een scriptie over informatiebedreiging.

In deze scriptie wordt licht geworpen op het belang van informatie voor economische processen in de globaliserende (westerse) wereld. Vervolgens wordt de bedreiging van informatie geïnventariseerd en geïllustreerd aan de hand van een case-study over het spionagenetwerk Echelon. Met behulp van de dan reeds verzamelde informatie is een duidelijk beeld te creëren over de mate van bedreiging en het belang van economische informatie. Hiermee stel ik interviews op die vervolgens gehouden worden met betrokken

personen van internationaal georiënteerde organisaties. Het doel hiervan is inzicht te krijgen in de mate van overeenstemming van de risicoperceptie met het ware risico.

Tevens wil ik van dit voorwoord gebruik maken om de mensen te bedanken die mijn studietijd tot een succes hebben gemaakt. Bijzondere dank aan mijn ouders voor hun steun in alle opzichten, en aan mijn scriptiebegeleider voor het mogelijk maken van dit onorthodoxe scriptieonderwerp. Ook gaat een dankwoord uit naar alle familie, vrienden en docenten die mij zowel bewust als onbewust enorm gesteund hebben. Zij zijn er teveel om op te noemen, daarom echter niet minder dank. Leads PR b.v., waar ik stage heb gelopen, en Mark Bergsteijn wil ik in het bijzonder noemen. Dank aan allen!

Marcel van Oers
Hilversum, Juni 2001

H1, INLEIDING

1.1 Omschrijving probleemgebied

"Treinstaking legt het land plat!" kopt de krant van vrijdag 6 april 2001[1]. Een groot conflict tussen vakbonden en de directie van de Nederlandse Spoorwegen toont de afhankelijkheid van de samenleving van de fysieke infrastructuur. Maar buiten het blikveld ontstaat ondertussen een andere infrastructuur waar we net zozeer van afhankelijk beginnen te worden: de communicatie- en informatie-infrastructuur. Zoals disfunctioneren van de fysieke infrastructuur een land kan bedreigen, zo levert disfunctioneren van informatiestromen tegenwoordig evenzeer een bedreigende situatie op. Enkele incidenten geven een eerste teken aan de wand, zoals een circulerend 'I love you'-computervirus wat een grote schade heeft aangericht[2]. Het is tijd om de ogen te openen voor het toenemende belang van informatie in de samenleving.

Het toenemende belang van informatie is ook de wetenschap niet ontgaan. Zo beschrijft Naisbitt (1982) de huidige westerse economieën als informatie-economieën. Kenmerkend voor deze economische vorm is het cruciale belang van communicatie en informatie. De opkomst van informatie-technologie hangt hiermee samen (Naisbitt, 1982). Deze ontwikkelingen hebben verstrekkende gevolgen voor de samenleving in het geheel. Er zijn vele geluiden te horen dat de nieuwe samenleving utopiaanse visies levensvatbaarheid zal inblazen. Toch zijn daar vele vraagtekens bij te zetten. De samenleving kan ongekend baat hebben bij de opkomst van de informatie-samenleving met haar bijbehorende informatie-technologie, echter dienen we de keerzijdes van de medailles niet uit het oog te verliezen. Welke tol gaan we betalen of zou betaald kunnen gaan worden? Immers, effecten van informatie-technologie kunnen een duaal karakter hebben. Het kan leiden tot meer vrijheid en gelijkheid. Maar evenzeer tot een hogere mate van controle en toezicht (Walton, 1989).

Een quote van DigitaLiberty[3] spreekt uitsluitend over de positieve effecten van de nieuwe samenleving. Hun uitgangspunt is gebaseerd op het idee dat de maatschappelijke problemen van technische aard zijn en dat die vervolgens met dezelfde techniek opgelost worden. In dit voorbeeld wordt geschreven over privacy die vrijheid zal kennen in persoonlijke en economische relaties door middel van encryptie. Los van de vraag of encryptie afdoende is, is

een eerste elementaire vraag: zijn de bedreigde partijen voldoende op de hoogte om zich vervolgens genoeg te wapenen? Deze scriptie doet daar onderzoek naar op het gebied van bedrijfseconomische informatie.

1.2 Probleemstelling

De centrale vraagstelling in deze scriptie luidt:

"In hoeverre is er bedreiging voor bedrijfseconomische informatie, en zijn Nederlandse transnationale organisaties zich bewust van dit risico?"

De rode draad is of de perceptie van informatiebedreiging in de pas loopt met de werkelijke risico's. Dit roept de volgende deelvragen op:

- *"Wat is het belang van bedrijfseconomische informatie voor transnationale organisaties?"*
- *"Wat is de trend in bedrijfseconomische informatie voor transnationale organisaties?"*
- *"In hoeverre wordt bedrijfseconomische informatie van transnationale organisaties bedreigd?"*
- *"Wat is de perceptie ten opzichte van de veiligheid van bedrijfseconomische informatie van Nederlandse transnationale organisaties?"*
- *"Zijn de maatregelen voor beveiliging van informatie in Nederlandse transnationale organisaties afdoende gezien de informatiebedreiging?"*

Het antwoord op de eerste deelvraag levert inzicht in de mate van dreiging voor de economie en individuele bedrijven die voort kan komen uit tekortkomende informatiebeveiliging. De deelvraag wordt beantwoord aan de hand van een analyse van het belang van bedrijfseconomische informatie voor transnationale organisaties. Bij deze analyse breng ik ook de trend in de bedrijfseconomische informatie in kaart. Hiermee beantwoord ik de tweede deelvraag. Tevens kan ik aan de hand van dezelfde analyse de bedreigingen voor bedrijfseconomische informatie aangeven. Vervolgens benader ik deze bedreiging praktijk-gericht met een case-study. Daarmee wordt dan de derde deelvraag beantwoord. De antwoorden op de overige twee deelvragen blijken uit interviews die ik zal houden bij Nederlandse transnationale organisaties.

De beantwoording van de vijf deelvragen tezamen levert een schat aan informatie op voor de beantwoording van de centrale vraagstelling. Door samenvoeging en interpretatie van deze informatie kan ik een eerste beschrijving van de stand van zaken maken op het gebied van de bedreiging van informatie en de informatiebeveiliging. Hiermee kan de centrale vraagstelling beantwoord worden. Ook komen hier aanreikingen voor verdergaand onderzoek uit voort, alsmede richtlijnen voor omgang met de hedendaagse stand van zaken. Overigens is deze scriptie een exploratie van dit onderzoeksgebied waarbij dient opgemerkt te worden dat er meer en uitgebreider onderzoek nodig zal zijn om een beter beeld van de probleemstelling te krijgen. Helaas echter is een scriptie te beperkt om reeds dieper op het onderwerp in te gaan.

1.3 Operationalisatie

Zoals blijkt uit de centrale vraagstelling richt deze scriptie zich mede op de risicoperceptie van informatiebedreiging. Hierbij gaat het om risicoperceptie bij Nederlandse internationale organisaties. Bij internationale bedrijfseconomische processen zijn namelijk veel bedreigingen voor informatie mogelijk en er spelen zeer hoge economische belangen. Dergelijke organisaties zijn daarom een goede case om inzicht in de centrale vraagstelling te krijgen. Vandaar dat gekozen is voor dit internationale aspect.

Bedrijfseconomische informatie is gedefinieerd als: “Informatie ten behoeve van de bedrijfsvoering, die van belang is voor het functioneren van de betreffende organisatie”. Indien er over vertrouwelijkheid van communicatie gesproken wordt, wordt er in deze scriptie op gedoeld dat: “De zender de communicatie absoluut niet in andere handen wil laten komen dan de door hem benoemde ontvangers”. Bedrijfsspionage is hier gedefinieerd als: “Intentionele interceptie van bedrijfseconomische communicatie en informatie ten behoeve van economische doeleinden”. Nederlandse transnationale organisaties zijn gedefinieerd als: “Nederlandse organisaties die structurele uitwisseling van informatie hebben met vestigingen buiten Nederland”. Encryptie is: “Het coderen van gegevens die in de computer worden opgeslagen of elektronisch worden verzonden. Het doel van encryptie is het onleesbaar maken van gegevens voor niet-intentionele ontvangers”.

De risicoperceptie van bedreiging van bedrijfseconomische informatie wordt gemeten met behulp van interviews. Voor deze interviews worden Nederlandse transnationale organisaties geselecteerd die de meest intensieve bedrijfseconomische informatie hebben met grote

belangen voor de betreffende organisaties. Voor dergelijke organisaties is de probleemstelling van deze scriptie zeer relevant, waardoor de meting van de risicoperceptie representatief resultaat opleveren kan. De interviews werpen een licht op de deelvragen en met name op de percepties.

Voor de interviews met dergelijke organisaties worden dertien organisaties geselecteerd. De exacte wijze van selectie wordt uitgebreid beschreven in hoofdstuk vier. De keuze om slechts dertien organisaties te interviewen komt voort uit het feit dat deze scriptie explorerend is en hierdoor geen ruimte biedt voor een intensieve diepgang in dit deel van de scriptie en omdat de risicoperceptie geanalyseerd wordt bij Nederlandse transnationale organisaties met intensieve, structurele informatiestromen waarbij veiligheid van de informatie een cruciale rol speelt bij het functioneren van de organisatie. Er zijn simpelweg niet al teveel van dergelijke organisaties in Nederland.

De inventarisatie van de belangen en trends in bedrijfseconomische informatie voor transnationale organisaties is in een algemeen kader geschreven en niet specifiek toegepast op de dertien organisaties die geïnterviewd zullen worden. Op deze manier heeft deze inventarisatie een grotere wetenschappelijke waarde, daar deze dan ook buiten de context van deze scriptie bruikbaar is. Ditzelfde geldt ook voor de beschrijving van de bedreiging van bedrijfseconomische informatie. Ter illustratie van deze bedreiging voeg ik in hoofdstuk drie een case-study toe naar het spionagenetwerk Echelon. Dit netwerk wordt beheerd door de Amerikaanse National Security Agency (NSA) en lijkt gebruikt te worden voor economische doeleinden. Echelon is als case-study gekozen omdat het de theoretische bedreiging van informatie, en van vertrouwelijke communicatie in het bijzonder, goed in de praktijk illustreert.

1.4 Maatschappelijke relevantie

Informatiebeveiliging heeft de laatste jaren in veel bedrijven en organisaties enorm aan belang gewonnen. Sinds kort is er zelfs een ISO-normering in gebruik genomen voor informatiebeveiliging (daarover meer in § 5.4). Kortom, informatiebeveiliging heeft absoluut een plaats op de kaart gekregen. Maar informatiebeveiliging komt niet uit de lucht vallen. Er is natuurlijk ook een bedreiging voor informatie. En het ziet er naar uit dat deze bedreiging de komende jaren alleen maar groter zal worden. Er dient dus met de juiste middelen

geanticipeerd te worden. Daarvoor dient er echter wel duidelijkheid te zijn over de stand van zaken omtrent de dreiging voor informatie. Deze scriptie wil meer duidelijkheid geven over deze dreiging en de ontwikkelingen daarin.

De scriptie gaat ook dieper in op intentionele bedreiging van informatie met verkeerde bedoelingen. Intentionele informatiebedreiging kan namelijk een liberale marktwerking verstoren. Dit is in strijd met de uitgangspunten van de betrokken Europese regelgeving. Deze uitgangspunten zijn juist gericht op de bevordering van marktwerking in de informatie-maatschappij. Zo zegt het actieplan van de Europese Commissie *Europe's Way to the Information Society* (17 juli 1994) op pagina 10: "The creation of the information society will be entrusted to the private sector…". De Europese Commissie stelt zich voor dat met behulp van verdere liberalisering een klimaat voor concurrentie kan worden geschapen waarbinnen de marktkrachten hun werk doen. De Nota van minister Sorgdrager van Justitie (1998) over de elektronische snelweg heeft soortgelijke uitgangspunten van marktwerking. Maar hoe kunnen de marktkrachten hun werk doen indien er sprake is van onder andere stelselmatige spionage door concurrenten, zeker indien deze geholpen worden door hun overheden? De Amerikaanse overheid lijkt met behulp van haar NSA het buitenland stelselmatig te bespioneren op communicatie gebied. Hiervoor wordt het Echelon-netwerk gebruikt. Echter zijn er vermoedens dat dit netwerk niet alleen gebruikt wordt voor de nationale veiligheid, maar ook voor economische doeleinden. In hoofdstuk drie vindt u daar een case-study over.

Een inventarisatie van de dreiging en het bewustzijn op het gebied van bedrijfseconomische informatie is niet alleen van belang voor de visie op marktwerking. Want afgezien daarvan is vertrouwelijkheid van informatie en communicatie, wat ook een belangrijk onderdeel van informatiebeveiliging is, een elementair recht van de mens en dus ook van organisaties. De Universele Verklaring van de Rechten van de Mens is hier zeer duidelijk over. In artikel 12 staat hierover: 'Niemand zal onderworpen worden aan inmenging in zijn persoonlijke aangelegenheden, in zijn gezin, zijn tehuis of zijn briefwisseling, noch aan enige aantasting van zijn eer of goede naam. Tegen een dergelijke inmenging of aantasting heeft een ieder recht op bescherming door de wet'. De strekking van dit artikel is in de Amerikaanse grondwet in het vierde amendement te vinden: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized'. Vrijwel alle zichzelf democratisch noemende naties hebben

soortgelijke zaken opgenomen in de wetgeving. Onrechtmatige inbreuk op communicatie en informatie is een directe inbreuk op dit basisrecht en dient aan het licht gebracht te worden. Spaans (1998) waarschuwt in deze zin ook al. Hij acht het niet onwaarschijnlijk dat het democratische gehalte van onze rechtstaat in de toekomst wel eens op het belangrijke punt van goede omgang met informatie getoetst zou kunnen worden.

Oude morele kwesties krijgen in een digitale omgeving een nieuwe dimensie. De specifieke karakteristieken van informatie- en communicatietechnologie, zoals anonimiteit, snelheid, het grote bereik en het gemak van de digitale manipulatie geven een extra urgentie aan op zich conventionele vraagstukken (Hamelink, 1999). Zo ook geldt dit voor informatiebedreiging. Op zich zijn bedreigende zaken zoals bedrijfsspionage niets nieuws. De vraag kan zelfs gesteld worden wat ouder is: het oudste beroep ter wereld of spionage. Echter voegt de digitaliserende omgeving een nieuwe dimensie toe aan dit probleem. Nieuwe technieken brengen grootse mogelijkheden voor vriend en vijand en dat maakt deze tijden tumultueus. Deze scriptie poogt in een dergelijk kader het meer omvattende probleemgebied 'informatiebedreiging' in kaart te brengen. Bovendien wordt niet alleen de bedreiging van informatie geïnventariseerd, maar ook de perceptie van deze bedreiging. Aan de hand van deze gegevens valt af te leiden in hoeverre deze elkaar ontlopen. Dit kan als leidraad dienen voor nieuwe maatregelen ter bescherming van de informatie en daarmee de economie.

1.5 Indeling van de scriptie

Om zinnige uitspraken over risicoperceptie van de bedreiging van informatie voor Nederlandse transnationale organisaties te doen, inventariseer ik allereerst de mate van werkelijke bedreiging. Om daartoe te komen analyseer ik in *hoofdstuk twee* het belang van informatie voor dergelijke organisaties. Vervolgens geef ik in hetzelfde hoofdstuk de trendmatige ontwikkelingen aan in deze informatie. Hieraan voeg ik toe in hoeverre de bedrijfseconomische informatie bedreigd kan worden en wat de recente en de te verwachten ontwikkelingen hieraan veranderen.

Zodra dit theoretische gedeelte is uitgewerkt stapt *hoofdstuk drie* deels in de praktijk. Dit bestaat namelijk uit een beschrijving van de bedreigingen voor bedrijfseconomische informatie in een praktijkgericht kader. Om dit compleet te maken illustreer ik het met een case-study over het hoogst geheime Anglo-Amerikaanse spionagenetwerk Echelon, dat, zoals

reeds hierboven vermeld, wereldwijd stelselmatig onze communicatie bespioneert, waarbij de verkregen informatie vermoedelijk niet alleen wordt gebruikt voor nationale veiligheid, maar ook voor economische doeleinden. De feiten hierover worden in dit hoofdstuk op een rij gezet.

Het *vierde hoofdstuk* is een volledige overstap naar de praktijk. In dit hoofdstuk beschrijf ik de opzet van interviews met Nederlandse transnationale organisaties over de dreiging voor informatie. Deze interviews dienen een beeld te geven van het bewustzijn van de bedreiging van informatie bij dergelijke organisaties. Tevens zal hieruit blijken in hoeverre hun omgang met informatie is aangepast aan de bedreiging. De resultaten van de interviews worden ook in dit hoofdstuk weergegeven.

