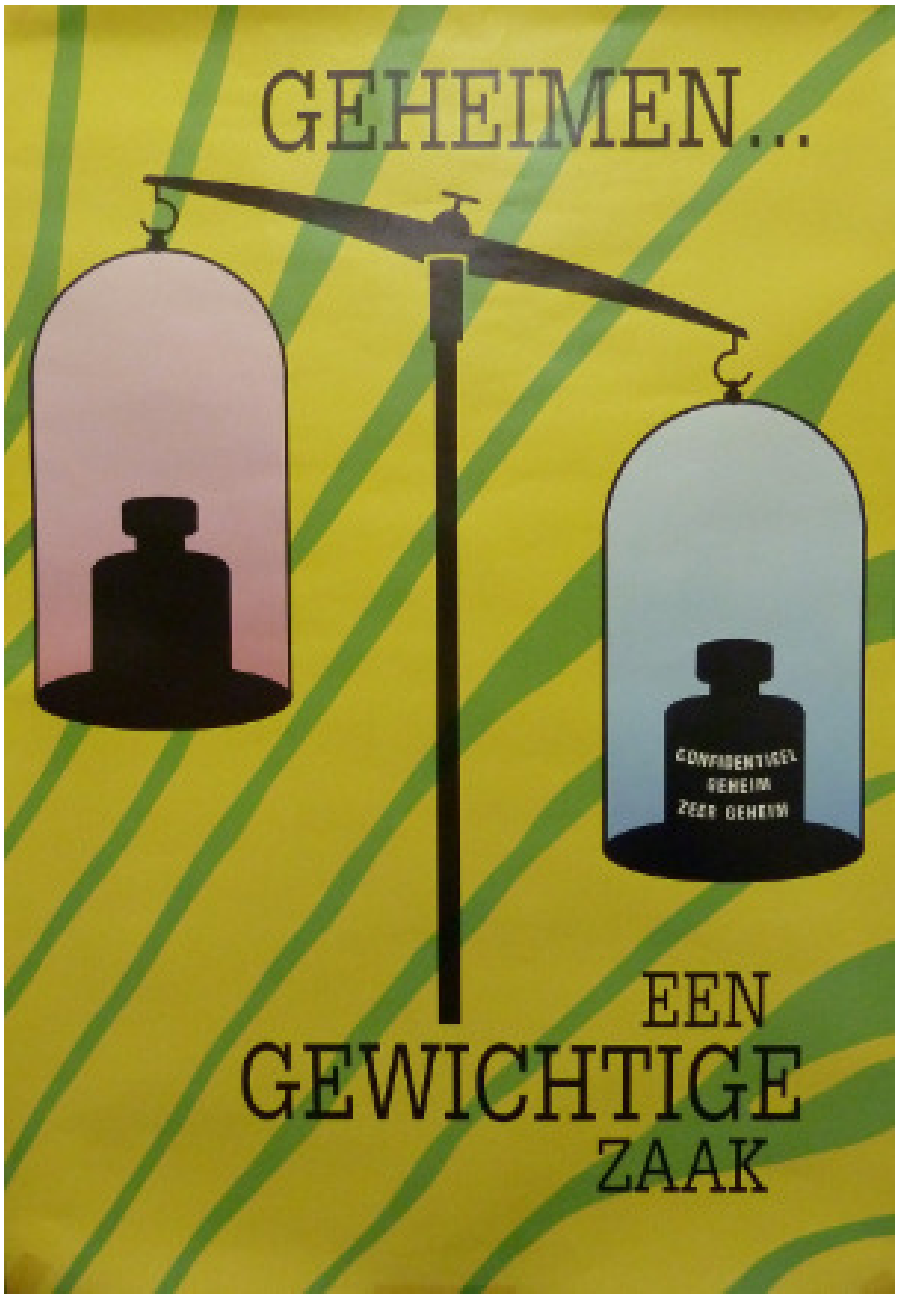
GEHEIMen, LEKker belangRIJK

Een onderzoek naar intentionele en verwijtbare compromittering van gerubriceerde en gevoelige informatie binnen de Rijksoverheid



Masterthesis mr. J.H. Maat
Master of Security Science & Management
Delft TopTech, Technische Universiteit Delft
Leergang 2009-2011

GEHEIMen, LEKker belangRIJK

Een onderzoek naar intentionele en verwijtbare compromittering van gerubriceerde en gevoelige informatie binnen de Rijksoverheid

Masterthesis mr. J.H. Maat
Master of Security Science & Management (MSSM)
Delft TopTech, Technische Universiteit Delft
Leergang 2009-2011

Begeleider:	Prof. dr. M.J. van den Hoven, hoogleraar morele filosofie, Technische Universiteit Delft
Examencommissie:	Prof. dr. B.J.M. Ale, (voorzitter) Hoogleraar Veiligheidskunde Technische Universiteit Delft en programmadirecteur MSSM; Prof. mr. dr. E.F. ten Heuvelhof, Hoogleraar Bestuurskunde Technische Universiteit Delft; Dhr. A.J. Jonge Vos, Nationaal Coördinator Bewaking en Beveiliging; Mr. B.J. Swagerman, Vice President KLM Security Services; Mr. M. van Vianen, (vm.) Shell Manager Global Security; Mw. H.J. Balledux-Vercauteren, Project Manager Delft TopTech (secretaris)
Examendatum & -locatie:	25 mei 2011, Science Centre Technische Universiteit Delft, Mijnbouwstraat 120 te Delft

Het onderzoek is afgesloten op 25 april 2011

Deze masterthesis is op persoonlijke titel geschreven. De inhoud geeft niet noodzakelijkerwijs het standpunt van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties weer.

Informatie over verkrijgbaarheid: http://nl.linkedin.com/in/johrimaat of http://www.johrimaat.nl

Afbeelding omslag:
Bewustwordingsposter Rijksoverheid over omgang met staatsgeheimen uit Koude Oorlog, foto auteur

INHOUD

Tabellen en figuren

Casussen

VOORWOORD

Security kan heel beknopt gedefinieerd worden als de beveiliging tegen opzettelijke inbreuken op veiligheid. Een extreem voorbeeld hiervan is terrorisme. Maar ook inbraken, spionage, zinloos geweld op straat, integriteitsschendingen, het kraken van computersystemen en sabotage zijn voorbeelden van security vraagstukken.

Deze vraagstukken vormen het uitgangspunt voor de opleiding Master of Security Science & Management (hierna: MSSM), verzorgd door Delft TopTech van de Technische Universiteit Delft. In deze executive master leren security managers hoe zij bedreigingen van veiligheid kunnen identificeren, oorzaken kunnen onderscheiden, tegenmaatregelen kunnen ontwerpen en onderbouwde besluiten kunnen nemen om security te managen.

Ter afronding van de opleiding MSSM – leergang 2009-2011 – is deze masterthesis geschreven. Omdat ik in mijn functie bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (hierna: BZK) onder meer medeverantwoordelijk ben voor het informatiebeveiligingsbeleid heb ik gekozen voor het onderwerp 'lekken' om op af te studeren.

De keuze voor dit onderwerp is op 15 februari 2010 vastgelegd, vlak voor de grote reeks aan onthullingen van documenten waarmee WikiLeaks bij een groot publiek bekend raakte (WikiLeaks, g.d.): de Amerikaanse helikopteraanval op journalisten in Irak ('Collateral Murder', onthulling 5 april 2010), de oorlog in Afghanistan ('Task Force 373', onthulling 25 juli 2010), de oorlog in Irak ('SIGACTS', onthulling 23 oktober 2010) en als – voorlopig – grande finale de openbaarmaking van een zeer groot aantal Amerikaanse diplomatieke berichten ('Cablegate', onthulling 28 november 2010).

Hiermee was WikiLeaks een 'blessing in disguise', want er is niets zo vervelend voor een onderzoeker, als wanneer 'zijn' onderwerp 'hot' is voordat het onderzoek afgerond en gepubliceerd is. Maar bij nader inzien leverde de discussie over het verschijnsel WikiLeaks ook interessante informatie op en onderstreepte het nogmaals het belang van 'een onderzoek naar de factoren van intentionele en verwijtbare compromittering van gerubriceerde en gevoelige informatie'. Deze thesis gaat dus niet over WikiLeaks, maar WikiLeaks komt er wel in voor. Het onderzoek is afgerond op 25 april 2011.

De opleiding MSSM is gefinancierd door mijn werkgever, het ministerie van BZK. Deze masterthesis is echter op persoonlijke titel en grotendeels in eigen tijd geschreven. De inhoud van deze masterthesis geeft niet noodzakelijkerwijs het standpunt van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties weer.

Deze thesis is de afsluiting van een intensieve periode waarbij de kennis over security is verbreed en verdiept. Niet alleen door het lezen van literatuur en het volgen van colleges, maar vooral ook door de uitwisseling van gedachten en ervaringen met (gast)docenten en medestudenten. Aan hen gaat mijn dank uit, evenals aan hen die het privé en op het werk mogelijk hebben gemaakt dat ik de opleiding MSSM heb kunnen volgen.

Tot slot een woord van dank aan de respondenten van de enquête, de geïnterviewde personen, de overige deskundigen die ik gesproken heb en mijn afstudeerbegeleider prof. dr. Jeroen van den Hoven. Hun input is van groot belang geweest voor het onderzoek en heeft tal van nieuwe inzichten opgeleverd.

Den Haag, april 2011

Mr. Johri Maat

1. INLEIDING

1.1 Inleiding

> Vrouwen blijken echt geen geheimen te kunnen bewaren. Binnen 47 uur en een kwartier zal het geheim dan ook met minimaal een persoon gedeeld worden. Ongeacht hoe persoonlijk of vertrouwelijk de informatie is. Afhankelijk van de aard van het geheim, is het meest waarschijnlijk dat de echtgenoot, beste vriendin of moeder deelgenoot wordt gemaakt. [….]
> De meeste vrouwen (50 procent) klappen uiteindelijk uit de school omdat het betreffende geheim hen niet lekker zit. Ook een brandend verlangen om te roddelen is voor 30 procent een reden om de gevoelige informatie toch te delen. Een of twee glaasjes wijn helpen eventuele goede bedoelingen die de helft van de vrouwen heeft, alsnog om zeep.
> Een kwart van de vrouwen (27 procent) vertelt geheimen niet door, maar simpelweg omdat ze ze al binnen een dag vergeten zijn. (Van Lintel, 2009)

Waarom is dit fragment uit een nieuwsbericht als zo prikkelend of – voor mannen wellicht – grappig te beschouwen? Omdat de conclusie is dat de gemiddelde vrouw geen geheimen kan bewaren? Omdat ruim een kwart van de vrouwen het geheim na een dag alweer vergeten is? Of komt het doordat geheimen en het onthullen daarvan zowel nieuwsgierigheid als afkeuring opwekken?

In deze thesis gaat het over geheimen, het lekken van geheimen en het voorkomen van het lekken van geheimen. In paragraaf 1.2 zal de probleemstelling geformuleerd worden. In paragraaf 1.3 wordt de relevantie van het onderzoek aangegeven. De centrale onderzoeksvraag met de deelvragen en de afbakening van het onderzoek worden in paragraaf 1.4 behandeld. De onderzoeksaanpak wordt in paragraaf 1.5 beschreven. Dit hoofdstuk wordt in paragraaf 1.6 afgesloten met een leeswijzer.

1.2 Probleemstelling

Binnen de Nederlandse overheid is het uitgangspunt dat overheidsinformatie openbaar is:
“Het bestuursorgaan dat het rechtstreeks aangaat, verschaft uit eigen beweging informatie over het beleid, de voorbereiding en de uitvoering daaronder begrepen, zodra dat in het belang is van een goede en democratische bestuursvoering” (artikel 8, eerste lid, Wet openbaarheid van bestuur; hierna: WOB).

De wet stelt echter ook beperkingen, bijvoorbeeld ter bescherming van de eenheid van de Kroon en de veiligheid van de Staat, bedrijfs- en fabricagegevens en persoonsgegevens (artikel 10, eerste lid, WOB) en ten aanzien van persoonlijke beleidsopvattingen (artikel 11 WOB). Openbaarmaking van deze informatie heeft dan in ieder geval nadelige gevolgen voor het betrokken departement en leidt in sommige gevallen zelfs tot schade voor de Staat of haar bondgenoten.

Dit soort informatie behoort binnen de Rijksoverheid gerubriceerd te zijn volgens het Voorschrift informatiebeveiliging Rijksdienst – Bijzondere Informatie (hierna: Vir-bi). Het niveau van rubricering dient dan aangegeven te zijn op het document (bijvoorbeeld ‘Departementaal Vertrouwelijk’ of ‘Staatsgeheim Zeer Geheim’) en de informatie dient op een voorgeschreven wijze behandeld te worden voor wat betreft de wijze van verwerking, transport, opslag en vernietiging.

Als dit inderdaad het geval is zou men kunnen spreken van ‘formele geheimen’. Als er geen sprake is van een formele rubricering in de zin van het Vir-bi – het staat er letterlijk niet op – maar de houder van de informatie weet of behoort te weten dat de informatie gevoelig is en dat openbaarmaking een afbreukrisico vormt, dan zou men kunnen spreken van ‘materiële geheimen’.

Ondanks de beveiligingsvoorschriften die gelden voor gerubriceerde informatie en de prudentie die men zou mogen verwachten bij gevoelige informatie komt het geregeld voor dat deze informatie toch gecompromitteerd raakt. Er is dan sprake van ‘kennisname door niet gerechtigden’. Er wordt dan wel gesproken van het ‘lekken’ of ‘uitlekken’ van geheimen. Veelal is de informatie dan ook via de media bij een groot publiek bekend geworden.

Recente voorbeelden uit 2009 en 2010 zijn het weekbericht van de Vertegenwoordiging van Nederland te Oranjestad, Aruba (Mentens, 2009), de Miljoenennota (Miljoenennota opnieuw uitgelekt, 2010), de notulen van de Ministerraad inzake de Westerschelde (Rijksrecherche onderzoekt lek ministerraad, 2010), de Dalai Lama-Telegraafzaak (Van der Graaf & Kuitert, 2009) en de concept-kabinetsreactie op het Irak-rapport van de commissie Davids (Kabinet heeft reactie op Irak-rapport bijna af, 2010). Internationaal 'hoogtepunt' is de publicatie van circa 250.000 documenten aangaande het diplomatieke berichtenverkeer van de Verenigde Staten – 'Cablegate' – via de website van WikiLeaks sinds eind 2010 (Lovink & Riemens, 2010).

1.3 Relevantie onderzoek

De hiervoor genoemde reeks voorvallen uit 2009 en 2010 roept de vraag op waaróm er gelekt wordt. Onderzoek naar dit verschijnsel is zowel wetenschappelijk als maatschappelijk relevant.

Vanuit wetenschappelijk opzicht is onderzoek relevant omdat, gebaseerd op een verkenning in de Nederlandse literatuur (waaronder in het systeem van het Wetenschappelijk Onderzoek en Documentatiecentrum, geraadpleegd 14 juni 2010), sinds de onderzoeken van Bovens, Geveke en De Vries in 1993 en Beenakkers en Grapendaal in 1995 geen uitvoerig wetenschappelijk onderzoek gedaan lijkt te zijn. Wel zijn er twee commissies geweest die onderzoek hebben gedaan naar het verschijnsel lekken: de Commissie Lemstra naar aanleiding van diverse lekincidenten binnen het ministerie van Defensie (rapportage in 2005, conclusies zijn opgenomen als bijlage VIII) en de Commissie Prinsjesdagstukken naar aanleiding van het bij herhaling uitlekken van Prinsjesdagstukken (rapportage in 2010). Hoewel deze rapporten waardevolle inzichten opleveren is de focus hiervan wel beperkt tot respectievelijk Defensie en het proces rond de Prinsjesdagstukken. Naast de wetenschappelijke relevantie bestond er binnen het ministerie van Binnenlandse Zaken en Koninkrijksrelaties – de werkgever van de auteur – ook een praktische behoefte aan een actueel onderzoek.

Vanuit maatschappelijk opzicht is onderzoek relevant omdat lekken als een probleem wordt gezien. Lekken schaadt namelijk het vertrouwen dat men in de (Rijks)overheid heeft bij (buitenlandse) overheden, bedrijven en burgers. Overheden kunnen gaan twijfelen of geheimen nog wel gedeeld kunnen worden. Bedrijven die – soms verplicht – commerciële en concurrentiegevoelige informatie aan de overheid overdragen lopen risico op concurrentievervalsing. Burgers kunnen in hun privacy geschaad worden. Daarnaast is er een moreel probleem: Als men geen geheimen kan bewaren, hoe zit het dan met andere belangen? In de Kwetsbaarheidsanalyse spionage schrijft de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD) hierover:

> Het openbaar bestuur en het Nederlandse bedrijfsleven kunnen grote schade oplopen door het weglekken van gevoelige beleidsstrategieën, -visies en standpunten. De andere partij kan, gebaseerd op deze kennis, immers beter gewogen beslissingen nemen over de in te zetten strategie, ten koste van de Nederlandse overheid of het Nederlandse bedrijfsleven. […] Informatie kan uiteraard ook bewust door werknemers worden prijsgegeven. Uiteenlopende motieven als geld, persoonlijk gewin, erkenning/ego, persoonlijke overtuiging, of gevoelens van onvrede of wraak kunnen hier een rol bij spelen. Inlichtingenofficieren spelen, zeker als er achtergrondinformatie over iemand beschikbaar is, bewust in op dergelijke gevoelens, om ze uiteindelijk voor hun eigen doelen aan te wenden. (Kwetsbaarheidsanalyse Spionage 2010:13, 40)

1.4 Vraagstelling

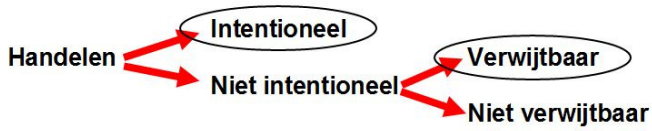
In deze thesis staat de volgende onderzoeksvraag centraal:
'Welke factoren spelen een rol bij het intentioneel en verwijtbaar compromitteren van gerubriceerde en gevoelige informatie?'

In de thesis zal in plaats van 'intentioneel en verwijtbaar compromitteren' ook de term 'lekken' gebruikt worden. De termen 'gerubriceerde informatie' en 'gevoelige informatie' zullen in de thesis ook samengevat worden als 'geheimen'.

Ter beantwoording van deze centrale onderzoeksvraag zijn de volgende deelvragen geformuleerd:

a. Waarom zijn er geheimen?
b. Waarom worden geheimen gelekt?
c. Hoe worden geheimen gelekt?
d. Welke maatregelen zijn mogelijk tegen het lekken van geheimen?

Het onderzoek wordt daarbij beperkt tot het *intentioneel* en *verwijtbaar* handelen door de persoon die een gerechtigde houder is van de gerubriceerde of gevoelige informatie of die anderszins toegang heeft. In strafrechtelijke zin zou men kunnen spreken van 'opzet' en 'schuld'. Hierbij is het verwijtbaar handelen weer een verbijzondering van het *niet intentioneel* handelen. Dit wordt gevisualiseerd in figuur 1.1.



Figuur 1.1: Beperking tot intentioneel en verwijtbaar handelen

Hoewel de focus aanvankelijk gericht zou zijn op het intentionele handelen, is er voor gekozen de focus ook uit te breiden naar het verwijtbare handelen. Een deel van de lekken wordt namelijk veroorzaakt door zaken als onachtzaamheid, onkunde en onprofessioneel handelen, soms met grote gevolgen (Casus 1).

Casus 1: Britse antiterreurchef Quick weg na blunder

"Londen, 9 april 2009 – Het hoofd van de antiterreurdienst van Scotland Yard, commissaris Bob Quick, heeft vanmorgen gedwongen zijn functie neergelegd na een blunder die een antiterreuractie in gevaar heeft gebracht.

De gewraakte foto van Bob Quick (Foto Political Pictures)

Quick, in de Britse media al afgeschilderd als 'commissaris Kluns', stelde zijn positie ter beschikking kort na de arrestatie van twaalf verdachten die een aanslag in Noordwest-Engeland zouden hebben willen plegen. Invallen op een tiental adressen in Liverpool, Manchester en Clitheroe vergden de inzet van honderden politiemensen op een riskant uur: de avondspits.

De operatie moest worden vervroegd, omdat Quick details daarover leesbaar voor camera's onder zijn arm meedroeg, toen hij in Downing Street de minister van Binnenlandse Zaken ging inlichten.

De arrestaties van de verdachten – twee voor de bibliotheek van Liverpools John Moore University waar honderden studenten met luidsprekers gemaand werden bij de ramen weg te blijven, en twee anderen in een doe-het-zelfzaak in Clitheroe – waren de climax van een maandenlange undercover-operatie. Op Quicks documenten ('Operatie Pathway – Secret') waren namen van politiemensen en locaties van de verdachten te lezen.

Zodra deze inhoud rond het middaguur bekend werd, vaardigde het ministerie van Defensie een – zeldzame – D-notice uit, die media verbiedt te publiceren om redenen van staatsveiligheid. Maar buitenlandse media zijn daaraan niet gebonden. Toen de details toch uitlekten, wachtte de antiterreurbrigade niet tot het gebruikelijke uur in de vroege ochtend om in te grijpen. De vrees was dat de verdachten óf op de vlucht zouden slaan óf hun plannen vervroegd zouden uitvoeren."

(Jippes, 2009)

Er wordt in het onderzoek dus niet gekeken naar het niet verwijtbare lekken, te weten de factoren die buiten de directe invloedsfeer van betrokkene liggen, zoals technisch falen of overmacht en actieve

spionage door inlichtingendiensten of criminelen in de vorm van afluisteren, hacking of afgifte onder dwang. Hierover is recent uitvoerig gerapporteerd in het 'Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010' van GOVERT.NL en de 'Kwetsbaarheidsanalyse Spionage 2010' van de AIVD. Volledigheidshalve wordt opgemerkt dat de scheiding tussen verwijtbaar en niet verwijtbaar handelen niet heel scherp is, er is een grijs gebied. Als bijvoorbeeld regels onvoldoende bekend zijn gemaakt is er eerder sprake van niet verwijtbaar handelen, dan wanneer deze regels door betrokkene niet of onvoldoende gelezen zijn.

Verder is er ook een afbakening in tijd. Er wordt actief gekeken naar de periode 2004-2010, reden hiervoor is dat het belangrijkste juridische kader dat in dit onderzoek wordt gehanteerd, het Vir-bi, in 2004 van kracht is geworden. Het Vir-bi zal overigens naar verwachting in 2011 vervangen worden door het Voorschrift informatiebeveiliging – gerubriceerde informatie (Vir-gi) waarin meer aandacht is voor zaken als risicomanagement en het rubriceringsproces. Tot slot wordt het onderzoek afgebakend tot de Nederlandse Rijksoverheid, reden hiervoor is de noodzaak tot beperking en de toegankelijkheid tot de bronnen voor de onderzoeker.

1.5 Onderzoeksaanpak

De onderzoeksaanpak is een route die leidt naar de beantwoording van de centrale onderzoeksvraag. In het onderzoek is gekozen voor een aanpak die exploratief en kwalitatief van aard is, met een juridische inslag. Hierbij is van uiteenlopende open en gesloten bronnen gebruik gemaakt.

De open bronnen bestaan uit wet- en regelgeving, vakliteratuur, Kamerstukken, openbare onderzoeksrapporten, jurisprudentie en berichtgeving over casuïstiek.

De gesloten bronnen bestaan uit – gesplitst semi-gestructureerde – interviews met (ervarings) deskundigen op het terrein van geheimen en lekincidenten (zie bijlage I). De verzameling van respondenten is gemêleerd: topambtenaren, onderzoekers, specialisten op het terrein van informatiebeveiliging, een opsporingsambtenaar en een journalist. Er is bewust voor gekozen om geen 'lekkers' te interviewen. Het traceren van deze actoren zou veel tijd kosten en de kans dat men mee zou werken aan het onderzoek werd erg klein geacht, zeker ook gezien de positie van de onderzoeker.

Ter voorbereiding op de interviews is een enquête uitgevoerd die door middel van een vragenlijst (bijlage II) is verspreid onder de Beveiligingsambtenaren (BVA) van alle – destijds – dertien departementen. De respons hierop was honderd procent. De uitkomsten van de enquête worden ook in deze thesis beschreven, maar niet herleidbaar tot op departementaal niveau. Dit is een bewuste keuze. Deze masterthesis is een openbare publicatie omdat het een poging is een bijdrage te leveren aan het vakgebied van security science & management. Maar om geen kwetsbaarheden te creëren voor de personen en organisaties die medewerking hebben verleend aan het onderzoek, zijn de achterliggende data en integrale gespreksverslagen afgeschermd. Deze zijn slechts in te zien door de afstudeerbegeleider en examencommissie MSSM na het tekenen van een geheimhoudingsverklaring. Alle geïnterviewde personen hebben ingestemd met het opnemen in deze thesis van tot op de persoon herleidbare citaten.

Zoals bij meer deelterreinen binnen en buiten security is men bij lekken veelal geneigd incident gedreven op te treden, maar "door de focus op incidenten raken meer structurele ontwikkelingen onderbelicht" (Van Rossum, 2010:3). In feite is er sprake van 'actie → reactie'. Men loopt dan achter de feiten aan, want het kwaad is al geschied. In sommige gevallen is zelfs sprake van een overreactie.

Daarom wordt binnen het vakgebied van security steeds meer de nadruk gelegd op een aanpak op basis van risicoanalyse, waarbij de nadruk niet ligt op reactief, maar op proactief handelen (Reason, 2000:769; Schneier, 2003:14-15; Overbeek, Roos Lindgreen & Spruit, 2005:5-20; Van Mil, Dijkzeul & Van der Pennen, 2006:6; Scharenborg, 2007:28-29; Code voor Informatiebeveiliging 2007:13; Talbot & Jakeman, 2008:175; Handreiking Risicoanalyse, 2009:13; Kwetsbaarheidsanalyse Spionage 2010:11; Handleiding Kwetsbaarheidsanalyse spionage, 2011:4). De nuances kunnen verschillen, maar de aanpak bestaat pakweg in alle methodes uit het bepalen van de belangen, de dreigingen en kwetsbaarheden, de te nemen maatregelen en de (geaccepteerde) restrisico's.

1.6 Leeswijzer

Deze voornoemde aanpak is ook de leidraad geweest voor de indeling van deze thesis. Hierbij dient men wel te bedenken dat een harde scheiding niet mogelijk is. Enige overlap zal er daarom wel zijn.

Het theoretisch kader wordt in hoofdstuk 2 behandeld. Hierin worden bovenstaande begrippen zoals ‘intentionele en verwijtbare compromittering’, ‘gerubriceerde en gevoelige informatie’, het begrip ‘risico’ en modellen voor risicomanagement nader geduid.

In hoofdstuk 3 wordt ingegaan op het belang van geheimen. Waarom zijn er geheimen en waarom worden geheimen gelekt? Dit wordt behandeld aan de hand van de ethische, de juridische en de politiek-bestuurlijke dimensie.

In hoofdstuk 4 wordt ingezoomd op de dreigingen en kwetsbaarheden. Hierbij ligt de nadruk op de vraag hoe geheimen worden gelekt. In dit hoofdstuk komen ook de uitkomsten van de enquête, de interviews en de gegevens van de Rijksrecherche aan bod.

In hoofdstuk 5 wordt nader ingegaan op de te nemen maatregelen en restrisico’s. Welke maatregelen zijn er mogelijk tegen het lekken van geheimen?

Het onderzoek wordt in hoofdstuk 6 op basis van het voorgaande afgesloten met de conclusies en aanbevelingen naar aanleiding van de centrale onderzoeksvraag.

Voor het gemak van de lezer bevatten de bijlagen ook een lijst van gehanteerde afkortingen (bijlage III) en een lijst van gehanteerde begrippen (bijlage IV).

2. THEORETISCH KADER

2.1 Inleiding

In dit hoofdstuk worden een aantal kernbegrippen in het onderzoek op hoofdlijnen nader geduid. In paragraaf 2.2 wordt ingegaan op de begrippen 'informatie' en 'informatiebeveiliging'. In paragraaf 2.3 worden de begrippen 'risico's' en 'risicomanagement' in kort bestek uitgelegd. 'Human Error' en het 'Swiss Cheese Model' komen wat uitgebreider aan bod in paragraaf 2.4. Het 'Bow Tie Model' wordt in paragraaf 2.5 behandeld. In paragraaf 2.6 wordt ingegaan op de gelaagdheid van maatregelen en 'practical drift'. Gerubriceerde en gevoelige informatie – 'geheimen' – komen in paragraaf 2.7 aan bod. Tot slot wordt de 'intentionele en verwijtbare compromittering' – het 'lekken' – in paragraaf 2.8 behandeld.

2.2 Informatie en informatiebeveiliging

Informatie is te definiëren als de betekenis die de mens aan de hand van bepaalde afspraken toekent aan gegevens, of de kennistoename als gevolg van het ontvangen en verwerken van bepaalde gegevens. Gegevens kunnen gedefinieerd worden als de objectief waarneembare weerslag van feiten op een drager, zoals de letters op papier of de 'enen en nullen' op een digitale datadrager. De gegevensverwerking is te vergelijken met een fabricageproces, de gegevens zijn de grondstof en de informatie is het eindproduct. Bij het verwerken van gegevens kan gebruik gemaakt worden van een informatiesysteem, dit is een "[…] samenhangende gegevensverwerkende functionaliteit die kan worden ingezet om één of meer bedrijfsprocessen te kennen, te ondersteunen, of te besturen. Een informatiesysteem kan de volgende componenten bevatten: apparatuur, programmatuur, gegevens, procedures en mensen" (Overbeek, Roos Lindgreen & Spruit, 2005:8).

Elke organisatie is in meer of mindere mate afhankelijk van informatie in het bedrijfsproces. Daarom is het van belang dat deze informatie betrouwbaar is. De drie voornaamste kwaliteitsaspecten van betrouwbaarheid zijn beschikbaarheid, integriteit en vertrouwelijkheid (ook wel exclusiviteit genoemd). Beschikbaarheid is de mate waarin gegevens of de functionaliteit op het gewenste moment beschikbaar is voor de gebruiker. Integriteit is de mate waarin de gegevens of de functionaliteit correct zijn. Vertrouwelijkheid is de mate waarin de toegang tot de gegevens of de functionaliteit is beperkt tot degenen die daartoe bevoegd zijn (Overbeek, Roos Lindgreen & Spruit, 2005:10; Vir-bi, 2004:17). Informatie kan voor een organisatie een dusdanige waarde hebben dat het verdwijnen van de vertrouwelijkheid (in deze thesis ook exclusiviteit genoemd) tot risico's of directe schade leidt. In deze thesis gaat het om het aspect vertrouwelijkheid van de betrouwbaarheid van informatie. De kwaliteitsaspecten beschikbaarheid en integriteit worden verder buiten beschouwing gelaten.

Het is de informatiebeveiliging die toeziet op de betrouwbaarheid van informatie. In het Voorschrift informatiebeveiliging rijksdienst 2007 (hierna: Vir; het Vir-bi is hiervan een uitwerking) wordt informatiebeveiliging gedefinieerd als "het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen" (artikel 1 onder a Vir).

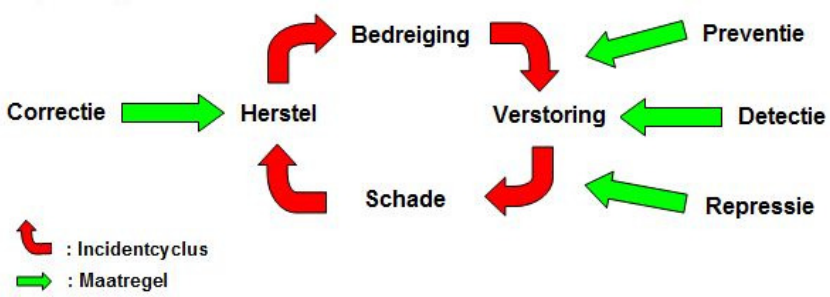
De betrouwbaarheid – waaronder dus de vertrouwelijkheid waarop deze thesis zich richt – van informatie wordt beïnvloed door (be)dreigingen en kwetsbaarheden. Een (be)dreiging is een gebeurtenis of een proces die in potentie een verstorende invloed heeft op de betrouwbaarheid van een object. De kwetsbaarheid is de mate waarin het betreffende object voor deze (be)dreiging gevoelig is (Overbeek, Roos Lindgreen & Spruit, 2005:10-11). Zich manifesterende bedreigingen kunnen dus leiden tot het falen van een of meerdere kwaliteitsaspecten van de betrokken processen.

2.3 Risico en risicomanagement

De term ‘dreiging’ wordt binnen het security domein onderscheiden van de term ‘risico’: “When security professionals talk about *risk*, they take into consideration both the likelihood of the threat and the seriousness of a successful attack” (Schneier, 2003:20). Willett definieert risico als “the objectified uncertainty regarding the occurrence of an undesired event” (Ale, 2009:4). Een risico in relatie tot informatiebeveiliging “is de gemiddelde schade over een gegeven tijdsperiode, die verwacht wordt doordat één of meer bedreigingen leiden tot een verstoring van één of meer objecten van de informatievoorziening” (Overbeek, Roos Lindgreen & Spruit, 2005:12).

Deze schade kan al dan niet van financiële aard zijn en bestaat uit directe schade (zoals aan apparatuur, programmatuur en gegevensverzamelingen) en uit indirecte of gevolgschade (zoals verstoring van bedrijfsprocessen, het overtreden van wet- en regelgeving, verlies van opdrachten en imagoschade). Een organisatie kan een zeker schadeniveau verwerken zonder dat de bedrijfsprocessen daardoor in gevaar gebracht worden. De risico’s zijn tot dat niveau acceptabel en kunnen dan worden geaccepteerd. Vanaf een bepaald schadeniveau komen de bedrijfsprocessen echter in gevaar. Door het treffen van maatregelen is het mogelijk om de gelopen risico’s te verkleinen (Overbeek, Roos Lindgreen & Spruit, 2005:12-13).

Door middel van een risicoanalyse kan men bepalen tegen welke bedreigingen maatregelen getroffen moeten worden. De incidentcyclus bestaat uit: de bedreiging, de verstoring, de schade en het herstel. Op deze incidentcyclus zijn vier maatregelen mogelijk: preventie, detectie, repressie en correctie. De incidentcyclus en de maatregelen vormen samen de beveiligingscyclus (zie figuur 2.1).



Figuur 2.1: Incidentcyclus + maatregelen = Beveiligingscyclus (naar: Overbeek, Roos Lindgreen & Spruit, 2005:15-16)

De preventieve of eerstelijns maatregelen richten zich op het voorkomen van de verstoring en kunnen zowel permanent als ‘getriggerd’ (men ziet de verstoring aankomen) van aard zijn. De repressieve of tweedelijns maatregelen hebben tot doel de negatieve invloed van de verstoring te minimaliseren. Detectie is van belang om de verstoring op te kunnen merken en correctie is van belang voor het onderhoud en beheer (Overbeek, Roos Lindgreen & Spruit, 2005:15-18). “De belangrijkste maatregelen die we in beschouwing dienen te nemen zijn dus preventieve maatregelen (permanent en getriggerd) en repressieve maatregelen (inclusief verzekeren). Detectieve maatregelen worden daarbij als onderdeel beschouwd van de preventieve en repressieve maatregelen die ze ondersteunen” (Overbeek, Roos Lindgreen & Spruit, 2005:18). Schneier vat het als volgt samen: “Prevention, detection, and response systems are a triad; in concert, they provide dynamic security, resilient failure, and defense in depth” (Schneier, 2003:149-150).

De wijze waarop met risico’s wordt omgegaan kan gedefinieerd worden als risicomanagement: “The organized way of keeping risk under control” (Ale, 2009:62). Hiervoor zijn tal van modellen beschikbaar, zoals het ‘Swiss Cheese Model’ en het ‘Bow Tie Model‘. In beide modellen spelen de maatregelen – de barriers – een belangrijke rol.

2.4 Human Error en het Swiss Cheese Model

Mensen kunnen – intentioneel of verwijtbaar – fouten maken, en die fouten kunnen leiden tot verstoringen of ongevallen. James Reason heeft onderzoek gedaan naar die menselijke fouten, ook

wel ‘human error’ genoemd. Het probleem van 'human error' kan volgens Reason op twee manieren bekeken worden: de persoonsgerichte benadering en de systeembenadering.

2.4.1 Persoonsgerichte benadering

De al lang bestaande en wijdverspreide persoonsgerichte benadering legt de focus op de onveilige handeling – fouten en overtredingen – van het individu als actor in een kritisch proces. De oorzaak van de onveilige handeling wordt verklaard door zaken als vergeetachtigheid, onoplettendheid, gebrek aan motivatie, achteloosheid, onzorgvuldigheid of roekeloosheid, veelal zijn ze intentioneel of verwijtbaar. De tegenmaatregelen zijn voornamelijk gericht op het reduceren van het ongewenste gedrag en omvatten onder meer postercampagnes, nieuwe en aanvullende procedures, disciplinaire maatregelen en dreigen met aansprakelijkheid. "Followers of this approach tend to treat errors as moral issues, assuming that bad things happens to bad people" (Reason, 2000:768). Fouten worden in deze benadering dus als een ethisch probleem gezien.

De persoonsgerichte benadering is volgens Reason dominant omdat het emotioneel meer bevrediging geeft om de schuld bij een individu neer te leggen dan het aanpakken van systeemfouten in instituties. Bovendien zijn individuen vrij om hun gedrag te bepalen, dus ook om te kiezen voor een veilige of een onveilige modus. Als er dan iets fout gaat, dan lijkt het logisch te zijn dat er een of meerdere individuen hier verantwoordelijk voor zijn. Het zoeken naar een mogelijkheid om een onveilige handeling van een individu los te koppelen van de verantwoordelijkheid van de organisatie als instituut is ook duidelijk in het belang van de bestuurders, ook in juridische zin.

De persoonsgerichte benadering kent echter serieuze tekortkomingen. Hoewel sommige onveilige handelingen tot desastreuze gevolgen kunnen leiden, gebeurt dat in de meeste gevallen niet. Een voorbeeld in het kader van dit onderzoek kan dat illustreren (Casus 2).

Casus 2: De onbeveiligde usb-stick

“Een mooi voorbeeld van het niet opzettelijk verliezen van een onbeveiligde usb-stick gebeurde tijdens een overleg. De medewerker moest wat uitprinten en is daarbij de usb-stick vergeten bij een andere partij.

Enige tijd later is de usb-stick gevonden en terugbezorgd bij Bureau BVA. Toen bleek dat de usb-stick onbeveiligd was en privé-eigendom van de ambtenaar. Degene die de usb-stick vond had absoluut geen kennis mogen kunnen nemen van de inhoud van de informatie die op de usb-stick stond. Verder bleek dat op de usb-stick zo ongeveer alle documenten stonden die de betreffende ambtenaar in zijn tijd bij BZK geschreven had, naast wat privé zaken zoals foto’s en muziek.

Dit is een mooi voorbeeld van een combinatie van factoren die grote gevolgen kan hebben. Dat iemand een usb-stick vergeet of verliest, dat kan gebeuren. Maar doordat geen gebruik was gemaakt van de standaard voorgeschreven usb-stick ontstond een groot probleem. De leidinggevende had hierin ook een rol, deze had zich ervan moeten vergewissen dat de informatie op een beveiligde usb-stick stond en aandacht moeten besteden aan het werk van de medewerker, bijvoorbeeld een extra controle of er niets vergeten was. De BZK-informatie stond op een privé usb-stick die onbeveiligd was. Privé en werk liepen hierdoor door elkaar heen en dat kan dit soort gevolgen hebben. En omdat er tegenwoordig zo ontzettend veel informatie op een usb-stick past, is de schade vaak ook groter dan pakweg tien jaar geleden toen nog diskettes gebruikt werden.”

(Interview E.P. Grobbe, 20-12-2010)

Het meenemen van vertrouwelijke informatie op een onbeveiligde usb-stick leidt tot een kwetsbaarheid. Maar deze kwetsbaarheid manifesteert zich pas op het moment dat de usb-stick in onbevoegde en kwaadwillende handen geraakt. Het kan dus jarenlang goed gaan dat iemand vertrouwelijke informatie onbeveiligd meeneemt.

Daarnaast is effectief risicomanagement in sterke mate afhankelijk van een cultuur van het rapporteren en analyseren van tegenvallers, incidenten, bijna ongelukken en ‘free lessons’. Zonder dat is het niet mogelijk verborgen valkuilen te ontwaren en te leren waar de kritieke grenzen van risico's liggen. Vertrouwen in de medewerkers is een essentieel element in een 'meldcultuur' zodat ook een ‘rechtvaardige cultuur’ ('just culture') ontstaat. Hiermee wordt gedoeld op een collectieve bewustwording van handelingen die onschuldig zijn en handelingen die laakbaar zijn: "Engineering a just culture is an essential early step in creating a safe culture" (Reason, 2000:768-769). Een andere tekortkoming van de persoonsgerichte benadering is dat deze geen rekening houdt met de context

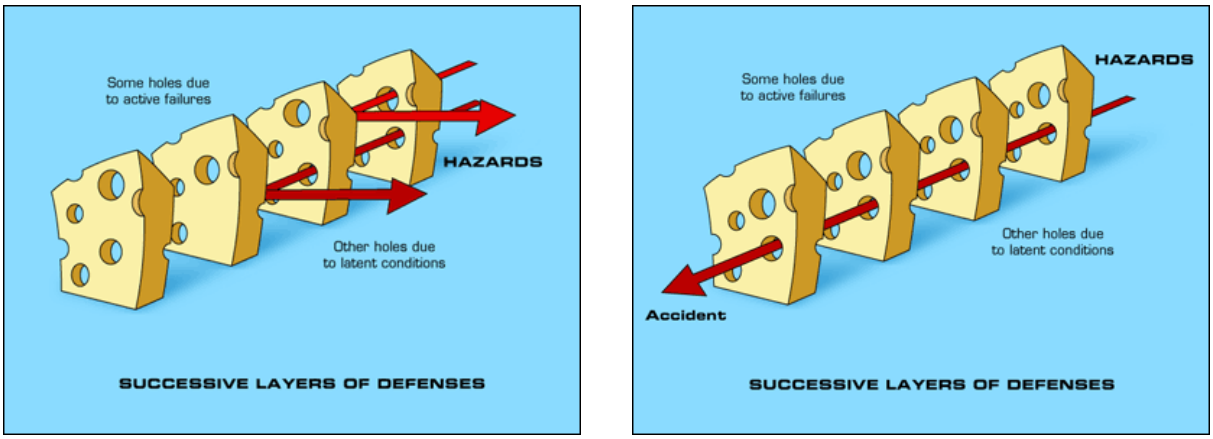
waarin de onveilige handelingen verricht zijn. Volgens Reason raken twee factoren buiten beeld. Ten eerste zijn het vaak de beste mensen die de grootste fouten maken. Ten tweede hebben ongelukken de neiging om niet ad random plaats te vinden, maar in patronen, ongeacht de betrokken functionarissen (Reason, 2000:769).

2.4.2 Systeembenadering

Tegenover de persoonsgerichte benadering staat de systeembenadering. Het uitgangspunt hiervan is dat mensen feilbaar zijn en dat fouten altijd verwacht kunnen worden, ook in de best functionerende organisaties. De 'human error' is in deze benadering niet zozeer een oorzaak ('cause'), als wel een gevolg ('consequence') van het systeem. De fouten zitten als het ware ingebakken in de werkomgeving en organisatieprocessen. Bij het ontwerpen van de tegenmaatregelen is het uitgangspunt dat de mens als actor niet veranderd kan worden, maar wel de omstandigheden waarin de mens als actor functioneert. Wanneer een ongeval zich voordoet is het niet van belang wíe er geblunderd heeft, maar hoe en waarom de maatregelen gefaald hebben. Door maatregelen in het systeem te bouwen kunnen menselijke fouten ondervangen worden (Reason, 2000: 768). Deze maatregelen dienen dan wel onafhankelijk van elkaar te werken, zodat de oorzaak van het falen van de ene maatregel niet ook leidt tot het falen van de andere maatregel.

2.4.3 Swiss Cheese Model

In de systeembenadering spelen maatregelen ("defences, barriers and safeguards") een belangrijke rol. Deze kunnen bestaan uit technische en organisatorische maatregelen en hebben als doel potentiële aantastingen van belangen te beschermen. Meestal geschiedt dit ook effectief, maar er zijn altijd zwakke plekken. In de ideale situatie is elke laag intact, maar in werkelijkheid lijken de barrières door de gaten meer op plakjes Zwitserse kaas die - in tegenstelling tot die in de kaas - zich continu openen, sluiten en verplaatsen. Als er meerdere lagen zijn zal een enkel gat de dreiging niet doorlaten, maar als alle lagen op hetzelfde traject een gat vertonen, kan een dreiging doordringen en een ongeval veroorzaken. In figuur 2.2, het Swiss Cheese Model, wordt dit schematisch weergegeven. Dit barrièremodel is in 1990 door Reason geïntroduceerd (Reason 2000:768-770). Dit model wordt vaak aangehaald bij risicoanalyses in relatie tot ‘human errors’ (Talbot & Jakeman 2008:197; Ale 2009:25-26).



Figuur 2.2: Swiss Cheese Model. Links worden de dreigingen door de maatregelen ‘gestopt’. Rechts weten de dreigingen door te dringen waarop de ongewenste gebeurtenis zich manifesteert

De gaten in de maatregelen kennen twee oorzaken: actieve fouten en latente condities.
Actieve fouten hebben een directe en gewoonlijk kortdurende impact op de integriteit van de maatregel, ze worden bewust of onbewust veroorzaakt door de direct betrokken actor.

Latente condities zijn echte systeemfouten die gecreëerd zijn door beslissingen van de ontwerpers, de bouwers en het hogere management. Latente condities kunnen de werkomstandigheden aantasten, bijvoorbeeld door tijdsdruk, onderbezetting, onvoldoende middelen, oververmoeidheid en onervarenheid. Daarnaast kunnen ze langdurige gaten in de maatregelen creëren zoals onbetrouwbare alarmsystemen en indicatoren, onwerkbare procedures, ontwerp- en constructiefouten. Deze latente condities kunnen lange tijd verborgen blijven, tot ze zich als ongeval manifesteren in combinatie met actieve fouten. "Unlike active failures, whose specific forms are often hard to foresee,

latent conditions can be identified and remedied before an adverse event occurs. Understanding this leads to proactive rather than reactive risk management" (Reason, 2000:769).
Aan de hand van de volgende casus kan het Swiss Cheese Model toegepast worden (Casus 3).

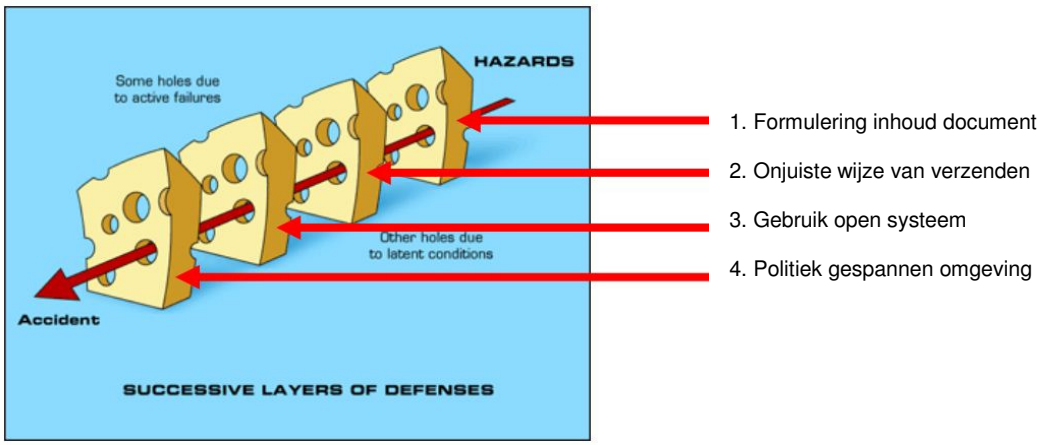
Casus 3: Het doorgezonden e-mailbericht met onversleutelde bijlage

"Een bekend voorbeeld, dat uitgebreid in de media is behandeld, is de affaire rond het Weekbericht van de Vertegenwoordiging van Nederland te Oranjestad (Aruba) in februari 2009. Weekberichten worden door de Vertegenwoordigingen opgesteld om de politieke en ambtelijke leiding te informeren over de lokale situatie, vergelijkbaar met de diplomatieke berichten. In het bewuste weekbericht was een kwalificatie opgenomen over de heer Croes, de minister van Justitie van Aruba, die gemakkelijk negatief geïnterpreteerd kon worden. Het weekbericht was onversleuteld per e-mail naar Nederland gestuurd. Een van de ontvangers was een medewerker van een ander departement. Vanuit zijn account is dit – met onduidelijke oorzaak – doorgestuurd naar een medewerker van de heer Croes. De heer Croes heeft vervolgens het weekbericht openbaar gemaakt. Het was een serieuze affaire waar de politiek-bestuurlijke verhoudingen tussen Nederland en Aruba onder geleden hebben.

Het interne onderzoek van BZK heeft de gang van zaken gereconstrueerd, maar het is nooit duidelijk geworden door welke omstandigheden het document vanuit het andere departement naar Aruba doorgestuurd is. Uit het onderzoek bleek dat het document wel gerubriceerd was, maar dat het niet op de juiste manier behandeld is. Het had nooit onversleuteld verzonden mogen worden. Vanuit BZK zijn ook direct maatregelen genomen die herhaling voorkomen. Bedenk wel, het heeft ruim een jaar geduurd voordat de verhoudingen genormaliseerd waren. [Er zijn geen aanwijzingen gevonden van opzet van het lekken. JHM] De informatie was niet versleuteld, dat was verwijtbaar. De betrokken ambtenaar had de risico's moeten kennen en er naar moeten handelen. Of de medewerker van het andere departement het document met opzet heeft doorgestuurd is niet te bepalen, zelf heeft deze aangegeven geen verklaring te hebben hoe het heeft kunnen gebeuren. De afdoening hierin lag bij het andere departement, ik kan daar verder niets over zeggen. Waar wel sprake van opzet was, was bij de ontvanger in Aruba. De heer Croes heeft het bericht bewust in de openbaarheid gebracht en er veel aandacht op weten te richten. Staatssecretaris Bijleveld heeft zelf in een interview aangegeven dat ze het 'niet chic' vond dat minister Croes het bericht in de openbaarheid heeft gebracht, 'Het had niet zo'n groot gedoe hoeven worden' waren haar letterlijke woorden."

(Interview E.P. Grobbe, 20-12-2010)

Uit deze casus kunnen de volgende actieve fouten en latente condities gehaald worden (gevisualiseerd in figuur 2.3):
1. In het document was een kwalificatie opgenomen die gemakkelijk negatief geïnterpreteerd kon worden (wijze van formuleren inhoud).
2. Het document was wel gerubriceerd, maar werd niet op de juiste wijze behandeld, het document werd namelijk onversleuteld verzonden (onjuiste wijze van verzenden).
3. Het document kwam bij een persoon terecht die het al dan niet bewust door kon sturen naar een andere ontvanger buiten de kring van gerechtigden (gebruik open systeem).
4. Er was een ongerechtigde ontvanger die het document uiteindelijk om politieke redenen in de openbaarheid bracht en zo de politiek-bestuurlijke verhoudingen schade toebracht (politiek gespannen omgeving).



Figuur 2.3: Casus 3 toegepast op het Swiss Cheese Model

2.4.4 Error Management

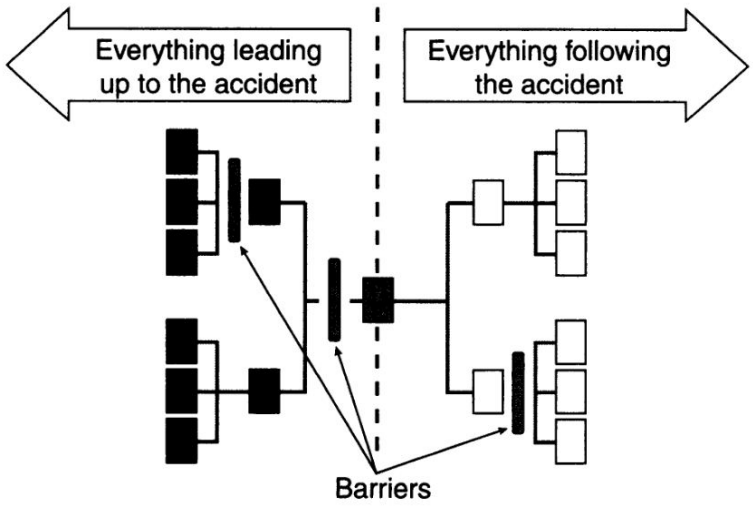
Reason beschrijft 'Error Management' als een instrument om onveilige situaties te managen dat zich richt op het individu, het team, de taak, de werkomgeving en het instituut. Enerzijds heeft het als doel gevaarlijke fouten te voorkomen, en anderzijds – omdat dit toch niet altijd te voorkomen valt – het creëren van een systeem dat beter in staat is om ongevallen op te vangen en de schadelijke effecten te beperken. Error management is vaak terug te vinden in 'High Reliability Organisations' (hierna: HRO). Dit zijn complexe organisaties, zoals vliegdekschepen, luchtverkeersleidingcentra en kerncentrales, die moeten opereren onder grote mentale druk in een gevaarlijke en interactieve omgeving waarbij weinig foutmarge toegestaan is.

> Most managers of traditional systems attribute human unreliability and strive to eliminate it as fast as possible. In high reliability organisations, on the other hand, it is recognised that human variability in the shape of compensations and adaptations to changing events represents one of the system most important safeguards. Reliability is 'a dynamic non-event'. (Reason, 2000:770)

Daarmee zijn HRO's het voorbeeld van een systeembenadering waarin rekening wordt gehouden met de mogelijkheid van het falen van een maatregel. Nu zal niet elke overheidsorganisatie als een HRO te beschouwen zijn, maar men kan er wel van leren.

2.5 Bow Tie Model

Een ander bekend model voor risicoanalyse is het Bow Tie Model. In dit model gaat het in essentie om de onderlinge relaties van de risico's, maatregelen en consequenties. De naam van het model is ontleend aan de vorm die doet denken aan een vlinderdas (figuur 2.4). De knoop van de vlinderdas wordt gevormd door de manifestatie van het risico: de ongewenste gebeurtenis (het incident). Aan de preventieve zijde (links) staan de bedreigingen die tot het incident hebben kunnen leiden. Aan de repressieve zijde (rechts) staan de mogelijke gevolgen (schade) van het incident (Talbot & Jakeman 2008:198-204).



Figuur 2.4: Bow Tie Model (Ale, 2009:49)

In het Bow Tie Model zijn barrières mogelijk die voorkomen dat een bepaalde fout daadwerkelijk plaatsvindt en/of de ongewenste gebeurtenis werkelijk leidt tot ongewenste consequenties: "Possible types of intervention are (1) to remove a cause, or (2) prevent progression of an unwanted pathway by introducing a barrier" (Ale, 2009:62). Net als bij het Swiss Cheese Model draait het in dit model om het al dan niet succesvol tegenhouden van de dreiging. Het Bow Tie Model kan ook gezien worden als twee Swiss Cheese Models achter elkaar, waarbij de linker kant zich richt op het voorkomen van de ongewenste gebeurtenis en de rechter kant zich richt op het voorkomen van de hieruit volgende ongewenste consequenties (Talbot & Jakeman, 2008:201).

Omdat in het Bow Tie Model zowel gekeken wordt naar de bedreigingen vóór de ongewenste gebeurtenis als de gevolgen ná de ongewenste gebeurtenis is dit minder bruikbaar voor dit onderzoek. Want zodra het geheim geopenbaard is, is het kwaad al geschied: “Een geheim dat is uitgelekt is geen geheim meer. Het is zoals met ouder worden: een onomkeerbaar proces” (Hins, 2008:149). Uiteraard zijn er maatregelen te nemen om de gevolgen van de compromittering te beperken – bijvoorbeeld persoonsbeveiliging, een andere identiteit en verhuizen bij het uitlekken van een lijst van informanten – maar dat valt buiten het kader van dit onderzoek.

2.6 Gelaagdheid aan maatregelen

Een ongewenste gebeurtenis kan meerdere oorzaken hebben. Hoe meer lagen aan onafhankelijk werkende maatregelen er zijn, des te kleiner de kans dat een dreiging zich kan manifesteren.

2.6.1 Ensure no single point of vulnerability

Dit principe wordt ook toegepast in het Amerikaanse normenkader ‘Computer Security’: “Ensure no single point of vulnerability. Security designs should consider a layered approach to address or protect against a specific threat or to reduce vulnerability” (Stoneburner, Hayden & Feringa, 2004:13).

‘Computer Security’ is als normenkader vergelijkbaar met de Nederlandse ‘Code voor Informatiebeveiliging’: “Toepassing van meer dan één barrière biedt extra bescherming, omdat het falen van één enkele barrière niet betekent dat de beveiliging onmiddellijk is gecompromitteerd” (Code voor Informatiebeveiliging, 2007:38), ook al wordt in de Code voor Informatiebeveiliging alleen gedoeld op fysieke barrières, niet op organisatorische maatregelen.