In het laatste hoofdstuk, *hoofdstuk vijf*, interpreteer ik de resultaten van de interviews aan de hand van de conclusies van de hoofdstukken twee en drie.

---

[1] Begin april 2001 dreigde een treinstaking. Op 5 april 2001 vond deze daadwerkelijk plaats. Veel kranten openden met een dergelijke kop.

[2] Internet-onderzoeksbureau Pro Active heeft becijferd dat in Nederland ongeveer 220.000 computers met 'I love you' geïnfecteerd zijn geraakt. Wereldwijd is de schade op 10 miljard dollar geschat.

[3] *DigitaLiberty, 6 december 1994*: "The economies of the developed world are now making a major transition from an industrial base to an information base. As they do, the science of cryptology will finally and forever guarentee the unbreachable right of privacy, protecting individuals, groups, and corporations from the prying eyes and gasping hands of sovereigns. We will all be free to conduct our lives, and most importantly our economic relations, as we each see fit."
DigitaLiberty is een organisatie van voorvechters voor volledige vrijheid in digitale ruimtes, zie ook: http://www.digitalib.org.

H2, BEDRIJFSECONOMISCHE INFORMATIE

"Belang, trends en bedreigingen"

2.1 Introductie

Zoals vermeld in de inleiding analyseert dit hoofdstuk de rol van bedrijfseconomische informatie voor transnationale organisaties. Aangezien in deze scriptie onderzoek wordt gedaan naar de bedrijfseconomische informatie, benader ik de rol van informatie vanuit een economisch perspectief. Ouwersloot (1994) heeft uitvoerig geschreven over informatie- en communicatiedefinities vanuit een economisch perspectief. Daarbij ziet hij informatie niet als een statische hoedanigheid. Hij benadert informatie als proces of activiteit, als overdracht van kennis. In deze zin is informatie onlosmakelijk verbonden met het begrip communicatie. Dit is een goede aanzet voor de analyse van dit hoofdstuk, aangezien informatie dus zowel procesmatig als inhoudelijk gezien kan worden. Dit pas ik toe door de analyse op twee niveaus uit te voeren: 1) de fysieke communicatie infrastructuur voor transnationale organisaties en 2) de inhoudelijke informatie die in deze infrastructuur zit en daarover beweegt. Dit tweede niveau kijkt dus naar het inhoudelijke belang van de informatie. Op alle twee de niveaus analyseer ik het belang, de ontwikkeling en de daaruit voortkomende bedreiging voor bedrijfseconomische informatie. Tot slot geef ik een deelconclusie waarin ik een terugkoppeling maak naar de deelvragen.

2.2 De communicatie infrastructuur

Het belang van de infrastructuur

Alleyne (1995) beschrijft communicatie als essentieel voor de creatie van 'communities', op zowel binnenlands als op internationaal niveau. Daarbij is communicatie in zijn beschrijving noodzakelijk voor de verwerking van informatie. Voor transnationale organisaties hebben deze twee processen de laatste decennia veel meer belang gekregen. Door het fuseren en samenwerken van bedrijven is informatie-uitwisseling belangrijker geworden terwijl tegelijkertijd, door de expansiedrift, de fysieke afstanden groter worden. Ook staten gaan mee

in deze trend. Markten worden in toenemende mate internationaal geopend en in Europa is zelfs sprake van een soort mega-fusie tussen een groot aantal westerse staten onder de noemer van de Europese Unie.

Dus terwijl fysieke afstanden groter worden is het belang van Alleyne's 'community'-vorming alleen maar groter geworden. Informatie moet verder gebracht worden, in een hoger tempo met groter belang. Dit belang heeft logistiek gezien onze hele samenleving veranderd. Naisbitt sprak in die zin dan ook al in 1982 van de ontwikkeling in de richting van de informatie-economie. Deze ontwikkeling is alleen maar versneld doorgegaan en vele mensen zijn het er dan ook over eens dat we tegenwoordig in een informatie-maatschappij leven. Deze informatie-maatschappij legt een enorme nadruk op de ontwikkeling van informatie-technologie (Ouwersloot, 1994). Dankzij deze informatie-technologie worden we enorm geholpen in de wensen ten opzichte van communicatie. Zo is communicatie steeds efficiënter mogelijk. Toch heeft de informatie-technologie er niet alleen voor gezorgd dat communicatie efficiënter kan zijn, maar het heeft ook tot een overall toename in communicatie gezorgd (Attewell, 1996).

Communicatie faciliteren is niet meer uitsluitend een overheidstaak, het is uitgegroeid tot een transnationale economische sector op zich met een groot aandeel in de algehele economie. De bedrijven uit deze sector investeren astronomische bedragen in nieuwe communicatie-infrastructuren[1], terwijl anderen soft- and hardware ontwikkelen ter verbetering van de verzending, ontvangst, verwerking en opslag van de informatie die over deze infrastructuren beweegt. Tevens is de Nasdaq-index na de Dow Jones-index de meest genoemde beursindex van de Verenigde Staten geworden. In de Nasdaq-index zijn onevenredig veel ICT-bedrijven vertegenwoordigd.

De ontwikkeling van de infrastructuur

Fulk & DeSanctis (1995) merkten op dat organisatievormen aan verandering onderhevig zijn door ontwikkelingen van nieuwe elektronische communicatie-technologie. In hun beschrijving zijn de volgende vijf ontwikkelingen in communicatie van essentieel belang: hogere snelheid, verlaging van de kosten, grotere bandbreedte, toenemende verbondenheid en een integratie van communicatie met computertechnologie. Deze trends zijn de laatste jaren zeer belangrijk gebleken en blijven in toenemende mate belangrijker worden.

Zo is een toenemende snelheid van communicatie nog immer van belang voor organisaties. Dit leidt tot diverse voordelen zoals onder andere reductie van de tijd tussen fabricage en

aflevering[2]. Door deze tijdsreductie kunnen organisaties flexibeler produceren dan met gestandaardiseerde systemen. Dit geeft de gebruiker/afnemer meer maatwerk door de continue aanpassing aan zijn wensen. In de hedendaagse economie is de druk op organisaties om hieraan te voldoen hoog (Castells, 1996). Verlaging van de kosten is van groot belang geworden voor het ontsluiten van de openende en geopende wereldmarkten. De grotere bandbreedte is zo essentieel geworden in de hedendaagse samenleving dat er miljardenbedrijven zijn ontstaan met als hoofddoel consument en bedrijven hogere bandbreedte te leveren[3]. Toenemende verbondenheid is overal zichtbaar geworden. Met het internet zijn we één grote aaneenschakeling geworden. De drang tot voortzetting van deze trend is zo groot dat de Japanse regering een IT-hoofdkwartier inricht met als doelstelling elke Japanner breedbandtoegang tot het wereldwijde netwerk te geven[4]. De integratie van communicatie en computertechnologie leidt tot een convergentie van communicatie in het dagelijkse leven. Hierdoor zijn communicatie-toepassingen nauwelijks meer zichtbaar, maar des te meer in gebruik. Easypay van Shell is een voorbeeld van een dergelijk concept. Hierbij betaalt de tankende automobilist automatisch met een speciaal horloge. Ook rekeningrijden kan van dergelijke toepassingen gebruik maken. De kans is groot dat dergelijke 'verborgen' communicatie de komende jaren enorm toe zal nemen, met name door de technologische infrastructurele ontwikkelingen zoals GPRS[5], alsmede de gemakszucht van de consument.

De bedreigingen door de inrichting van de infrastructuur

Nu kijken we aan de hand van de vijf eerder genoemde trendmatige ontwikkelingen in communicatie in hoeverre de bedreigingen in het communicatielandschap hierdoor veranderen en veranderd zijn. Allereerst kan algemeen opgemerkt worden dat hogere eisen aan communicatie gepaard gaan met het gebruik maken van faciliterende voorzieningen en bedrijven. Veelgebruikte faciliterende voorzieningen om aan de hogere eisen te kunnen voldoen zijn digitale formats. Maar digitale formats kunnen interceptie in de hand werken. Veel digitale informatie is namelijk letterlijk uit de lucht te plukken doordat deze door de lucht verstuurd wordt[6]. Tevens zijn vaak, onder andere voor de faciliterende voorzieningen, faciliterende bedrijven nodig. Dit zijn meestal telecommunicatie bedrijven. Dit brengt altijd het probleem met zich mee dat de communicatie over andermans netwerken gaat lopen, en vaak ook door meerdere landen met de daarbij behorende verschillende wetten. De kans op ongewenste interceptie neemt hiermee toe. Allereerst omdat vrijwel alle telecombedrijven aftapbaar dienen te zijn[7] en ten tweede omdat zij logbestanden kunnen bijhouden en dus

gegevens ongewenst bewaren[8]. Simpel gezegd is de immer complexer wordende communicatie gevoeliger voor misbruik dan oorspronkelijke face-to-face communicatie.

De reeds genoemde toenemende verbondenheid van communicatie verlengt de interne communicatie. Want communicatie kanalen worden zowel interorganisatorisch als intraorganisatorisch meer en meer gekoppeld (Morton, 1996). *Interorganisatorische* communicatie-koppelingen brengen met zich mee dat de communicatie meer punten op de communicatie-infrastructuur moet passeren. Een deel van die infrastructuur ligt vrijwel altijd noodgedwongen buiten de organisaties zelf. Dit brengt dus veel meer interceptie punten voor deze communicatie met zich mee[9]. *Intraorganisatorisch* brengt dit het risico met zich mee dat werknemers meer te weten komen over het bedrijf dan wenselijk is voor superieuren (Sproull & Kiesler, 1991). En met hedendaagse communicatiemogelijkheden is het voor de betreffende werknemers een fluitje van een cent om informatie het bedrijf uit te smokkelen. Bij vrijwel alle bedrijven is het voor kwaadwillende werknemers uitermate eenvoudig om interne, vertrouwelijke informatie in verkeerde handen te laten vallen. Vaak voldoet simpelweg een e-mailtje met attachment om bijvoorbeeld een kopie met cruciale database-gegevens ongemerkt in andermans handen te laten komen. Hoe eenvoudig en hoeveel informatie met behulp van een ZipDrive wel niet uit kan lekken is helemaal niet te overzien. Een andere illustratie van de mindere mate van controle over de eigen communicatie bij de toenemende verbondenheid is dat in Australië één beschadigde, onderzeese communicatiekabel de helft van het internetverkeer in dit hele continent heeft platgelegd[10].

De integratie van communicatie met computertechnologie brengt een lager bewustzijn van communicatie met zich mee. Immer meer toepassingen maken gebruik van communicatie zonder dat gebruikers zich hier bewust van zijn. Door dit ontbrekende bewustzijn wordt er ook niet stil gestaan bij de mogelijke consequenties van dergelijke communicatie. Maar de consequenties zijn onder andere dat het gevaar bestaat dat informatie door dergelijke communicatie ongewenst in het bezit van derden komt of bijvoorbeeld gemanipuleerd wordt. Dit gevaar is extra groot doordat zeer veel informatie lange tijd bewaard wordt in log-bestanden. Ter illustratie: bij het gebruik van een Creditcard of chipkaart staan maar weinigen stil bij het feit dat er communicatie plaats vindt.

2.3 Het inhoudelijke belang

Het belang van de informatie-overdracht

Wat voor transnationale organisaties het belang van de inhoud van de bedrijfseconomische communicatie is, die zich door het zojuist beschreven communicatielandschap een weg baant, kan het beste uitgelegd worden op drie niveaus: interorganisatorische, intraorganisatorische en externe communicatie.

Interorganisatorische communicatie is essentieel voor samenwerking, onderhandeling en uitwisseling van informatie met andere bedrijven en organisaties. Elke organisatie is onderdeel van zijn context en is in een bepaalde mate afhankelijk van andere organisaties. Bedrijfseconomisch gezien leidt dit tot een mate van informatie-uitwisseling tussen organisaties. De uitwisseling van gegevens tussen leveranciers en afnemers is een voorbeeld. Informatiesystemen worden in vele gevallen hierop afgestemd, maar ook integraties van systemen van verschillende organisaties zijn zeer gebruikelijk. Vliegtuigreserveringssytemen zijn hier een goed voorbeeld van.

Intraorganisatorische communicatie is het medium waarmee een organisatie zijn werknemers informeert. De informatie is belangrijk voor het inlichten, motiveren, opleiden en stimuleren van werknemers.

Onder externe communicatie versta ik hier de communicatie naar de doelgroep. De communicatie van de organisatie met de doelgroep is essentieel. Allereerst kan de doelgroep hierdoor namelijk bewuster gemaakt worden van de aanwezigheid van de organisatie. Immers, een intensievere externe communicatie leidt bij de doelgroep tot een hoger bewustzijn van aanwezigheid van de organisatie als aanbieder (Franzen & Bouwman, 1999). Tevens wordt er wel gezegd: ‘je bent wat je communiceert’. Dit kan natuurlijk niet volledig onderbouwd worden, maar door het informeren van de doelgroep met behulp van communicatie kan een organisatie zich positioneren op een markt (Raaij & Antonides, 1997). Zeker in de eerder genoemde informatie-economie is het belang van positionering in vele sectoren zeer hoog, aangezien bij veel producten de productkwaliteit nauwelijks meer verschilt. Andersson & Strömquist (1988) stellen dan ook dat in de huidige economie de nadruk op verkoop is komen te liggen in plaats van op productie.

De ontwikkeling in informatie-overdracht

Het kenmerk van globalisering is de uitbreiding over de hele wereld. Door de toenemende globalisering speelt informatie een immer belangrijkere rol in het functioneren van transnationale organisaties. Fysieke afstanden worden groter terwijl acties sneller ondernomen moeten worden. Globalisering gaat gepaard met nauwe interorganisatorische samenwerkingen en mega-fusies. De laatste jaren is er een sterke groei in internationale fusies en overnames geweest, zoals blijkt uit een onderzoek van KPMG[11]. Het mag duidelijk zijn dat door de fusies en interorganisatorische samenwerkingen de uitwisseling van informatie tussen organisaties almaar belangrijker wordt.

Er is reeds aangegeven dat informatiesystemen interorganisatorisch op elkaar afgestemd en geïntegreerd worden. Veel bedrijven maken hiervoor gebruik van Electronic Data Interchange (EDI). Bij EDI vindt de data-uitwisseling plaats via een gesloten, niet openbaar netwerk[12]. Nu vindt data-uitwisseling echter meer en meer plaats via een koppeling van een intranet op het internet, een open netwerk. Hierbij wordt dan het gesloten intranet van de onderneming gedeeltelijk opengesteld voor handelspartners. Deze toepassingen zijn al wijd verbreid: er ontstaan overal virtuele marktplaatsen op het internet en (business-to-business) e-commerce neemt een vlugge loop. Eén van de grote voordelen hiervan is dat internet, in tegenstelling tot EDI, de mogelijkheid biedt data in een veelvoud aan vormen uit te wisselen.

Tevens neemt het belang van intraorganisatorische informatie toe. Immers, de over de wereld uitbreidende bedrijven moeten de interne informatie stroom goed op gang houden om het gedachtegoed van het hoofdkantoor over te brengen.

De externe communicatie ter informering van de doelgroep is en blijft zeer belangrijk. Vrijwel alle nieuwe markten die ontgonnen worden zijn open voor marktwerking. Externe communicatie is dus van belang voor positionering. Tevens worden de consumenten steeds meer in de gelegenheid gesteld om informatie en diensten via internet aan te vragen, op te zoeken en te regelen. Hierbij worden vaak delen van netwerken, net zoals beschreven bij de interorganisatorische informatie-uitwisseling, opengesteld voor de consument.