Ook Schneier onderschrijft het belang van gelaagdheid aan maatregelen: “Good security systems are resilient. They can withstand failures; a single failure doesn’t cause a cascade of other failures. They can withstand attackers, including attackers who cheat” (Schneier, 2003:120). Dit is een belangrijk uitgangspunt voor security officers, kwaadwillenden houden immers geen rekening met ‘spelregels’. Een voorbeeld van het zich niet houden aan de spelregels – in dit geval het embargo – is de volgende casus (Casus 4).

Casus 4: Het Prinsjesdagstuk onder embargo

“In 2009 zijn op vrijdag 11 september om 16.00 uur de Miljoenennota, de MEV [Macro Economische Verkenningen, JHM] en alle afzonderlijke begrotingshoofdstukken in één doos gebundeld onder embargo voor alle Kamerleden beschikbaar. Voor de grotere fracties zijn vijf dozen beschikbaar, voor kleinere fracties twee en het lid Verdonk ontvangt één doos met stukken. Tevens ontvangt de Voorzitter één doos met stukken. Op zaterdag 12 september 2009 is, ook om 16.00 uur, voor de fracties het Belastingplan 2010 beschikbaar.

Op vrijdag 11 september om 16.03 uur komt het ANP met een persbericht, met veel cijfers en feiten die afkomstig zijn uit de Prinsjesdagstukken. Kort daarna (om 16.19 uur) verschijnt een bericht op NOS Teletekst waarin wordt gemeld dat de gemiddelde Nederlander er volgend jaar een kwart procent in koopkracht op achteruit gaat: "Dat blijkt uit stukken die het kabinet op Prinsjesdag presenteert en waar de NOS de hand op heeft weten te leggen." Om 16.30 uur komt de NOS met een extra journaal. Op zaterdag 12 september toont RTL Nieuws in de uitzending van 19.30 uur de Miljoenennota en de MEV.

Op maandagmiddag 14 september deelt (volgens een ANP-bericht van 16.14 uur) Tweede Kamerlid en financieel woordvoerder Paul Tang (PvdA) mee dat hij "begrotingscijfers" voor 2010 heeft verstrekt aan RTL Nieuws. Naar later blijkt gaat het om het embargo-exemplaar van de MEV.”

(De Wijkerslooth de Weerdesteijn, De Beaufort & Borst-Eilers, 2010:20-21)

Deze casus geeft echter ook het belang van de gelaagdheid van maatregelen aan. Naast het embargo, waarbij vertrouwd wordt op de belofte van geheimhouding, heeft men ook aanvullende maatregelen genomen, zoals het aanbrengen van een watermerk. Hierdoor kon – achteraf – de bron van het lek achterhaald worden. Journalisten houden overigens wel rekening met dit soort beveiligingsmaatregelen: "We hebben nog steeds een potje ouderwetse Tipp-Ex op de redactie. We verwijderen namen, adressen, nummers. De rand met het faxnummer knippen we eraf en dan

kopiëren we het nog een keer" (Interview F. Wester, 03-02-2011). Als de bron dan toch gevonden wordt is dat wel zuur voor zowel de lekker als de journalist:

> Daar waren we echt ziek van. We hadden speciaal blaadjes achter de pagina's gedaan tegen doorschijnen en de voorpagina overgetikt. We wisten dat er merkingen konden zijn door interpunctieverschillen, punten en komma's. Maar we wisten niet dat het watermerk er met speciale software uitgefilterd kon worden. (Interview F. Wester, 03-02-2011)

2.6.2 Practical drift

Die 'spelregels' waar Schneier aan refereerde worden niet alleen genegeerd door kwaadwillenden. Ook intern kan het voorkomen dat men de 'spelregels' niet hanteert. Maatregelen zoals regels, procedures en middelen worden voorgeschreven vanuit een bepaalde verwachting van risico's. Zeker als bij het bepalen van de maatregelen wordt uitgegaan van 'worstcase scenario's' kunnen deze belastend zijn voor het werken onder normale omstandigheden, ze passen dan niet in de meeste gevallen (daarom kunnen regels en procedures van HRO's zoals vliegdekschepen en kerncentrales niet één-op-één overgenomen worden door 'normale' organisaties zoals een ministerie). Dit kan leiden tot het overtreden van de regels.

Scott Snook heeft dit beschreven in zijn onderzoek 'Friendly Fire' naar de oorzaken van het neerschieten van twee Amerikaanse Black Hawk helikopters door eigen gevechtsvliegtuigen op 14 april 1994: "When the rules don't match, pragmatic individuals adjust their behavior accordingly; they act in ways that better align with their perceptions of current demands. In short, they break the rules" (2000:193).

Snook noemt dit 'practical drift', dit is "the slow, steady uncoupling of local practice from written procedure" (2000:220). Terwijl men zelf afwijkt van de norm gaat men er ondertussen vanuit dat de ander zich wel aan de norm houdt: "It is the fact that individuals in different subgroups act based on the assumption that people outside their own unit are behaving in accordance with the original set of established rules" (Snook, 2000:198). Hierdoor ontstaan ongelukken, zoals 'friendly fire'.

Het verschijnsel van practical drift is ook te zien bij verwijtbaar lekken. Bijvoorbeeld in geval men gerubriceerde informatie bij het tijdelijk verlaten van de ruimte niet opbergt omdat er vanuit wordt gegaan dat de toegangsbeveiliging tot het gebouw of de sociale controle op de gang voorkomt dat kwaadwillenden beschikking krijgen over de gerubriceerde informatie. Een ander voorbeeld is het onversleuteld per e-mail verzenden van gerubriceerde informatie omdat dit 'binnen het netwerk van de organisatie' blijft, zonder hierbij rekening te houden met zaken als het automatisch doorsturen van e-mail – bijvoorbeeld naar een huisadres of andere collega's bij vakantie – of het per abuis doorsturen naar een andere partij door een typefout in de adressering. Maar zelfs het beginsel 'need to know, nice to know' is hier een voorbeeld van: de houder van de gevoelige informatie deelt de informatie met een derde – uit sensatiezucht of om interessant te doen – onder voorwaarde dat dit 'entre nous' blijft, dat het niet met derden gedeeld wordt. Deze derde deelt het opnieuw met een onbevoegde om dezelfde reden en onder dezelfde voorwaarde.

2.7 Gerubriceerde en gevoelige informatie (geheimen)

In paragraaf 2.2 is het begrip informatie al behandeld. In deze paragraaf wordt nader ingegaan op gerubriceerde en gevoelige informatie. De uitleg van deze begrippen wordt beperkt tot deze vormen van informatie van de Rijksoverheid. Gerubriceerde en gevoelige informatie tezamen worden in deze thesis geheimen genoemd.

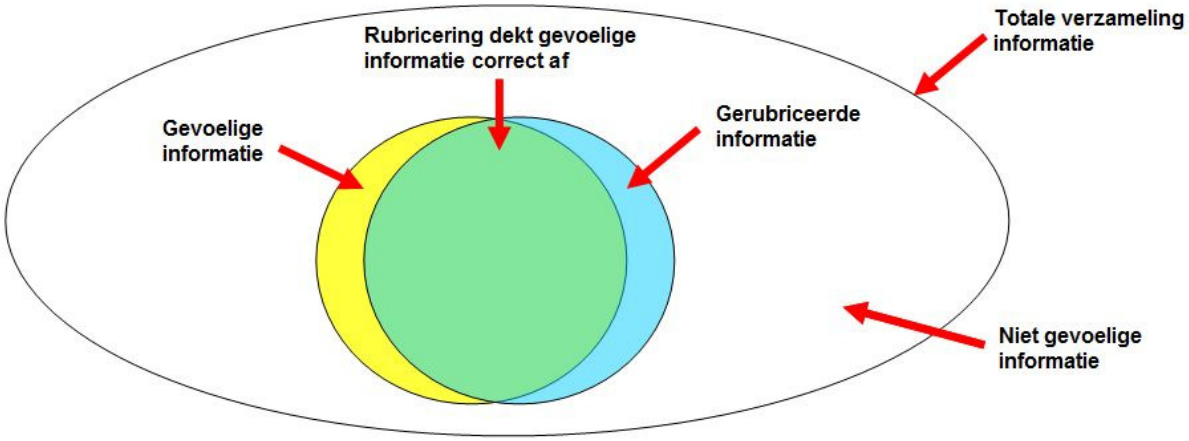
Schneier geeft overigens aan dat er een onderscheid te maken is in geheimen die veerkrachtig ('resilient') zijn en in geheimen die broos ('brittle') zijn. Veerkrachtige geheimen zijn eenvoudig te wijzigen wanneer compromittering geconstateerd of vermoed is, bijvoorbeeld pincodes en wachtwoorden, als het goed is worden deze ook regelmatig vervangen. Broze geheimen zijn moeilijk te wijzigen, het zijn: […] system-wide secrets and can include security procedures, details about vulnerabilities and targets, and access details" (Schneier, 2003:126).

Zoals in hoofdstuk 1 al is aangegeven, zijn er uitzonderingen op het beginsel dat alle overheidsinformatie openbaar is. Die uitzonderingen kunnen bijvoorbeeld van toepassing zijn op informatie die raakt aan de eenheid van de Kroon, de veiligheid van de Staat, bedrijfs- en fabricagegevens en persoonsgegevens (artikel 10, eerste lid, WOB) en ten aanzien van persoonlijke beleidsopvattingen (artikel 11 WOB). Als openbaarmaking van deze informatie nadeel of schade oplevert voor het betrokken departement, de Staat en/of een van zijn bondgenoten, dan is er sprake van gevoelige informatie en behoort deze gerubriceerd te zijn.

2.7.1 Eclips Model

Als deze informatie inderdaad gerubriceerd is, dan wordt dat in het Vir-bi bijzondere informatie genoemd: “staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries” (artikel 1 onder a, Vir-bi). Het is dus mogelijk dat de informatie wel gevoelig is, maar dat het door een omissie niet gerubriceerd is, terwijl dat wel zo had moeten zijn. Ook kan er sprake zijn van informatie die gevoelig is omdat bijvoorbeeld het interne beraad nog niet is afgerond. Daarom wordt in deze thesis ook de term gevoelige informatie gebruikt. Andersom is het ook mogelijk dat informatie wel gerubriceerd is, maar niet gevoelig. De informatie is dan ten onrechte of overgerubriceerd.

In figuur 2.5 wordt dit geïllustreerd. Idealiter past binnen de totale verzameling informatie de blauwe schijf met gerubriceerde informatie naadloos over de gele schijf met gevoelige informatie, daar waar ze elkaar overlappen zijn ze groen: de rubricering dekt de gevoelige informatie correct af. In de praktijk is dat niet altijd het geval. De linker gele ‘sikkel’ is onbedekt, deze gevoelige informatie is ten onrechte niet gerubriceerd. De rechter blauwe ‘sikkel’ bedekt informatie die niet gevoelig is, deze informatie is overgerubriceerd. Dit noem ik het ‘Eclips Model’ vanwege de overlap en de twee sikkels.



Figuur 2.5: Eclips Model: De twee sikkels geven de ten onrechte gerubriceerde en niet-gerubriceerde informatie weer. Idealiter is er een volledige overlap van gerubriceerde en gevoelige informatie

2.7.2 Formele en materiële geheimen

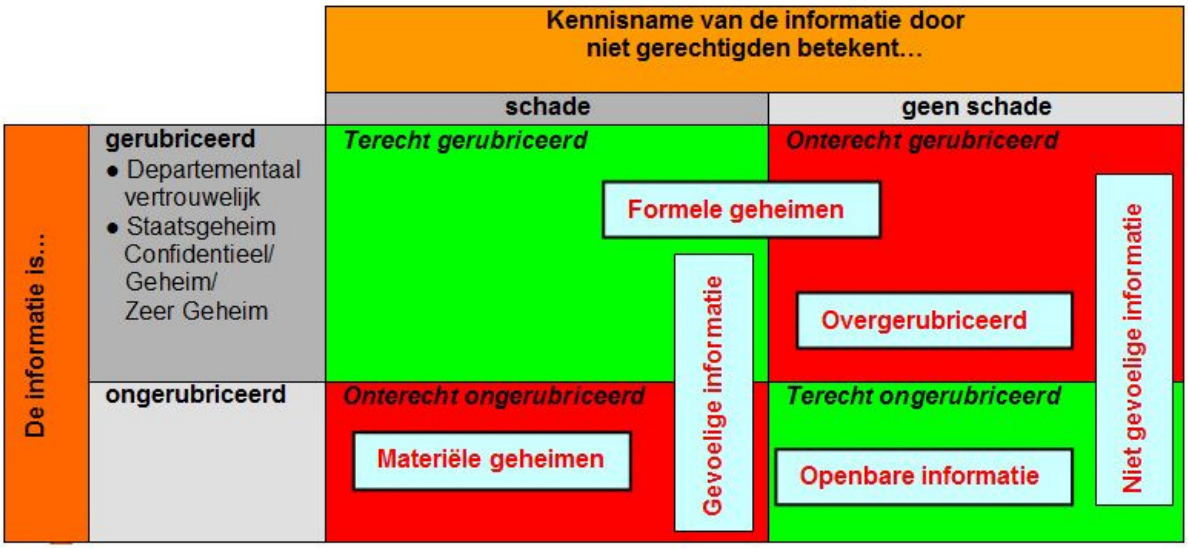
Gerubriceerde informatie wordt onderverdeeld in staatsgeheime en departementaal vertrouwelijke informatie. Er is sprake van een staatsgeheim wanneer er sprake is van “bijzondere informatie waarvan de geheimhouding door het belang van de Staat of zijn bondgenoten wordt geboden” (artikel 1 onder b Vir-bi). Naar gelang van de schade, ernstige schade of zeer ernstige schade die het kennisnemen door niet gerechtigden kan toebrengen van de Staat of zijn bondgenoten wordt een staatsgeheim (ook wel afgekort tot: Stg.) gerubriceerd als respectievelijk Stg. Confidentieel, Stg. Geheim en Stg. Zeer Geheim (artikel 5, eerste lid, Vir-bi). Onder het regime van het Vir-bi valt dus ook gerubriceerde informatie van bondgenoten, de Europese Unie en de Noord-Atlantische Verdrags-Organisatie (zie bijlage V voor een vergelijking van de diverse internationale beveiligings-rubriceringen). Bijzondere informatie die geen staatsgeheim is wordt als Departementaal Vertrouwelijk gerubriceerd indien kennisnemen door niet gerechtigden nadeel kan toebrengen aan het belang van één of meer ministeries (artikel 5, tweede lid, Vir-bi).

Het niveau van rubricering dient aangegeven te zijn op het document (bijvoorbeeld 'Departementaal Vertrouwelijk' of 'Staatsgeheim Zeer Geheim') en de informatie dient op een voorgeschreven wijze behandeld te worden voor wat betreft de wijze van opslag, vervoer en vernietiging: "Bijzondere informatie wordt zodanig beveiligd dat alleen personen die daartoe zijn gerechtigd bijzondere informatie kunnen behandelen of inzien voor zover dit noodzakelijk is voor een goede uitoefening van hun taak en dat inbreuken op de beveiliging worden gedetecteerd en gedegen onderzoek naar (mogelijke) inbreuken mogelijk is" (artikel 12, eerste lid, Vir-bi).

Als aan de formele eisen uit het Vir-bi voldaan is zou men kunnen spreken van 'formele geheimen'. Het kan echter ook voorkomen dat aan de formele eisen uit het Vir-bi niet voldaan is – het staat er letterlijk niet op – maar de houder van de informatie begreep of had behoren te begrijpen dat de informatie gevoelig is en openbaarmaking een afbreukrisico vormt, dan zou men kunnen spreken van 'materiële geheimen'. Deze redenering is ook terug te vinden in het Wetboek van Strafrecht:

> Hij die enig geheim waarvan hij weet *of redelijkerwijs moet vermoeden* dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie. (Artikel 272, eerste lid, Sr; cursivering JHM)

De positie van de formele en materiële geheimen ten opzichte van gevoelige en gerubriceerde informatie wordt geïllustreerd in figuur 2.6.



Figuur 2.6: Relatie gevoelige en gerubriceerde informatie: Formele en materiële geheimen

2.7.3 Geheimen en openbaarmaking

Aan het begin van deze paragraaf is aangegeven dat alle overheidsinformatie in beginsel openbaar is. Het rubriceren van informatie betekent dat er een beveiligingsregime op van toepassing is. In tegenstelling tot wat gedacht zou kunnen worden is het niet zo dat wanneer gerubriceerde informatie op grond van de WOB wordt opgevraagd, dit verzoek zonder meer kan worden geweigerd. Per geval wordt bezien of tot openbaarmaking kan worden overgegaan. Van openbaarmaking kan slechts worden afgeweken indien daarvoor een grond aanwezig is zoals bedoeld in de artikelen 10 en 11 van de WOB (Vir-bi, 2004:10). In veel gevallen zal hier sprake van zijn, maar als uit – ambtelijke of rechterlijke – toetsing blijkt dat de informatie ten onrechte gerubriceerd is, of wanneer de noodzaak vervallen is, dan kan de informatie gederubriceerd en vervolgens openbaar gemaakt worden.

De Commissie Wallage – dat de toekomst van de Overheidscommunicatie onderzocht heeft – heeft enkele kanttekeningen geplaatst bij het weigeren van openbaarmaking:

> Terwijl de WOB vanuit de burger bezien een grote stap voorwaarts was, is de omgang ermee binnen de overheid veelal defensief van karakter gebleven. Veel van de bestuurlijke en

ambtelijke energie is blijven steken in debatten over de uitzonderingsgronden bij passieve openbaarheid. (Wallage et al., 2001:37)

Rubriceringen zijn in beginsel gebonden aan een termijn van maximaal tien jaar of een bepaalde gebeurtenis en vervallen daarna automatisch (artikel 6, eerste lid, Vir-bi). Slechts in een beperkt aantal gevallen geldt een langere rubriceringstermijn, maar ook dan moet na uiterlijk twintig jaar opnieuw beoordeeld worden of de rubricering herzien of beëindigd kan worden (artikel 6, tweede en derde lid, Vir-bi). Dit houdt mede verband met de kosten die verbonden zijn aan de beveiligingsmaatregelen voor gerubriceerde informatie (Vir-bi, 2004:13).

2.8 Intentionele en verwijtbare compromittering (lekken)

De termen lekken of uitlekken worden geregeld gebruikt wanneer geheimen in de openbaarheid komen. Toch blijkt het lastig te zijn hier een goede wetenschappelijke definitie voor te vinden. Bovendien bestaan er diverse soorten lekken. In deze paragraaf wordt hier nader op ingegaan.

2.8.1 Lekken gedefinieerd

Voor de term (uit)lekken in relatie tot informatie bestaan verschillende definities zoals (niet limitatief):

- Een geheim (opzettelijk) laten uitlekken (De Boer, 1996:618; “Uitlekken”, g.d.).
- Het (van iemand in een organisatie) onbevoegd en voortijdig interne informatie naar buiten bekendmaken (“Lekken”, g.d. a).
- Het verschijnsel dat vertrouwelijke informatie terechtkomt bij iemand die volgens de eigenaar van die informatie, die informatie niet zou mogen hebben (“Lekken”, g.d. b).
- Vertrouwelijke informatie uit besloten vergaderingen en beleidsdocumenten doorgespeeld aan de pers met de bedoeling de loop van de besluitvorming te beïnvloeden (Bovens, 't Hart & Van Twist 2007:178).
- Het naar buiten brengen van vertrouwelijke informatie (Bovens, Geveke & De Vries 1993:62).
- Het op basis van anonimiteit in de openbaarheid brengen van vertrouwelijke informatie door beklederes van politiek-bestuurlijke posities (Bovens, Geveke & De Vries 1993:62).
- Elk handelen of nalaten van handelen dat tot gevolg heeft dat die informatie op basis van anonimiteit zonder autorisatie in de openbaarheid komt, waarvan een ieder gelet op het vertrouwelijke karakter daarvan weet of in redelijkheid kan weten dat geheimhouding geboden is (Lemstra, Brouwers, Niessen, Wuisman & Schouten, 2005:17).

Ook aan de respondenten is tijdens de interviews gevraagd naar hun eigen definitie van lekken. Deze liepen evenzeer uiteen als de bovenstaande definities. Zo werd het geautoriseerd handelen bij de ene respondent wel onder lekken geschaard en bij de andere niet, hetzelfde gold voor het opzettelijk en niet opzettelijk handelen. Voor sommige respondenten was de rol van de media essentieel en voor andere niet. Tot slot waren er respondenten voor wie lekken de intentie moest hebben op het beschadigen van een andere partij of om een politiek of maatschappelijk belang te dienen.

In ieder geval is – zowel in de literatuur als bij de respondenten – het onthullen van een geheim, van de vertrouwelijkheid, essentieel. In het Vir-bi wordt geen definitie van 'lekken' gegeven, daarvoor is de term wellicht te informeel. Wel wordt de term compromittering gedefinieerd: “de kennisname dan wel de mogelijkheid tot kennisnemen door een niet gerechtigde van bijzondere informatie” (artikel 1 onder g).

Ten onrechte wordt bij lekken altijd een verband gezocht met openbaarmaking via de media, zoals een krant, een televisieprogramma of een organisatie via internet. Dit is niet altijd het geval. In de Kwetsbaarheidsanalyse Spionage van de AIVD wordt veelvuldig gesproken over ‘weglekken’ van informatie (2010, p. 13, 18, 20, 27, 30, 31, 33, 34, 42, 47, 51, 53). Het gaat daarbij niet om lekken naar de media, maar om het verdwijnen van informatie naar vreemde mogendheden. Verder kan gedacht worden aan vertrouwelijke informatie dat ‘rond zingt’ binnen een bepaalde groep die niet gerechtigd is om kennis te hebben van deze informatie, zonder dat dit via de media bekend gemaakt is. Dit kan binnen een organisatie zijn, maar ook tussen gemeenschappen van mensen of organisaties, zoals in onderstaande casus (Casus 5).

Casus 5: Het domme lek

"Er was eens een onderzoek naar een illegale vuurwerkhandel. Het was een langdurig onderzoek, het ging om een grote hoeveelheid illegaal vuurwerk. Een van de betrokken rechercheurs kon niet met zijn vrouw mee naar een verjaardag omdat hij voorbereidingen moest treffen voor het oprollen van deze vuurwerkhandel.

Toen men op de verjaardag vroeg waarom de rechercheur er niet bij was zei zijn vrouw dat hij naar [plaatsnaam, JHM] moest, 'Iets met vuurwerk of zo'. Op dat feestje was ook een jongeman aanwezig die dit opving. Hij vermoedde dat het wel eens om de illegale handel kon gaan waar hij ook zijn vuurwerk haalde. Hij belde met de handelaar om hem in te lichten van zijn vermoeden, wellicht zat er wel een gratis vuurwerkpakket in. De handelaar nam geen risico en heeft de hele nacht doorgewerkt om de loods leeg te halen. Bij de inval door de politie bleek de loods helemaal leeg.

De zaak was stuk. En dat alleen maar omdat hij zijn vrouw had verteld dat hij naar die bepaalde plaats moest voor een vuurwerkzaak en zijn vrouw dit zich liet ontglippen. Er was geen boos opzet, maar het is een mooi voorbeeld van een dom lek. Daarom moet je heel terughoudend zijn richting je naaste omgeving over dit soort zaken, ook al vertrouw je je eigen vrouw nog zo veel. Als je niets aan je vrouw verteld hebt weet je ook zeker dat bij een lekzaak het in ieder geval niet per ongeluk via haar gegaan is."

(Interview H. Hummel, 28-12-2010)

Verder is het, zoals reeds aangegeven in paragraaf 1.4, voor de definitiebepaling van 'lekken' van belang dat de persoon die een gerechtigde houder is van de gerubriceerde of gevoelige informatie of die anderszins toegang heeft, *intentioneel* of *verwijtbaar* handelt, zoals men in het strafrecht spreekt van 'opzet' en 'schuld'.

Met intentioneel handelen in de zin van het strafrechtelijke opzet (dolus) wordt bedoeld dat de dader zich bewust was wat deze wilde (Van Bemmelen, Van Veen, Knigge & De Jong, 1998:57). De persoon had de intentie om een bepaald doel te bereiken. Met verwijtbaar handelen in de zin van de strafrechtelijke schuld (culpa) wordt bedoeld dat de dader pas iets te verwijten valt als deze 'het kon helpen', 'er iets aan kon doen'. Schuld heeft daarom te maken met de mogelijkheid van keuze. Het gedrag kan de dader verweten worden als deze de (reële) mogelijkheid had zich anders te gedragen dan hij of zij deed (Van Bemmelen, Van Veen, Knigge & De Jong, 1998:39). Factoren die buiten de directe invloedsfeer van betrokkene liggen, zoals technisch falen of overmacht en actieve spionage door inlichtingendiensten of criminelen in de vorm van afluisteren, hacking of afgifte onder dwang, vallen binnen dit onderzoek buiten de definitie van lekken.

In deze thesis wordt onder lekken verstaan:
Het intentioneel of verwijtbaar compromitteren van gerubriceerde of gevoelige informatie door een persoon die hiervan gerechtigd houder is of anderszins toegang heeft.

2.8.2 Indelingen van lekken

Er zijn in de literatuur diverse indelingen van lekken gevonden. De belangrijkste indeling die in diverse onderzoeken steeds weer terug komt is die van Bovens, Geveke en De Vries (Beenakkers & Grapendaal, 1995:17; Lemsta et al., 2005:15-17).

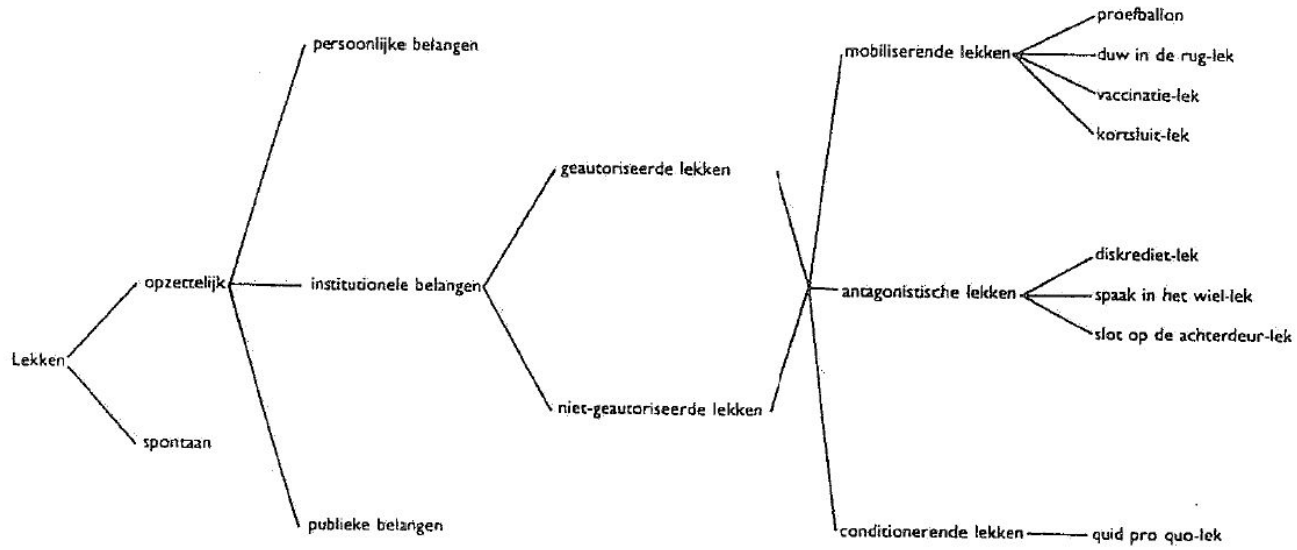
Bovens, Geveke en De Vries verstaan onder lekken "het op basis van anonimiteit in de openbaarheid brengen van vertrouwelijke informatie door beklederes van politiek-bestuurlijke posities" (1993:62). In hun publicatie richten zij zich vooral op lekken via de media.

Zij maken een eerste onderscheid tussen spontaan en opzettelijk lekken. Onder spontaan lekken verstaan zij niet intentionele daden zoals versprekingen, het verliezen van een vertrouwelijk stuk en een afgeluisterd gesprek (Bovens, Geveke & De Vries, 1993:64). Ook het uitlokken van lekken door een journalist die op basis van 'snippers' informatie een vermoeden ontwikkeld heeft en dat vervolgens bij diverse bronnen verifieert – die hun mond voorbij praten – wordt onder spontaan lekken verstaan:

> Vaak voegt elke gesprekspartner in zo'n situatie relevante gegevens toe, hetzij omdat men in de veronderstelling verkeert dat anderen de vertrouwelijkheid ook hebben geschonden en men dus lekt in commissie, hetzij om te laten zien dat men ook insider is, of omdat men bang is dat het verhaal eenzijdig blijft en slecht voor de eigen positie zal uitpakken. Zo ontstaat

langzaam de lek en wordt de grens tussen bewust en onbewust lekken geleidelijk overschreden. (Bovens, Geveke & De Vries, 1993:65)

Opzettelijke lekken komen voort uit persoonlijke, publieke en institutionele belangen. Deze onderverdeling is schematisch weergegeven in figuur 2.7.



Figuur 2.7: Een verfijnde typologie van politiek-ambtelijke lekken (uit: Bovens, Geveke & De Vries, 1993:69)

Persoonlijke belangen kunnen zowel materieel als immaterieel van aard zijn. Bij materiële belangen gaat het vooral om geld of waardevolle zaken die men krijgt voor informatie die voor derden waardevol is, zoals subsidieregelingen, monetaire koerswijzigingen en persoonsgegevens. Bij deze motieven is er al gauw sprake van corruptie, fraude of (bedrijfs)spionage (Bovens, Geveke & De Vries, 1993:65). Bij immateriële belangen gaat het om het maken of breken van een carrière, het verhogen van de eigen status of ten behoeve van de relatie met de journalist (Bovens, Geveke & De Vries, 1993:66).

Lekken vanwege publieke belangen zijn gericht op het onthullen van (vermeende) misstanden binnen de organisatie of maatschappij, zoals fraude, wetsovertredingen, mismanagement of andere vormen van deviant bestuur waarbij er een sterke verwantschap bestaat met klokkenluiden, werkweigering en andere vormen van intentioneel burgerschap (Bovens, Geveke & De Vries, 1993:66).

In hun publicatie richten Bovens, Geveke en De Vries zich vooral op het lekken vanuit institutionele belangen. Men lekt dan in het belang van de eigen afdeling, het departement of de sector als een van de vele strategieën en tactieken in het (bureau)politieke spel: “Met het naar buiten brengen van vertrouwelijke informatie wordt getracht de eigen institutionele positie in de besluitvorming te verstevigen en die van rivalen te ondermijnen (Bovens, Geveke & De Vries, 1993:67). Als het lekken plaatsvindt met medeweten, toestemming of (stilzwijgende) instemming van een hoger geplaatste in de organisatie – van afdelingshoofd tot de minister – is er sprake van geautoriseerd lekken (Bovens, Geveke & De Vries, 1993:68). Het lekken vanuit institutionele belangen is weer te onderscheiden in mobiliserende lekken, antagonistische lekken en conditionerende lekken.

Mobiliserende lekken zijn gericht op het beïnvloeden van de eigen achterban, de publieke en politieke opinie. Voorbeelden hiervan zijn het 'proefballonnetje', veelal een geautoriseerd lek om de stemming voor een bepaald beleidsvoornemen te peilen, het 'duw-in-de-rug-lek' om steun voor een bepaald beleid te verwerven (in de Angelsaksische literatuur ook wel een 'plant' genoemd), het 'vaccinatie-lek' om juist verzet tegen een bepaald beleid te creëren en het 'kortsluit-lek' om hiërarchische en formele procedures te omzeilen en zo de aandacht te trekken van de politieke en ambtelijke top (Bovens, Geveke & De Vries, 1993:69-70).

Onder antagonistische lekken wordt verstaan het vanuit frustratie een persoon of een instelling in een kwaad daglicht stellen. Voorbeelden hiervan zijn het 'diskrediet-lek', variërend van vermeende incompetentie en disloyaliteit tot fraude, corruptie of afwijkende seksuele gewoonten, het 'spaak-in-het-wiel-lek' om zaken die in de doofpot dreigen te geraken er weer uit te halen of om besluitvorming

te verhinderen, te vertragen, te saboteren of stop te zetten en het 'slot-op-de-achterdeur-lek' om te zorgen dat bepaalde besluiten niet meer teruggedraaid kunnen worden. Deze laatste vorm hebben vaak een 'positieve' boodschap zoals mogelijke belastingverlagingen of salarisverhogingen. Men wordt voor een voldongen feit gesteld en terugdraaien of ontkennen leidt tot prestige- of legitimiteitsverlies (Bovens, Geveke & De Vries, 1993:70-71).

Conditionerende lekken zijn gericht op de media die een belangrijke rol vervullen bij het informeren van het publiek, het promoten van beleid, het verwerven van steun of het hinderen van tegenstanders. Lekken van vertrouwelijke informatie is dan een manier om een goede relatie op te bouwen en in stand te houden: de journalist heeft met de vertrouwelijke informatie een primeur en de politicus of ambtenaar zijn verhaal in de krant. Lekken met het oog op het kweken van goodwill noemen Bovens, Geveke en De Vries het ‘quid-pro-quo-lek’ (1993:70-72). Een voorbeeld hiervan is de reactie die door een journalist aan de politicus wordt gevraagd, nadat deze iets, direct of via de voorlichter, aan dezelfde journalist heeft laten lekken. De politicus verkrijgt dan naamsbekendheid als beloning voor informatie. Als dit te vaak gebeurt kan het wel op gaan vallen:

> Zo reconstrueren voorlichters ook lekken waar ze zelf niet achter zitten; ze pakken alle artikelen van de journalist die over het lek berichtte, en kijken dan welke politici positief in die stukken langskomen; zeer waarschijnlijk zit daar dan degene tussen die een dealtje heeft gesloten. Het is een eindeloos kat-en-muisspel, en sommige politici bedingen nu bij journalisten: ‘Ik wil niet geciteerd worden in jouw stuk wanneer in datzelfde stuk ook anonieme bronnen worden opgevoerd’. (Luyendijk, 2010:73)

Naast de indeling van Bovens, Geveke en De Vries noemen Beenakkers en Grapendaal de indelingen van Hess, van Brants, van Van Venetië en Eringa (Beenakkers & Grapendaal, 1995:18-19).
De indeling van Hess richt zich op de relatie tussen media en overheid en wordt onderverdeeld naar het ego-lek, het goodwill-lek, het beleidslek, het lek uit wrok, het proefballonlek, het klokkenluiderslek en het lekken zonder doel.
De indeling van Brants maakt onderscheid tussen het morele lek, het lek uit profijt, het politieke lek en het journalistieke lek.
Van Venetië noemt het emotionele lek (de lekker is verontwaardigd over het beleid), het strategische lek, het lek voor de aardigheid (omdat men de journalist mag) en het lek per ongeluk.
Tot slot wordt het onderscheid van Eringa genoemd waarbij er vanuit wordt gegaan dat lekken vrijwel altijd opzettelijk, met een specifiek vooropgezet doel geschiedt: financieel gewin, manipulatie en rancune.

In dit onderzoek is de indeling van Bovens, Geveke en De Vries aangehouden omdat deze typologie het meest uitgebreid is.

3. HET BELANG VAN GEHEIMEN EN HET LEKKEN ERVAN

3.1 Inleiding

In dit hoofdstuk wordt ingegaan op gerubriceerde en gevoelige informatie – samengevat als 'geheimen' – als belang. Waarom zijn er geheimen en waarom zijn deze belangrijk? Het belang van geheimen wordt vanuit drie dimensies bekeken: de ethische dimensie, de juridische dimensie en de politiek-bestuurlijke dimensie in respectievelijk de paragrafen 3.2, 3.3 en 3.4. Dit hoofdstuk wordt afgesloten met het belang van duiding in paragraaf 3.5.

3.2 De ethische dimensie van geheimen en het lekken ervan

In deze paragraaf wordt ingegaan op de ethische kant van het geheim. Is het ethisch bezwaarlijk om een geheim te lekken? En is het dan *altijd* ethisch bezwaarlijk om een geheim te lekken? Door middel van een korte beschrijving van de ethiek en drie hoofdstromingen in de normatieve ethiek en vervolgens de toepassing hiervan wordt getracht een antwoord te formuleren op deze vragen.

3.2.1 Ethiek

De ethiek is een zogenoemde praktische stroming binnen de filosofie waarin wordt nagedacht over de praxis, het menselijk handelen. Het woord ethiek komt van het Griekse 'èthos' wat gebruik, gewoonte of zeden betekent. Zedenleer, praktische filosofie en moraalfilosofie zijn synoniemen van het woord ethiek.

> Het gaat in de ethiek niet om de niet-menselijke wereld, maar over de mens; en dan niet over de mens als wezen dat kennis vergaart, of dat al dan niet gelooft, maar over de mens als een wezen dat handelend optreedt. Het praktische van de ethiek zit 'm echter niet alleen in het object, maar ook in het doel: het gaat in dit nadenken-over-de-praxis *om* de praxis zelf: het gaat erom het handelen zo goed mogelijk te laten zijn. De ethiek denkt na over hoe het handelen moet zijn oftewel de moraal. Ze is een normatieve discipline. (Van Tongeren, 2003:15-16)

De ethiek wordt onderscheiden in descriptieve, prescriptieve en normatieve ethiek. In de descriptieve of beschrijvende ethiek gaat het om het bestuderen en beschrijven van moraal zonder dat zelf een moreel standpunt wordt ingenomen. De vraag of een handeling goed of slecht is, wordt niet door de descriptieve ethiek beantwoordt, maar door de prescriptieve ethiek. Bij prescriptieve of voorschrijvende ethiek wordt een moreel standpunt ingenomen (en uitgedragen) inzake handelingen en gebeurtenissen. Binnen de normatieve ethiek worden theorieën ontwikkeld die voorschrijven welke handelingen van de mens goed dan wel fout zijn (Vaartjes 2008). De normatieve ethiek kent weer drie hoofdstromingen die in de volgende subparagraaf nader toegelicht worden.

3.2.2 Deugdethiek, consequentialisme en deontologie

Er zijn drie hoofdstromingen in de normatieve ethiek: de deugdethiek, het consequentialisme en de deontologie (Becker, 2007:40). De deugdethiek richt zich op de persoon en zijn morele kwaliteiten, namelijk houding en karakter. Het consequentialisme en de deontologie richten zich op de handelingen (Van Tongeren & Becker, 2009:59).

De deugdethiek of deugdenethiek richt zich op de ontwikkeling van het karakter om de juiste moraal te bepalen. Deze traditie begon bij de Griekse Aristoteles (384-322 v.C.). In zijn 'Ethica Nicomachea' schrijft hij: "Iedere vaardigheid en ieder onderzoek lijkt – evenals iedere handeling en ieder voornemen – op iets goeds uit te zijn. Daarom zegt men terecht dat het goede datgene is waarop alles uit is" (Van Tongeren, 2003:38). Vanaf de Oudheid tot aan de Verlichting was de deugdethiek een dominante benadering van morele dilemma's. Een belangrijke bijdrage aan de deugdethiek is geleverd door Thomas van Aquino (1225-1274), die spreekt over vier kardinale deugden, de 'virtues cardinales'. Virtue is Latijn voor deugd. Het woord 'kardinale' is afgeleid van het Latijnse woord 'cardo' dat, 'scharnierpin', 'spil' of 'as' betekent. Kardinale deugden zijn dan ook deugden die onmisbaar zijn voor een deugdelijk leven. Deze deugden zijn zo belangrijk omdat ze in elke mogelijke andere deugd

aanwezig zijn. De vier kardinale deugden zijn moed, gematigdheid, verstandigheid en rechtvaardigheid (Becker, 2007:86). Binnen de deugdethiek wordt een moreel dilemma dus benaderd door te beredeneren hoe een deugdzaam mens zou handelen in de gestelde situatie. Past de keuze bij die situatie, is die keuze duurzaam en blijft men bij deze keuze trouw aan het eigen karakter?

Het consequentialisme of gevolgenethiek evalueert de uitkomst (de consequentie, het gevolg) van een handeling om een oordeel te vellen. De morele juistheid van een handeling wordt bepaald door het resultaat (de gevolgen) van de handeling. Heiligt het doel de middelen? Een belangrijke school binnen het consequentialisme is het utilitarisme. Hierbij is de juiste handeling die handeling waarvan het resultaat het meeste nut oplevert voor iedereen die door de handeling wordt geraakt, dan wel voor een zo groot mogelijk aantal mensen. Een van de belangrijkste grondleggers van het utilitarisme is Jeremy Bentham (1748-1832), hij definieert het utilitarisme als volgt:

> Onder het principe van utiliteit versta ik het principe dat een handeling goed- of afkeurt al naar gelang de neiging die de handeling vertoont om het geluk van de betrokken partij te vermeerderen of te verminderen, of wat hetzelfde is, dat geluk te bevorderen of te verhinderen. Ik heb het oog op alle handelingen, dus niet alleen het handelen van privé-personen, maar ook alle regeringsmaatregelen. Onder utiliteit versta ik die eigenschap van een zaak waardoor het de neiging vertoont om nut, voordeel, vreugde, het goede of het geluk te bevorderen, of om onheil, pijn, kwaad of ongeluk te voorkomen voor de partij om wiens belang het gaat: wanneer die partij de gemeenschap in het algemeen is, dan gaat het dus om het geluk van de gemeenschap en wanneer die partij een bepaalde persoon is, dan gaat het om het geluk van het individu. (Jeurissen, 2001:83)

De handeling zelf is niet juist of onjuist, het gaat er dus om of de gevolgen juist zijn. Het utilitarisme is verder uitgewerkt door John Stuart Mill (1806-1873). In ‘Utilitarianism’ nuanceert Mill het rechtlijnige ‘greatest happiness’-principe van Bentham door te stellen dat er kwalitatief verschillende soorten geluk bestaan:

> The creed which accepts as the foundation of morals ‘utility’ or the ‘greatest happiness principle’ holds that actions are right in proportion as they tend to promote happiness; wrong as they tend to produce the reverse of happiness. By happiness is intended pleasure and the absence of pain; by unhappiness, pain and the privation of pleasure. (Driver, 2007:48)

Het begrip ‘geluk’ slaat niet zozeer op directe behoeftebevrediging maar refereert aan het geheel van menselijke activiteiten, ín en dóór het verrichten van activiteiten: “En verschillen in activiteiten leiden tot kwalitatieve verschillen tussen gelukservaringen. Intellectuele activiteit en goed handelen tegenover de medemens verschaffen onvergelijkbaar veel meer vreugde dan meer banale activiteiten” (Becker, 2007:44).

Interessant is het werk van Nicollò Machiavelli (1469-1527), die zowel filosoof als politicus was. In ‘De heerser’ (Il Principe) schrijft Machiavelli:

> Een verstandig heerser kan noch mag zijn woord houden wanneer dit hem schade berokkent en wanneer de redenen die hem tot zijn belofte gebracht hebben, zijn weggevallen. Als de mensen allemaal goed waren, zou dit advies niet juist zijn. Maar omdat ze slecht zijn en ze ook ten opzichte van jou hun woord niet zullen houden, hoef jij dit evenmin tegenover hén te doen. (….) Want de mensen zijn zó onnozel en richten zich zó op hun directe behoeften dat iemand die bedriegt altijd wel iemand vindt die zich wil laten bedriegen. (Machiavelli, 1995:124-125)

Dit is een voorbeeld van utilistisch denken: het doel heiligt de middelen, niet zozeer vanuit het eigenbelang van de heerser, maar vooral vanuit het belang van de staat, ook al maakt hij zich daarbij niet altijd geliefd:

> Toch moet een heerser ervoor zorgen dat hij op zodanige wijze gevreesd wordt dat hij, ook al slaagt hij er niet in de liefde van zijn onderdanen te winnen, toch in elk geval hun haat weet te ontlopen. Want gevreesd en niet gehaat worden kan heel goed samengaan. (Machiavelli, 1995:121)

De deontologie – ook bekend als plichtsethiek, plichtenleer en beginselleer – gaat in op de vraag of een handeling intrinsiek goed of fout is ('deon' is Grieks voor 'plicht'). Het gaat uit van absolute gedragsregels, een handeling die slecht is, is volgens de deontologie *altijd* slecht, ook als de uitkomst goed zou zijn. Een belangrijk leerstuk van de deontologie is het categorisch imperatief van Immanuel Kant (1724-1804): "Handel alleen volgens die maxime [grondregel, JHM] waarvan je tegelijkertijd kunt willen dat zij een algemene wet wordt" (Becker, 2007:62). Volgens Kant is een deugdzaam mens iemand die zichzelf als levend wezen respecteert, zijn talenten ontwikkelt en het welzijn van anderen nastreeft. Deze drie verplichtingen zijn niet rechtens afdwingbaar. De volmaakte plicht jegens anderen is dat wel. Wie een belofte doet, verplicht zichzelf daartoe. Wie bewust een valse belofte doet, liegt dus, neemt tegelijkertijd een verplichting op zich en ontslaat zichzelf van die verplichting. Dat is een contradictie en kan dus niet tot natuurwet worden verheven.

Met het voornoemde onderscheidt de deontologie zich van het utilitarisme, waarin sommige daden die normaal gesproken als 'slecht' gepercipieerd worden, dat in bepaalde omstandigheden niet zijn. Vanuit het utilitarisme is liegen bijvoorbeeld niet per definitie verkeerd, immers, in tijden van oorlogen kunnen met leugens veel mensenlevens worden gered. Vaak wordt hierbij verwezen naar onderduikers en nazipraktijken tijdens de Tweede Wereldoorlog (Becker, 2007:65). Een ander voorbeeld waarbij het onderscheid tussen deontologie en utilitarisme naar voren komt is martelen. Vanuit deontologisch perspectief is martelen altijd slecht, een mens mag een ander mens niet doden of pijnigen, terwijl vanuit utilitaristisch perspectief martelen aanvaardbaar is om erger leed te voorkomen. Bijvoorbeeld om bij een ontvoerder de verblijfplaats van de ontvoerde te achterhalen (Miller, Blackler & Alexandra, 2006:148) of om van een terrorist te achterhalen waar en hoe een aanslag plaats zal vinden (Miller, Blackler & Alexandra, 2006:283).

3.2.3 Toepassing van de normatieve ethiek op het lekken van geheimen

De zeer beknopte beschrijving van de normatieve ethiek hierboven doet natuurlijk geen recht aan tweeënhalf millennium denken en schrijven over morele dilemma's. Toch is het hopelijk voldoende om in het licht van deze paragraaf de normatieve ethiek – de vraag of een handeling goed is of niet – toe te passen op het lekken van geheimen.

In het kader van dit onderzoek gaat het om hoe ambtenaren omgaan met bijzondere informatie. Ambtenaren zijn bijzondere werknemers, ze dienen namelijk het publieke belang. Max Weber (1864-1920) heeft de ambtenaar binnen de bureaucratie uitgebreid beschreven. De door Weber beschreven bureaucratie is een normatief model – dus niet persé een exacte weergave van de werkelijkheid – voor de organisatie van de werkzaamheden van ambtenaren en het reguleren van hun gedrag. In dit model worden ambtenaren geacht zich dienstbaar op te stellen en loyaal te conformeren aan de wensen van de politieke gezagsdragers. "De politiek is de baas (het primaat van de politiek), van ambtenaren wordt verwacht, zo niet geëist, dat zij de regels uitvoeren zoals die door de politiek zijn opgesteld (het leerstuk van de ambtelijke loyaliteit)" (Karssing & Spoor, 2009:73-74). Hierin past geen eigen afweging of bijzondere informatie tóch openbaar zou moeten zijn, dat is aan de politieke bestuurder. Weber wordt gezien als iemand uit de deontologische stroming van Kant (Becker, 2007:68).

Er zit echter ook een deugdethische kant aan het ambtenaarschap, dit is terug te vinden in artikel 50, eerste lid, van het Algemeen Rijksambtenarenreglement: "De ambtenaar is gehouden de plichten uit zijn functie voortvloeiende nauwgezet en ijverig te vervullen en zich te gedragen, zoals een goed ambtenaar betaamt." Het 'niet-lekken' van informatie behoort daar ook toe (Lemstra et al., 2005:12).

Zoals in hoofdstuk 1 al is aangegeven is overheidsinformatie over beleid – inclusief voorbereiding en uitvoering – in beginsel openbaar (artikel 8 WOB). Uiteraard zijn er wel uitzonderingsgronden, zoals persoonsgegevens en de veiligheid van de Staat (artikel 10 WOB). Vanuit utilitaristisch perspectief zou je kunnen stellen dat het geheimhouden van informatie of juist de onthulling ervan de 'greatest happiness' moet dienen. Informatie kan geheim zijn omdat bekendheid in een bredere kring schade kan opleveren voor de organisatie, de Staat of haar bondgenoten. Het naar buiten brengen van staatsgeheimen is een strafbaar feit (artikelen 98, 98a, 98b, 272 en 463 Sr). Deontologisch gezien is het lekken van een geheim dan ook nooit goed te praten. Als in het ene geval de informatie geheim moet blijven, dan is compromittering in een ander geval niet opeens 'goed'.

Utilitaristisch gezien ligt dat anders, daar gaat het immers om de gevolgen. Informatie kan namelijk geheim zijn verklaard, terwijl er inhoudelijk geen reden voor is. Bijvoorbeeld omdat de steller van het

document zich vergist heeft (bijvoorbeeld door een verkeerd documentformat) of een onjuiste inschatting van het belang van de informatie heeft gemaakt. Is het onjuist om bijzondere informatie te compromitteren die inhoudelijk geen enkele schade kan toebrengen? Informatie kan ook geheim zijn verklaard om het eigen falen te maskeren of om mogelijke criticasters informatie te onthouden. Informatie kan geheim verklaard worden om misstanden binnen de organisatie te verhullen of zelfs voort te kunnen laten duren. Het omgekeerde geldt overigens ook, bepaalde informatie kan een dusdanige aard hebben dat het gerubriceerd *had* moeten zijn en dat de betrokken persoon zich dat ook had moeten realiseren. De belangen tot het geheim verklaren van informatie én tot het compromitteren hiervan kunnen van persoonlijke, institutionele en publieke aard zijn (Bovens, Geveke & De Vries, 1993:65-66).

Organisaties en individuele medewerkers realiseren zich soms niet of onvoldoende wat de waarde is – ook voor anderen – van de informatie waarover zij beschikken of waartoe zij toegang kunnen verschaffen (AIVD, 2009:47). Dit kan soms heel sluipend in een organisatiecultuur ontstaan (zie ook subparagraaf 2.6.2 over practical drift):

> [Een integriteitsfunctionaris schetste, JHM] hoe mensen tijdens integriteitstrajecten worden geconfronteerd met een van de problemen die in die organisatie leven: omgaan met vertrouwelijke informatie. Hiervoor bestaan duidelijke regels die strikt nageleefd moeten worden. Die regels zijn onvoorwaardelijk verplichtend; wanneer mensen naar willekeur met vertrouwelijke informatie omgaan, kan [de organisatie, JHM] niet goed functioneren. Mensen die betrapt worden op grove schendingen, worden fors gestraft. De medewerkers van de organisatie worden geacht van de regels op de hoogte te zijn en zijn dat ook meestal. Maar dat 'op de hoogte zijn' kent gradaties. In de cultuur van een organisatie sluipen onvermijdelijk slordigheden waarin te soepel met regels wordt omgegaan. (Van Tongeren & Becker 2009:59)

Dit heeft een deugdethisch perspectief, het gaat er immers om hoe een deugdzaam mens zou handelen in de gestelde situatie. Past de keuze bij die situatie, is die keuze duurzaam en blijft men bij deze keuze trouw aan het eigen karakter?

Hanson en Ceppos hebben een viertal vragen geformuleerd om te bepalen of het ethisch is om te lekken en of het in sommige gevallen zelfs ethisch *verplicht* is om te lekken:

1. Wat is de status van de informatie? Is deze gerubriceerd of zit er een intellectueel eigendomsrecht op? Als dat zo is moet de informatie het waard zijn om te lekken.
2. Heeft de potentiële lekker een formele of informele plicht om de informatie juist te beschermen? Is de informatie verkregen omdat een ander de geheimhoudingsplicht geschonden heeft? Is van beide sprake, dan moet het een serieuze zaak zijn die onthuld wordt.
3. Betreft het publieke informatie, zoals beleid en het handelen als bestuurder, of betreft het zaken in de persoonlijke levenssfeer, zoals seksuele geaardheid, persoonlijke financiën of privégesprekken? Lastig hierbij wordt het wanneer het privéleven vermengd raakt met het publieke optreden.
4. De belangrijkste overweging is of er sprake is van een publiek belang van een lek en de schade die het veroorzaakt. Als gelekt wordt puur uit eigenbelang van de lekker, dan is dat fout. Als het lek een illegale overheidsdaad waar individuen schade van ondervonden hebben aan het licht brengt, dan is het ethisch eenvoudiger te verantwoorden.
   (Hanson & Ceppos, 2006)

Dit model lijkt op de diverse klokkenluidersregelingen die in de afgelopen decennia – mede naar aanleiding van het onthullen van geheimen – ontwikkeld zijn. Voor het Rijk en de politie geldt bijvoorbeeld dat misstanden gemeld kunnen worden indien sprake is van een vermoeden van een misstand, te weten:

> 1° een schending van wettelijke voorschriften of beleidsregels; 2° een gevaar voor de gezondheid, de veiligheid of het milieu; 3° een onbehoorlijke wijze van handelen of nalaten, die een gevaar vormt voor het goed functioneren van de openbare dienst; bij de organisatie waarin de melder werkt of heeft gewerkt of bij een andere organisatie indien hij uit hoofde van zijn ambtenaarschap met die organisatie in aanraking is gekomen en kennis heeft gekregen van de misstand" (artikel 1, eerste lid, onder e, Besluit melden vermoeden van misstand bij

> Rijk en Politie). De bruikbaarheid van deze regeling zal zich de komende jaren moeten bewijzen. Veelal is vanuit individueel standpunt een lek naar de media te verkiezen boven een formele procedure waarbij persoonlijke repercussies nooit helemaal uit te sluiten zijn. (Jeurissen, 2001:37)

Daar komt bij dat klokkenluiders net als andere personen die compromitteren ook persoonlijke motieven kunnen hebben om te lekken, bijvoorbeeld het uitschakelen van concurrentie of uit wraak. Voor de informatie die naar buiten komt maakt dat niet uit, de inhoud daarvan is immers dezelfde. Dit is zeer utilitaristisch, het doel heiligt de middelen, denk aan Machiavelli.

3.2.4 Lekken is in beginsel niet ethisch

In deze paragraaf is het ethische perspectief op het lekken van geheimen geschetst. Centraal stonden hierbij de vragen of het ethisch bezwaarlijk is om een geheim te lekken, en zo ja, of het dan *altijd* ethisch bezwaarlijk is om een geheim te lekken. Uit deze paragraaf blijkt dat dit vanuit (tenminste) drie standpunten te benaderen valt. De deugdethische benadering is subjectief en daardoor lastig in te vullen. De deontologische benadering is vrij rigide, er wordt namelijk geen onderscheid gemaakt tussen onbewust en bewust lekken. De meest reële benadering is de utilistische. Het lekken van geheimen is in beginsel niet ethisch, maar, zoals Hanson en Ceppos stellen:

> In general, leaks will always be part of a free society, and even more so in the era of so many competing news sources, including blogs and dueling websites. We also need to have some caution about claims that unethical leaks have occurred. British Lord Northcliffe had it right when he said that 'news is what someone, somewhere does not want printed. The rest is advertising.' (Hanson & Ceppos, 2006)

Bij het bepalen of een lek ethisch verantwoord is, dient er ten eerste een onderscheid te zijn tussen bewust en onbewust lekken. Daarnaast is lekken uit eigenbelang (persoonlijk gewin in welke vorm dan ook) onethisch, maar kan lekken uit een algemeen belang ethisch verantwoord zijn.

3.3 De juridische dimensie van geheimen en het lekken ervan

In het vorige hoofdstuk zijn de wet- en regelgeving rond geheimen en het lekken daarvan al diverse malen aan de orde geweest. In deze paragraaf wordt nader op de juridische dimensie ingegaan. Eerst worden de bepalingen behandeld en vervolgens de jurisprudentie.

3.3.1 Geheimen binnen het Nederlandse rechtsbestel

Binnen het Nederlandse rechtsbestel worden geheimen en het lekken ervan op meerdere plaatsen behandeld. Binnen het kader van dit onderzoek zijn de volgende Nederlandse wetten en regelingen relevant:

- Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM): artikel 10;
- Wetboek van Strafrecht (Sr): artikelen 98, 98a, 98b, 98c, 272 en 463;
- Ambtenarenwet (AW): artikel 125a, derde lid;
- Wet bescherming staatsgeheimen (Wbs): geheel;
- Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv): artikelen 85 en 86;
- Wet openbaarheid van bestuur (WOB): artikelen 10 en 11;
- Algemeen Rijksambtenarenreglement (ARAR): artikel 51;
- Voorschrift informatiebeveiliging rijksdienst 2007 (Vir): geheel;
- Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004 (Vir-bi): geheel.