De bedreiging door de informatie-overdracht

De toegenomen data-uitwisselingen tussen organisaties onderling, en tussen organisaties en consumenten geven een enorme druk op de beveiliging van de informatie. Indien delen van netwerken partieel worden opengesteld voor geautoriseerde partners buiten de organisatie, of zelfs voor willekeurige consumenten, dient men zich goed te realiseren dat dit ook een nadere

toegang kan geven tot andere delen van netwerken. En vaak is het niet de bedoeling dat die partners of consumenten inzage in die laatste delen kunnen krijgen. Tevens leiden de toepassingen voor meer data-uitwisselingen tussen de organisaties onderling, en haar consumenten meestal tot een toename van het aantal communicatie-koppelingen. Deze toename in het aantal communicatie-koppelingen biedt dus ook meer kans op het in- en uitstromen van ongewenste informatie of bedreigingen voor informatiesystemen. Zeker indien deze toepassingen via het internet lopen, aangezien dan een ongelimiteerd aantal mensen en informatie deze koppelingen kunnen bereiken. Dus is een bedreiging in welke vorm dan ook veel dichterbij. Veel grote gebruikers zien EDI dan ook als een betrouwbaarder voertuig voor hun informatie dan het internetverkeer. In 1998 was het EDI-verkeer in de Verenigde Staten nog veertien maal omvangrijker dan het commerciële verkeer via internet[13]. Maar de verwachting was al dat deze verhouding in de komende jaren drastisch zou wijzigen in het voordeel van internet (Hamelink, 1999) en deze voorspelling is ook in rap tempo aan het uitkomen.

2.4 Redenen voor beveiliging

Speerpunten voor beveiliging van informatie in organisaties zijn de operationaliteit, integriteit en vertrouwelijkheid. Uiteraard verschilt per organisatie de nadruk die op elk van deze drie aspecten wordt gelegd, maar globaal gezien zijn dit de belangrijkste factoren voor het beveiligen van informatie.

Informatie dient *operationeel* te zijn. Dat wil zeggen dat deze beschikbaar moet zijn wanneer zij nodig is, en bewerkbaar moet zijn waar gewenst. Als informatie verdwijnt, gemanipuleerd wordt, of niet oproepbaar is komt de bedrijfsvoering in gevaar. Hoe kan immers een correcte factuur aan een klant worden gestuurd indien de informatie over de verrichte diensten gewist, gemanipuleerd of niet beschikbaar is? En dit is slechts één aspect van de noodzaak voor (correcte) informatie in de operationele bedrijfsuitvoering.

De *integriteit* van informatie heeft verschillende kanten. Een organisatie beschikt vaak over gegevens van haar klanten waar integer mee omgegaan dient te worden. Tevens willen organisaties hun imago niet laten aantasten door slachtoffer te worden van informatielekkage. Informatiebeveiliging dient er in dit geval dus voor te zorgen dat er integer met informatie

wordt omgegaan. Het falen hierin hoeft zich niet te vertalen in operationele schade, maar in meer abstracte schade aan de reputatie van de betreffende organisatie.

Het belang van de mate van *vertrouwelijkheid* verschilt per boodschap en per organisatie. Echter zijn er fundamentele punten in een organisatie aan te geven waar vertrouwelijkheid van groot belang is. Deze zijn:

- Industrieel geheim
- Strategische informatie
  – productontwikkeling
  – marktexploitatie
  – communicatief
- Financiële informatie
  – financiële gegevens die niet verplicht bekend gemaakt hoeven te worden
  – beursgevoelige informatie

Uiteraard verschilt wederom per organisatie het belang van vertrouwelijkheid op de verschillende punten, maar voor iedere organisatie is de vertrouwelijkheid van (een deel van) deze punten essentieel voor hun resultaat en de overlevingskansen. Om dit te illustreren, analyseren we het aan de hand van de drie fundamentele punten in een organisatie waar vertrouwelijkheid van groot belang kan zijn.

1) Industrieel geheim: indien je als organisatie producten produceert die geen ander produceren kan, maar hierop geen patent aanvragen kan, dan is het geheimhouden van de productformule van levensbelang voor de productcyclus. Echter moet de productformule (deels) beperkt intraorganisatorisch circuleren om tot vervaardiging van het product te komen. Indien deze intraorganisatorische communicatie uitlekt en misbruikt wordt, kost dit de organisatie de unieke situatie op de markt met alle desastreuze gevolgen van dien. Coca Cola is een onderneming waar dit belang duidelijk zichtbaar is. Tevens hebben veel organisaties Research en Development afdelingen. Het doel van deze afdelingen is het ontwikkelen van nieuwe producten waarmee een voordeel op de opponent behaald kan worden. Gezien dit doel spreekt het voor zich dat veel research en development met een hoge mate van vertrouwelijkheid gepaard dient te gaan.

2) Strategische informatie: vrijwel elke organisatie heeft opponenten die graag willen weten in welke richting de betreffende organisatie zich beweegt. Indien de opponent door bemachtiging van informatie of communicatie de strategie van de organisatie kan achterhalen, kan deze tegenmaatregelen nemen die zeer ten koste van de organisatie gaan. Er kan

bijvoorbeeld een zorgvuldig geplande, en miljoenen kostende communicatiecampagne waardeloos gemaakt worden door net eerder met een goedkoop, slap aftreksel van een dergelijke campagne te komen. Hierdoor lijkt de originele campagne een imitatie, en deze zal daarom uiterst ineffectief zijn. Terwijl de waarheid omgekeerd is.

3) Financiële informatie: indien vertrouwelijke financiële gegevens van een organisatie onderschept worden door een opponent, geeft dit de opponent een inzicht in zwakke punten van de organisatie in kwestie. Hierdoor kan de organisatie direct in de achillespees geraakt worden door de opponent. Tevens heeft veel vertrouwelijke financiële informatie potentieel veel invloed op een eventuele beurskoers. Dus als de organisatie een beursgenoteerde onderneming is, kan informatielekkage groot ongecontroleerd effect hebben op beurskoersen.

2.5 Conclusie

Aan de hand van de zojuist beschreven informatie kan de eerste deelvraag beantwoord worden. Deze luidt: *"Wat is het belang van bedrijfseconomische informatie voor transnationale organisaties?"*. Uit dit hoofdstuk blijkt dat bedrijfseconomische informatie allereerst noodzakelijk is voor de cohesie/gemeenschapsvorming van een organisatie en haar netwerk. Er dient immers informatie uitgewisseld te worden binnen de organisatie, tussen organisaties en met de klanten.

Trendmatig gezien blijkt dat bedrijfseconomische informatie steeds belangrijker wordt. Infrastructureel gezien noemde ik de vijf ontwikkelingen in communicatie die volgens Fulk & DeSanctis (1995) van grote invloed waren op organisaties. Deze vijf ontwikkelingen blijken nog immer belangrijker te worden. Tevens blijft de overdracht van communicatie, en daarmee de rol van informatie aan belang winnen, terwijl fysieke afstanden groter worden. Hiermee is dan de tweede deelvraag ook beantwoord, die luidde namelijk: "*Wat is de trend in bedrijfseconomische informatie voor transnationale organisaties?"*.

Tevens blijkt dat deze trendmatige ontwikkelingen theoretisch gezien kunnen leiden tot een toenemende mate van bedreiging van bedrijfseconomische informatie van transnationale organisaties. Wat hiervan in de praktijk terechtkomt beschrijf ik in het volgende hoofdstuk. Aan de hand daarvan kan de derde deelvraag beantwoord worden.

[1] Telecombedrijven betaalden in het jaar 2000 miljarden Euro's voor UMTS-licenties in onder andere Groot-Brittannië en Nederland.
[2] Deze tijdsreductie wordt door veel organisaties bereikt met JIT (Just-In-Time)-systems. Andere illustraties van IT-toepassingen die zorgen voor kostenreductie en tijdsbesparing, zoals EDI, worden beschreven door Morton (1996).
[3] Versatel en Chello, van UPC, zijn voorbeelden van bedrijven die zich expliciet aanbieder van breedbanddiensten noemen.
[4] Zie persbericht DPA/ANP, onder andere gepubliceerd in de Metro, 10-11-00: "Japan graag koploper op digitale snelweg".
[5] De invoering van een GPRS-netwerk voor mobiele telefoons maakt het mogelijk om mobiele apparaten in constante verbinding te laten staan met de netwerkoperator zonder dat dit extra kosten met zich meebrengt. Vanaf dan wordt er dus niet meer betaald voor de tijd dat de verbinding online is (want deze verbinding is constant online), maar slechts voor de verstuurde data. Dit in grote tegenstelling tot haar voorloper: WAP. WAP is namelijk een verbinding waarbij constant opnieuw ingebeld moet worden. Dit kost tijd en geld en dat levert een te grote barrière op voor services die frequent online dienen te zijn, zoals bijvoorbeeld rekeningrijden. Naar verwachting is GPRS over ongeveer 1,5 jaar de nieuwe mobiele standaard. De opvolger van GPRS zal UMTS worden. Ook een UMTS-netwerk biedt de mogelijkheid om constant online te zijn.
[6] Er is diverse apparatuur op de markt die straling van (communicatie-) signalen kan reconstrueren. Zo kunnen onder andere beelden van monitoren op afstand gereconstrueerd worden.
[7] De Nederlandse telecommunicatiewet, zoals ingegaan op 15 december 1998, stelt dat telecombedrijven aftapbaar moeten zijn.
[8] Het Zwitserse telecombedrijf Swisscom gaf eind 1997 toe de bewegingen van meer dan een miljoen mobiele bellers na te gaan en vast te leggen. Ook in Nederland worden bewegingen van mobiele bellers vast gelegd.
[9] Software-ontwikkelaars proberen deze problemen op te lossen door software te ontwikkelen die berichten bewust om knooppunten op het internet heen leidt en die in staat zijn zichzelf te vernietigen. Een voorbeeld van een dergelijke producent is AbsoluteFuture met het softwarepakket SafeMessage.
[10] Zie Parool 21/11/00: 'Internetverkeer Australië plat".
[11] Dit onderzoek werd gepubliceerd op 15-01-01. Informatie hierover is te vinden op: http://www.kpmg.nl/KPMG/bibliotheek/persbericht_overzicht.html?ID=294703&BU=KNL.
[12] Deze netwerken worden VAN's genoemd, de zogenoemde Value Added Networks.
[13] Business Week, 22 juni 1998.

H3, BEDREIGINGEN VOOR BEDRIJFSECONOMISCHE INFORMATIE

"Mogelijkheden in de praktijk en een case-study"

3.1 Introductie

Zoals blijkt uit hoofdstuk twee wordt informatie almaar belangrijker door de hedendaagse maatschappelijke en bedrijfsmatige ontwikkelingen. Tevens werken deze ontwikkelingen grotere bedreigingen voor bedrijfseconomische informatie in de hand. In dit hoofdstuk benaderen we deze bedreigingen praktijk gericht. Dit bestaat uit een inventarisatie van de gevaren die op de loer liggen voor de bedrijfseconomische informatie van transnationale organisaties. Daarop volgt een case-study naar het spionagenetwerk Echelon. Dit Amerikaanse netwerk zou stelselmatig onze communicatie monitoren, en daarmee zeer veel informatie verzamelen. Hier zet ik bekende en onbekende feiten op een rij. De inventarisatie van bedreigingen voor bedrijfseconomische informatie, tezamen met de case-study Echelon zullen genoeg informatie leveren voor de beantwoording van de derde deelvraag. Deze luidde: *"In hoeverre wordt bedrijfseconomische informatie van transnationale organisaties bedreigd?"*. De beantwoording, tezamen met de informatie uit hoofdstuk twee vormen de basis voor de inhoud van de interviewvragen van het volgende hoofdstuk.

3.2 Inventarisatie van de bedreigingen

Neumann (1995) onderscheidt drie niveaus waarop veiligheid van communicatie en informatiesystemen in het geding komt. Op deze niveaus komen dus de informatie en communicatie zelf ook in gevaar. Deze niveaus zijn daarmee eveneens zeer geschikt voor de inventarisatie van de bedreigingen van bedrijfseconomische informatie. Ik zal allereerst de drie niveaus beschrijven, om ze vervolgens per niveau toegepast uit te diepen. De drie te onderscheiden niveaus zijn:

- Technologisch: deze bedreiging schuilt in de discrepantie tussen wat een systeem werkelijk kan verwezenlijken en wat er van het betreffende systeem verwacht wordt.

- Sociaal-technisch: deze bedreiging schuilt in een verkeerde interactie tussen mens en machine. Ook al voldoet het communicatie- en/of informatiesysteem aan de technische normen, kan er door verkeerde interactie met de gebruiker fouten optreden die bedreigend kunnen zijn.
- Sociaal: de sociale bedreiging omtrent communicatie- en informatiesystemen bestaat uit een mogelijke discrepantie tussen de technische doelstelling van het systeem en de persoonlijke doelstelling van de gebruiker. Indien er op dit niveau bedreigingen voor de informatie zijn, komen dezen meestal voort uit opzettelijk misbruik van het systeem.

Wat betreft het *technologische niveau* dient allereerst opgemerkt te worden dat de, reeds in hoofdstuk twee beschreven, trend tot digitalisering per definitie een groot technologisch gevaar met zich meebrengt. De digitale technologie is substantieel anders dan mechanische systemen. In de laatste wordt een kleine fout gebruikelijk omgezet in een kleine fout terwijl in computersystemen de verandering van één bit genoeg kan zijn om verwoesting aan te richten[1] (Neumann, 1995). De hiermee gepaard gaande bedreigingen zijn heel groot. Digitale systemen hebben namelijk hard- en software tekortkomingen. Dit maakt deze systemen gevoelig voor disfunctioneren. Het disfunctioneren kan door derden veroorzaakt worden, zowel intentioneel als niet-intentioneel. Allereerst bespreek ik enige voorbeelden van bedreiging door intentionele disfunctionering door derden, vervolgens zal ik de bedreiging van niet-intentioneel veroorzaakte disfunctionering beschrijven.

Voorbeelden van bedreigingen voor informatie die voortkomen uit intentionele disfunctionering zijn legio:

- Denial of Service attacks (DoS): een overload aan toegestuurde informatie die leidt tot het falen van het systeem.
- Hacken van computers: het indringen in een computersysteem zonder toestemming.
- Virus-attacks: aanvalsprogrammatuur dat andere programma's infecteert en beschadigt. Een virus verspreidt zich in een computersysteem.
- Worms: specifieke aanvalsprogrammatuur die in andermans programma's geplaatst kan worden. Een goed geplaatste worm kan op afstand controle hebben over de geïnfecteerde programma's.

Een *DoS* vindt regelmatig plaats tegen gevestigde bedrijven. De schade is meestal urenlange uitval van de systemen. Dit leidt dus tot een grote operationele schade. Virussen hebben een

soortgelijke impact, maar zij kunnen tevens de hardware blijvend beschadigen. Echter kan er geen informatie mee gestolen worden (alhoewel informatie bij vernietiging wel verloren kan gaan). Dit in tegenstelling tot *hacken*. Het hacken van een computersysteem is niet alleen desastreus indien de hacker slechte intenties heeft, maar het komt ook extreem vaak voor[2]. Direct bij een geslaagde hackaanval kan de aanvaller vertrouwelijke bedrijfsinformatie manipuleren, kopiëren en/of vernietigen. Een v*irus-attack* kan gericht zijn tegen specifieke ontvangers, maar kan zich ook willekeurig verspreiden. De schade van virussen kan gigantisch zijn, zo wordt de schade van het 'I love you'-virus uit 2000 geschat op 10 miljard dollar wereldwijd[3]. Een gerichte aanvaller kan nog een stap verder gaan en '*worms*' plaatsen. Een goed geplaatste worm geeft de indringer controle over andermans systemen zonder dat deze daarvan op de hoogte is. Een dergelijke aanval kan een bedrijf volledig ruineren. Zeker indien de aanvaller zo slim is om geen gebruik te maken van de mogelijkheid tot het overnemen van controle, maar zich beperkt tot inzage in alle informatie en vervolgens deze informatie voor economische doeleinden gebruikt. In dit geval kan dus zowel de integriteit als de vertrouwelijkheid ernstig in het geding zijn. Als wapen tegen hacken, virussen en worms hebben vele bedrijven netwerkbeveiliging. Echter geeft dit geen afdoende veiligheid. Allereerst zijn vele netwerken zelfs voor informatica-leken te kraken omdat op internet eenvoudig bedienbare software te vinden is waarmee een doorsnee Windowsgebruiker in staat is doorsnee netwerken te kraken en zelfs om programmatuur zoals worms te plaatsen en te bedienen[4]. Daarbij komt dat de benodigde mate van beveiliging slechts een subjectieve interpretatie is van de beveiliger (Bowyer, 1996). Ten tweede is de strijd tussen de echte hacker en beveiliger een wapenwedloop waar geen einde aan komt. Dus zelfs de meest hoogwaardige netwerkbeveiling voldoet nooit[5]. Daarbij hoeft een systeem vaak niet gekraakt te worden om toegang tot communicatie te krijgen. Vrijwel alle communicatie zendt signalen uit die te onderscheppen zijn. Mobiele telefonie is met een aangepaste laptop eenvoudig op te vangen. Maar zelfs de straling van monitoren is op te vangen en te reconstrueren. Hoe reëel deze bedreiging is wordt geïllustreerd door het feit dat het Pentagon uit angst hiervoor overweegt nieuwe monitoren aan te schaffen[6]. Tevens zijn vele andere vormen van communicatie af te luisteren met behulp van surveillance apparatuur. De digitale afluisterapparatuur is zeer minuscuul, waardoor camera's en microfoons eenvoudig in pennen en brillen verborgen kunnen zitten[7].