Het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) heeft ingevolge artikel 94 Grondwet rechtstreekse werking binnen het Nederlandse rechtsbestel. Dit betekent dat de Nederlandse rechter hier rechtstreeks aan toetst. Het eerste lid van artikel 10 EVRM luidt: "Een ieder heeft recht op vrijheid van meningsuiting. Dit recht omvat de vrijheid een mening te koesteren en de vrijheid om inlichtingen of denkbeelden te ontvangen of te verstrekken, zonder inmenging van enig openbaar gezag en ongeacht grenzen. […]". Waar het in de rechtsvragen in de volgende subparagraaf om draait zijn de al dan niet gerechtvaardigde beperkingen in het tweede lid:

> Daar de uitoefening van deze vrijheden plichten en verantwoordelijkheden met zich brengt, kan zij worden onderworpen aan bepaalde formaliteiten, voorwaarden, beperkingen of sancties, die bij de wet zijn voorzien en die in een democratische samenleving noodzakelijk zijn in het belang van de nationale veiligheid, territoriale integriteit of openbare veiligheid, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden, de bescherming van de goede naam of de rechten van anderen, om de verspreiding van vertrouwelijke mededelingen te voorkomen of om het gezag en de onpartijdigheid van de rechterlijke macht te waarborgen. (Artikel 10, tweede lid, EVRM)

De artikelen in het Wetboek van Strafrecht bepalen de strafbaarstelling van het lekken van geheimen. De artikelen 98 e.v. Sr gaan over staatsgeheimen, dus gerubriceerde informatie, niet over gevoelige informatie. De artikelen raken echter wel 'een ieder'. Artikel 463 Sr gaat over het 'kopiëren' of openbaren van 'geheime regeringsbescheiden' door ambtenaren (artikel 1, eerste lid, Ambtenarenwet definieert een ambtenaar als degene die is aangesteld om in openbare dienst werkzaam te zijn), dit artikel heeft dus geen betrekking op politici (bewindspersonen en Kamerleden) en andere niet-ambtenaren. Daarnaast heeft het geen betrekking op staatsgeheimen, maar op vertrouwelijke informatie waarmee een ambtenaar in zijn gewone ambtsuitoefening kan worden geconfronteerd. Artikel 272 Sr eerste lid gaat over de opzettelijke schending van de geheimhoudingsplicht en is algemeen van aard:

> Hij die enig geheim waarvan hij weet *of redelijkerwijs moet vermoeden* dat hij uit hoofde van ambt, beroep of wettelijk voorschrift dan wel van vroeger ambt of beroep verplicht is het te bewaren, opzettelijk schendt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie. (Artikel 272, eerste lid, Sr; cursivering JHM)

Samenvattend kan gesteld worden dat de artikelen 98 e.v. Sr betrekking hebben op formele geheimen, artikel 463 Sr betrekking heeft op materiële geheimen en dat artikel 272 Sr als een paraplu gaat over beide categorieën.

De geheimhoudingsplicht van de ambtenaar in het Wetboek van Strafrecht is al aan de orde geweest, maar ook in de Ambtenarenwet is een bepaling opgenomen over geheimhouding: "De ambtenaar is verplicht tot geheimhouding van hetgeen hem in verband met zijn functie ter kennis is gekomen, voor zover die verplichting uit de aard der zaak volgt" (artikel 125a, derde lid, AW). Dit is verder uitgewerkt in het Algemeen Rijksambtenarenreglement (hierna: ARAR). Artikel 51 ARAR bepaalt dat bij indiensttreding de ambtseed- of belofte wordt afgelegd. Hierin is ook een passage opgenomen die betrekking heeft op de geheimhoudingsplicht:

> Ik zweer/beloof dat ik plichtsgetrouw en nauwgezet de mij opgedragen taken zal vervullen en zaken die mij uit hoofde van mijn functie vertrouwelijk ter kennis komen of waarvan ik het vertrouwelijke karakter moet inzien, geheim zal houden voor anderen dan die personen aan wie ik ambtshalve tot mededeling verplicht ben. (Besluit Vaststelling formulier eed/belofte rijksambtenaren, 1998:1)

De Wet bescherming staatsgeheimen regelt het aanwijzen van 'verboden plaatsen'. Zoals genoemd in de artikelen 98 e.v. Sr. Het geeft de locaties waar structureel met veel geheime informatie wordt gewerkt extra bescherming. Voorbeelden van verboden plaatsen zijn de locaties van de Algemene Inlichtingen- en Veiligheidsdienst, de Nationaal Coördinator Terrorismebestrijding en het Nationaal CrisisCentrum.

De artikelen 85 en 86 Wiv zijn een verbijzondering van de artikelen 98 e.v. Sr voor wat betreft de verplichting tot geheimhouding van een ambtenaar die betrokken is bij de uitvoering van de Wiv. Het gaat dan bijvoorbeeld om medewerkers van de Algemene Inlichtingen- en Veiligheidsdienst en de Militaire Inlichtingen- en Veiligheidsdienst.

De artikelen 10 en 11 WOB, het Vir en het Vir-bi zijn in hoofdstuk 2 al behandeld.

3.3.2 Jurisprudentie over geheimen en het lekken ervan

Eerder is al aangegeven dat weigering van openbaarmaking op grond van de WOB mogelijk is. Dit dient dan wel deugdelijk gemotiveerd te zijn. De rechtbank 's-Gravenhage overwoog hieromtrent in een WOB-verzoek naar twee gerubriceerde documenten over het 'stelsel van speciale eenheden':

“Het is immers aan verweerder om het besluit te onderbouwen en – waar nodig – een belangenafweging te maken en aan de rechter om haar te toetsen, met inachtneming van het uitgangspunt van de WOB dat openbaarheid regel is” (Rechtbank ’s-Gravenhage 19 juli 2007, rolnummer 06/7997, LJN: BK8847).

Vooral het Europees Hof voor de Rechten van de Mens (hierna: EHRM) heeft – als hoogste rechtsinstantie – interessante jurisprudentie opgeleverd op het terrein van geheimen en het onthullen ervan. Hierbij draait het dan om artikel 10 van het EVRM, dat over de vrijheid van meningsuiting gaat.

In 1991 wees het EHRM het bekende ‘Spycatcher’ arrest inzake de geheimhoudingsplicht (EHRM 26 november 1991, 13585/88, Observer and Guardian v. The United Kingdom). Aanleiding was de publicatie in 1985 van het boek 'Skycatcher' van Peter Wright, een voormalige medewerker van de Britse geheime dienst MI5. In zijn memoires ging hij in op de organisatie, methoden en medewerkers van MI5. Het boek werd daarom in het Verenigd Koninkrijk vooraf verboden. Ondanks dit verbod werd het boek heimelijk het land binnen gesmokkeld en diverse Britse kranten, zoals The Observer en The Guardian, wilden hier over berichten, maar ook dat werd door de overheid verboden. Het EHRM oordeelde echter dat na het verschijnen van het boek de informatie dusdanig beschikbaar was dat daarmee de noodzakelijkheid van het verbod was ontvallen. Doordat het object van de geheimhoudingsplicht niet langer vertrouwelijk was, mocht hierover worden gepubliceerd (Asscher, 2002:117). Een gelijkluidend oordeel velde het hof in het Sunday Times arrest (EHRM 26 november 1991, 13166/87, Sunday Times v. The United Kingdom).

Ook in latere arresten van het EHRM wordt bevestigd dat het weinig zin heeft om geheimen te beschermen die al zijn uitgelekt. Een Nederlandse zaak ging om het krakersblad 'Bluf!' (EHRM 9 februari 1995, 16616/90, Bluf! v. The Netherlands). De oplage van dit blad was op 29 april 1987 door het Openbaar Ministerie in beslag genomen omdat daarin een zes jaar oud dossier van de Binnenlandse Veiligheidsdienst werd gepubliceerd. Omdat de politie de drukplaten niet in beslag had genomen wisten de Bluf!-medewerkers diezelfde nacht een nieuwe oplage te drukken. Hiervan werden de volgende dag - Koninginnedag - circa 2.500 exemplaren op straat verkocht. Het Openbaar Ministerie vorderde via de rechter de onttrekking aan het verkeer van de exemplaren die reeds in beslag waren genomen. Het EHRM oordeelde dat de bescherming van de informatie niet langer gerechtvaardigd was met de onttrekking aan het verkeer. De informatie was namelijk al breed bekend geworden. De onttrekking aan het verkeer was in ieder geval niet noodzakelijk in een democratische samenleving (Hins, 2008:153).

In het arrest Dammann (EHRM 25 april 2006, 77551/01, Dammann v. Switzerland) draaide het onder meer om de vraag of de overheid die vertrouwelijkheid van informatie wil waarborgen voldoende beveiligingsmaatregelen heeft genomen om die te verzekeren. De Zwitserse journalist Viktor Dammann schreef een artikel over een grote bankroof en wilde meer te weten komen over de achtergrond van een aantal gearresteerde verdachten. Dammann belde met het Openbaar Ministerie, maar er waren geen Officieren van Justitie aanwezig. De administratief medewerkster die hem te woord stond was zo onder de indruk dat zij een bekende journalist aan de telefoon had dat zij meteen de justitiële documentatie van de gearresteerden naar hem toe faxte. Hiermee schond de administratief medewerkster haar ambtsgeheim. Dammann werd veroordeeld wegens uitlokking van schending van het ambtsgeheim. Het EHRM oordeelde dat deze veroordeling ten onrechte was, want wanneer een lidstaat de geheimhouding van dit soort gevoelige informatie wil waarborgen moet ze maar betere beveiligingsmaatregelen nemen. Het tekortschieten van de administratief medewerkster viel Zwitserland aan te rekenen. Het EHRM was daarbij van oordeel dat de journalist geen list of bedrog heeft toegepast om aan de informatie te komen. Bovendien heeft hij journalistiek behoorlijk gehandeld door de informatie die hij niet voldoende relevant achtte niet te publiceren. Relevant was ook de vraag hoe zwaar het algemene belang is om informatie die door een niet aan de overheid toe te rekenen lek naar buiten is gekomen te publiceren.

Dommering noemt in de annotatie op het arrest Dammann twee vergelijkbare zaken waarbij vertrouwelijke informatie per abuis bij de pers terecht kwam. De eerste betrof een faxbericht met de opschriften 'vertrouwelijk' en 'persoonlijk' van een advocaat aan het ministerie van Financiën dat per ongeluk bij de Geassocieerde Persdiensten (hierna: GPD) terecht kwam. De tweede betrof de geheime zitting in het proces Mink K. waar per ongeluk de microfoon open was blijven staan, zodat het verhandelde ter zitting in de wachtkamer was te horen. "Het Hof Den Haag achtte in het geval van de faxvergissing de normen van de maatschappelijke zorgvuldigheid overschreden, omdat de redactie

niet van de per ongeluk ontstane doorbreking van de vertrouwelijkheid had mogen profiteren (Hof 's-Gravenhage 4 maart 1999, Mediaforum 1999-4, nr. 21). De Raad van de Journalistiek achtte in het geval Mink K. de journalistieke normen overschreden (Dommering, 2007:1262-1263). Van de ontvanger van informatie wordt dus verwacht dat men terughoudend is met het ge- of misbruiken van deze informatie. Maar deze journalistieke terughoudendheid kent wel grenzen: "Denk aan een journalist die een vertrouwelijk gesprek opvangt tussen twee ministers die van plan zijn de Tweede Kamer te misleiden. Niemand mag verwachten dat deze journalist afziet van publicatie" (Hins, 2008:158).

In de zaak Stoll (EHRM 10 december 2007, 69698/01, Stoll v. Switzerland) draaide het om de publicatie op 26 januari 1997 van een gerubriceerd document in het Zwitserse nieuwsblad 'Sonntags-Zeitung' door de journalist Martin Stoll. In dit arrest overwoog het EHRM dat de wijze waarop de vertrouwelijke of geheime informatie is verkregen van belang is voor de vraag in hoeverre sprake is van artikel 10, tweede lid, EVRM. De verantwoordelijke voor het lekken van de informatie was niet de journalist. Het EHRM herhaalde in deze zaak de overweging uit 'Dammann' dat "it is primarily up to States to organise their services and train staff in such a way as to ensure that no confidential or secret information is disclosed". Het EHRM stelde daarbij dat "in that regard, the authorities could have opened an investigation with a view to prosecuting those responsible for the leak". Ondanks het feit dat de journalist niet strafbaar gehandeld heeft voor wat betreft de verkrijging van de geheime informatie, kon hij ook niet beweren dat hij onbekend was met het feit dat openbaring van het document zou leiden tot een strafbaar feit.

3.3.3 Perpetuum mobile van regelgeving

Bij de constatering dat er geheimen gelekt zijn kan – net als bij andere incidenten – in sterke mate sprake zijn van reactief optreden. Er kan zelfs sprake zijn van morele paniek. "Hiervan is sprake als onrust ontstaat rond in de media breed uitgemeten incidenten, die worden toegeschreven aan één veronderstelde oorzaak. Om de rust te herstellen, wordt de vermeende oorzaak via nieuwe wetgeving de kop ingedrukt." (Boekhout van Solinge, 2010:2583).

Interessant verschijnsel daarbij is dat men dan veelal regels en maatregelen invoert die nog strenger of uitgebreider zijn dan de regels en maatregelen die toch al niet gevolgd werden. De eerste periode na een dergelijk incident zullen de top van de organisatie, de leidinggevenden en de medewerkers nog wel alert zijn, maar op een bepaald moment verslapt de aandacht en wordt het 'ongemak' die de beveiligingsmaatregelen veroorzaken als ernstiger gepercipieerd dan het risico op een nieuw incident (practical drift). Als een nieuw incident zich vervolgens manifesteert constateert men dat de regels niet gevolgd zijn en worden er nieuwe – strengere – regels ingevoerd. Hiermee creëert men een perpetuum mobile van regelgeving.

De Commissie Lemstra – die het lekken binnen het ministerie van Defensie onderzocht – geeft een interessant voorbeeld hiervan. Voor het per faxapparaat verzenden van gerubriceerde informatie dient men gebruik te maken van een beveiligd apparaat. Het gebruik daarvan is omslachtiger dan het gebruik van een normaal faxapparaat. "Teneinde toch gebruik te kunnen maken van het normale faxapparaat is het voorgekomen – zo is de commissie verteld – dat de rubricering wordt weggelakt" (Lemstra et al., 2005:30). Andere voorbeelden zijn het lager rubriceren of zelfs niet rubriceren van de informatie om verplichte beveiligingsmaatregelen te omzeilen.

De Commissie Lemstra probeerde daarom dan ook dit patroon te doorbreken door aan te geven dat er geen snelle remedie bestaat tegen lekken: "de oplossing moet niet worden gezocht in nieuwe regels maar in onderkenning van cultuur, structuur, beveiligingssystemen, gedrag en werkwijze binnen de organisatie en vervolgens in langdurige investeringen op deze punten" (Lemstra et al., 2005:75).

3.4 De politiek-bestuurlijke dimensie van geheimen en het lekken ervan

Naast de ethische en juridische dimensie van geheimen en het lekken ervan bestaat er ook een politiek-bestuurlijke dimensie. In deze dimensie hebben zowel het hebben van geheimen als het lekken van geheimen een instrumenteel (ethisch utilistisch) karakter.

3.4.1 Geheimhouding kan instrumenteel zijn

Overleg kan niet altijd in een open setting plaatsvinden. Dat geldt binnen en tussen organisaties, maar ook op internationaal niveau. “Sommige geheimen zijn nuttig. Zeker, er zijn geheimen met behulp waarvan verantwoordelijkheden worden ontlopen. Maar diplomaten en andere onderhandelaars moeten hun werk in stilte kunnen doen. En van sommige geheimen is openbaarmaking echt gevaarlijk” (Buruma, 2011:57). Minister Donner van Binnenlandse Zaken en Koninkrijksrelaties omschreef het in een brief aan de Tweede Kamer naar aanleiding van de publicatie van diplomatieke berichten van de ambassade van de Verenigde Staten in Den Haag over contacten met Nederlandse bewindspersonen, parlementariërs en ambtenaren (onderdeel van de circa 250.000 documenten uit Cablegate, WikiLeaks) als volgt:

> De onderlinge informatie-uitwisseling tussen ambassades en de betrokken departementen is essentieel voor het bewaren van de internationale orde en vrede. [...] In het moderne verkeer tussen landen vinden op talloze plaatsen en niveaus contacten plaats. Deze zijn soms rechtstreeks maar veelal zullen die lopen via het ambassadepersoneel. De tijd dat contacten zich uitsluitend beperkten tot ministers en gevolmachtigde ministers ligt ver achter ons. Het is de bestaansreden van ambassades; luisteren, informatie verstrekken en waar mogelijk de mening en het oordeel gunstig beïnvloeden. De vertrouwelijkheid van deze communicatie moet gewaarborgd zijn. (Kamerstukken II 2010-11, 32 500 V, nr. 145:3)

Ook premier Rutte ging in zijn wekelijkse persconferentie op 14 januari 2011 in op de publicatie van diplomatieke berichten en het belang van vertrouwelijke contacten:

> Het is ontzettend interessant om dat allemaal te lezen, ik begrijp dat wel. Maar het is natuurlijk voor het diplomatieke verkeer - en ik sta hier niet als een soort ‘old school’ politicus - niet handig. Want als ik zelf in contact met diplomaten dingen zeg en ik weet dat dat met enige vertraging bij u in het half acht nieuws zit dan remt dat mij natuurlijk om ‘all out’ te gaan, om mijn volledige mening te geven. En in die zin is het belangrijk dat die vertrouwelijkheid van die contacten gehandhaafd blijft, dat is hier niet gelukt. En dat geeft op zichzelf dan weer een interessant inkijkje. (Rutte, 2011 [transcript JHM])

3.4.2 Lekken kan instrumenteel zijn

Aan de andere kant kan lekken net zo instrumenteel zijn als geheimhouding. In de politiek-bestuurlijke arena kan lekken worden ingezet om een bepaald beeld te schetsen – het ‘spinnen’ – van de eigen partij of de wederpartij, net zoals framing en liegen.

> Nergens is lekken zo gewoon als in de politiek. Honderden keren per jaar lekken overheidsstukken uit. Gemeenteraadsleden en Kamerleden lekken informatie uit om zelf in de krant te komen met een reactie op het gelekte nieuws. Ambtenaren lekken stukken om het standpunt van hun wethouder of minister eerder in de krant te krijgen dan dat van een andere wethouder of minister. Ministers zelf lekken ook, om een andere minister af te troeven. De overheid is het enige schip dat van boven lekt. (Van Venetië & Luikenaar, 2006:122)

Een goed voorbeeld wordt gegeven door de journalist Joris Luyendijk die in 2010 een maand vertoefde in en om het Buitenhof en verslag deed van zijn ervaringen met politici, woordvoerders, lobbyisten en media:

> Stel, je wil als kabinet een draconische 300 miljoen bezuinigen op de gehandicaptenzorg. Dan lek je het plan om 500 miljoen te gaan bezuinigen. Daarop komen functioneel woedende belangenbehartigers voor de gehandicapten ‘in opstand’, waarna je het bedrag deemoedig terugbrengt tot 300 miljoen. In zo’n opzet wint iedereen: het kabinet krijgt dekking voor zijn 300 miljoen bezuiniging; de gehandicaptenorganisaties hebben aan hun achterban bewezen dat ze ‘pal’ staan; en de overvraagde journalisten hebben zeker drie verhalen waarvoor ze nauwelijks research hebben hoeven doen. (Luyendijk, 2010:75-76)

In dit voorbeeld is er sprake van een strategisch of geautoriseerd lek, waarbij gerubriceerde of gevoelige informatie intentioneel naar buiten wordt gebracht door of namens een bewindspersoon. Strikt genomen is er dan geen sprake van lekken omdat de handeling geautoriseerd is voor zover de bewindspersoon voor deze informatie ook politiek verantwoordelijk is. Hierop is het leerstuk van de ministeriële verantwoordelijkheid van toepassing. Wat dit voorbeeld extra gecompliceerd – en

daarmee interessant – maakt, is dat de 'geheime' informatie in casu feitelijk onjuiste informatie is, bedoeld om de tegenstander te misleiden. Deze achtergrond dient echter niet bekend te worden bij de tegenstander en is daarmee het werkelijke geheim.

In de literatuur wordt het voorbeeld genoemd van premier Willem Drees die destijds altijd de namen van kandidaten voor burgemeestersbenoemingen liet uitlekken omdat er in die tijd nog diverse kandidaten met een dubieus oorlogsverleden rondliepen. Als er na een bepaalde periode geen negatieve berichten naar boven kwamen kon de kandidaat benoemd worden (Bovens, Geveke & De Vries, 1993:67).

Een variant hierop is het lekken in de vorm van een driehoekje: een ambtenaar lekt iets aan een Kamerlid, die lekt dat vervolgens naar een journalist, deze kopt het verhaal in de krant, waarna het Kamerlid er vervolgens weer vragen over stelt, die de ambtenaar dan weer moet beantwoorden (Bovens, Geveke & De Vries, 1993:76).

In 'Het Grote Lobbyboek' wordt lekken als een van de instrumenten van beïnvloeding door lobbyisten genoemd: "Een veel toegepaste listigheid om beslissers aan jouw kant te krijgen is het toespelen van vertrouwelijke informatie aan de pers: lekken dus. […] Het toespelen van vertrouwelijke informatie aan de pers is een manier om de lobbyboodschap in één klap aandacht te geven en medestanders te verleiden in de pers de kant van de lekker te kiezen." (Van Venetië & Luikenaar, 2006:121). In hun handboek geven Van Venetië en Luikenaar ook een handleiding lekken:

> Lekken is simpel als je je aan een paar basisregels uit de 'lekkologie' houdt.
> - Beslis waarom je informatie wilt laten lekken. Lek nooit iets uit aardigheid of omdat je een journalist een onthulling gunt. Bedenk vooraf hoe anderen in de krant kunnen reageren op het nieuws.
> - Lek bij voorkeur aan een journalist die je al kent. Kan de journalist scoren met een onthulling, dan is hij al gauw op jouw hand. Journalisten zijn zuinig op hun geheime bronnen. Politici lekken ook graag naar journalisten als een soort verzekeringspremie. Zo'n journalist zal zich wel twee keer bedenken voor hij een vernietigend stuk over je schrijft. Maar blijf altijd op je hoede.
> - Lek alleen als je zeker weet dat het lek moeilijk te traceren is. Lek dus alleen als de informatie bij meerdere belanghebbenden bekend is.
> - Maak een afspraak over de manier waarop de journalist jouw reactie opschrijft of geef namen van anderen die hij kan bellen voor een reactie.
> - Lekken kan op elke locatie. De overdracht hoeft niet persé plaats te vinden in een verlaten parkeergarage.
> - Voor ambtenaren kan lekken riskant zijn. De kans bestaat dat hun politieke baas de rijksrecherche in de arm neemt om het lek op te zoeken.
>
> (Van Venetië & Luikenaar, 2006:124)

3.4.3 Bezwaren tegen lekken als politiek-bestuurlijk instrument

Politiek-bestuurlijk kleven er ook bezwaren aan het geautoriseerd lekken. De Commissie Lemstra benoemt deze in haar rapport naar aanleiding van lekken binnen het ministerie van Defensie. In de eerste plaats is er sprake van een strafbaar feit als een ambtenaar lekt, ook als dat in opdracht van een bewindspersoon gebeurt. Maar veel belangrijker is dat het 'geautoriseerd lekken' een verkeerd signaal geeft aan de ambtelijke organisatie en het afbreuk doet aan de voorbeeldfunctie van de bewindspersonen: "Lekken door of namens de bewindspersonen kan door het ambtelijke apparaat worden opgevat als een legitimatie voor ongeautoriseerde lekken" (Lemstra et al., 2005:18).

Naast de directe schade die kan optreden door het lekken van gerubriceerde of gevoelige informatie kan er ook sprake zijn van indirecte schade. Lekken kan namelijk het imago en het vertrouwen in het politiek-bestuurlijke systeem aantasten:

> Als ik nu op tv een journalist trots als eerste zie wapperen met de nog geheime miljoenennota, denk ik niet meer: wow, wat knap dat hij die nu al heeft. Na deze maand [als rapporteur voor de sociëteit Nieuwspoort voor o.a. journalisten en politici, JHM] denk ik: wat heeft de lekkende ambtenaar of politicus hiervoor teruggekregen? (Luyendijk, 2010:87)

De Commissie Lemstra ziet ook de schadelijke gevolgen voor de interne verhoudingen binnen de organisatie:

> In normatieve zin heeft lekken een negatieve klank. Lekken brengt grote schade toe aan de organisatie; veel groter dan het enkele feit dat vertrouwelijke of geheime informatie – hoe schadelijk dit ook is indien het bijvoorbeeld om staatsgeheimen gaat – op straat komt te liggen. Het imago van de totale organisatie wordt door het lekken beschadigd; het vertrouwen van de buitenwereld in de gehele organisatie wordt beschaamd. Daarnaast bederft het de sfeer binnen de organisatie. De verhouding tussen het ambtelijke apparaat en de politieke leiding komt onder druk te staan. Het lekken van vertrouwelijke of geheime informatie zet ook de onderlinge verhoudingen op scherp. Medewerkers kijken elkaar vragend aan wie er gelekt heeft. Onschuldige medewerkers worden in het kader van een (strafrechtelijk) onderzoek ondervraagd, hetgeen als zeer belastend wordt ervaren. Lekken bedreigt de eenheid binnen de organisatie en zet medewerkers tegen elkaar op. “Lekken is oncollegiaal”, zo heeft de commissie vernomen en heeft een groter negatief effect dan alleen het feit dat wat geheim had moeten blijven, openbaar is gemaakt. (Lemstra e.a, 2005:8)

In de vorige subparagraaf werd het laten lekken van kandidaten voor een burgemeesterbenoeming als instrumenteel voorbeeld genoemd. Er zitten echter ook keerzijden aan het uitlekken van de namen van kandidaten voor dergelijke posities, zo gaf de voormalige Secretaris-Generaal van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties aan:

> Openbaarmaking brengt de betrokken kandidaten schade toe. Het laten lekken van kandidaten maakt dat de beslissingsvrijheid van de minister of ministerraad wegvalt. Het kan namelijk zijn dat er bepaalde bezwaren zijn tegen een kandidaat, bijvoorbeeld omdat deze te licht is voor de functie. Als de kandidaat zelf en de Commissaris der Koningin dit niet hebben ingezien, dan moet de minister zo’n benoeming kunnen voorkomen. Maar als bekend wordt dat er bezwaren zijn tegen een burgemeester van een kleine gemeente die solliciteert naar een grotere gemeente, dan loopt deze schade op. De positie van de burgemeester in het college en de gemeenteraad verzwakt ook op het moment dat bekend wordt dat deze weg wil maar het niet doorgaat. Het belang van de geheimhouding geldt overigens niet alleen bij burgemeesterbenoemingen, maar ook bij benoemingen van SG’s en DG’s.
> (Interview J.W. Holtslag, 11-01-2011)

3.5 Het belang van duiding

In dit hoofdstuk zijn de ethische, de juridische en de politiek-bestuurlijke dimensie van geheimen en het lekken ervan behandeld. Er is echter een facet dat nog nader toegelicht dient te worden, namelijk het belang van duiding.

Bij ongecontroleerde openbaarmaking ontstaat namelijk het probleem dat de informatie niet geduid wordt, het kader waaruit de informatie genomen is ontbreekt. Hierdoor is het niet goed mogelijk om de status van de informatie te bepalen. Betreft het actuele informatie of is deze verouderd? Is de informatie een eerste aanzet in een brainstormsessie of is het (bijna) staand beleid? Is de informatie gebaseerd op concrete feiten of is het een (onjuiste) perceptie van de steller? Allemaal vragen die bij het uitlekken van informatie gesteld zouden kunnen worden.

Dat is ook de kritiek die geuit is op het lekken van de circa 250.000 diplomatieke berichten van de Verenigde Staten – ‘Cablegate’ – via de website van WikiLeaks sinds eind 2010:

> De context waarbinnen de stukken worden gepubliceerd, is relevant. [...] Het feit dat WikiLeaks de stukken integraal plaatst geeft de lezer de gelegenheid zijn eigen mening te vormen over de materie. Maar het feit dat WikiLeaks de stukken niet of nauwelijks duidt – dat laat WikiLeaks over aan een aantal kranten waar ze mee samenwerkt – maakt haar zaak niet sterker. Door duiding van de stukken zou WikiLeaks een vergelijkbare rol als een journalist in kunnen nemen. Journalisten worden door het EHRM dikwijls beschouwd als ‘public watchdog’. Zij vervullen een bijzondere rol in het democratische proces. Om die reden mogen zij eerder vertrouwelijke stukken publiceren.
> (Alberdingk Thijm & Antic, 2010)

> Van oudsher werd de onderzoeksjournalistiek gekenmerkt door drie fasen: het aan de oppervlakte krijgen van de feiten, het tegen het licht houden van de feiten en het rangschikken van deze feiten in een begrijpelijk discours. WikiLeaks doet het eerste, beweert ook het tweede te doen, maar laat het derde volledig achterwege.
> (Lovink & Riemens, 2010:2)

Daarnaast is ook de authenticiteit van uitgelekte geheime documenten niet altijd te achterhalen, zeker niet indien de organisatie waaruit de documenten afkomstig zijn hier geen mededelingen over wil of kan doen. Dit was ook de reactie van minister Donner van Binnenlandse Zaken en Koninkrijksrelaties naar aanleiding van vragen vanuit de Tweede Kamer inzake WikiLeaks:

> Maar ook indien de documenten zouden zijn wat beweerd wordt dat zij zijn, dan nog kan de Nederlandse regering geen commentaar geven op de inhoud daarvan. Het betreft immers ambtsberichten van Amerikaanse functionarissen. Ze bevatten weergaven, percepties en inschattingen van het ambassadepersoneel over de Nederlandse situatie en gesprekken die gevoerd zouden zijn met onder anderen ministers, Kamerleden en ambtenaren. De weergave van een gesprek bevat niet noodzakelijkerwijze de inhoud van dat gesprek. Dat is begrijpelijk. Het betreft immers een verslag waarin vooral nadruk wordt gelegd op wat de verslaggever begrijpt, hoort en wil weergeven. De weergave en duiding van de gewisselde informatie en ander bronmateriaal in een bericht komt enkel voor rekening van de steller ervan.
> (Kamerstukken II 2010-11, 32 500 V, nr. 145:2)

4. DREIGINGEN EN KWETSBAARHEDEN VAN GEHEIMEN

4.1 Inleiding

In dit hoofdstuk wordt ingezoomd op de dreigingen en kwetsbaarheden van gerubriceerde en gevoelige informatie. Hierbij ligt de nadruk op de vraag *hoe* geheimen worden gelekt.

De kwetsbaarheid van informatie komt aan de orde in paragraaf 4.2. In paragraaf 4.3 worden de resultaten van een enquête onder de Beveiligingsambtenaren van de – destijds – dertien departementen weergegeven. In paragraaf 4.4 worden de cijfers en een aantal onderzoeken van de Rijksrecherche beschreven. Mede op basis van de uitkomsten van de enquête – en het literatuuronderzoek – is een reeks interviews gehouden met deskundigen. De uitkomsten hiervan worden beschreven in paragraaf 4.5. Aparte aandacht is voor Het Nieuwe Werken in paragraaf 4.6. Dit hoofdstuk wordt in paragraaf 4.7 afgesloten met een overzicht van dreigingen en kwetsbaarheden ten aanzien van geheimen, gebaseerd op de voorgaande paragrafen en deels ook op basis van de dreigingen en kwetsbaarheden die in de voorgaande hoofdstukken al aan de orde kwamen.

4.2 De kwetsbaarheid van informatie

In elke procesvorm waarin informatie zich bevindt, bestaan dreigingen en kwetsbaarheden: bij verwerking, opslag, transport en vernietiging. Talbot en Jakeman hebben dat als volgt beschreven:

> Information is vulnerable to a variety of threats. Organisations and even individuals can collect information by exploiting security vulnerabilities in information systems. The most important part on an information system is the people that use and operate the system. People and the information they have access to are also vulnerable to security threats and exploitation. In addition, human error and equipments malfunction may threaten the security of valued information. (Talbot & Jakeman, 2008:114)

De mens is dus de zwakste schakel. Het bekendste recente voorbeeld hiervan is waarschijnlijk de ‘Cablegate’ affaire die via WikiLeaks geopenbaard werd (Casus 6).

Casus 6: ‘Cablegate’ via WikiLeaks

“Het Amerikaanse afgeschermde militaire netwerk om gevoelige data te delen blijkt toegankelijk voor meer dan 3 miljoen mensen. Geheime data kon zo makkelijk uitlekken, naar onder meer Wikileaks.

Het netwerk, Secret Internet Protocol Router Network, oftewel Siprnet, geeft toegang tot een van de grootste databases ter wereld, met onder meer alle diplomatieke correspondentie van ambassades in de belangrijkste steden ter wereld. Tot aan de laagste Amerikaanse militair had iedereen in overheidsdienst er toegang toe. Op internet zijn vele links naar Amerikaanse overheidsdocumenten over Siprnet te vinden. Zondag [28 november 2010, JHM] publiceerden de websites van kranten en weekbladen als Le Monde, Der Spiegel, The Guardian en El Pais een gedeelte van 250.000 documenten die in de afgelopen tientallen jaren via Siprnet zijn verstuurd. De documenten zijn door Wikileaks aan de kranten gestuurd als voorzorgsmaatregel voor het geval Wikileaks door een ddos-aanval zou worden getroffen. Die angst voor een dergelijke aanval lijkt terecht te zijn. Wikileaks was zondag vrijwel niet bereikbaar.

De Amerikaanse regering heeft naar aanleiding van de actie van Wikileaks aangekondigd de beveiliging van Siprnet op te voeren. Zo zou het downloaden van informatie op een externe drager als een usb-stick niet meer mogelijk zijn. Daarnaast wordt bekeken wie toegang moet krijgen tot welke informatie. Al eerder vaardigde de Amerikaanse regering een document uit met nieuwe securiteitmaatregelen. Overigens staat een handleiding voor Siprnet gewoon online. De toegang tot informatie via Siprnet is gegroeid sinds de aanval op de twee torens van het World Trade Center op 11 september 2001. De toenmalige Amerikaanse regering van George W. Bush besloot informatie over wereldwijde dreigingen breder beschikbaar te maken onder overheidspersoneel. Bij een laatste officieel onderzoek kwam naar voren dat meer dan 3 miljoen mensen toegang hadden tot Siprnet. Dat was echter al in 1993 het geval, zegt The Guardian.

De informatie die zondagavond uit de gelekte documenten naar buiten kwam, was voor het overgrote deel (nog)

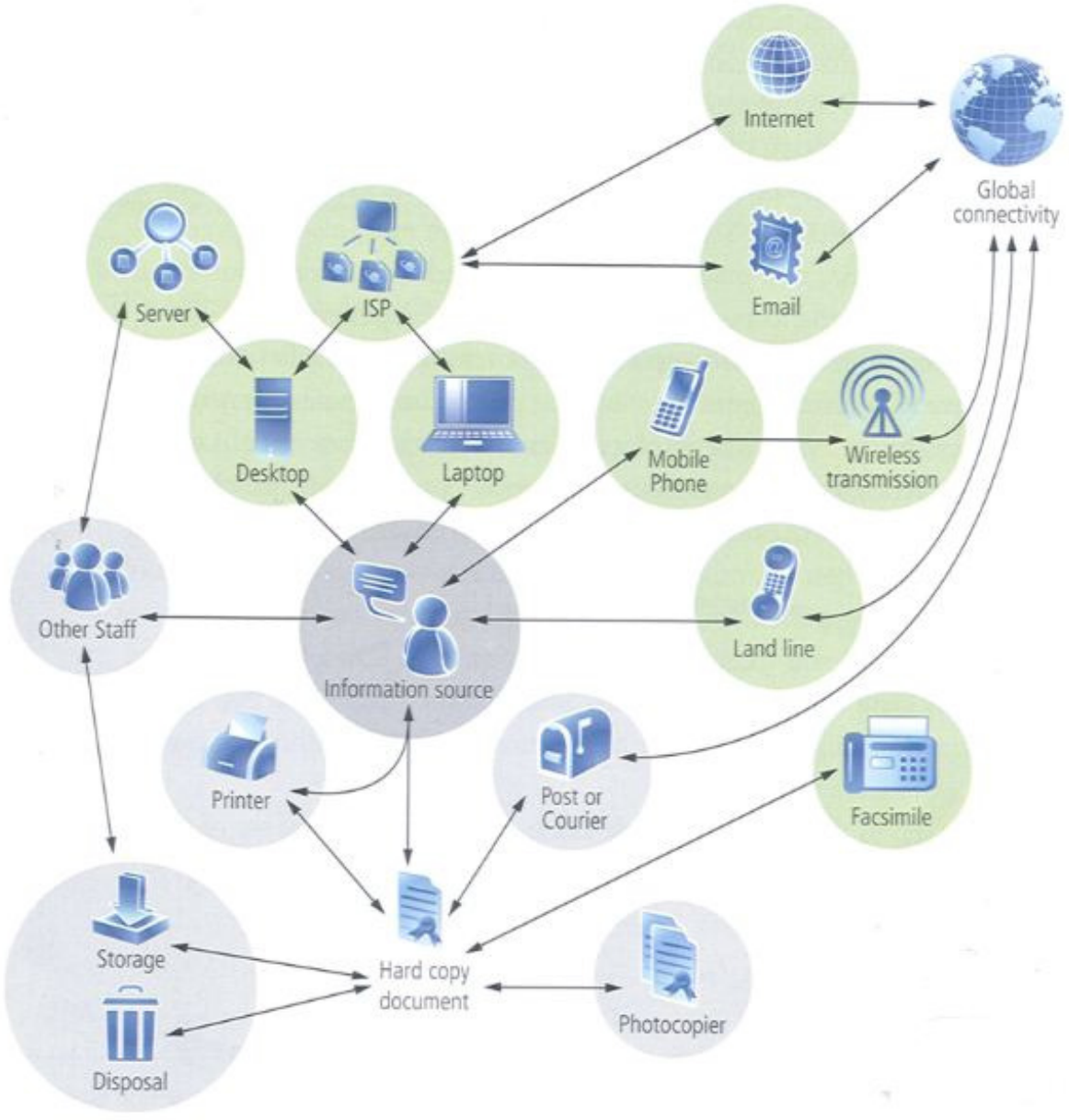
niet explosief. […] Buiten enkele zwaardere onderwerpen, zoals Iran, China en Rusland, gaan veel documenten over dagelijkse observaties en beoordelingen ervan. Overigens is Bradley Manning, de soldaat die ervan verdacht wordt dat hij de informatie heeft gelekt aan Wikileaks, al eerder dit jaar gearresteerd door de Amerikaanse autoriteiten."

(Schoemaker, 2010)

Deze casus geeft – voor zover bekend, het strafrechtelijk onderzoek liep nog bij het afronden van deze thesis – een aantal dreigingen en kwetsbaarheden weer:

- een grote digitale verzameling van gerubriceerde en gevoelige informatie;
- een grote groep gebruikers (meer dan drie miljoen) die toegang heeft tot alle documenten (interessant genoeg met als doel een andere dreiging – terrorisme – te bestrijden);
- de informatie was zonder beperkingen naar een mobiele datadrager te kopiëren – zoals zelf gebrande muziek cd's van Lady Gaga (König, 2011:7).

Talbot en Jakeman hebben dit soort kwetsbaarheden gevisualiseerd in een weergave van informatiestromen die typerend is voor veel organisaties (figuur 4.1).



Figuur 4.1: Voorbeeld van informatiestromen en kwetsbaarheden (Talbot & Jakeman 2008:114).

Kwetsbaarheden worden onder meer veroorzaakt door de (onjuiste) wijze van verzenden, digitaal opslaan, fysiek opbergen en vernietigen. Het figuur laat ook zien dat informatie vanuit een organisatie snel wereldwijd verspreid kan worden, of dit nu geoorloofd is of – zoals bij 'Cablegate' (casus 6) – niet: "Each step exhibits its own vulnerabilities and risk of compromise or lost of information. These may be exploited if the relevant security strategies are not in place" (Talbot & Jakeman 2008:114).

Interessant aan het figuur is dat de kwetsbaarheden vooral toegenomen lijken te zijn door de ontwikkelingen van de afgelopen decennia op het terrein van de informatie- en communicatie-technologie. Zaken als mobiele telefonie, e-mail, internet, digitale gegevensdragers met hoge opslagcapaciteit zijn tegenwoordig tegen lage kosten voor vrijwel iedereen beschikbaar gekomen. Dit is een ontwikkeling die ook al door Bovens, Geveke en De Vries is waargenomen als een factor van infrastructurele aard (1993:76).

Maar ook het niet of onjuist vernietigen van digitale gegevensdragers of documenten kan al tot lekincidenten leiden. Informatie kan dan door onbevoegden gevonden worden. Soms vinden deze de documenten of digitale gegevensdragers 'per ongeluk', soms doordat ze er bewust naar op zoek zijn in bijvoorbeeld afvalcontainers, dit wordt ook wel 'dumpsterdiving' genoemd. Deze methode wordt zowel toegepast bij (bedrijfs)spionage als door journalisten (Casus 7).

Casus 7 : Balkenende berispt Kabinet der Koningin

"Het kabinet heeft maatregelen genomen om te voorkomen dat stukken over het koningshuis nog een keer op straat komen te liggen. Dat heeft premier Balkenende gezegd in reactie op een uitzending van tv-programma Nova, dat gisteren meldde dat het Kabinet der Koningin 'geblunderd' heeft omdat het 'zeer vertrouwelijke' stukken over het Koningshuis in een vuilniscontainer heeft gegooid.

Nova heeft de container van het Kabinet der Koningin zeven keer geleegd en naar eigen zeggen 24 vuilniszakken met gevoelige informatie gevonden. […] In de vuilniszakken zat onder meer een vertrouwelijk document over staatsbezoeken. Daarin stond welke bezoeken tot 2011 door het staatshoofd zullen worden afgelegd. Koningin Beatrix had de lijst opgesteld. Verder vond Nova agenda's tot juli van de koningin, prins Willem-Alexander en prinses Màxima. Ook bevatte het afval werkroosters van het kabinet, telefoonnummers, dossierlijsten en visitekaartjes."

(NRC Handelsblad, 30 mei 2007)

Talbot en Jakeman geven aan dat de bedreigingen van de informatie van organisaties talrijk zijn, maar dat ze grofweg in drie categorieën ingedeeld kunnen worden: "Threats from 'inside the system', 'against the system' and 'despite the system'" (2008:115). In dit onderzoek gaat het om dreigingen door personen 'inside the system' die als intentioneel en verwijtbaar te beschouwen zijn.

4.3 Enquête onder Beveiligingsambtenaren departementen

In mei 2010 is een enquête uitgezet onder de Beveiligingsambtenaren van de dertien departementen. De Beveiligingsambtenaar is de functionaris die namens de Secretaris-Generaal op strategisch niveau verantwoordelijk is voor de integrale beveiliging (informatiebeveiliging en fysieke beveiliging) van het departement. De respons was honderd procent. Vanwege de gevoeligheid van het onderwerp is toegezegd dat de resultaten geanonimiseerd weergegeven zullen worden. De vragenlijst en de totaalresultaten zijn opgenomen als bijlage II. De uitkomsten van de enquête zijn gebruikt voor de interviews. In de vragenlijst is de Vir-bi-term 'bijzondere informatie' gebruikt om staatsgeheime en departementaal vertrouwelijke informatie mee aan te geven. De term 'bijzondere informatie' zal met het invoeren van het Vir-gi – voornemens in 2011 – vervangen worden door 'gerubriceerde informatie'.

4.3.1 Aantal gemelde gevallen van lekken

Van de dertien departementen gaven er zeven aan dat in de periode 2004-2009 sprake is geweest van een of meerdere gevallen van lekken van bijzondere informatie. Hierbij ging het in totaal om 39 bekende gevallen, waarbij in alle gevallen onderzoek is geweest.

Het is wel van belang hierbij in ogenschouw te nemen dat het hier gaat om de *gemelde* gevallen. Bovens, Geveke en De Vries gaven al aan dat een kwantitatieve analyse naar lekken onmogelijk is

door het heimelijke aantal ervan (1993:73). Het werkelijke aantal gevallen van lekken van bijzondere informatie zal hoger zijn, net zoals het aantal voertuigen dat te hard rijdt hoger is dan het aantal voertuigen dat hiervoor geflitst wordt. Het aantal meldingen en onderzoeken is dan ook indicatief voor de omvang van het verschijnsel. Veelbetekenend is het antwoord van Frits Wester, politiek verslaggever van RTL Nieuws, op de vraag hoe vaak er gelekte informatie aangeboden wordt: "Soms gebeurt dat meerdere keren per dag en dan weer dagen niets. Het één lokt het andere uit. Het is een onderdeel van het politieke proces. Het gebeurt met grote regelmatigheid, maar het is moeilijk te kwantificeren" (Interview F. Wester, 03-02-2011).

4.3.2 Onderzoeken naar de lekken

Binnen de zeven departementen die aangaven te maken gehad te hebben met het lekken van bijzondere informatie was in alle gevallen een interne partij (veelal de BVA) verantwoordelijk voor het uitvoeren van het onderzoek. Een departement gaf aan gebruik te maken van een commerciële partij, vier departementen gaven aan dat de Rijksrecherche betrokken was bij een of meerdere onderzoeken.

Alle zeven departementen gaven aan dat er uitspraken te doen waren naar de oorzaken van het lekken. Vier departementen gaven aan dat er in een of meerdere gevallen sprake was van bewust lekken, zeven departementen gaven aan dat er in een of meerdere gevallen sprake was van onbewust lekken. Een departement gaf aan dat er sprake is geweest van technisch falen en twee departementen gaven aan dat er in een of meerdere gevallen sprake was van andere oorzaken, namelijk werkdruk, onvoldoende veilige middelen, politieke druk of persoonlijk financieel gewin.

4.3.3 Maatregelen tegen lekken

Alle dertien Beveiligingsambtenaren gaven aan dat binnen het eigen departement voldoende maatregelen beschikbaar zijn op het terrein van regelgeving (Vir-bi, departementale regelingen) om lekken tegen te gaan. Hierbij werd door een respondent de nuancering gemaakt dat het ook om het bewustzijn van de regelgeving gaat.

Gevraagd naar het oordeel of binnen het eigen departement voldoende maatregelen beschikbaar zijn op het terrein van technische voorzieningen (cryptomiddelen, kluizen, bijzonder papier, veiligheidsenveloppen) om lekken tegen te gaan gaven tien van de dertien respondenten aan dat dit het geval is. Drie departementen gaven aan dat dit niet het geval is.

Tien van de dertien respondenten gaven aan dat binnen het eigen departement voldoende maatregelen beschikbaar zijn op organisatorisch terrein (procedures en gespecialiseerde functionarissen) om lekken tegen te gaan. Drie departementen gaven aan dat dit niet het geval is.

Als laatste werd gevraagd naar het niveau van informatiebeveiligingsbewustzijn (men kent de regels en handelt ernaar) binnen het departement om lekken tegen te gaan. Acht respondenten gaven aan dat dit het geval is, vijf gaven aan dat dit niet het geval is.

4.3.4 'Dark number' aan lekincidenten

Opmerkelijk is dat diverse respondenten aangaven zich zorgen te maken over het bewustzijn inzake informatiebeveiliging binnen de eigen organisatie. Het betrof in alle gevallen de departementen waar men ervaring heeft opgedaan met lekincidenten en het onderzoeken daarvan. Dit zou er op kunnen duiden dat binnen de departementen waar meer aandacht is voor lekken (al dan niet door incidenten hieromtrent) een beter beeld bestaat van de omvang van het probleem en zaken ook eerder gemeld worden. Dit verschijnsel toont sterke overeenkomsten met de zogenoemde 'integriteitsparadox': Een grotere alertheid binnen de organisatie leidt tot een toename van het aantal meldingen van mogelijke schendingen. Hierdoor lijkt het dat de organisatie gevoeliger is dan organisaties waar minder of geen aandacht is voor integriteit (Huberts & Neelen, 2005:140). Bij bestuurders kan dit ten onrechte tot de teleurstelling leiden dat de extra inspanningen contraproductief blijken te zijn. In werkelijkheid hebben deze organisaties juist een beter beeld en is er minder sprake van een 'dark number'.

4.4 Onderzoeken Rijksrecherche naar schending geheimhoudingsplicht

Bij het uitlekken van geheimen wordt vaak gewezen naar de Rijksrecherche als dé onderzoeksinstantie om de dader op te sporen. De Rijksrecherche is als opsporingsinstantie

onderdeel van het Openbaar Ministerie en richt zich op de opsporing van door (semi) overheidsfunctionarissen gepleegde misdrijven. Het gaat dan wel om strafbare gedragingen die in ernstige mate de integriteit van de rechtspleging en de integriteit van het openbaar bestuur raken. Als een 'typische rijksrecherchezaak' wordt het onderzoeken van de schending van het ambtsgeheimen (artikel 272 Sr) genoemd (Aanwijzing taken en inzet rijksrecherche, 2010A033). De Rijksrecherche verricht alleen feitenonderzoeken en opsporingsonderzoeken. De Coördinatiecommissie Rijksrecherche beslist over de inzet van de Rijksrecherche.

4.4.1 Voorbeelden van onderzoeken van de Rijksrecherche naar lekken

De Rijksrecherche heeft in de onderzochte periode diverse onderzoeken gedaan naar de schending van de geheimhoudingsplicht. Hieronder worden enkele voorbeelden gegeven.

In 2005 deed de Rijksrecherche onderzoek naar een medewerker die als tolk (audiobewerker) werkzaam was bij de Algemene Inlichtingen- en Veiligheidsdienst (hierna: AIVD). Deze werd er van verdacht staatsgeheime documenten te hebben weggenomen of gekopieerd. Hij zou deze verstrekt hebben aan een lid van een criminele groepering. Eén van de verdachten uit deze criminele groepering bleek bij zijn aanhouding in het bezit te zijn van een zogenaamde ‘stand van zaken’ van het tegen hem en de groepering lopende onderzoek. Ook werd de AIVD-medewerker er van verdacht kopieën van opgenomen telefoongesprekken en observatieverslagen uit datzelfde onderzoek in zijn bezit te hebben – deze werden thuis bij hem aangetroffen – terwijl deze niet buiten het gebouw van de AIVD mogen komen. De tolk is voor deze feiten veroordeeld (Jaarbericht Rijksrecherche 2005, 2006:4; Hoge Raad 7 juli 2009, rolnummer 07/10741, LJN: BG7232, AIVD-medewerker).

Een jaar later – in 2006 – deed de Rijksrecherche wederom onderzoek bij de AIVD, ditmaal naar het uitlekken van staatsgeheimen door een voormalige medewerker van de AIVD via twee journalisten van de Telegraaf. Het ging hierbij om gekopieerde werkdossiers van de toenmalige Binnenlandse Veiligheidsdienst met gevoelige, operationele gegevens over de periode 1996 – 2000 (Jaarbericht Rijksrecherche 2006, 2007:6). De voormalige medewerker is hiervoor veroordeeld (Hoge Raad 11 juli 2008, rolnummer C06/306HR, LJN: BC8421, Telegraaf-zaak; Hoge Raad 25 maart 2008, rolnummer 02387/06 B, LJN: BB2875, Verschoningsrecht journalist).

Een zeer langlopend lekonderzoek van de Rijksrecherche was de zaak onder de codenaam ‘Vancouver’. Het ging hierbij om het stelselmatig lekken vanuit de politieorganisatie. Het onderzoek is regionaal gestart en vervolgens door de Rijksrecherche onderzocht. De verdachten zijn vrijgesproken. In deze zaak is een modus operandus van een van de verdachten op een interessante wijze beschreven. Aan betrokkene is een aan een medewerker van de Nationale Recherche gerichte envelop meegegeven met het verzoek deze af te geven in Driebergen. In deze envelop bevond zich een – deels gefingeerd – proces-verbaal met informatie omtrent een ontmoeting tussen personen in het criminele milieu. Betrokkene heeft vervolgens – onderweg naar Driebergen – op een parkeerplaats langs de autoweg, de envelop geopend, het proces-verbaal met behulp van een dubbelgevouwen papiertje vastgepakt en uit de envelop gehaald, aantekeningen gemaakt op een briefje en dat briefje in een soort hoesje gestopt (Hof Amsterdam 23 december 2009, parketnummer 23-000759-08, LJN: BK7623, Vancouver).

De Rijksrecherche deed in 2007 onder meer onderzoek naar het schenden van het ambtsgeheim van een generaal inzake de wijze waarop Nederlandse militairen Irakese arrestanten hebben ondervraagd voordat ze werden overgedragen aan de Irakese autoriteiten. De generaal werd een transactie aangeboden en hij heeft deze voldaan, hetgeen een erkenning van schuld is (Jaarbericht Rijksrecherche 2007, 2008:10).

In 2009 deed de Rijksrecherche een uitgebreid onderzoek naar het uitlekken van de Staatsgeheim Zeer Geheime notulen van de Ministerraad van 28 augustus 2009 over de uitdieping van de Westerschelde en het ontpolderen van de Hedwigepolder in Zeeuws-Vlaanderen. Het onderzoek richtte zich vooral op het Ministerie van Algemene Zaken, maar ook andere departementen zijn bij het onderzoek betrokken. De Rijksrecherche concludeerde dat tenminste 235 personen de mogelijkheid tot inzage of kopiëren hebben gehad van het betreffende document. De dader van het lekken is nooit gevonden (Proces-verbaal van Bevindingen Feitenonderzoek 'Dieze', 2010:27).

Verder heeft de Rijksrecherche in 2009 onderzoek gedaan naar het uitlekken van de noodregeling van het ministerie van Financiën en De Nederlandsche Bank (hierna: DNB) voor de DSB Bank (2009). De

uitkomst van het onderzoek was dat op zondagavond 11 oktober 2009 de groep van personen die van het aanstaande verzoek bij de rechtbank op de hoogte was groter was dan vijfhonderd, verspreid over veel instanties, ook buiten de overheid. De bron van de informatie is niet gevonden. Ongeveer de helft van de meer dan vijfhonderd betrokkenen wist of kon met grote zekerheid voorspellen dat de noodregeling die zondag zou worden aangevraagd. De andere helft wist zoveel dat zij dat met redenen omkleed konden vermoeden (Kredietcrisis, Kamerstukken II 2009/10, 31 371, nr. 300:1-2).

De Rijksrecherche is in 2009 ook betrokken geweest bij het onderzoek naar een journaliste van de Telegraaf, een medewerkster van de AIVD en een voormalig medewerker van de AIVD. Op 23 maart 2009 publiceerde de journaliste in de Telegraaf het artikel “AIVD faalt”. Een eigen analyse van de AIVD wees uit dat de journaliste over gegevens moest beschikken van binnen de AIVD. Vrijwel direct werd besloten de telefoon van de journaliste af te luisteren om zo het lek binnen de AIVD op te sporen. Op 4 juni 2009 verscheen van de hand van deze journaliste een tweede artikel over het bezoek van de Dalai Lama aan Nederland en de veiligheidsaspecten die daarmee gemoeid waren. Het onderzoek van de AIVD wees uit dat de (voormalige) AIVD-medewerkers de bron waren van de journaliste. Zij werden gearresteerd en vervolgd. De AIVD rapporteerde de onderzoeksgegevens in een ambtsbericht van 11 juni 2009 aan het Openbaar Ministerie. De rechtbank oordeelde dat het afluisteren disproportioneel en dus onrechtmatig verkregen was. Al het bewijsmateriaal tegen de (voormalige) AIVD-medewerkers, vergaard in het onderzoek van de AIVD, alsmede in het opsporingsonderzoek, betrof ‘fruits of the poisonous tree’ en moest om die reden buiten beschouwing blijven. Hierdoor bestond er onvoldoende wettig bewijs om tot een veroordeling te komen (Rechtbank Haarlem 14 juli 2010, rolnummer 15/700461-09, LJN: BN1195 en rolnummer 15/700462-09, LJN: BN1191).

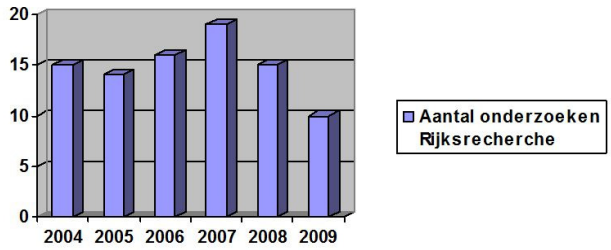
Naast feiten- en opsporingsonderzoeken kan de Rijksrecherche in bijzondere gevallen ook bijstand verlenen aan derden. Zo hebben in 2009 twee Rijksrechercheurs onderdeel uitgemaakt van het onderzoeksteam van de Commissie Prinsjesdagstukken dat onderzoek deed naar de embargoregeling en het uitlekken van de Macro Economische Verkenning uit de Prinsjesdagstukken door het PvdA Kamerlid Paul Tang (De Wijkerslooth de Weerdesteijn, De Beaufort & Borst-Eilers, 2010:9,11).