Ook niet intentioneel is er op het technologische niveau een bedreiging. Het probleem van digitalisering van systemen is dat dit een virtueel karakter met zich meebrengt. Vele files

hebben geen hard-copies meer en bestaan uitsluitend nog in digitale formats. Als er door technologische gebreken een fout optreedt in de digitale format, dan is er vaak niet meer te achterhalen wat de originele informatie was. Dit zou onder andere een probleem zijn bij digitale verkiezingen: de stembiljetten zijn er niet fysiek.

Echter is het ook van belang de beveiliging niet uitsluitend technisch te beschouwen want op het sociaal-technische niveau liggen ook bedreigingen op de loer. Al voldoet een systeem aan de technische normen, dan blijft er het risico van foutief gebruik door de gebruiker. Zo worden computers vaak slecht, of helemaal niet afgesloten. Dit geeft derden eenvoudig toegang tot belangrijke operationele systemen of (vertrouwelijke) informatie. Tevens zijn er veel organisaties waar werknemers elkaars passwords kennen of een algemene toegangscode gebruiken, die technisch gezien uitsluitend voor de systeembeheerder bedoeld is. Slordigheid is vaak de fout. Voor transnationale organisaties is er tevens het probleem van verschillende landen en wetten. Hierdoor gelden niet alleen verschillende regels voor (vaak eenzelfde) systeem, maar ook wordt er in verschillende samenlevingen anders omgegaan met systemen alsmede dat er vaak andere opvattingen (over b.v. punctualiteit) op nagehouden worden. Het bijkomende probleem is dat de systemen uit onderdelen bestaan die met elkaar samenhangen en die elkaar beïnvloeden. Als één onderdeel niet (goed) functioneert, heeft dit effect op vele onderdelen en/of op het gehele systeem. Elk onderdeel kan een zwakke schakel zijn die het geheel beïnvloedt (Hamelink, 1999: 117).

Tot slot is er het sociale niveau. Deze bedreiging is vrijwel niet sluitend te maken met beveiliging, maar is wel zeer groot. Uiteraard is manipulatie, vernietiging, kopiëren en inzien van (eventueel vertrouwelijke) informatie met slechte intenties al zo oud als informatie zelf. Echter faciliteert digitalisering dit gigantisch. Allereerst omdat werknemers over het algemeen meer toegang krijgen tot information sharing systems (Sproull & Kiesler, 1991). Ten tweede omdat het bijzonder opvalt indien iemand stapels documenten meeneemt, maar het zal niemand opvallen indien iemand een ZIP-disk meeneemt waar bij wijze van spreken informatie ter grootte van twaalf boekenkasten op kan staan. En dit geldt niet alleen voor de ZIP-disk, maar ook voor de beschrijfbare CD, een laptop en noem maar op. En wie denkt dat er geen mensen met verkeerde intenties rond zouden lopen, kan zich ook eens gaan afvragen waarom er gevangenissen zijn. Je kan er dus simpelweg niet van uitgaan dat elke werknemer met uitsluitend de beste intenties rondloopt.

3.3 Case-study Echelon

Dat bedreiging van informatie niet uitsluitend een theoretisch verhaal is, wordt geïllustreerd met het verhaal 'Echelon'. Deze case-study over Echelon toont een bedreiging van informatie op het deelgebied vertrouwelijkheid. Het is uiteraard maar één van de vele potentiële bedreigingen voor vertrouwelijkheid van communicatie en informatie. En hoewel het gezien kan worden als een vreemde eend in bijt van de potentiële bedreigingen, is het er wel een die gigantische impact op mondiaal zakenniveau kan hebben. Tevens illustreert het hoe techniek informatiebedreiging in de hand kan werken. Vandaar de keuze voor deze case-study.

Echelon is een reusachtig spionagenetwerk dat wereldwijd stelselmatig communicatie onderschept. Het is voortgekomen uit de samenwerking in spionage tussen Engeland en Amerika in de tweede wereldoorlog. Na deze oorlog besloten beide landen actief samen te blijven werken bij spionage onder de naam UKUSA. Dit netwerk werd geleid door de Amerikaanse National Security Agency (NSA). Vervolgens namen Canada, Nieuw Zeeland en Australië deel in dit netwerk, wat uiteindelijk bekend werd als het Echelon netwerk. Dit netwerk werd als eerste aan het licht gebracht door Hager (1996) in het boek: *'Secret Power: New Zealand's role in the International Spy Network'*. Voor dit boek interviewde hij meer dan vijftig mensen die werken, of gewerkt hebben voor inlichtingendiensten die bij Echelon betrokken zijn. Twee jaar later volgde in 1998 een uitgebreid rapport van het Europees Parlement over Echelon[8]. Uit onder andere deze bronnen blijkt dat communicatie-interceptie structureel plaats vindt met behulp van ten minste vijf bases over de hele wereld, satellieten, onderzeeërs en aftapping van kabels. Zonder enige selectie wordt alle onderschepte informatie stelselmatig met behulp van keyword-search doorzocht, zoals een zoekmachine op internet dit doet. Deze keyword-search is in alle talen mogelijk.

Economische bedreiging

Talloze geruchten zijn bekend dat Echelon individuele Amerikaanse bedrijven bevoordeelt. Zo lijken General Motors, Raytheon en Boeing cruciale vertrouwelijke informatie toegespeeld gehad te hebben van de NSA waardoor zij Europese concurrenten de loef af staken. Maar allereerst kijken we algemener naar de activiteiten van veiligheidsdiensten. Officieel houdt een veiligheidsdienst zich bezig met het in beeld brengen van bedreigingen. Een belangrijke taak hierbij is informatieverzameling. Om een goed beeld te hebben van de potentiële bedreiging wordt niet alleen militaire informatie, maar ook wetenschappelijke en technische

communicatie onderschept. Veel wetenschappelijke en technologische kennis is in handen van bedrijven die staatsleverancier zijn. Daar is de grens tussen bedrijfsspionage en staatsspionage dus onduidelijk. Daarbij is het interceptienetwerk even capabel voor economische doeleinden als voor defensieve doeleinden zonder enige verandering toe te passen. De communicatie wordt toch reeds onderschept. Er hoeven slechts andere keywords gebruikt te worden.

Cools & Hoogenboom (1996) stellen dat het einde van de koude oorlog de politieke machtsstrijd heeft veranderd. De machtsstrijd wordt meer en meer langs economische lijnen voortgezet nu het tijdperk van de grote ideologische conflicten naar de achtergrond is gedrongen. Zij spreken van een grensvervaging tussen het militaire en het economische denken en handelen ten aanzien van de verwerving van kennis. Een illustratie hiervoor is de uitspraak van de voormalige CIA-directeur Stansfield Turner: "We will have to spy on the more developed countries – our allies and friends with whom we compete economically". Criminoloog Cools gaat zelfs zover om te stellen dat 80% van de totale wereldspionage zich situeert in en om het bedrijfsleven (Cools, 1996). Daaraan wil ik toevoegen dat een NSA met haar 40.000 werknemers en een budget van 8 miljard gulden per jaar ten tijde van afnemende militaire druk toch haar budget zal moeten kunnen rechtvaardigen[9].

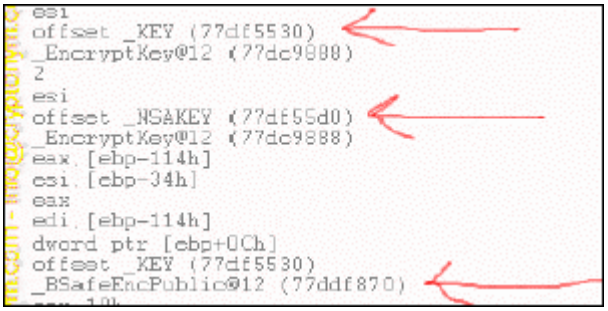
Wat wijst hierop?

Een inlichtingen- en veiligheidsdienst zoals de NSA werkt zeer ondoorzichtig. Er is een grote mate van geheimhouding omtrent het gevoerde beleid, methoden en resultaat, aangezien de informatie die deze dienst vrijgeeft ook ingezien kan worden door de vijanden die door deze dienst onder de loep genomen worden. Dus geeft een veiligheidsdienst over het algemeen zeer weinig informatie vrij, aangezien het haar effectiviteit direct beïnvloedt. Dit brengt wel het gevaar met zich mee dat een dergelijke dienst er een geheime agenda op nahoudt die in strijd is met de wensen van de bevolking en/of de democratische principes van de betrokken staat. Keer op keer blijken inlichtingendiensten dergelijke verborgen agenda's gehad te hebben. Ter illustratie: de FBI is sinds het voorjaar van 2000 subject van onderzoek naar het gebruik van haar cyberspionageprogramma Carnivore, aangezien zij hier teveel informatie over achterhield[10]. Ook de NSA geeft niet graag ruchtbaarheid aan haar acties. Zo werd pas recent bekend dat zij sinds 1947 onder de naam UKUSA tezamen met Engeland, Australië, Nieuw Zeeland en Canada internationale communicatie intelligence (COMINT) toepast. Dit werd maart 1999 bekend gemaakt door de Australische regering. Het rapport *An appraisal of*

Technologies of Political Control, dat in opdracht van het Europees Parlement opgesteld werd, stelt dat Echelon onderdeel uitmaakt van het UKUSA systeem. Tevens wordt gesteld dat Echelon voornamelijk is ontworpen ter interceptie van non-militaire communicatie. Het is derhalve aannemelijk dat het ontworpen is voor interceptie van communicatie van overheden, organisaties en het zakenleven[11]. Eén van de reacties op dit rapport kwam van voormalig CIA-directeur James Woolsey. In de *Wall Street Journal* van 17 maart 2000 zegt hij dat Amerika inderdaad het Europese bedrijfsleven heeft bespioneerd. Dit gebeurde niet om economische geheimen te bemachtigen, maar om de omkooppogingen van Europese bedrijven te dwarsbomen. Europese bedrijven doen volgens hem namelijk veel aan omkoping. Als er echter uitsluitend wordt gespioneerd om illegale omkoping te voorkomen, waarom wordt het dan niet publiekelijk bekend gemaakt om de daders te vervolgen?

Volgens onderzoek van de Amerikaanse nieuwszender NBC News profiteert het Amerikaanse bedrijfsleven wel degelijk van de spionage-activiteiten van de veiligheidsdiensten. Het onderzoek stelt dat spionage met commerciële doeleinden plaatsvindt door de Amerikaanse overheid en dat individuele bedrijven worden bevoordeeld. Het noemt ook namen van bevoordeelde bedrijven. Zo zouden volgens dit onderzoek Raytheon, Hughes Network Systems en Boeing hulp van inlichtingendiensten gekregen hebben voor het bemachtigen van mega-contracten in het buitenland ten koste van Europese bedrijven[12].

Opvallend hieraan is dat al deze genoemde bedrijven grote leveranciers zijn voor de Amerikaanse defensie diensten. Deze bedrijven staan daardoor altijd al in nauw contact met overheids- en veiligheidsdiensten. Dit leidt al snel tot belangenverstrengeling. Dat samenwerking van de NSA met het bedrijfsleven tot inbreuk op de bedrijfseconomische communicatie van derden kan leiden toont het volgende aan: het E-mailprogramma Lotus Notes bevatte een toegangscode voor de NSA, waardoor het voor de laatstgenoemde eenvoudiger werd om de communicatie van de gebruikers van Lotus Notes te onderscheppen[13]. Belangrijk om hierbij op te merken is dat Lotus Notes een veelgebruikt E-mailprogramma van parlementsleden was. Ook Microsoft lijkt een dergelijke code voor de NSA toe te passen. Volgens beveiligingsdeskundige Andrew Fernandes van het Canadese computerbedrijf Cryptonym bevat het besturingsprogramma Microsoft Windows een geheime toegangssleutel voor de NSA (zie figuur 1).



Figuur 1: broncode van Windows met de NSAKEY (bron: NRC)[14].

In een reactie hierop liet Microsoft weten dat Windows slechts beveiligingssleutels bevat, opdat bedrijven buiten medeweten van de gebruiker programma's en aanvullingen kunnen installeren. Microsoft ontkent echter dat de NSAKEY in Windows bedoeld is voor de NSA. Volgens de softwaregigant heeft de door Fernandes ontdekte sleutel de naam NSAKEY om aan te geven dat de versleutelingsexponenten van Windows voldoen aan Amerikaanse exportbeperkingen. Toch is de naam NSAKEY zeer verdacht. Het kwam nooit eerder voor dat een sleutel in Windows een naam had, wat erop kan duiden dat Microsoft het karakter van de sleutel geheim wilde houden, maar dat een slordige programmeur vergat de naam weg te halen. Volgens expert Bruce Schneier is er niets aan de hand, omdat een spionagedienst als de NSA de hulp van Microsoft niet nodig heeft[15]. Echter heeft de NSA in het eerder genoemde voorbeeld van Lotus Notes laten zien dat zij wel degelijk het bedrijfsleven nodig heeft.

Opvallende feiten

– De intercontinentale communicatiekabels lopen grotendeels door deelnemende Echelonlanden. Deze zijn dus toegankelijk voor dit netwerk. Ook de kabels die niet door deze landen lopen zijn toegankelijk. Amerikaanse onderzeeërs hebben op diverse kabels interceptie apparatuur aangebracht (Sontag & Drew, 1998). En mocht het gebruik van onderzeeërs eerst nog vreemd klinken, dan heeft het incident met het neergestorte, bemande spionagevliegtuig boven China in het voorjaar van 2001 duidelijk gemaakt dat de Verenigde Staten geen middelen weren voor spionage[16].

- Technisch gezien is de kennis aanwezig. De FBI heeft met het cyberspionageprogramma Carnivore reeds toegang tot al het e-mail- en dataverkeer van de Amerikaanse burgers en kan hiermee duizenden e-mails per seconde met behulp van keyword-search controleren[17].
- Volgens de website van de NSA (http://www.nsa.gov/) is hun mission statement: *"The ability to understand the secret communication of our foreign adversaries while protecting our own communications – a capability in which the United States leads the world – gives our nation a unique advantage."* Zeer opmerkelijk dat zij hier spreken over een unieke bevoordeling van de natie in plaats van expliciet defensieve taal.
- Op 18 december 1991 werden in Amerika achttien privé-detectives en Social Security Administration (SSA) werknemers aangeklaagd op grond van het aan- en verkopen van vertrouwelijke informatie die onder andere gegenereerd was door FBI-computers. Dus al gebruikt de NSA haar informatie niet economisch, dan is er het risico dat dit incidenteel illegaal toch gebeurt.
- De Canadees Mike Frost was twintig jaar lang lid van de Canadese inlichtingendienst en betrokken bij het spionagenetwerk Echelon. Hij onthulde dat Margaret Thatcher in haar tijd als premier een Canadese geheim agent het doen en laten van twee van haar ministers liet bespioneren met behulp van het Echelon-netwerk. Deze onthullingen deed Frost in het Amerikaanse TV-programma *60 Minutes* van CBS op 30 januari 2000. Thatcher verdacht deze ministers niet van dienstverband met vreemde mogendheden, maar wilde de politieke opvattingen weten die tegenstrijdig waren met haar persoonlijke opvattingen.

3.4 Conclusie

Uit hoofdstuk twee bleek reeds dat de belangen en trends in informatie in de internationale bedrijfseconomie een theoretische toenemende bedreiging met zich meebrengen. In dit hoofdstuk is het in een praktijk gericht kader gezet. Hiermee kan ik de derde deelvraag beantwoorden. Deze luidde: *"In hoeverre wordt bedrijfseconomische informatie van transnationale organisaties bedreigd?"*. Uit dit hoofdstuk blijkt dat de vertrouwelijkheid van bedrijfseconomische informatie direct bedreigd wordt op alle drie de beschreven niveaus van Neumann (1995). Deze bedreiging is sterk toegenomen door de ontwikkelingen in de communicatie-infrastructuur en het inhoudelijk belang van informatie, zoals beschreven in hoofdstuk twee.