4.4.2 Aantal onderzoeken Rijksrecherche

Op basis van de Jaarberichten Rijksrecherche uit de periode 2004 tot en met 2009 kan gesteld worden dat het aantal onderzoeken van de Rijksrecherche naar schendingen van de geheimhoudingsplicht vrij constant is. Alleen het aantal onderzoeken in 2009 was bijna een derde lager. De cijfers over 2010 waren bij het afronden van dit onderzoek nog niet bekend.

Jaartal	Aantal
2004	15
2005	14 *
2006	16
2007	19
2008	15
2009	10

*) Inclusief corruptie



Figuur 4.2: Aantal onderzoeken Rijksrecherche naar schending geheimhoudingsplicht

Tijdens het interview met de plaatsvervangend directeur Rijksrecherche is de vraag gesteld of het feit dat het aantal lekonderzoeken door de Rijksrecherche vrij constant is, verband houdt met het aantal meldingen dat binnenkomt of dat er een limiet is aan het aantal lekonderzoeken dat wordt ingenomen: “Het aantal meldingen van lekken zal meer kunnen zijn. De selectie wordt gedaan door het parket van het Openbaar Ministerie. De zaken die in de Jaarberichten staan zijn de zaken met voldoende vlees om het bot om onderzocht te worden” (Interview H. Hummel, 28-12-2010).

4.5 Materiedeskundigen over dreigingen en kwetsbaarheden van geheimen

Er zijn tien interviews afgenomen met diverse materiedeskundigen (zie bijlage I). De inhoud van deze interviews is als achtergrondinformatie gebruikt en ook deels verwerkt in de overige hoofdstukken en

casussen. De interviews zijn gesplitst semi-gestructureerd opgezet. Hierdoor is het mogelijk deze paragraaf aan de hand van een aantal thema's in te delen.

4.5.1 Ontwikkelingen fenomeen lekken

Sinds de onderzoeken van Bovens, Geveke en De Vries in 1993 en Beenakkers en Grapendaal in 1995 is ruim vijftien jaar verstreken. In deze periode heeft bijvoorbeeld de technische infrastructuur, zoals de brede beschikbaarheid van e-mail en goedkope digitale gegevensdragers met grote capaciteit, een enorme vlucht gemaakt. Het is interessant om te zien welke ontwikkelingen de respondenten hebben gezien bij het fenomeen lekken.

- "Het lekken hoort erbij, het wordt minder erg gevonden. De tijden zijn veranderd, informatie wordt niet meer als waardevol gezien. De druk is vaak niet aanwezig om veilig met informatie om te gaan." (Interview H.G. Geveke, 17-06-2010)
- "Het lekken wordt gemakkelijker en gewoner. Mensen denken dat ze er mee weg kunnen komen. Denk aan WikiLeaks of de bouwfraude. Een significant deel van ons werk bestaat uit lekonderzoeken." (Interview R. Prins, 31-12-2010)
- "De grootste verandering die mij opvalt, is de gewenning. Men windt zich niet meer zo op over lekken. Onderzoek door de Rijksrecherche heeft soms geen zin meer omdat bleek dat Staatsgeheimen bij wijze van spreken 150 keer gekopieerd zijn. Het besef van het belang van geheimhouding is minder aanwezig en in de top realiseert men zich minder dat je er iets aan kan doen. Het gaat dan vooral om bewustwording, techniek is ondersteunend." (Interview J.W. Holtslag, 11-01-2011)
- "Bij de politie is het lekken afgenomen. Dat komt door een toegenomen bewustwording rond privacy, bijvoorbeeld door de Wet politiegegevens. Ook in brede zin is er al vele jaren veel aandacht geweest voor integriteit bij de politie. Binnen het openbaar bestuur valt nog wel wat te verdienen. Denk aan publiek-private samenwerking, politiek en commercie zitten dan dicht op elkaar, dat kan tot het lekken van informatie leiden om zo een deal rond te krijgen. Informatie is geld waard bij het gunnen van opdrachten." (Interview H. Hummel, 28-12-2010)

4.5.2 Het hoe en waarom van het lekken van geheimen

In de voorgaande hoofdstukken is op basis van de literatuur al aandacht besteed aan de typologie van lekken, de achtergrond en de wijze waarop gelekt wordt. Ook aan de respondenten is de vraag voorgelegd hoe (op welke wijze) en waarom (met welk doel) er gelekt wordt.

- "Er zijn meerdere voorbeelden te geven. Het niet opzettelijk verliezen van een onbeveiligde usb-stick met vertrouwelijke data. Het in een posttransport verliezen van cd-roms met vertrouwelijke data. Het versturen van een mailbericht met een vertrouwelijke bijlage. Het verliezen van vertrouwelijke documenten in het openbaar vervoer. Het mogelijk bewust doorspelen van vertrouwelijke informatie naar de media. [...] [Het even 'in vertrouwen' inlichten van een collega of plaatsvervanger.] Op die manier raakt informatie snel in een te brede kring bekend. Dit is een verschijnsel dat men vaker ziet bij het uitlekken van informatie. Denk ook aan het bespreken van zaken in het openbaar, op het terras, tijdens recepties, in het openbaar vervoer en in het vliegtuig. Hier kunnen personen bijzitten die de informatie ongeoorloofd kunnen horen en zien. […] [Lekken geschiedt] onbedoeld door niet de juiste middelen voor handen te hebben, door de gemakkelijke weg te kiezen, de risico's te veel te relativeren of door spoedomstandigheden 'Het moest van m'n leidinggevende'. Bedoeld, daar kun je een heel boek over schrijven. Bijvoorbeeld maatschappelijk betrokken ambtenaren die vanuit burgerperspectief ontwikkelingen zien waar ze het niet mee eens zijn, waar ze zich zorgen over maken. Misschien wel vanuit een positieve grondslag, maar niet in het belang van de organisatie. Er kan ook een negatieve grondslag zijn, de ontevreden medewerker, een ontslag of een dreigend ontslag, reorganisatie of een personeelsconflict. Men kan dan lekken om druk op de organisatie te leggen om iets te doen of na te laten." (Interview E.P. Grobbe, 20-12-2010)
- "Er zijn volgens mij drie categorieën. De eerste is de strafrechtelijke, lekken met een criminele intentie. De tweede is dom lekken, denk aan verjaardagpraat, interessant lopen doen. De derde is diplomatiek of strategisch lekken. Dat zie je bij de burgemeestersbenoemingen of bijvoorbeeld bij het lekken uit de Ministerraad. Het heeft een politiek doel of het is om een journalist te behagen, zodat je later een wederdienst kunt krijgen. Strategisch lekken hebben we bij onderzoeken nooit kunnen aantonen, wel het strafrechtelijk lekken. De intentie om te lekken komt bij de onderzoeken niet naar boven. Vaak geeft men aan dat men de regels niet kende, dat men niet wist dat het stuk geheim was of vond men het geen probleem om het stuk te openbaren. De oorzaken van het lekken liggen ook bij de organisaties zelf. Men geeft de medewerkers niet de juiste technische

middelen. Of men voert geen goed personeelsbeleid, door bijvoorbeeld uitzendkrachten op gevoelige plekken te zetten." (Interview H. Hummel, 28-12-2010)

- "Medewerkers kunnen te veel bij informatie waar ze niets mee te maken hebben. Hierbij staat het beginsel van need to share soms op gespannen voet met het beginsel van need to know. […] Medewerkers hebben over het algemeen te weinig waardebesef, men denkt te weinig na, dat het onderwerp waar zij elke dag mee bezig zijn voor andere partijen interessant kan zijn. Stel dat je elke dag bezig bent met het berekenen van aardgasreserves. Je kunt dat vanuit een wetenschappelijk gezichtspunt benaderen. Maar die informatie is heel veel geld waard, die reserves zijn de basis voor onderhandelingen met bijvoorbeeld een gasleverancier als het Russische GazProm." (Interview R. Prins, 31-12-2010)
- "Neem de Prinsjesdagstukken. Deze werden onder embargo verspreid onder Kamerleden en in het ambtelijke apparaat. Dat werd dan vermenigvuldigd en verspreid onder de medewerkers. Daarbij kon wel eens wat bij de kopieermachine blijven liggen. Of er was een journalist die belde om informatie. Volgens mij was het zelden in de vorm van hard copy, maar vooral in mondelinge vorm. Het wordt allemaal steeds partijpolitieker, zaken kunnen dan door politiek assistenten 'geplugd' worden. Bijvoorbeeld beleid dat de minister vast laat weg zetten via de media." (Interview J.W. Holtslag, 11-01-2011)
- "Een interne notitie die voortijdig verstrekt wordt vind ik geen lekken, het geeft aandacht voor dat dossier en is tactische informatie. Een voorbeeld hiervan zijn de diverse beleidsvoorstellen van minister Opstelten die de laatste tijd steeds in de Telegraaf staan. Dat gebeurt bewust, dat is geen lekken. Lekken is het op eigen houtje verstrekken van informatie, zonder dat de verantwoordelijke voor die informatie daar weet van heeft. Dat gebeurt zowel door ambtenaren als door politici. Van strategisch lekken is sprake als het ene departement een plan van een ander departement laat lekken omdat ze het niet met dat plan eens zijn, om het plan op die manier te frustreren. Dan heb je nog lekken uit ijdelheid, ik weet iets, ik ben ergens bij geweest, ik ben belangrijk. Je kunt ook denken aan domme pech. Een nietje dat verkeerd zit waardoor er een pagina te veel is aangehecht of een fout bij het kopiëren. Tot slot heb je nog het melden van misstanden, het klokkenluiden. […] Hoe ontvang ik de informatie? Soms legt men het ergens neer. Het wordt ook wel per fax of e-mail verzonden. Soms wordt het ook voorgelezen aan de telefoon. Bij dat voorlezen moet je je wel weer afvragen hoe betrouwbaar het is, je moet het dan gaan verifiëren." (Interview F. Wester, 03-02-2011)

4.5.3 Rubriceren als een kunde

Als belangrijke oorzaak van het lekken wordt in de literatuur het op onjuiste gronden aanwijzen van rubriceringen genoemd. Rubriceren blijkt vaak lastig te zijn voor functionarissen. In paragraaf 2.7 is dat – mede aan de hand van het Eclips Model – al aan de orde geweest. Ook de Commissie Lemstra constateerde dit probleem:

> Eveneens heeft de commissie te horen gekregen dat een groot aantal gerubriceerde stukken óf te hoog óf ten onrechte gerubriceerd is óf ten onrechte niet gederubriceerd is. Van verschillende zijden, is de commissie erop gewezen dat 95% van het aantal gerubriceerde stukken zelfs ten onrechte is gerubriceerd. De commissie acht dit geen goede zaak. Door het stempel vertrouwelijkheid krijgt een document al gauw een zeker gewicht en een zekere nieuwswaarde, waarmee de kans op lekken wordt vergroot. Er is een inflatie in rubricering opgetreden, waardoor beveiligingsregels met voeten worden getreden. Bovendien bevestigt deze gang van zaken de indruk dat Defensie een organisatie is waarin zoveel mogelijk informatie verborgen moet blijven; wat op zichzelf al tot grote nieuwswaarde van de betrokken documenten leidt. (Lemstra et al., 2005:26-27)

Naar aanleiding van het onderzoek naar de besluitvorming rond de inval in Irak komt ook de Commissie Davids tot een vergelijkbare conclusie:

> Voor de vraag of informatie staatsgeheim is of niet, is uiteraard de inhoud van belang, maar daarnaast moet het criterium worden gelegd of aan de veiligheid van de staat schade kan worden toegebracht. Een ministerie kan in de verleiding komen om te trachten voor haar ongunstige berichten of hinderlijke vragen te voorkomen, door informatie te rubriceren of anderszins daarover niet of terughoudend openbaarheid te betrachten. Dat is uiteraard op zich niet een voldoende beschermingswaardig belang. (Davids, 2010:12)

De Commissie Davids heeft haar laatste conclusie van het rapport, nummer 49, hier ook aan gewijd, zij: “[…] heeft zich bij inzage van sommige staatsgeheime documenten afgevraagd welke de redelijke zin kan zijn van de nog steeds daaraan gehechte rubricering. Geschiedschrijving en waarheidsvinding worden hiermee zonder voldoende grond belemmerd” (Davids et al., 2010:429).

Figuur 4.3: Rubriceren als een kunde (illustratie John Morris)

Diverse respondenten gingen tijdens de interviews in op de kunde van het rubriceren:

- “Er is sprake van een inflatie van geheimen. Zaken worden geheim verklaard omdat het interessant is, uit gewoonte, om betwistbare informatie achter te houden en uit gemakzucht.” (Interview H.G. Geveke, 17-06-2010)
- “Je moet je bijvoorbeeld de vraag stellen of er bijvoorbeeld wel sprake is van een geheim. Classificeren is een vak apart dat niet elke ambtenaar verstaat. Je moet ook het ongebreideld rubriceren voorkomen. Soms worden zaken als een geheim betiteld terwijl die naar de inhoud helemaal geen geheim zijn.” (Interview H. Hummel, 28-12-2010)
- “Bij het ene departement was bepaalde informatie wel gerubriceerd en bij het andere departement was vergelijkbare informatie niet gerubriceerd, of op een ander niveau. Maar we zagen soms ook stukken waarbij we ons afvroegen of die niet eigenlijk gerubriceerd hadden moeten zijn, omdat openbaarmaking tot schade zou kunnen leiden.” (Interview J.J.G. van der Bruggen, 10-01-2011)

De Beveiligingsambtenaar van het ministerie van BZK ging in zijn interview in op het probleem dat niet elke ambtenaar weet wat een rubricering inhoudt en illustreerde dit aan de hand van een anekdote ten tijde van de Fitna-film van Wilders (Casus 8).

Casus 8: De Staatsgeheim Zeer Geheime Knipselkrant

In de aanloop van de lancering van [de film ‘Fitna’ van het Tweede Kamerlid Geert Wilders, JHM] in maart 2008 was er geregeld interdepartementaal politiek-bestuurlijk overleg. Voorafgaande aan zo’n overleg werd gevraagd of er stempels beschikbaar waren voor een Staatsgeheim Zeer Geheim stuk. Dit is de hoogste rubriceringsgraad en wordt – met uitzondering van de Ministerraadstukken – heel terughoudend toegepast. De persoon die om de stempels vroeg gaf aan dat hij veel exemplaren moest stempelen. Daarop werd gevraagd om hoeveel exemplaren het ging. Dat waren er meer dan twintig. Dat is zeer ongebruikelijk voor een Staatsgeheim Zeer Geheim document, want als het zulke kwetsbare informatie is, mag het in de regel niet zo breed verspreid worden. Bovendien dient dan ook een registratie plaats te vinden hoeveel documenten bijgemaakt zijn, waar deze zich bevinden en wanneer ze vernietigd zijn, dat gaat heel geprotocolleerd. Uiteindelijk bleek het te gaan om de knipselkrant over de Fitna-film! Los dat dit een dergelijke hoge rubricering niet verdient, bleek ook dat men na de vergadering dit document mee naar huis mocht nemen. Bij een Staatsgeheim Zeer Geheim stuk is dat uitgesloten. Eind van het verhaal was dat dit stuk niet gerubriceerd hoefde te worden. De les die hieruit getrokken kan worden is dat een bepaald dossier weliswaar heel gevoelig kan zijn, maar dat niet alle stukken in zo’n dossier gerubriceerd hoeven te zijn. Een kwestie van gezond verstand.

(Interview E.P. Grobbe, 20-12-2010)

4.5.4 Lekken uit frustratie of wrok

In paragraaf 2.8.2 is aangegeven dat frustratie of wrok motieven kunnen zijn om te lekken. Bijvoorbeeld vanwege ontslag dat als onterecht ervaren wordt of een onheuse bejegening door de leidinggevende of ambtelijke en politieke top. Ook ingrijpende bezuinigingen trekken een grote wissel op de loyaliteit van medewerkers, net zoals reorganisaties, inkrimpingen en structuurwijzigingen (Lemstra et al., 2005:40, 43). Aan diverse respondenten is gevraagd in hoeverre lekken uit frustratie of wrok speelt.

- "Dat gebeurt, uit rancune. Hoe hoger je stijgt, des te minder tegenspraak je krijgt. Men wordt omringd door een hofhouding, een muur van vertrouwelingen. Kritiek komt niet door die muur heen. Dat is slecht voor het functioneren als leidinggevende. Als je jarenlang niet bent tegengesproken denk je dat je alles mag. Sommige bewindspersonen dulden geen tegenspraak. Dan kunnen mensen gaan lekken. Ik heb eens een onderzoek gedaan naar zo'n situatie. Er was een leidinggevende met een hofhouding die de andere medewerkers slecht behandelde. Hij ging ook met dienstwagens op wintersport, met zijn hofhouding die er nauwelijks iets voor hoefden te betalen. Er was onvrede en hier werd over gelekt. We hebben tijdens het onderzoek niet alles boven water kunnen krijgen, we hadden een beperkte bevoegdheid, maar toch hebben we voldoende feiten boven water gekregen die aannemelijk maakten dat er zaken niet op orde waren." (Interview C.R. Niessen, 26-01-2011)
- "Dat komt ook voor. Maar met dat soort lekken moet je voorzichtig zijn, die informatie is gekleurd. Roddels over vreemd gaan doen we niet. Declaratiegedrag doen we wel als het aantoonbaar en fout is. Het is dan nieuwswaardig, het gaat er dan om hoe men met belastinggeld om gaat." (Interview F. Wester, 03-02-2011)
- "Ik vind voorbeeldgedrag heel belangrijk. Hierbij is het ook van belang dat je de ambtenaren aan je bindt in de zin van loyaliteit. Salaris alleen is gebleken een slechte motivator te blijven. Voor sommigen wordt het gekscherend ook wel eens gezien als een vorm van zwijggeld. Belangrijk is dat naast de tijdige correctie van het gedrag ook de waardering op z'n tijd wordt uitgesproken. Het belangrijkste voor leidinggevenden is dat zij met respect in de richting van hun medewerkers acteren. Pas dan zal de loyaliteit een kans krijgen. Loyaliteit is weer een belangrijke basis om gewenst gedrag te bevorderen. Dan is de loyaliteit er ook bij een zakelijk conflict. Als je geen respect meer hebt voor de leidinggevende of gezagsdrager valt de belemmering weg om deze in diskrediet te brengen. De veiligste manier om de leidinggevende of gezagsdrager in diskrediet te brengen is niet via de klokkenluidersregeling, maar via strategisch lekken de leidinggevende en/of diens organisatie in diskrediet te brengen. Politieke en ambtelijke top, maar ook leidinggevenden moeten daarom voorbeeldgedrag tonen richting hun medewerkers en ze ook respectvol bejegenen." (Interview H. Hummel, 28-12-2010)
- "Ik ben me hier altijd wel bewust van geweest, het risico van de 'angry ex-employee'. Dat komt nog redelijk vaak voor, ook buiten de departementen. Het is van belang om aandacht te hebben voor de wijze waarop je afscheid van elkaar neemt. Als er iets naars moest gebeuren, dan nam ik voorzorgsmaatregelen. Maar soms zie je niet aankomen dat iemand een binnenvetter is of juist iets gepland heeft, dat deze iets opbouwt. Dat is een groot risico. Het zou verstandig zijn om hier aandacht aan te besteden. Je moet mensen niet in een wanhoopspositie brengen. Ook als je afscheid van elkaar moet nemen moet je hier aandacht aan besteden. We moeten meer nadruk leggen op de cultuur dan op de harde maatregelen. […] Het is ook belangrijk dat je als politieke en ambtelijke top mensen niet onnodig schoffeert, je moet zakelijk zijn. Het zijn sterke benen die de weelde van zo'n positie kunnen dragen." (Interview J.W. Holtslag, 11-01-2011)

4.5.5 Lekt het schip van staat van boven?

De beruchtste plek van Den Haag rondom lekken is het Plein en de directe omgeving daarvan. Tijdens het onderzoek van de Commissie Lemstra naar lekken binnen Defensie typeerde een van de gehoorde journalisten 'Den Haag' als 'een grote kletsmachine'. In het eindrapport van de commissie gaf zij aan dat zowel de geïnterviewde journalisten als de geïnterviewde politici aangaven dat "in het algemeen niet de ambtenaren verantwoordelijk zijn voor het lekken van vertrouwelijke dan wel geheime informatie" (Lemstra et al., 2005:49).

Een bekend gezegde uit de BBC-serie 'Yes Minister' luidt: "The ship of state is the only ship that leaks from the top" (Lynn & Jay, 1994:442). Deze uitspraak wordt ook in de literatuur aangehaald (Van Venetië & Luikenaar, 2006:122) en ook door de respondenten tijdens de interviews. Dit suggereert dat het juist de top van de organisatie is waar het meest gelekt wordt. Lekt het schip van staat van boven?

- "Ik onderschrijf het gezegde dat het Schip van Staat het enige is dat vooral van boven lekt. Er zijn in de politieke en ambtelijke top namelijk veel overleggen waar gelekt kan worden, informatie is

alles, daar leeft men van het nieuws. Maar soms is het lekken gewoon een kwestie van opscheppen over wat men weet." (Interview J.W. Holtslag, 11-01-2011)
- "Het varieert van de echte ambtelijke top tot de secretaresse, en alles ertussen. Iedereen die informatie bezit. Vaak zijn het gewoon tips in de trant van 'houd dat eens in de gaten." (Interview F. Wester, 03-02-2011)
- "Dat weet ik niet. Ik denk het niet. Als het van boven lekt heeft het vaak wel meer impact. Lekken in het ruim worden minder snel gezien omdat het zich benedendeks afspeelt en dus aan het zicht is onttrokken. Het is goed om te beseffen dat de gevoelige informatie niet altijd bij de top zit, maar ook daaronder, zoals bij de administratief medewerkers en de secretaresses." (Interview H. Hummel, 28-12-2010)

4.5.6 Lekken, (g)een noodzakelijk kwaad

In de hoofdstukken 2 en 3 is al ingegaan op het instrumentele karakter dat lekken soms heeft. Lekken is dan een onderdeel van het politiek-bestuurlijke spel. Dat roept de vraag op of lekken een noodzakelijk kwaad is.

- "We kunnen heel goed zonder lekken. In sommige gevallen wordt er gelekt uit gewetensnood, om misstanden te melden. Dat is alleen acceptabel als er geen klokkenluidersregeling is." (Interview H.G. Geveke, 17-06-2010)
- "Nee, ik zie geen positieve uitkomst voor de organisatie. We hebben al voldoende mogelijkheden voor het melden van misstanden of andere zaken die onder de aandacht gebracht moeten worden. Daar voegt lekken niets aan toe. […] Geïnstitutionaliseerd lekken zou niet nodig moeten zijn." (Interview E.P. Grobbe, 20-12-2010)
- "Klokkenluiden is soms goed en in de politiek is lekken soms essentieel. Soms kan men formeel niets zeggen maar wel via een lek, dat noemt men dan een proefballonnetje. Wat ook tot lekken leidt is een organisatie waar een afdekcultuur bestaat. Waarbij men afgestraft wordt als men de nek een keer uitsteekt." (Interview R. Prins, 31-12-2010)
- "Het is kwaad, het is niet noodzakelijk." (Interview J.W. Holtslag, 11-01-2011)
- "Nee, ik vind van niet. Het hoort niet. Het beschadigt het vertrouwen van de buitenwereld in de organisatie. Het is alleen goed te praten waar openbaarheid geen groot goed is, waar de Wet openbaarheid van bestuur verkwanseld is, waar misstanden niet aan de kaak gesteld kunnen worden." (Interview C.R. Niessen, 26-01-2011)
- "Het is onlosmakelijk [van de politiek, JHM]. Het is van alle tijden en het gebeurt in ieder land." (Interview F. Wester, 03-02-2011)
- "Ik ben politicoloog. Ik snap vanuit dat gezichtspunt dat lekken gebeurt. De kabinetsreactie op ons rapport lekte bijvoorbeeld wel uit. In sommige gevallen is lekken verdedigbaar, maar dan kom je in de klokkenluidershoek. Lekken gebeurt vaak om politieke opportunistische redenen. Als Commissie zijn we er behoorlijk trots op dat het ons niet overkomen is." (Interview J.J.G. van der Bruggen, 10-01-2011, zie casus 9)

Casus 9: Het níet uitlekken van het rapport van de Commissie Davids

"De [Commissie van onderzoek besluitvorming Irak, ook bekend als de Commissie Davids, JHM] is bijna nog meer geprezen om de wijze waarop zij het rapport tot op de dag van de presentatie uit de publiciteit heeft kunnen houden dan om de inhoud van het rapport.

Lekken is in het Haagse circuit zo aan de orde van de dag dat niet lekken nieuws is. Geheimhouding is niet zo moeilijk. Er zijn enkele fysieke maatregelen genomen om de vertrouwelijkheid en geheimhouding te garanderen, maar die hadden meer te maken met het gegeven dat er met staatsgeheime informatie werd gewerkt dan met het oog op het lekken naar de pers. Daarnaast heeft de commissie ervoor gekozen om alle communicatie te laten verlopen via een communicatieadviseur die zelf pas in de slotfase inhoudelijk van het onderzoek op de hoogte was. Verder hebben we nooit het werkadres van de commissie aan de publiciteit prijsgegeven. Alle correspondentie verliep via e-mail of postbusnummer. Natuurlijk werden commissie- en stafleden persoonlijk wel geconfronteerd met – letterlijk – nieuwsgierige journalisten, politici, ambtenaren en collega's. Helaas voor hen vergeefs.

De belangrijkste reden dat het gelukt is om het rapport geheim te houden is heel simpel: degenen die de inhoud kenden (commissie, staf, drukkers, vertalers) hadden geen belang bij het lekken en andersom hadden degenen die belang hadden bij lekken (journalisten, wellicht sommige ambtenaren en politici) geen kennis van de inhoud."

(Van der Bruggen, 2010:93-94)

4.6 Het Nieuwe Werken

Aparte aandacht binnen dit hoofdstuk verdient 'Het Nieuwe Werken'. Met Het Nieuwe Werken (hierna: HNW) wordt gedoeld op het plaats- en tijdonafhankelijk werken dat binnen steeds meer organisaties, waaronder de Rijksoverheid, omarmd wordt. HNW wordt ondersteund door de laatste technologieën zoals social media (Twitter, Yammer, LinkedIn), cloud computingdiensten (Google Docs) en mobiele communicatie (smartphones voor spraak, e-mail en video). Kenmerkend is dat informatiestromen grotendeels gedigitaliseerd zijn en dat medewerkers en organisaties flexibeler omgaan met arbeidstijd en werkomgeving. Men wordt niet meer afgerekend op het aantal uren dat men op kantoor aanwezig is, maar op de productiviteit, de output. Doel hiervan is dat er beter programmatisch gewerkt kan worden en men kan besparen op zaken als huisvesting en reiskosten. Met behulp van social media kunnen ambtenaren makkelijker onderling overleggen en contact hebben met burgers (Maat, 2011:32).

Doordat opslag, transport en bewerking van data deels plaatsvinden buiten het eigen domein van de organisatie neemt de vluchtigheid van informatie toe. Hierin zit de grote kwetsbaarheid van HNW: de kans dat er (verwijtbaar) gelekt wordt neemt namelijk ook toe. Het gaat hierbij in ieder geval om drie factoren: werken in de publieke ruimte, gebruik mobiele gegevensdragers, vermenging van werk en privé. De risico's van HNW ten aanzien van spionage doordat buitenlandse mogendheden onder dwang toegang kunnen verkrijgen tot de gegevens in datacenters en op mobiele gegevensdragers (Spionage bij reizen naar het buitenland, 2010:1), valt buiten het kader van deze thesis.

4.6.1 Werken buiten de kantooromgeving

Bij HNW wordt veelal buiten de reguliere kantooromgeving gewerkt (hoewel werken op flexplekken op andere kantoorlocaties ook mogelijk zijn). Omdat men voor het verrichten van de werkzaamheden wel informatie nodig heeft, neemt men de informatie fysiek of digitaal mee, of men moet een verbinding leggen met de ICT-infrastructuur van de organisatie.

Het fysiek meenemen van documenten kent het risico van verlies, zeker als dit op een onzorgvuldige – dus verwijtbare – wijze geschiedt. Voorbeelden hiervan halen regelmatig de media, zoals de volgende casus (Casus 10).