Ter illustratie dat dit niet alleen een bedreiging is, maar ook een realiteit heb ik Echelon beschreven. Dit laat duidelijk zien dat doelgerichte intentionele spionage structureel toegepast kan worden. Dit levert een onbeschrijflijke economische bedreiging op voor individuele bedrijven. Zelfs als de NSA niet intentioneel economisch spioneert, dan nog is er een kans op incidenteel uitlekkende vertrouwelijke informatie die grote schade aan bedrijven kan aanrichten. Daarbij heeft de beschrijving laten zien dat de spionage technologisch absoluut mogelijk is. Sterker nog, er ligt dus al een volledige technische infrastructuur voor bedrijfseconomische spionage. En er dient niet vergeten te worden dat de NSA niet de enige inlichtingendienst is die een dergelijke bedreiging kan opleveren. Er zijn minstens dertig andere naties die soortgelijke organisaties exploiteren. Zo heeft Rusland de FAPSI[18] met maar liefst 54.000 werknemers, aldus het EU-rapport *'Interception Capabilities 2000'*. Tevens kunnen er tal van andere organisaties zijn die zich met bedrijfsspionage bezighouden. Dit kunnen bedrijven zijn die dit incidenteel doen ter verbetering van hun concurrentiepositie, of gespecialiseerde bedrijven die dit als core-business hebben. Maar er kan ook aan terroristische eenheden gedacht worden. Hoe dan ook, de middelen en doelen zijn hier volop voor aanwezig. En deze case-study is nota bene slechts een beschrijving van de bedreiging van vertrouwelijkheid van informatie, terwijl er ook nog de twee andere aspecten zijn: operationaliteit en integriteit. En ook hierover zijn uitgebreide illustraties van de bedreigingen mogelijk[19].

Al met al leidt dit tot een communicatieklimaat waarin alertheid voor bedrijfseconomische informatie op zijn plaats is. De bedreiging is dusdanig dat er met gepaste middelen op geanticipeerd dient te worden. Het volgende hoofdstuk inventariseert de perceptie van de dreiging bij Nederlandse transnationale organisaties.

---

[1] De potentiële kwetsbaarheid van digitale systemen was onder andere duidelijk zichtbaar bij het millenniumprobleem.
[2] Het Pentagon kreeg 22.144 virtuele offensieven te verwerken in 1999 (bron: Defense Information Systems Agency DISA).
[3] Bron: Internet-onderzoeksbureau Pro Active, Amsterdam.
[4] Op dit moment van schrijven kunt u dergelijke software vinden op: http://crash.to/attackgroup. Echter wijzigen deze illegale sites regelmatig van adres. Maar ze zijn altijd weer te vinden via legale portals zoals bijvoorbeeld http://hack.pagina.nl (eigendom: VNU).

[5] Zelfs de IT-bedrijven, die nota bene ontwikkelaar zijn van beveiliging, zijn slachtoffer. Zie ook ANP persbericht 8/11/00: *Na Microsoft nu Compaq slachtoffer van Nederlandse hacker*. Tevens stellen software-leveranciers reparatie-patches beschikbaar om de gaten in een systeem te dichten. Maar dat op zich is al geen bemoedigende gang van zaken.
[6] Zie Metro 9 augustus 2000: "Pentagon bang voor spionnen".
[7] Dergelijke geavanceerde afluisterapparatuur is te vinden op o.a. http://www.microelec.com Overigens lijkt Pakistan India zelfs te bespioneren met getrainde vogels met surveillance apparatuur, zie ook persbericht ANP 14/11/00.
[8] *An Appraisal of Technologies of Political Control*, opgesteld door de Omega Foundation in Manchester in opdracht van het Scientific and Technological Options Assessment (STOA) van het Europees Parlement.
[9] De Volkskrant van 24 januari 2001 stelt dat de NSA 40.000 werknemers telt en een jaarbudget van 8 miljard gulden heeft.
[10] De Amerikaanse justitie begon in de zomer van 2000 een onderzoek naar Carnivore, op grond van aanwijzingen dat dit cyberspionagesysteem te pas en te onpas wordt ingezet en dat controle erop onmogelijk is. Een rechtbank gelastte de FBI de documenten over Carnivore vrij te geven. Op een serie documenten was meer dan de helft van de tekst onleesbaar gemaakt. Minister Janet Reno van Justitie heeft nog geen definitief oordeel gegeven over het bestaansrecht van Carnivore.
[11] Het rapport *An appraisal of Technologies of Political Control* werd in februari 1998 gepubliceerd. Het is opgesteld door het Britse onderzoeksbureau Omega, in opdracht van de STOA van het Europees Parlement. Het is vrij op te vragen bij de EU of te zien op: http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm#1.
[12] Het onderzoek van NBC News is uitgevoerd onder redactie van Robert Windrem en gepubliceerd op 7 mei 2000. Uitgebreide informatie over dit onderzoek is verkrijgbaar bij NBC News. Een korte samenvatting is te vinden op http://www.msnbc.com/news/403435.asp.
[13] Zie artikel NRC van 8 september 1999, ook op http://www.nrc.nl/W2/Lab/Echelon/echelon08091999.html. Het komt erop neer dat de NSA 24 bit van de 64 bits versleuteling bezit, waardoor het ontcijferen exclusief voor de NSA eenvoudiger is.
[14] NRC Handelsblad 8 september 1999, ook op http://www.nrc.nl/W2/Lab/Echelon/echelon08091999.html.
[15] Idem als 14.
[16] Op 31 maart 2001 kwam een Amerikaans EP-3E spionagevliegtuig in botsing met een Chinese F-8 straaljager boven Chinees grondgebied. Het incident maakte duidelijk dat de Verenigde Staten aan zeer pro-actieve, internationale rechten schendende informatiewinning doet. Uit een rapportage van Newsweek (16 april 2001) blijkt bovendien dat de Verenigde Staten gewoon zijn het Chinese luchtruim te schenden voor spionagevluchten.
[17] Zie onder andere ANP persberichten 25/8/00, 27/9/00 en 21/11/00.
[18] FAPSI staat voor Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii, oftewel het 'Federale Bureau voor Regerings Communicatie en Informatie'. Haar functies zijn onder andere communicatieve spionage.
[19] Een interessante beschrijving van voorgekomen incidenten in organisaties door een gebrek aan informatiebeveiliging is te vinden in het februari-nummer 2000 van het Information Security Forum (ISF): "It could happen to you: A profile of major incidents."

H4, RISICOPERCEPTIE VAN INFORMATIEBEDREIGING

"Interviews"

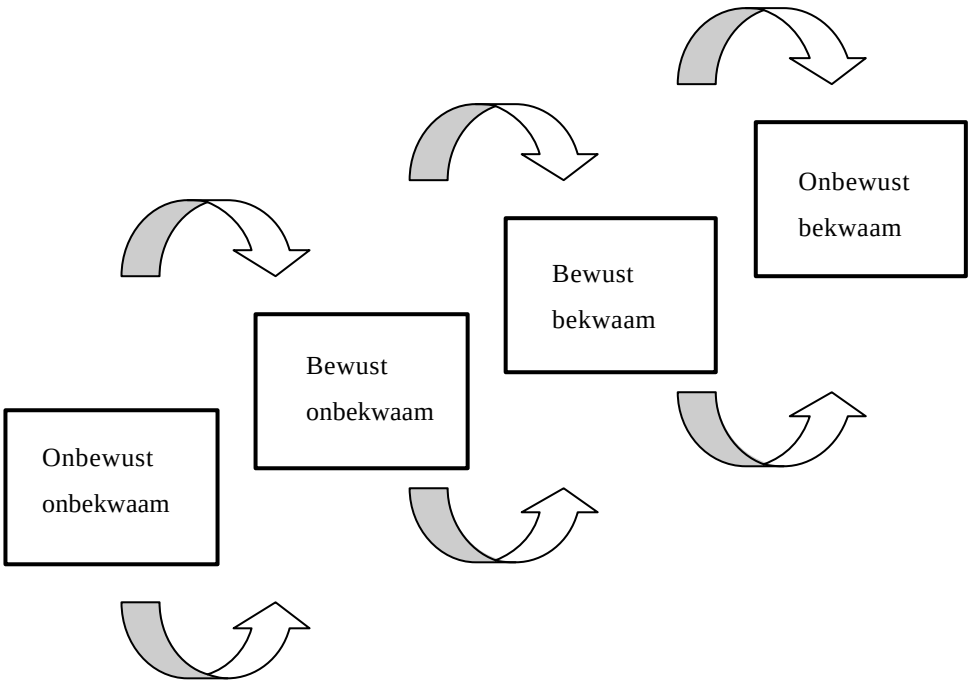
4.1 Introductie

In dit hoofdstuk worden de reeds beschreven issues uit deze scriptie in vraagvorm voorgelegd aan vooraanstaande Nederlandse organisaties die te maken hebben met dit probleemgebied. Binnen deze organisaties zijn de interviews gehouden met (één van) de expert(s) op dit gebied. Bij vrijwel elke organisatie is gebleken dat deze expert op het gebied van informatiebeveiliging een andere functienaam had. Een functienaam die de lading van de functie van de geïnterviewde expert goed dekt was meestal 'Corporate Information Security Officer'. Binnen de volgende organisaties is met een dergelijke expert gesproken over informatiebedreiging en informatiebeveiliging: AbnAmro, Akzo-Nobel, ASML, DSM, ING, KLM, KPN, Ministerie van Economische Zaken, NBV als onderdeel van de BVD, Philips, Rabobank, Shell en de Universiteit van Amsterdam. De resultaten van de interviews worden anoniem weergegeven. Voor een uitgebreide beschrijving van de vragen, het interview en de keuzes van en de verantwoording voor de geselecteerde organisaties verwijs ik u graag naar de bijlage.

4.2 Benadering

Het uitgangspunt van de interviews is geweest om niet alleen een concreet antwoord op een vraag te krijgen over hoe bepaalde zaken geregeld zijn, maar om met name inzicht te verwerven in de reden waarom men de zaken zo heeft geregeld. Zo is bijvoorbeeld uit het antwoord op de vraag of men aan automatische password-wijziging doet zelf weinig af te leiden. Er kunnen immers goede redenen zijn om hier wel of niet aan te doen. Daarom is er dieper door gevraagd. Op grond hiervan kan beoordeeld worden of dergelijke keuzes gemaakt zijn op basis van bewuste en reële afwegingen. Een rode draad is dan ook de vraag of de experts inzien waar de organisatie bekwaam is, en waar deze onbekwaam is op het gebied van informatiebeveiliging. Als er een zwakte in de informatiebeveiliging nog niet verholpen is,

maar de organisatie in kwestie is zich hier bewust van dan is deze tenminste bewust ‘onbekwaam’. Er kan verwacht worden dat deze organisatie vervolgens doorschuift op de leercyclus (zie figuur 2). Het grote gevaar schuilt in onbewust onbekwaam zijn.

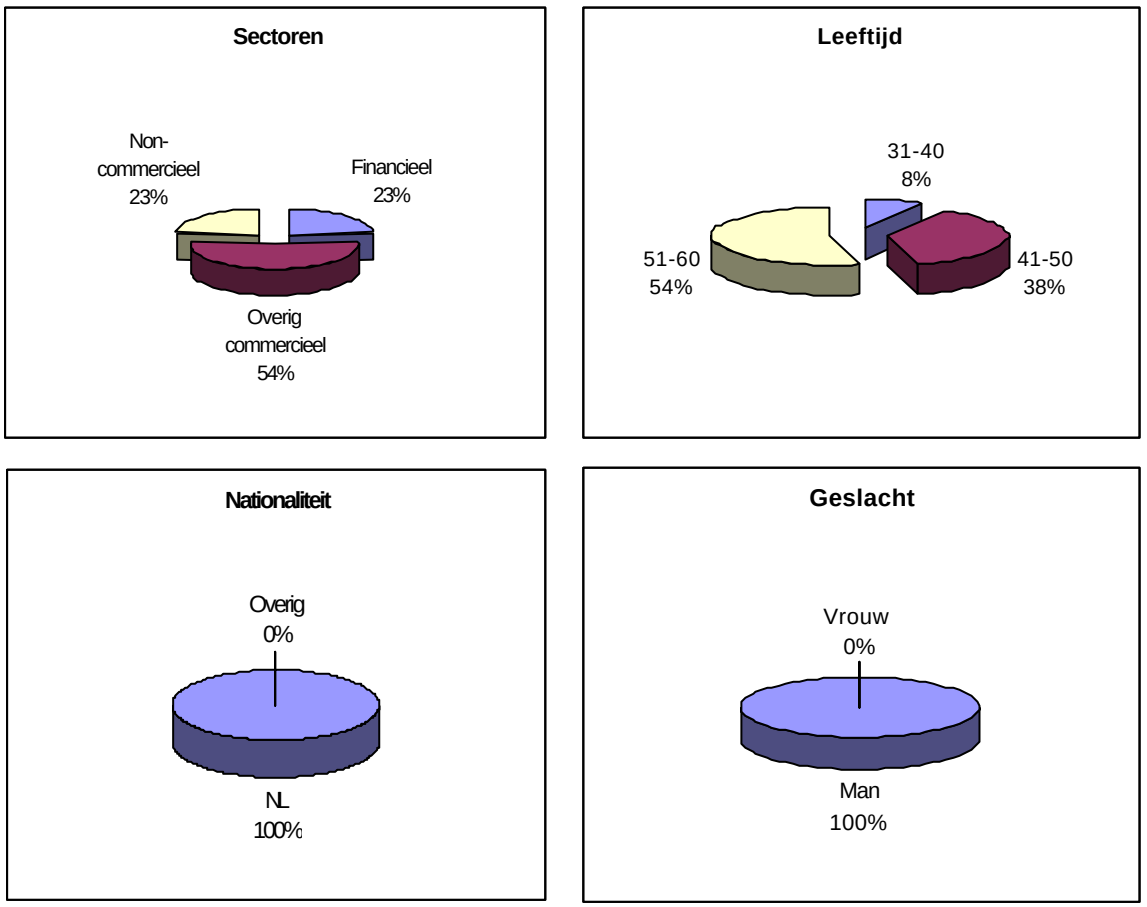


Figuur 2: leercyclus van Dubin (1962)

Figuur twee geeft een interessante visie op een leercyclus. Hierbij moet wel de kanttekening gemaakt worden dat deze leercyclus een algemeen karakter heeft. Toegespitst op informatiebeveiliging kan de expert wel bewust zijn van een risico, echter wil dat nog niet zeggen dat er ‘doorgeschoven’ dient te worden op de leercyclus. Informatiebeveiliging kan namelijk benaderd worden als een kostenafweging van risicoreductie. Er kan dus bewust gekozen worden een risico te lopen, aangezien de kosten van risicoreductie hoger kunnen zijn dan de baten. In dit geval is het ‘doorschuiven’ op de leercyclus niet van toepassing en in die zin moet het woord ‘bekwaam’ hier niet te letterlijk genomen worden. Het spreekt enigszins een waardeoordeel uit, terwijl dat bij informatiebeveiliging dus niet van toepassing hoeft te zijn (doorschuiven naar ‘onbewust bekwaam’ is beleidsmatig niet altijd de beste optie, alhoewel de leercyclus dit indirect suggereert).

4.3 Statistische gegevens

Alvorens de resultaten van de interviews te beschrijven wordt u enige extra informatie over de experts niet onthouden. In figuur drie, hieronder weergegeven, vindt u statistische gegevens over de geïnterviewde experts en organisaties. Het betreft de sectoren van de organisaties, de leeftijd, de nationaliteit en het geslacht van de experts. Mochten deze gegevens nog significante verschillen in antwoorden en/of opinies weergeven, zal hierop zeker teruggekomen worden.



Figuur 3: statistische gegevens van de geïnterviewden

4.4 Resultaat

De interviews openden met een beschrijving van de functie van de expert en de plaats waar informatiebeveiliging in de organisatie staat. Hieruit blijkt dat in informatiebeveiliging een duidelijke trend waarneembaar is tot centralisatie, in sterke tegenstelling tot de algemene trend tot decentralisatie. Ook is er in meerdere organisaties de laatste jaren een speciale, centrale informatiebeveiligings-afdeling ontstaan. Deze, vaak 'Information Security Offices' genoemde afdelingen, bestaan vrijwel allemaal nog maar maximaal drie jaar. De financiële dienstverleners vormen hierop een uitzondering. Informatiebeveiliging is daar van oudsher verweven met hun operationele diensten. Echter is ook, met name bij twee van de drie financiële dienstverleners, een duidelijke heroriëntatie in de richting van een integraler beleid van informatiebeveiliging zichtbaar. Als redenen voor meer aandacht en vaak ook centralisatie zijn veel gehoorde elementen: de organisaties worden meer en meer afhankelijk van hun netwerken. Deze netwerken worden partieel (geconditioneerd) opengesteld voor partners en/of klanten. Het aantal communicatiekoppelingen neemt toe, alsmede het belang en de kwantiteit van de informatie die hierdoor stroomt. Dit geeft automatisch een enorme druk op informatiebeveiliging. Eén van de experts stelde het als volgt: *"Indien je als organisatie ervoor kiest met meer openheid te handelen en mensen toegang gaat geven tot je domeinen, dan zul je goed op moeten passen dat je de kroonjuwelen buiten bereik houdt"*. Tevens wordt er hard gewerkt aan standaardisering. Zo is ook informatiebeveiliging in diverse organisaties een zeer belangrijk aspect geworden dat integraal in audits is opgenomen. Maar drie van de dertien organisaties gaven aan dat er, naast hun specifieke functie, geen specialistische afdeling voor informatiebeveiliging is. In deze gevallen was niet alleen de verantwoordelijkheid decentraal, maar ook de organisatie van informatiebeveiliging.

Om inzicht te krijgen in hoe er met de bedreigingen op de drie beschreven niveaus van Neumann (1995) omgegaan wordt, is er gevraagd naar het gebruik van diverse toepassingen om deze bedreigingen in te dammen. Allereerst werd er gevraagd naar beveiligingen omtrent de autorisatie van gebruikers van netwerktoepassingen. Het blijkt dat alle experts het eens zijn over de wenselijkheid van regelmatige passwordverandering. Op drie organisaties na is dit ook van toepassing in de gehele organisatie[1]. De overige drie hebben echter nog operationele moeilijkheden om dit uniform door te voeren, maar werken aan het probleem. In dat geval is de organisatie dus bewust onbekwaam en wordt eraan gewerkt om door te schuiven op de

leercyclus. Tevens wordt ingezien dat er afwegingen gemaakt moeten worden over de eisen die aan passwords gesteld worden. Het is bekend dat bij te hoge eisen de techniek omzeild wordt. Dat wil zeggen dat te ingewikkelde passwords bijvoorbeeld met een geel aanplakbriefje op het toetsenbord zitten.

Het volgende punt hierover betrof de zekerheid dat netwerktoepassingen niet bereikbaar zijn indien de werkplek verlaten is[2]. Acht organisaties hebben dit reeds door hun hele organisatie doorgevoerd. Drie organisaties zijn hier mee bezig en één organisatie vond deze toepassing niet noodzakelijk en wenselijk. Een laatste punt was de circulatie van passe-partouts[3] voor toepassingen. Zes experts hebben aangegeven dat de maatregelen dit tot vrijwel nul hebben gereduceerd. Echter gaven zes anderen aan dat dit naar hun mening nog absoluut teveel gebeurt en terug gedrongen dient te worden.

Deze zaken zijn technologisch nog behoorlijk af te dichten, maar zoals een expert terecht opmerkte: *"Je kan je organisatie nog zo geavanceerd beveiligen, maar vergeet je voordeur niet op slot te doen. In de kleine zaken worden de grootste fouten gemaakt. Zo hebben wij ernstige incidenten gehad door medewerkers die in de trein over vertrouwelijke zaken praatten."*. Awareness in de organisatie wordt dan ook als zeer belangrijk, en door enkelen als cruciaal, gezien. Gezien het grote belang van awareness is gevraagd of dit ook naar hun eigen management nodig is. Zeven experts gaven aan dat ook hun eigen (top)management meer bewust dient te zijn. Maar los van awareness gaven de experts ook te kennen dat er altijd rekening gehouden moet worden met werknemers met verkeerde intenties. En werknemers moeten nu eenmaal (eventueel beperkt) toegang hebben tot informatie om te kunnen werken. Procedureel zijn hier wel afdichtingen voor zoals bijvoorbeeld non-disclosure agreements, maar dat is geen garantie dat informatie toch misbruikt wordt. Verschillende experts bleven een duidelijk antwoord schuldig op de vraag hoe hier beter mee omgegaan kan worden. Twee experts daarentegen wilden werken aan betere traceerbaarheid van uitgelekte informatie en één expert kwam met het volgende: *"Eigenlijk zou iedereen zo verstandig moeten zijn om te berekenen hoeveel geld daadwerkelijk verdiend moet worden met fraude om elders voor een langere tijd met een gerust hart te kunnen vertoeven. Bij fraude zal namelijk net zo lang gezocht worden tot de onderste steen boven is. Ik kom dan op een bedrag van ten minste 10 miljoen gulden. Dat haal je met fraude niet zo snel bij elkaar. Daar moet men zich eigenlijk bewust van zijn."*.

Wat betreft preventie van virussen zeiden op één na alle experts dat preventie van nieuwe virussen niet sluitend gemaakt kan worden. De verspreidingstijd van het virus kan sneller zijn dan de update van de beveiliging. Mede hierom zien de meeste experts informatiebeveiliging dan ook als een wedloop. Echter geven slecht zeven experts aan dat hun organisatie op peil ligt wat betreft de informatiebeveiliging. De overig zes geven unaniem aan dat ze nog een inhaalslag te maken hebben, los van het wedloopkarakter. Overigens zien vrijwel alle experts informatiebeveiliging als een waarschijnlijkheidsreductie: het is naïef om te veronderstellen dat de boel 100% op slot kan. Je moet kosten en baten afwegen en dus risicoanalyses maken. Waar dat mogelijk is leg je de drempels hoog. Slechts één expert zei spontaan dat hun systemen en informatie onmogelijk toegankelijk konden zijn voor ongeautoriseerden. Opvallend was hierbij dat deze expert geen andere middelen leek te gebruiken dan alle anderen.

Wat betreft het belang van informatiebeveiliging wordt er per organisatie, en per unit, verschillend over gedacht. Soms wordt meer nadruk gelegd op operationaliteit, integriteit of vertrouwelijkheid. Indien er naar de bedreiging gevraagd werd, waren er zeer diverse antwoorden. De één ziet informatiebeveiliging als noodzaak voor operationaliteit, los van de vraag of er überhaupt bedreigingen zijn. Een ander noemt industriële spionage als de grootste bedreiging. Maar de noodzaak van informatiebeveiliging voor (in meer of mindere mate) operationaliteit en integriteit is door allen aangegeven. Over de noodzaak in verband met vertrouwelijkheid heersen grote verschillen. Iedereen geeft wel aan vertrouwelijke informatie te hebben, maar de één ziet geen gestructureerde bedreiging daarvoor terwijl de ander zelfs de georganiseerde misdaad als een potentiële bedreiging ziet en ook een praktijkvoorbeeld geeft waarin het misging. Hoogenboom (1996) noemt bedrijfsspionage zoiets als een geslachtsziekte: “Velen kunnen ermee besmet zijn, maar niemand wil erover praten”. Niet iedereen ziet gecoördineerde bedrijfsspionage als een issue. Maar zij die er wel over praten geven aan dat dit voor alle multinationals wel degelijk een issue is. Encryptie maakt bedrijfsspionage al moeilijker en opvallend is hier dan ook dat op één na alle experts soms gebruik maken van encryptie voor communicatiedoeleinden. Overigens vindt slechts één expert encryptie een sluitende oplossing. Tien anderen geven aan dat encryptie niet per definitie veilig genoeg is. Er moet kritisch gekeken worden naar zaken zoals sleutellengte. Uiteindelijk is de veiligheid afhankelijk van het belang van de informatie en de duur van vertrouwelijkheid. Elf experts geven ook aan dat encryptie codes deels bekend kunnen zijn bij

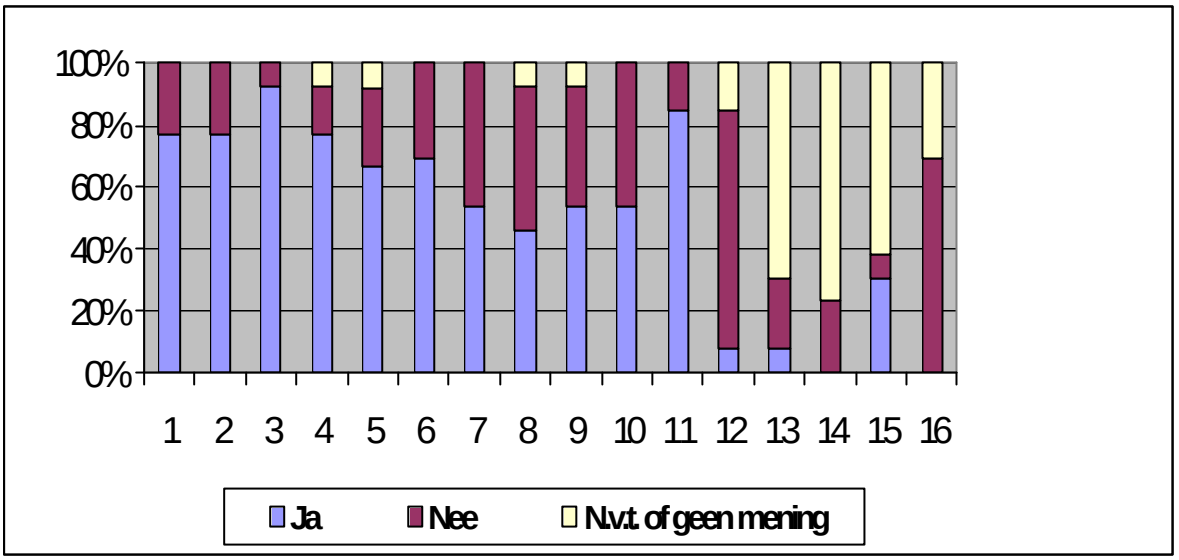
inlichtingendiensten. Verder filosoferend over de veiligheid van encryptie is het begrip 'traffic analysis' besproken. Dit gaat over het gevaar dat er informatie afgeleid kan worden uit het feit dat er op een bepaald moment meer of minder versleutelde boodschappen naar een bepaalde ontvanger gestuurd worden. Tevens kan versleuteling de nieuwsgierigheid naar de inhoud toe doen nemen, wat wellicht leidt tot grotere inspanningen om de versleuteling te ontcijferen[4]. In twee organisaties werd hiermee rekening gehouden. Een derde organisatie was zich er bewust van en overweegt maatregelen. Echter gaven maar liefst negen organisaties aan hier geen rekening mee gehouden te hebben en in die zin waren ze dus onbewust onbekwaam hierin.

Echelon bleek op het moment van vragen bij zeven experts bekend te zijn. Zes experts kenden dit dus niet. Opvallend was dat een enkeling spionage en zeker Echelon probeerde af te doen als 'teveel boekjes gelezen', terwijl vier experts die Echelon niet kenden niet twijfelden aan de technologische mogelijkheid van een dergelijk systeem evenals de zeven experts die wel bekend waren met Echelon. De meerderheid van deze laatste zeven experts zijn tevens van mening dat een dergelijk systeem niet alleen technisch mogelijk is, maar ook operationeel actief is. En er zijn ook uitgesproken meningen over de vraag of dit ook economisch aangewend wordt, hier vindt u er drie: *"Dat een dergelijk spionagenetwerk actief is leidt voor mij geen twijfel, en het zou me ook niet verbazen als dit meer uit economische motieven operationeel is dan uit militaire overwegingen.", "Het [spionage] is een zeer aantrekkelijk middel. Ook een president wordt uiteindelijk grotendeels afgerekend op economische voorspoed. Dus zelfs op het hoogste niveau zal hier de verleiding groot zijn."* en *"Spionage is niks nieuws. Het gebeurt op alle niveaus, dus ook hier. Echter ben ik ook heel benieuwd hoeveel Europa bij de Amerikanen heeft weggesnoept voordat we met een beschuldigende vinger wijzen."* Meerdere experts wilden de Amerikanen niet scherp veroordelen voor deze activiteiten, aangezien het hen niks zou verbazen als economische spionage vanuit Europa ook krachtig zou zijn. Overigens zagen de meeste experts hun eigen organisatie niet als doelwit voor Echelon.

In de Volkskrant verschenen in januari 2001 enige berichten over Echelon. Hierin stond ook dat Hewlett Packard liet weten in verband met angst voor inlichtingendiensten (mobiele) telefonie aan banden te leggen op hoog niveau[5]. Dit begint enigszins paranoïde te klinken, vandaar dat de experts gevraagd is of afraden van telefonie op het hoogste strategische niveau denkbaar is binnen hun organisatie. In negen organisaties is dit het geval.

Opmerkelijk terughoudend waren de experts met praten over toepassing van bug-detectie in en buiten de organisatie. Deels is dit logisch, aangezien het vaak valt onder fysieke beveiliging en daarmee wellicht buiten hun portefeuille. Soms gaven de experts dan ook te kennen dat ze hier niet van op de hoogte waren. Maar meerdere keren kwamen er opvallende antwoorden zoals *"Daar kan ik niet op in gaan dus ik kan ook niet vertellen of ze aangetroffen worden."* en *"Dat ligt buiten mijn bevoegdheid om hierover te praten."*. Wellicht is de volgende, algemenere opmerking van een expert de verklaring hiervoor: *"In het vak weten we allemaal dat informatiebeveiliging een reductie van risico's is. Helemaal uitsluiten kun je zaken niet. En als we over bepaalde zaken naar buiten brengen of dat er wel of niet is, dan denken mensen: 'he, laten we 's wat proberen' en dat willen we voorkomen."*.

In figuur vier is een uitgebreid overzicht te vinden van antwoorden op vragen waar een concreet 'ja' of 'nee' op mogelijk was. Dit geeft enig overzicht over de omgang met informatiebeveiliging in de ondervraagde organisaties. Echter was de reden van het beleid, en daarmee de opinies en visies, belangrijker dan deze concrete antwoorden. De samenvatting van de opinies en visies is daarom reeds hierboven beschreven. Figuur vier is op de volgende bladzijde weergegeven.



1. Is er een specialistische afdeling van meerdere personen die zich met informatiebeveiliging bezig houdt?
2. Vindt regelmatige password-verandering in de volledige organisatie plaats?
3. Wordt er encryptie gebruikt voor communicatie?
4. Is informatiebeveiliging een wedloop?
5. Is er voor gezorgd dat het netwerk op de computer onbereikbaar wordt indien de werkplek verlaten is?
6. Is een verbod op (mobiele) telefonie in uw organisatie denkbaar bij de hoogste classificaties?
7. Ligt informatiebeveiliging op peil (of is er nog een inhaalslag te maken)?
8. Circuleren er passe-partouts voor netwerktoepassingen?
9. Is awareness ook nodig naar uw management?
10. Heeft u van het spionagenetwerk Echelon gehoord?
11. Was het u bekend dat encryptie-codes deels bekend zijn bij de NSA?
12. Is encryptie per definitie voldoende veilig voor uw informatie en communicatie?
13. Bent u bekend met gebruik van 'bug-detectors'[6] door uw organisatie?
14. Zijn er wel eens bugs aangetroffen?
15. Is een bedrijfsschade van 64 miljard gulden in zeven jaar tijd in de Europese Unie door toedoen van Echelon, zoals het EU-rapport 'Interception Capabilities 2000' beweert, laag of hoog (ja=laag ; nee=hoog)?
16. Bent u bekend met actieve bedrijfsspionage door uw eigen organisatie?

Figuur 4: antwoorden concrete vragen

4.5 Conclusie

Terugkerende naar de probleemstelling kan nu een licht geworpen worden op de vierde en vijfde deelvraag. De vierde deelvraag luidt: *"Wat is de perceptie ten opzichte van de veiligheid van bedrijfseconomische informatie van Nederlandse transnationale organisaties?"*. De perceptie van de experts is na deze beschrijving van de interview-resultaten behoorlijk in beeld gebracht. Figuur vier voegt daar nog een grafisch overzicht aan toe. De vijfde deelvraag luidt: *"Zijn de maatregelen voor beveiliging van informatie in Nederlandse transnationale organisaties afdoende gezien de informatiebedreiging?"*. Uit de interview-resultaten is duidelijk geworden dat er niet gesteld kan worden of de maatregelen afdoende zijn. De organisaties komen namelijk uit verschillende branches en hebben daarom een verschillende focus op de deelaspecten van informatiebeveiliging. Tevens zien de meeste experts informatiebeveiliging als een waarschijnlijkheidsreductie. De mate van reductie van de waarschijnlijkheid wordt bepaald aan de hand van kosten/baten afwegingen en risicoanalyses. Een objectieve beoordeling van de genomen maatregelen is dus niet mogelijk indien de onderzoeker niet bekend is met de (financiële) afwegingen die achter de schermen meespelen. Kijken naar specifieke maatregelen zegt dus niet genoeg, maar de redenen voor de genomen maatregelen wel. Deze zeggen ons iets over het bewustzijn van de aanwezige bedreiging. Pas als er bewustzijn van de bedreiging is, kunnen er realistische kosten/baten afwegingen gemaakt worden.

Het volgende hoofdstuk gaat daar nog dieper op in door de theorie tegenover de praktijk te zetten. Daarmee wordt dan de centrale vraagstelling van deze scriptie beantwoord.

---

[1] Passwordverandering kan automatisch door de computer worden afgedwongen. De computer herinnert de gebruiker er aan dat deze zijn password moet veranderen.
[2] Onbereikbaarheid van netwerktoepassingen kan onder andere bereikt worden door locks op screensavers of door automatisch afslaan van het netwerk na een ingestelde tijd indien er geen activiteit op de toepassing is.
[3] Met een passe-partout wordt een uniek password bedoeld dat ongewenst door meerderen gebruikt wordt. Simpel gezegd dus of werknemers op de hoogte zijn van elkaars passwords.
[4] Traffic analysis kan goed geïllustreerd worden aan de hand van het volgende voorbeeld: indien er tien enveloppen verstuurd worden en op één staat met grote rode letters 'vertrouwelijk', dan is wellicht het risico het grootst dat men de envelop waar vertrouwelijk opstaat nader zal onderzoeken.
[5] Volkskrant 26 januari 2001, "Bedrijven niet bang voor Big Brother".
[6] Een bug-detector is een apparaat waarmee afluisterapparatuur opgespoord wordt.

H5, CONCLUSIES

5.1 Introductie

Om de probleemstelling van deze scriptie zo goed mogelijk te kunnen beantwoorden, is in paragraaf 1.2 de probleemstelling opgesplitst in vijf deelvragen. Deze deelvragen zijn vervolgens in het verloop van de scriptie aan de orde gekomen. Met behulp van de daaruit voortgekomen informatie, wordt in dit hoofdstuk de probleemstelling beantwoord. De kern van de probleemstelling is de centrale vraagstelling: *"In hoeverre is er bedreiging voor bedrijfseconomische informatie, en zijn Nederlandse transnationale organisaties zich bewust van dit risico?"*. De volgende paragraaf behandelt dit uitgebreid.

Een probleem stellen is één. Een tweede is om zinvolle suggesties te opperen die de omgang met het probleem vergemakkelijken. In deze scriptie wil ik mij niet beperken tot slechts het opmerken van een probleem. Vandaar dat ik de problematische kwesties, die voort komen uit dit onderzoek, nader analyseer. Tevens poog ik zinvolle handreikingen te geven voor de omgang met de bedreiging van informatie. Verder vindt u in paragraaf 5.5 een globale visie over het probleemgebied.

5.2 Beantwoording probleemstelling

De centrale vraag in de probleemstelling richt zich op de bedreiging voor de bedrijfseconomische informatie, en het bewustzijn van deze bedreiging bij Nederlandse transnationale organisaties. De bedreiging en beveiliging van informatie zijn reeds theoretisch en praktijkgericht benaderd. Voor het beantwoorden van de probleemstelling kijken we daarom naar de overeenkomsten en verschillen tussen de theorie en de praktijk. Hiermee wordt het beeld van de werkelijke bedreiging en het bewustzijn daarvan compleet gemaakt.

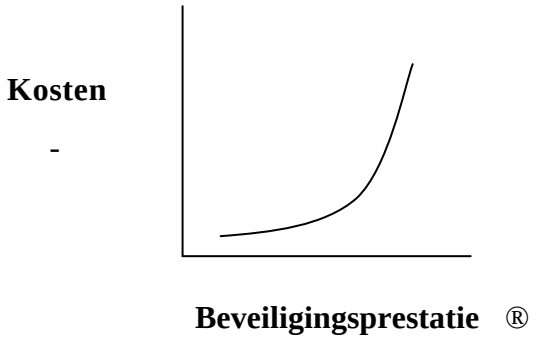
In hoofdstuk twee is geschreven over de ontwikkelingen in de communicatie-infrastructuur en het toenemende belang van informatie. Tezamen is gebleken dat dit een sterk toenemende bedreiging van informatie met zich meebrengt. Uit de interviews werd duidelijk dat de experts zich zeer bewust zijn van deze ontwikkelingen. Zij onderschrijven deze ontwikkelingen dan

ook. Tevens geven ze, weliswaar in verschillende bewoordingen, de operationaliteit, integriteit en vertrouwelijkheid als belangrijkste redenen voor informatiebeveiliging aan. De perceptie van de mate van de informatiebedreiging verschilt wel per expert. Deels kan dit verklaard worden door het feit dat de experts uit verschillende organisaties komen. Hierdoor ligt hun focus anders. Per organisatie verschilt immers het belang van operationaliteit, integriteit en/of vertrouwelijkheid van informatie. Hierdoor hebben ontwikkelingen op het gebied van informatiebedreiging per organisatie een andere relevantie. Mede daardoor is de omgang met deze bedreiging ook verschillend. Maar het verschil in de perceptie van de mate van de informatiebedreiging komt niet alleen voort uit het feit dat ze bij verschillende organisaties werken. Er bestaat weliswaar een consensus over de toenemende gevoeligheid van informatie door de immer complexer wordende infrastructuur voor communicatie en informatie, maar het bewustzijn hiervan en de scherpte van visie hierover verschilt per expert. Een enkeling wist bijvoorbeeld niet wat een worm is, en dat een worm door de aanvaller op afstand door computersystemen genavigeerd kan worden. Echelon illustreerde ook de zeer duidelijke verschillen in visies, los van de vraag of een dergelijk systeem ook daadwerkelijk een bedreiging voor hun organisatie zou kunnen zijn. Zoals ook beschreven in hoofdstuk vier is gebleken dat een enkeling Echelon afdoet als een overload aan James Bond-films, terwijl veel anderen er niet aan twijfelen dat een dergelijk spionagenetwerk bestaat en wellicht ook economisch gebruikt wordt. Toch lijkt de informatiebeveiliging bij de ondervraagde organisaties voornamelijk te staan of te vallen met de bewustwording (awareness). Want hoewel visies op de bedreigingen en beveiliging verschilden, bleek met name de effectiviteit van het beleid af te hangen van de mate waarin de informatiebeveiliger de organisatie weet te doordringen van het belang ervan.

5.3 Problematische kwesties

Uit de resultaten van de interviews komen een paar problematische kwesties naar voren. Bij een aantal zaken lijkt toch een vorm van onbewustheid te zijn. Dat blijkt onder andere uit de verschillende opinies in hoofdstuk vier. Maar los daarvan is alleen bewustwording ook geen sluitende oplossing voor de beveiliging van informatie. Informatiebeveiliging kan namelijk als een waarschijnlijkheidsreductie gezien worden. Hoe verder de risico's gereduceerd worden, hoe meer de kosten onevenredig oplopen (zie figuur 5). Er moeten dus afwegingen

gemaakt worden hoe ver gegaan dient te worden met de beveiliging. Tevens lijkt een waterdichte beveiliging niet te bestaan.



Figuur 5: kostentoename bij waarschijnlijkheidsreductie

Een tweede kwestie is de beveiliging tegen nieuwe virussen. Vrijwel alle experts gaven te kennen dat het onmogelijk is om gewapend te zijn tegen een nieuw virus. Weliswaar kan binnen korte tijd de beveiliging aangepast worden, maar dan kan het virus reeds schade aangericht hebben.

In hoofdstuk twee (§ 2.2) is aangetoond hoe dramatisch de techniek, toegenomen verbondenheid en de digitalisering een foutieve omgang met informatie kan faciliteren. Het ongewenst inzien, dupliceren en manipuleren van informatie is veel gemakkelijker geworden. Hierdoor is er met name intern een grotere bedreiging ontstaan. Dit probleem werd erkend door de experts, maar duidelijke antwoorden op deze kwestie zijn de meesten schuldig gebleven. Tevens maken bepaalde schakels de ketting van beveiliging zwak. Zo zijn laptops gevoelig omdat ze makkelijk gestolen kunnen worden, en blijven passwords circuleren of opgeschreven worden.

5.4 Handreikingen

Sinds kort is er een ISO-normering voor informatiebeveiliging. Dit is de ISO 17799 normering. Deze is afgeleid van de British Standard Code of Practice for Information Security, ook wel de BS7799 genoemd, en is de voorloper geweest van de industriestandaard.

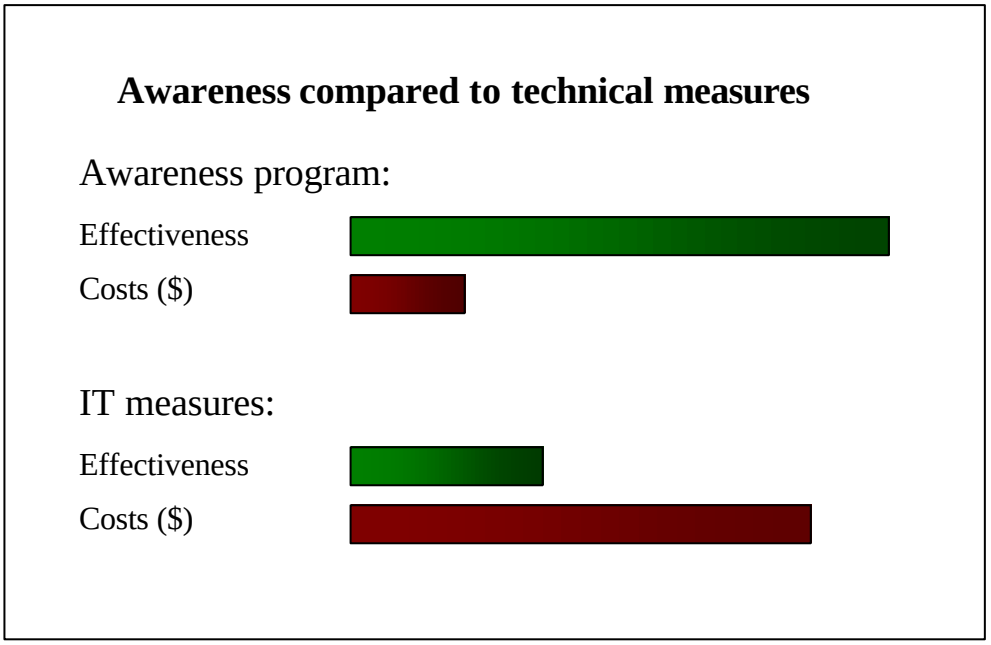
In principe is de BS7799 een complete leidraad voor informatiebeveiliging met uitgangspunten die op elke bedrijfstak van toepassing zijn. Dit kan een goede inspiratie of uitgangspunt voor beleid op het gebied van informatiebeveiliging zijn. Wie een stap verder gaat en de mogelijkheid heeft, kan kiezen voor certificering volgens de ISO-norm. In Nederland zijn KPMG en KEMA bevoegd voor certificering volgens de ISO 17799-norm.

Wat betreft de 'zwakke schakels' in de informatiebeveiliging, zoals laptops en passwords, zou de oplossing gevonden kunnen worden in het wegnemen van de redenen voor gevaarlijke omgang. Zoals enkele experts mij zeiden: *"Als de risicovolle elementen niet vermeden kunnen worden, neem daar dan de noodzaak tot foutief gedrag weg"*. Dus zolang er nog met passwords gewerkt moet worden, neem dan de noodzaak tot foutief gedrag ermee weg. Zorg daarom dat de communicatielijnen met de systeembeheerder kort zijn, zodat er snel een nieuw password beschikbaar is indien gewenst. Het denken in 'noodzaak wegnemen' is overal toepasbaar. Bij laptops bijvoorbeeld kan gedacht worden aan toepassingen die ervoor zorgen dat persoonlijke informatie op het netwerk overal beschikbaar is. Een IP Dial-in-Service is daar een voorbeeld van[1]. De noodzaak om informatie op de laptop op te slaan is dan weg. Bijkomend voordeel is dat de gebruiker minder indringend bewust gemaakt hoeft te worden om deze toepassingen te gebruiken. Deze toepassingen nemen namelijk niet alleen de noodzaak weg, maar komen tevens de gebruiker in zijn eigen wensen tegemoet. Hierdoor is het waarschijnlijker dat de gebruiker deze toepassingen, afgezien van de motivatie voor beveiliging, gebruiken zal. Dus noodzaak wegnemen is een interessante benadering, en extra effectief indien de gebruiker (een deel van) zijn eigen wensen ermee in vervulling ziet gaan.

Zoals reeds beschreven kan informatiebeveiliging benaderd worden als een waarschijnlijkheidsreductie. Hierbij is een kosten/baten afweging van toepassing. Echter kan deze afweging pas gemaakt worden na een risicoanalyse. Daarom pleit ik voor het integraal invoeren van risicoanalyses op het gebied van informatiebeveiliging. Overigens is dit standaard opgenomen in de BS7799.

Een bekende discussie is in hoeverre de techniek informatiebeveiliging kan afdichten. Het probleem is dat indien het technische muurtje te hoog opgetrokken wordt, eromheen gelopen zal worden. Een voorbeeld hiervan is de eis die aan een password wordt gesteld. Als een password uit een moeilijke combinatie van cijfers en letters moet bestaan, is vervolgens de kans groot dat het password op een geel briefje onder het toetsenbord terug te vinden is. Dit geeft eens temeer het grote belang van awareness bij de gebruikers aan. Eén expert heeft hier een interessante ervaring over uitgesproken. Voor hem is gebleken dat awareness creëren bij

de gebruikers voordeliger is dan technologische maatregelen (zie figuur 6). Echter werd daarbij opgemerkt dat awareness meer tijd en moeite kost dan technologische maatregelen.



Figuur 6: kosten vs. effectiviteit awareness en techniek

Uit deze scriptie is ook gebleken dat de techniek, toegenomen verbondenheid en de digitalisering informatielekkage dramatisch faciliteren. In dit opzicht schiet mijns inziens de techniek tekort. Ontwikkelingen in de richting van digitale watermerking lijken zeer welkom. Hiermee kan de informatielekkage weliswaar niet direct voorkomen worden, maar wel worden getraceerd. Met goede traceerbaarheid kan niet alleen de schade verhaald worden, maar er gaat ook een preventieve werking van uit. Wellicht kan het Secure Digital Music Initiative (SDMI)[2] als inspiratie dienen voor geavanceerdere ontwikkelingen voor toepassingen in onder andere databases.

Monitoring van netwerken moet ook veel aandacht verdienen. Met verfijnde monitoring kunnen ongewenste of ongebruikelijke informatiestromen gedetecteerd worden. Zeker in het geval van onbekende virussen biedt dit enige oplossing. Een virus verspreidt zich immers vaak door zich automatisch aan zoveel mogelijk ontvangers door te sturen. Zodra er hierdoor een ongebruikelijke informatiestroom op gang komt, kan er besloten worden tijdelijk

toepassingen stil te leggen totdat de oorzaak en de remedie duidelijk zijn. Dit leidt uiteraard tot enige operationele schade, maar in totaal beperkt het de volledige schade doordat verdergaande infectering en eventuele destructie voorkomen wordt. Tevens kan verbeterde monitoring van netwerken meer informatielekkage detecteren. Voor verfijning hiervan is nog een flinke weg te gaan, maar een focus hierop lijkt me niet onwenselijk. Monitoring is een soort technische variant op sociale controle. Want door sociale controle kan vreemdsoortig gedrag opgemerkt worden. Monitoring doet ditzelfde, maar dan technologisch op het netwerk.

Als afsluiting van deze paragraaf wil ik nog het volgende aanhalen. Het komt voor dat de ene organisatie informatiebeveiliging procedureel prachtig heeft afgedicht, terwijl een andere organisatie bijvoorbeeld zeer veel aan preventie doet. Maar samenhang in de aanpak lijkt cruciaal. Daarom wil ik nogmaals enkele van de genoemde handreikingen nader beschouwen. In het begin van deze paragraaf schreef ik over het wegnemen van de noodzaak van risicovolle handelingen. Dat is een vorm van preventie. Het feit dat informatiebeveiliging een waarschijnlijkheidsreductie is, vraagt tevens om detectie. Het beschreven ‘monitoren van netwerken’ is een vorm van detectie. De wenselijkheid van digitale watermerking komt voort uit de vraag naar traceerbaarheid. Wanneer deze middelen niet afdoende zijn rest er nog een optie: schadebeperking. In die zin zou ik de kern van beleid op het gebied van informatiebeveiliging als volgt willen samenvatten: preventie, detectie, repressie en schadebeperking. Indien deze vier elementen in de bedrijfsvoering in deze volgorde systematisch worden toegepast, moet dat leiden tot een effectieve beleidsmatige aanpak van informatiebeveiliging.

5.5 Overall

Nu de interpretatie tussen theorie en praktijk beschreven is, alsmede de problematische kwesties en de handreikingen, dient ondanks die punten geschreven te worden dat het belangrijkste ingrediënt voor succesvolle informatiebeveiliging bij alle geïnterviewde organisaties aanwezig is: aandacht voor het onderwerp. Echter kan dit zeker niet van menig andere organisatie gezegd worden. Uit eigen observaties en werkervaringen in andere organisaties blijkt dat er in vele organisaties geen enkel bewustzijn is over informatiebedreiging. Hierdoor ontbreekt zelfs de geringste aandacht voor dit onderwerp. En ook al hebben vele organisaties bij lange na niet de schaalgrootte om met

informatiebeveiliging om te gaan zoals de geïnterviewde organisaties dat doen, wil dat niet zeggen dat informatiebeveiliging genegeerd moet worden. Bewustzijn van informatiebedreiging is op elk niveau van belang, en beleid kan op elk niveau worden toegespitst. Laat het bewustzijn er komen alvorens het zich door incidenten onvermijdelijk zal opdringen.

Wat betreft de intentionele informatiebedreiging wil ik zeggen dat dit absoluut ontoelaatbaar is. Over hackers worden discussies gevoerd of zij nu 'cybercriminelen' zijn of dat zij juist op onschuldige wijze ons met de neus op de feiten drukken op het gebied van informatiebeveiliging. In deze discussie wil ik mij niet mengen, maar daar waar hackers voor economisch gewin opereren of waar organisaties en overheden zaken als spionage aanwenden voor economisch gewin vind ik dat een harde lijn getrokken moet worden: dit kan niet getolereerd worden en moet koste wat het kost aan het licht gebracht worden. In die zin wil ik een sterke kanttekening plaatsen bij het beleid van de Nederlandse overheid op dit gebied. Zij moet zich niet verhullen in vaagheden, maar actie ondernemen. En wat betreft Echelon lijkt zij een tegengesteld beleid te voeren. In plaats van bezinning op beschermende maatregelen lijkt de overheid, gesteund door Europese wetgeving de weg vrij te maken voor deelname in dit netwerk of voor het oprichten van een eigen soortgelijk netwerk. Sinds het bekend worden van Echelon zijn wetten zoals de Telecommunicatiewet aangenomen, die informatie afluisteren alleen maar faciliteert[3]. Ook weigerde de voorzitter van de Kamercommissie voor de inlichtingen- en veiligheidsdiensten, de heer Melkert, deelname aan onderzoek van het Europees Parlement naar Echelon. Hiervoor liet hij tijdens de hoorzitting in Brussel van 20 november 2000 verstek gaan. Als officieel standpunt bracht de Nederlandse regering naar buiten niets te weten van een Amerikaans netwerk, dat onder de naam Echelon zou opereren. In januari 2001 erkende de Nederlandse regering het bestaan van het netwerk Echelon. Daarnaast werd in het najaar van 2000 gedebatteerd in de kamer over een heroriëntatie van de BVD en het overheidsbeleid naar aanleiding van Europese rapporten over Echelon. Opties zoals actieve bedrijfseconomische spionage door de overheid werden genoemd. Los van de vraag of dit überhaupt haalbaar is, is het niet wenselijk. Ook in de gesprekken met de dertien organisaties is mij te kennen gegeven dat niemand hiervan gediend is.

Tot slot bleek uit de interviews dat de media moeten uitkijken wie zij aan de schandpaal der informatiebedreiging nagelen. De berichten die ons de laatste maanden hebben bereikt over incidenten blijken totaal geen representatief beeld te geven van welke incidenten daadwerkelijk plaats vinden. Allereerst weten de media maar een selectief deel van de

incidenten bloot te leggen. Vervolgens worden deze incidenten uit hun verband getrokken en de betrokken organisaties worden onterecht diep door het slijk getrokken. Dit meld ik met name aangezien zich onder de respondenten enkele van dergelijke organisaties bevonden. En uit de interviews bleek nu juist dat de informatiebeveiliging van deze organisaties absoluut niet onder doet voor die van de overige organisaties, eerder andersom.

5.6 Besluit

Nu alles gezegd lijkt te zijn besluit ik deze scriptie graag met de opmerking dat het schrijven hiervan mij een genoegen is geweest. Ik heb veel kennis kunnen opdoen, toetsen, toepassen en beschrijven. Zonder de uitgebreide gesprekken met de experts was dit niet mogelijk geweest: dank aan allen. In het bijzonder wil ik de ING, KLM en Shell noemen daar zij mij uitgebreid van extra informatie voorzagen en tevens uitgebreide presentaties gaven. Mijn hoop is dat deze scriptie alle experts hier ook wat voor terug geeft. Mocht dit niet het geval zijn, laat ons dan voldoening vinden in de gedachte dat deze scriptie in elk geval voor andere organisaties, studenten en geïnteresseerden een bron van informatie en inspiratie mag zijn. Aangezien ik deze scriptie veel meer uit interesse heb geschreven dan als afstudeeropdracht, ben en blijf ik altijd open staan voor opinies, visies en kritiek op het beschrevene. Vertel me wat u als lezer ervan vond op Marcel.vanOers@zonnet.nl. Ik zie uw reactie met genoegen tegemoet! Tot ziens in de digitale wereld.

[1] Een IP Dial-in-Service maakt het mogelijk om vanuit een willekeurige lokatie in te kunnen bellen op een netwerk.
[2] SDMI is een werkgroep die voor de muziekindustrie digitale watermerking ontwikkelt. Hiermee wil de muziekindustrie online verkoop van muziek mogelijk maken, alsmede illegaal kopiëren van deze muziek onmogelijk maken.
[3] In hoofdstuk twee is al kort toelichting gegeven op de Telecommunicatiewet. Meer informatie vindt u op: http://www.nrc.nl/W2/Nieuws/1998/07/01/Med/telecomwet.html.

L i t e r a t u u r l i j s t

Alleyne, M. (1995), *International Power and International Communication*. Oxford: MacMillan.

Andersson, Å. & Strömquist, U. (1988), 'The emerging C-Society.' In Batten, D. & Thord, R. (red.), *Transportation for the Future*. Berlijn: Springer-Verlag.

Attewell, P. (1996), 'Information Technology and the Productivity Challenge.' In: Kling, R. (red.), *Computerization and Controversy*. San Diego: Academic Press.

Bowyer, K. (1996), *Ethics and Computing, Living Responsibly in a Computerized World*. Los Alamitos (California): IEEE Computer Society Press.

Castells, M. (1996), *The Rise of the Network Society*. Cambridge Ma: Blackwell Publishers.

Cools, M. (1996), 'Informatiebeveiliging en industriële spionage.' In: Cools, M. & Hoogenboom, A. (red.), *Kwetsbare kennis, over bedrijfseconomische spionage en informatiebeveiliging*. Alphen aan den Rijn: Samson.

Cools, M. & Hoogenboom, A. (1996), *Kwetsbare kennis, over bedrijfseconomische spionage en informatiebeveiliging*. Alphen aan den Rijn: Samson.

Dubin, P. (1962), *Human Relations in Administration*. Englewood Cliffs (NJ): Prentice-Hall.

Franzen, G. & Bouwman, M. (1999), *De mentale wereld van merken*. Alphen aan den Rijn: Samsom.

Fulk, J. & DeSanctis, G. (1995), 'Electronic Communication and Changing Organizational Forms.' In: *Organization Science*, Vol. 6, pp. 337-347.

Hager, N. (1996), *Secret Power: New Zealand's role in the International Spy Network*. Nelson: Craig Potton.

Hamelink, C. (1999), *Digitaal fatsoen: Mensenrechten in Cyberspace*. Amsterdam: Boom.

Hoogenboom, A. (1996), 'Waardevolle en kwetsbare kennis: over financieel-economische informatieposities.' In: Cools, M. & Hoogenboom, A. (red.), *Kwetsbare kennis, over bedrijfseconomische spionage en informatiebeveiliging*. Alphen aan den Rijn: Samson.

Morton, M. (1996), 'How information technology can transform organizations.' In: Kling, R. (red.), *Computerization and Controversy*. San Diego: Academic Press.

Naisbitt, J. (1982), *Megatrends – Ten new directions transforming our lives*. New York: Warner.

Neumann, P.G. (1995), *Computer Related Risks.* New York: Addison-Wesley.

Ouwersloot, H. (1994), *Information and communication from an economic perspective.* Amsterdam: Vrije Universiteit.

Raaij, W. & Antonides, A. (1997), *Consumentengedrag: een sociaal-wetenschappelijke benadering.* Utrecht: Lemma.

Sproull, L. & Kiesler, S. (1991), 'Beyond efficiency.' In: Sproull, L. & Kiesler, S. (red.), *Connections: New ways of working in the networked organization*. Cambridge: M.I.T. Press.

Sontag, S. & Drew, C. (1998), *Blind man's bluff: the untold story of American submarine espionage*. New York: Public Affairs.

Spaans, J. (1998), *De gecontroleerde samenleving*. Hoogeveen: Spaans.

Walton, R. (1989), 'The Relationship between Information Technology and Organization – Crucial, Complex and manageable.' In: Walton, R., *Up and Running. Integration Information Technology and the Organization.* Boston: Harvard Business School Press.

BIJLAGE 1

"Opzet interviews"

Algemene informatie

De doelstelling van de interviews is om inzicht te verwerven in de perceptie van informatiebedreiging bij Nederlandse transnationale organisaties. Hiervoor is met experts op het gebied van informatiebeveiliging van dergelijke organisaties gesproken. Zij hebben diverse vragen over informatiebedreiging en informatiebeveiliging voorgelegd gekregen. Deze vragen zijn niet voldoende om een volledig beeld te vormen over de (kwaliteit van) informatiebeveiliging van de organisatie, echter is dat ook niet de pretentie. Het directe antwoord op de vraag is namelijk niet cruciaal, belangrijker is de reden van het antwoord. Bijvoorbeeld: uit het antwoord op de vraag of men aan automatische password-wijziging doet is weinig af te leiden. Er kunnen immers goede redenen zijn om dit wel, dan wel niet te doen. Daarom is er dieper door gevraagd naar de reden om dit wel of niet te doen. Hiermee kan beoordeeld worden of dergelijke keuzes zijn gemaakt op basis van bewuste en reële afwegingen. Met verschillende vragen over verschillende facetten van informatiebeveiliging en –bedreiging valt er op deze wijze een aardig beeld te vormen over de perceptie van de risico's. Verder is er overige informatie verzameld: de sector waar de organisatie deel van uitmaakt en de leeftijd, nationaliteit en het geslacht van de expert. Alle interviews hebben tussen januari en april 2001 plaats gevonden. Gedetailleerde informatie over welke organisaties om welke redenen zijn geïnterviewd, over wie de experts zijn, over het interview en over de vragen zelf zijn te vinden in deze bijlage.

De organisaties

Gezien de centrale vraagstelling van dit onderzoek zijn de volgende criteria van belang bij de selectie van de organisaties. De organisatie dient Nederlands te zijn, significant transnationaal te opereren en bereid te zijn deel te nemen aan dit onderzoek. Dit onderzoek biedt maximaal ruimte voor vijftien interviews. Om inzicht te krijgen in een eventueel verschil van visie tussen commercieel georiënteerde organisaties en niet-commercieel georiënteerde organisaties zijn er drie niet-commerciële organisaties geselecteerd. Vervolgens zijn de meest bekende en grote organisaties geselecteerd die aan de criteria voldeden. Dit zijn:

Commercieel:	AbnAmro, Akzo-Nobel, ASML, DSM, ING, KLM, KPN, Philips, Rabobank en Shell.
Non-commercieel:	Ministerie van Economische Zaken, Nationaal Bureau voor Verbindingsbeveiliging (NBV) als onderdeel van de Binnenlandse Veiligheidsdienst (BVD), en de Universiteit van Amsterdam (UvA).

De volgende organisaties hebben geen deel genomen aan het onderzoek.

Weigeraars:	Ahold (reden: over beveiliging wordt niet met externen gesproken) en UPC (reden: te druk).
Overig:	Heineken en Unilever: in de beschikbare tijd is er geen datum gevonden waarop zowel de interviewer als de expert tijd konden maken.

De experts

Binnen de betreffende organisaties zijn de interviews voorgelegd aan een expert op het gebied van informatiebeveiliging. Bij voorkeur de hoogst mogelijke expert in de organisatie. Bij vele organisaties is dit gelukt en waar dat niet is gelukt is gesproken met experts die wat betreft positie nabij een dergelijk persoon staan waardoor het kennisniveau van het probleemgebied hoog genoeg is. Er moet dus gedacht worden aan mensen die op het gebied van informatiebeveiliging beleidsmatig hoofd zijn voor danwel de gehele (!) organisatie, of een groot deel daarvan. De experts worden in dit onderzoek anoniem gehouden, aangezien dat vaak gewenst is.

Het interview

De interviews zijn open gesprekken met latente sturing door de interviewer. Met een open benadering verzamelt de interviewer zoveel mogelijk informatie over het onderwerp van dit onderzoek, met op de achtergrond het leidmotief dat er sowieso in het gesprek antwoorden worden gegeven op een aantal elementaire vragen van de interviewer. Tijdens de interviews loopt er een cassette mee zodat de interviewer alle concentratie op het gesprek kan hebben, en tevens zeker is van het feit dat de informatie correct wordt vastgelegd.

De vragen

De elementaire vragen zijn:

1. Is er een specialistische afdeling van meer dan één persoon die zich met informatiebeveiliging bezig houdt?
2. Vindt regelmatige password-verandering in de volledige organisatie plaats?
3. Wordt er encryptie gebruikt voor communicatie?
4. Is informatiebeveiliging een wedloop?
5. Is er voor gezorgd dat het netwerk op de computer onbereikbaar wordt indien de werkplek verlaten is?

6. Is een verbod op (mobiele) telefonie in uw organisatie denkbaar bij de hoogste classificaties?
7. Ligt informatiebeveiliging op peil (of is er nog een inhaalslag te maken)?
8. Circuleren er passe-partouts voor netwerktoepassingen?
9. Is awareness ook nodig naar uw management?
10. Heeft u van het spionagenetwerk Echelon gehoord?
11. Was het u bekend dat encryptie-codes deels bekend zijn bij de NSA?
12. Is encryptie per definitie voldoende veilig voor uw informatie en communicatie?
13. Bent u bekend met gebruik van 'bug-detectors' door uw organisatie?
14. Zijn er wel eens bugs aangetroffen?
15. Is een bedrijfsschade van 64 miljard gulden in zeven jaar tijd in de Europese Unie door toedoen van Echelon, zoals het EU-rapport 'Interception Capabilities 2000' beweert, laag of hoog?
16. Bent u bekend met actieve bedrijfsspionage door uw eigen organisatie?

Opinies en visies over de volgende deelvragen zijn geïnventariseerd:

1. Hoe steekt de informatiebeveiliging beleidsmatig in elkaar?
2. Waar komt de bedreiging van informatie vandaan?
3. In hoeverre wordt de bedreiging voor informatie en communicatie door opponenten gecoördineerd?
4. Hoe moet er met onzichtbare facetten, zoals imagoschade maar ook informatielekkage, van de informatiebedreiging omgegaan worden?
5. In hoeverre is informatie te beveiligen?
6. Wat zijn de invloeden van de ICT-revolutie geweest en wat staat ons nog te wachten?
7. Hoe moeten we de rol van overheden in informatiebedreiging en –beveiliging zien?

Al deze vragen zijn dus niet opgesomd behandeld, maar in een open gesprek ter sprake gekomen waarbij ik op de elementaire vragen een duidelijk ja of nee wilde horen en over de overige vragen opinies en visies wilde horen. Tevens leveren zowel de elementaire vragen als de deelvragen in een open gesprek meer interessante en relevante informatie op. De expert krijgt daarom in het interview alle ruimte om 'extra' informatie te geven. Dit leverde ook zeer veel extra en interessante informatie op. Tevens liepen hierdoor vele interviews behoorlijk uit. Volgens de planning behoorde een interview 45 minuten te duren, maar vrijwel alle gesprekken hebben zich dusdanig interessant ontwikkeld dat ze enorm uitliepen. Eén keer liep het zelfs uit tot 2,5 uur (!) en nog hadden we het gevoel veel gespreksstof over te hebben.