Casus 10: Politierechter raakt dossiers kwijt

“Een Haagse politierechter heeft voor enorme opschudding gezorgd op het paleis van justitie door vijf uiterst vertrouwelijke dossiers kwijt te raken. De vrouwelijke rechter, mr. B., verloor de stukken toen ze onverwacht naar huis moest vanaf haar werk. Ze had de dossiers in een plastic zak gestopt en onder haar snelbinder gebonden. ‘Eenmaal bij haar woning ontdekte ze dat de zak weg was. Ze is onmiddellijk de route teruggefietst, maar dat leverde niets op. Hierop heeft ze de sectievoorzitter, de politie en het openbaar ministerie op de hoogte gebracht’, bevestigt een woordvoerster van de Haagse rechtbank.

Tot grote verontwaardiging van de bekende Haagse strafpleiter mr. Ad Westendorp, verzuimde de vrouw echter om in de zaken die vorige week dienden de verdachten en raadslieden te waarschuwen dat de dossiers op straat lagen. Pas nadat iemand de papieren in de zak had gevonden en die naar de redactie van het misdaadprogramma van Peter R. de Vries bracht, stuurde de rechtbank een excuusbrief. In een reactie liet de rechtbank gisteren weten deze gang van zaken achteraf zeer te betreuren: ‘We hebben tijdens enkele zittingen de mensen niet op de hoogte gesteld, maar hadden dat inderdaad beter wel kunnen doen. De rechtbank is zich er zeker van bewust dat dit een fout is geweest.’

In de gisteren verstuurde excuusbrief staat onder meer dat de rechter de zaken heeft behandeld op basis van een kopie van de originele stukken. ‘Dit is zeer kwalijk. Vooral in de zaak van mijn cliënt was het absoluut van belang dat er kleurenfoto's te zien waren en in plaats van zwart-witte kopieën’, foetert Westendorp. ‘Het ging om iemand die is opgepakt omdat zijn auto vol lag met speelgoedpistooltjes die zijn zoontje op allerlei kermissen had gewonnen. Op originele foto's is door de kleuren juist overduidelijk te zien dat alles nep is, maar nu dus niet meer. Daarbij heeft het openbaar ministerie de pistooltjes ook al laten vernietigen, dus wij staan met onze rug tegen de muur. Nu is mijn cliënt veroordeeld.’"

(Jongbloed 2009)

Het verlies van de dossiers betekende in dit geval niet alleen dat de informatie uitgelekt is, doordat het ook de originele documenten betrof is – zo stelt de raadsman – ook de interpretatie van de inhoud van de informatie bemoeilijkt.

Daarom heeft een digitale verbinding met de organisatie de voorkeur. Idealiter geschiedt dat via een VPN-verbinding (Virtual Private Network) met de nodige beveiligingsmaatregelen om hacken tegen te gaan. De medewerker heeft dan een virtuele digitale werkplek die gelijk is aan die op kantoor (Overbeek, Roos Lindgreen & Spruit, 2005:178). Hier zijn kosten aan verbonden en soms is de snelheid beperkt. Daarom kan de verleiding bestaan om buiten de eigen ICT-voorzieningen om te gaan werken. Men mailt bijvoorbeeld bestanden – al dan niet via automatisch doorsturen – naar een privé e-mailadres en plaatst de bestanden in een openbare maar 'afgeschermde' werkomgeving. Als dit ook geschiedt bij gerubriceerde of gevoelige informatie is de controle over deze informatie weg en is de kans aanwezig dat onbevoegden – per abuis – toegang krijgen tot deze informatie. Dit speelt zeker wanneer de medewerker de organisatie verlaat, deze heeft dan immers nog steeds de beschikking over de informatie. Externe toegang via een VPN maakt het ook voor kwaadwillende medewerkers eenvoudiger om intentioneel te lekken, zeker als er onbeperkte toegang is tot alle data en het gebruik van de voorzieningen niet gemonitord wordt. Ook als een medewerker onzorgvuldig omgaat met zijn of haar inloggegevens (zoals het delen hiervan met collega's en zelfs gezinsleden) leidt dit tot grote kwetsbaarheden voor de organisatie. Het werken in de publieke ruimte kan ook letterlijk genomen worden. Lekken gaat sneller in een omgeving waar onbevoegden eenvoudig mee kunnen lezen en luisteren zoals in de horeca en het openbaar vervoer (Maat, 2011:33).

4.6.2 Gebruik mobiele gegevensdragers

Om mobiel te kunnen werken is het gebruik van mobiele gegevensdragers zoals smartphones, usb-sticks en notebooks/tablet-pc's noodzakelijk. Het is dan wel van belang dat deze voorzien zijn van de juiste beveiliging (zoals encryptie). Wanneer dit niet het geval is, bijvoorbeeld omdat deze er nooit geweest is, het verouderd is of omdat de gebruiker het verwijderd heeft omdat het zo lastig werken is, ontstaan er weer risico's op lekken bij verlies van de gegevensdrager. Het risico neemt verder toe als deze informatie gerubriceerd of gevoelig is en wanneer er meer informatie op staat dan noodzakelijk is voor het vervullen van de werkzaamheden (zoals in casus 2). Als medewerkers privé-apparatuur gebruiken voor hun werkzaamheden ('Bring Your Own') is de kans ook groot dat hierop data van de organisatie opgeslagen wordt. Bij vertrek van de medewerker of bij het afdanken van de apparatuur is de kans dat de informatie bij onbevoegden komt ook groot. Daarnaast is het bij privé-apparatuur gecompliceerd om onderzoek te doen naar aanleiding van vermoedens van integriteitsschendingen (Maat, 2011:33-34).

4.6.3 Vermenging werk en privé

Door het tijdonafhankelijke werken bij HNW is het eerder onduidelijk of men als privépersoon of als ambtenaar iets doet. Bijvoorbeeld bij het delen van informatie via social media. De kans dat men onbewust gerubriceerde of gevoelige informatie deelt neemt ook toe, bijvoorbeeld doordat een bericht voor een bepaalde ontvanger naar een grotere gebruikersgroep gezonden wordt of omdat men informatie (telefonisch) bespreekt in een onjuiste omgeving (bijvoorbeeld op een feestje als in casus 5). Daarnaast kan door HNW tot onthechting van de organisatie leiden, waardoor de 'politiek-bestuurlijke sensitiviteit' van de ambtenaar afneemt (Maat, 2011:34).

Naast de voordelen van HNW zijn er dus ook nadelen: "Als je Het Nieuwe Werken vanuit de informatiebeveiliging niet goed faciliteert, dan vinden de medewerkers het zelf uit, maar dan wel op een manier dat je er geen controle meer op hebt" (Interview R. Prins, 31-12-2010). De keuze van de middelen en beveiligingsmaatregelen bepalen hierbij mede de kwetsbaarheid van het proces.

4.7 Overzicht van dreigingen en kwetsbaarheden ten aanzien van geheimen

Op basis van het voorgaande is het mogelijk een overzicht te maken van dreigingen en kwetsbaarheden ten aanzien van geheimen. Deze worden op de volgende pagina in een matrix weergegeven (figuur 4.4).

Uiteraard is dit een model. Dreigingen en kwetsbaarheden kunnen in de praktijk door elkaar heen lopen. Bij het intentioneel handelen dienen de maatregelen primair gericht te zijn op de dreiging en secundair op de kwetsbaarheid. Omdat het lekken met opzet gebeurt, is het aannemelijk dat men een

wijze kiest die eenvoudig is of moeilijk te achterhalen. Bij verwijtbaar handelen is dit juist andersom, daar is primair de kwetsbaarheid van belang en secundair de dreiging. Door het bewustzijn te vergroten is de kans op het wegnemen van het verwijtbare handelen groot.

	Dreigingen, achtergrond van handelen	**Kwetsbaarheden, het is mogelijk om**
INTENTIONEEL HANDELEN	Persoonlijk, gericht op: • beloning in de vorm van geld, goederen of diensten • versterken van de eigen positie of het verzwakken van de positie van een tegenstander • het vergroten van de eigen status, bijv. om te laten zien dat men een insider is (opscheppen) • wrok of frustratie jegens een persoon of organisatie	• inzage te geven tijdens een gesprek, direct of indirect ('even weglopen') • fysieke overdracht van papieren documenten of digitale gegevensdragers te realiseren, al dan niet tijdelijk ('uitlenen') • digitale overdracht van bestanden te realiseren, al dan niet via een omweg om sporen te vermijden • mondelinge overdracht in persoon of telefonisch (eventueel anoniem) te realiseren, waarbij de informatie exact wordt gegeven of juist 'off the record' of omschreven in de vorm van 'achtergrond-gesprekken'
	Institutioneel, al dan niet geautoriseerd, gericht op het strategisch belang zoals het voortbestaan van het eigen onderdeel, te onderscheiden in: • mobiliseren • antagonistisch (hinderen) • conditioneren (quid pro quo)	
	Publiek belang, gericht op het melden van misstanden (de dreiging is in dit kader relatief)	
VERWIJTBAAR HANDELEN	• Slordigheid • Onbekendheid met regels • Onderschatting risico of belang • Gebrek aan bewustzijn • Gebrek aan motivatie • Gebrek aan kennis en vaardigheden om op juiste wijze met gerubriceerde of gevoelige informatie om te gaan	• binnen organisatie vat te krijgen op dreigingen uit linkerkolom
		• ongeautoriseerde toegang tot gerubriceerde informatie te verkrijgen
		• een te grote kring van geïnformeerden te laten ontstaan
		• zich te vergissen in de aard van de gevoelige informatie
		• zich te verspreken tegenover niet gerechtigde (bijv. door social engineering, gebruik bewustzijnsverminderende middelen als alcohol en drugs)
		• mee te lezen of te luisteren op openbare plaats (terras, OV, congres, vliegtuig, horeca)
		• digitale gegevensdragers te verliezen
		• papieren documenten te verliezen
		• op onjuiste wijze op te bergen (niet afgesloten, gedeelde wachtwoorden, onjuist sleutelbeheer)
		• op onjuiste wijze digitale bestanden te verzenden (verkeerd e-mailadres, onversleuteld)
		• e-mailberichten automatisch door te zenden (auto-forwarden)
		• op onjuiste wijze papieren documenten te verzenden
		• de informatie onjuist te verwerken door een rubriceringsgebrek
		• de informatie op onjuiste wijze te vernietigen (wegwaaien, 'dumpsterdiving', onvolledig wissen)

Figuur 4.4: Overzicht van dreigingen en kwetsbaarheden geheimen

In het volgende hoofdstuk zal ingegaan worden op de maatregelen die men kan nemen om het lekken van geheimen te voorkomen en de restrisico's die men moet accepteren. Dan zal het bovenstaande figuur ook worden aangevuld met twee kolommen met daarin de te nemen maatregelen en restrisico's.

5. MAATREGELEN TEGEN LEKKEN EN RESTRISICO'S

5.1 Inleiding

In dit hoofdstuk wordt nader ingegaan op de te nemen maatregelen en restrisico's. Welke maatregelen zijn mogelijk tegen het lekken van geheimen?

Vertrouwelijkheid en beschikbaarheid staan op gespannen voet met elkaar. Grofweg geldt dat hoe meer maatregelen worden genomen om informatie af te schermen voor niet-gerechtigden, des te eerder sprake zal zijn dat gerechtigde personen niet tijdig toegang tot die informatie kunnen krijgen, bijvoorbeeld doordat een wachtwoord-verificatiemechanisme tijdelijk uit de lucht is of een vergeten medewerkerspas waardoor de gebruiker geen of moeilijker toegang kan krijgen (Dekker, Veugen & Etalle, 2006:19). De mogelijk te nemen maatregelen kúnnen dus nadelen met zich meebrengen. Daarom is het van belang dat de maatregelen proportioneel worden toegepast: de zwaarte van de maatregel dient in overeenstemming te zijn met de dreiging op en de kwetsbaarheid van het belang.

Deze maatregelen kunnen worden onderscheiden in technische maatregelen en organisatorische maatregelen die in de volgende twee paragrafen op hoofdlijnen behandeld worden. Met technische maatregelen wordt gedoeld op de 'hard copy' (fysieke) en digitale maatregelen tegen lekken. Deze worden behandeld in respectievelijk paragraaf 5.2 en paragraaf 5.3. Met organisatorische maatregelen wordt gedoeld op het gedrag van mensen. Deze komen aan de orde in paragraaf 5.4. De restrisico's worden behandeld in paragraaf 5.5 en in paragraaf 5.6 staat een integraal overzicht van dreigingen, kwetsbaarheden, maatregelen en restrisico's van geheimen.

Het onderscheid tussen technische en organisatorische maatregelen is overigens niet heel scherp, ze staan in relatie tot elkaar. Zoals de directeur van het informatiebeveiligingsbedrijf Fox-IT, R. Prins, het tijdens het interview aangaf:

> Informatiebeveiliging is geen technisch probleem. Je moet techniek toepassen waar het kan, maar het gaat vooral om het gedrag van de mensen die met de informatie omgaan. Zorg voor educatie over de techniek, dan kunnen medewerkers zelf afwegingen maken. Dan voelen ze zich ook verantwoordelijk. (Interview R. Prins, 31-12-2010)

5.2 Hard copy maatregelen tegen lekken

In de literatuur gaat tegenwoordig veel aandacht uit naar de digitale aspecten van de beveiliging van informatie (Overbeek, Roos Lindgreen en Spruit, 2005:211; Talbot & Jakeman, 2008:105,114). Maar het is van oudsher papier dat als fysieke gegevensdrager wordt gebruikt en ook nu is dat nog steeds een belangrijk medium (andere gegevensdragers zoals was- en kleitabletten, stenen tafelen, bamboestroken en andere historische of etnografische methoden worden hier verder buiten beschouwing gelaten). Er is in deze paragraaf gekozen voor de term 'hard copy' maatregelen omdat de term 'fysieke maatregelen' binnen de informatiebeveiliging een veel bredere lading dekt (Overbeek, Roos Lindgreen en Spruit, 2005:19). In de volgende subparagrafen wordt ingegaan op de maatregelen die letterlijk op papier te nemen zijn.

5.2.1 Geheimschrift of codes

In de eerste plaats is het mogelijk de informatie op een wijze te noteren dat niet gerechtigden er geen logisch verband in zien. Hierin ligt ook de oorsprong van cryptografie (Overbeek, Roos Lindgreen & Spruit, 2005:163). De informatie wordt letterlijk in geheimschrift – het systematisch hergroeperen van het alfabet – of door middel van codes – woorden of symbolen die een van te voren afgesproken betekenis hebben – weergegeven. In de dagelijkse praktijk is deze maatregel waarschijnlijk minder bruikbaar, met uitzondering van het bewaren van wachtwoorden en pincodes.

5.2.2 Aangeven van rubricering, merking en rubriceringsduur

Voorts kan bij wijze van attendering op het papier worden aangegeven dat er sprake is van gerubriceerde informatie zoals 'Departementaal Vertrouwelijk' of 'Staatsgeheim Confidentieel'. Er is

dan sprake van een formeel geheim en de gerechtigde houder van het document weet dan dat deze er zorgvuldig mee om moet gaan. Een rubricering kan worden aangevuld met een merking wat een bepaalde wijze van behandelen aangeeft. Zo kan een merking worden gebruikt om het domein aan te geven waarop het document betrekking heeft, bijvoorbeeld 'Crypto', of om een speciale verspreiding aan te geven op 'need-to-know' basis, bijvoorbeeld 'NL-eyes only' wanneer de informatie niet met buitenlandse functionarissen gedeeld mag worden of 'NL/GE eyes only' gebruikt voor informatie die alleen met Duitsland mag worden uitgewisseld (Vir-bi 2004:13, 49).

Daarnaast kan de duur van de rubricering aangegeven worden. Dit is niet zonder reden, beveiligingsmaatregelen brengen als regel extra werkzaamheden en daardoor extra kosten met zich mee. Onnodig beveiligen moet daarom worden vermeden. Om deze reden gaat het Vir-bi er vanuit dat rubriceringen in beginsel tijdelijk zijn. De rubricering is gebonden aan een termijn van maximaal tien jaar of aan een bepaalde gebeurtenis zoals de afloop van onderhandelingen. Indien de rubricering is gebonden aan een bepaalde gebeurtenis moet dit op de informatiedrager zijn aangegeven door degene die de inhoud van de informatie vaststelt. De rubricering vervalt automatisch na een periode van maximaal tien jaar of nadat de bepaalde gebeurtenis heeft plaatsgevonden (Vir-bi, 2004:13). Het beëindigen van een rubricering nadat de noodzaak hiertoe weggevallen is voorkomt ook dat het draagvlak van geheimhouding wegvalt.

5.2.3 Herleidbaarheid

Een volgende stap is het individueel herkenbaar maken van het document. Het wordt dan herleidbaar waar het document vandaan komt. Vaak gebeurt dit door het zichtbaar nummeren van het document. Als er vermoedens zijn dat het document zal gaan uitlekken, dan kan men per afgedrukt document referentiepunten aanbrengen. Bijvoorbeeld door minieme en onopvallende tekstwijzigingen aan te brengen of door typografische kenmerken als interpunctie en afbrekingen. Gebruikers van gelekte informatie zoals journalisten weten dat deze methodiek kan worden toegepast. Daarom wordt niet altijd het originele document getoond, typt men soms een te tonen document over of wordt de tekst alleen voorgelezen of omschreven (Interview F. Wester, 03-02-2011).

Het herleidbaar maken kan ook door middel van een grafische techniek. De eenvoudigste vorm is het 'meeprinten' van een watermerk. Het uitlekken van de Macro Economische Verkenningen (casus 4) is op deze manier aan het licht gekomen. Er zijn ook meer geavanceerde technieken waarbij in plaats van de afgedrukte tekst het papier zelf herleidbare kenmerken bezit. Voorbeelden van anti-kopieer beveiligingstechnieken zijn 'Screen Angle Modulation' (SAM) en 'Li Frequency Trap' (LIFT) waarbij gebruik wordt gemaakt van rasterpatronen en de resolutiebeperkingen van kopieermachines. Een kopie van een dergelijk document vertoont een tekst – bijvoorbeeld 'KOPIE' of een uniek nummer – of een verstoring van het beeld, waardoor duidelijk blijkt dat het om een kopie gaat (De Heij, 2010:176; Many people, many solutions, z.j.:1-2). Het is dan wel van belang dat er een registratie plaats vindt. Een voorbeeld van een dergelijk document is opgenomen als bijlage VII (De SAM-techniek is hierop niet werkelijk toegepast, hiervoor is een gespecialiseerde drukker noodzakelijk).

5.2.4 Kopieerblokkade

Het kopiëren van teksten kan ook beperkt of voorkomen worden door de kleur van het papier. Een zeer eenvoudige techniek die al decennia bekend is, is het afdrukken van het originele document op donker gekleurd of gewolkt papier. De kopieermachine kan hierop niet scherpstellen waardoor de kopie onleesbaar wordt. Deze eenvoudige beveiliging is echter deels te ondervangen door kopieermachines met kleurenfilters.

Een nieuwe techniek is 'Restricted content detection' waarbij de te kopiëren tekst door de kopieerapparatuur kan worden herkend op 'verboden woorden' die door de beheerder van de kopieerapparatuur zijn ingevoerd. Bijvoorbeeld de rubriceringniveaus 'Departementaal Vertrouwelijk' of 'Staatsgeheim Confidentieel'. Wil een gebruiker van de apparatuur een document printen, scannen of faxen en wordt een van de verboden woorden door het apparaat herkend, dan wordt de opdracht geweigerd. Beheerders en informatie beveiligingsfunctionarissen kunnen ook vanuit het systeem worden gewaarschuwd dat een mogelijke poging van ongeautoriseerd kopiëren heeft plaatsgevonden (Uniflow, Enhanced security, 2010).

5.2.5 Verpakken, opbergen en vernietigen

Maatregelen kunnen ook gericht zijn op de wijze van verpakken voor vervoer, opbergen en vernietigen van documenten. Een blunder zoals het openlijk meenemen van gevoelige documenten door de Britse

antiterreurchef, waardoor deze te fotograferen waren (casus 1), kan eenvoudig worden voorkomen door deze deugdelijk te verpakken, bijvoorbeeld in een map, een veiligheidsenvelop of (veiligheids)koffer.

Hetzelfde geldt voor de wijze van opbergen en vernietigen van documenten. In het Vir-bi zijn duidelijke normeringen hieromtrent aangegeven (Vir-bi, 2004:39-42, 49-54). Een voorbeeld hiervan is de snippergrootte per rubriceringsniveau die de papiervernietiger moet maken (Vir-bi, 2004:41). Door documenten eerst te versnipperen zijn lekincidenten, waarbij geheime documenten door dumpsterdiving gevonden worden (zoals in casus 7), eenvoudig te voorkomen.

De vernietiging dient dan wel op de juiste wijze te gebeuren. Een papiervernietiger die bijvoorbeeld stroken maakt is vanuit het oogpunt van informatiebeveiliging bezien waardeloos, deze is alleen geschikt voor het onbruikbaar maken van papier.

5.3 Digitale maatregelen tegen lekken

De digitale maatregelen tegen lekken kunnen zich richten op de opslagbeveiliging en de communicatiebeveiliging.

Informatie die is opgeslagen op een desktop of laptop kan beveiligd worden door volledige versleuteling van de harddisk. Dit is ook mogelijk voor informatie die is opgeslagen op centrale servers binnen een netwerk waarbij de informatie door verschillende personen kan worden benaderd. Hetzelfde geldt voor usb-sticks en externe harddisks. Hierbij is het de informatiedrager die beschermd is doordat geen toegang mogelijk is tot de gegevens. Het is ook mogelijk om de informatie te beschermen door de bestanden zelf te versleutelen. Naast het versleutelen van de informatie en het beperken van de toegang hiertoe is het ook mogelijk om achteraf inzichtelijk te maken wie wanneer toegang tot bepaalde gerubriceerde informatie heeft gehad:

> Je moet mensen laten zien dat ze gepakt kunnen worden als ze lekken. […] Op technisch vlak kun je denken aan logging, zodat je kan zien wie welke documenten heeft ingezien, je maakt dan een audittrail. Denk ook aan detectiemechanismen zodat er een alarm afgaat als gerubriceerde informatie verzonden wordt of een externe harde schijf aan een usb-poort wordt gekoppeld en de informatie wordt overgepompt. Zit iemand in een directory te zoeken waar hij niets te zoeken heeft? Dit is ook van belang voor Het Nieuwe Werken. (Interview R. Prins, 31-12-2010)

In de volgende subparagrafen komen vormen van opslagbeveiliging aan de orde: Acces Control, Digital Rights Management en Audit-Based Access Control.

In het kader van dit onderzoek wordt bewust afluisteren van communicatie (spionage) buiten beschouwing gelaten. Het is echter ook mogelijk dat door verwijtbaar handelen informatie bij de verkeerde partij belandt. Dat kan bijvoorbeeld door een typfout in de adressering van een e-mailbericht of een faxbericht. Maatregelen die gericht zijn op het voorkomen van spionage kunnen daarom ook van nut zijn voor het voorkomen van het uitlekken van informatie. Bijvoorbeeld gesloten netwerken en beveiligde (crypto)telefonie, zowel via vaste verbindingen als via mobiele verbindingen.

5.3.1 Access Control

Van een traditioneel Access Control (hierna: AC) systeem is sprake wanneer gegevens worden opgeslagen in een beschermde database en alleen vooraf bepaalde gebruikers inzage kunnen krijgen in de gegevens. De gebruiker dient zich hiervoor te authenticeren door middel van bijvoorbeeld een wachtwoord. Op basis van een lijst waarin de toegangsrechten per gebruiker staan beschreven kan het AC systeem bepaalde opgevraagde gegevens wel of niet vrijgeven. AC heeft als nadeel dat er geen controle is nadat de gegevens zijn vrijgegeven. De geautoriseerde gebruiker zou bijvoorbeeld de gegevens per e-mail kunnen versturen naar een andere ongeautoriseerde gebruiker waardoor uiteindelijk de gegevens alsnog in verkeerde handen valt (Dekker, Veugen & Etalle, 2006:19). Een voorbeeld van dit laatste is gegeven in casus 3, ‘Het doorgezonden e-mailbericht met onversleutelde bijlage’. Een ander voorbeeld is casus 6 ‘Cablegate via WikiLeaks waarbij de gegevens vanuit een database gebrand zijn op zogenaamde muziek cd’s.

5.3.2 Digital Rights Management

Het nadeel van AC wordt ondervangen bij het gebruik van Digital Rights Management (hierna: DRM). Bij DRM worden de gegevens alleen in vercijferde vorm aangeboden. Hierdoor kan men alleen met speciale hardware of software de gegevens gebruiken. Wat de gebruiker met de gegevens mag doen wordt bepaald door persoonsgebonden licenses. DRM heeft als nadeel dat gebruikers alleen speciale software en hardware, vaak van een enkele fabrikant, kunnen gebruiken om de gegevens te lezen of te bewerken. Wanneer binnen of tussen organisaties verschillende hardware en software gebruikt worden kan dit tot problemen leiden (Dekker, Veugen & Etalle, 2006:19).

5.3.3 Audit-Based Access Control

Audit-Based Access Control (hierna: ABAC) is een alternatief voor de bovenstaande systemen. Met deze methode kan men het spanningsveld tussen vertrouwelijkheid en beschikbaarheid oplossen. In ABAC wordt alleen achteraf bekeken of de gebruiker zich kan verantwoorden voor toegang tot gegevens. Men noemt dit a-posteriori access control. Hierbij kan een auditor achteraf een gebruiker om verantwoording vragen. Hiertoe wordt bijvoorbeeld via logging geregistreerd welke gebruiker welke gegevens heeft opgevraagd. Naast deze audit trail wordt aan de gebruiker gevraagd om zelf de toegekende rechten te verzamelen en te bewaren als bewijsmateriaal tijdens latere audits. In een dergelijke audit log kan de gebruiker voor latere verantwoording ook details opslaan over de omstandigheden waaronder gegevens werd opgevraagd (Dekker, Veugen & Etalle, 2006:19-20).
De ontwikkelaars van ABAC onderkennen dat het niet geschikt is voor alle situaties. Misbruik is namelijk in eerste instantie niet uitgesloten. De kans op controle en een eventuele sanctie achteraf moet misbruik voldoende afschrikken. Dit maakt ABAC bijvoorbeeld ongeschikt voor systemen met grote aantallen gebruikers in verschillende landen, wanneer gebruikers moeilijk zijn te achterhalen (zoals bij Cablegate, casus 6). De waarde van sommige gerubriceerde of gevoelige informatie is soms zo groot dat oneerlijke gebruikers de gevolgen van sancties voor lief nemen (Dekker, Veugen & Etalle, 2006:20).

Een combinatie van de drie hiervoor beschreven systemen is overigens ook mogelijk. De eigenschappen worden weergegeven in figuur 5.1.

	AC	DRM	ABAC
Bijhouden van toegekende rechten	Centraal	Decentraal	Decentraal
Encryptie van gegevens vereist	Nee	Ja	Nee
Authenticatie	a-priori	a-priori	a-priori
Autorisatie	a-priori	a-priori	a-posteriori
Controle na verleende toegang	Nee	Ja	Ja
Verplichtingen achteraf	Nee	Nee	Ja

Figuur 5.1: Verschillende systemen voor toegangscontrole (naar: Dekker, Veugen & Etalle, 2006:20)

5.3.4 Vernietigen van digitale gegevensdragers

Wat voor het vernietigen van documenten geldt, zoals beschreven in paragraaf 5.2.5, geldt ook voor wissen en vernietigen van digitale gegevensdragers (Casus 11).

Casus 11: Jongen vindt gevangenis-pc op straat

"Een 16-jarige jongen uit Arnhem heeft een oude computer met vertrouwelijke gegevens over gedetineerden in de Arnhemse gevangenis De Berg aangetroffen op straat. De jongen onderzocht de computer samen met docenten en zag toen de documenten. De computer is teruggegeven aan de gevangenis. De jongen plukte de computer vorige week van straat in Arnhem-Zuid en trof er gespreksverslagen met en rapportages over gedetineerden op aan. Een woordvoerder van justitie noemt het een 'buitengewoon ernstige' kwestie. 'We zijn de jongen zeer erkentelijk dat de computer is teruggebracht.'

Justitie heeft het incident onderzocht en concludeert dat de computer rond 2003 door de gevangenis is weggegeven en dat de laatste eigenaar het ding aan de weg heeft gezet. 'Overbodige computers werden tot 2004 helemaal opgeschoond en bijvoorbeeld aan scholen gegeven. Bij het opschonen van deze pc is vermoedelijk iets misgegaan. Tegenwoordig worden computers niet meer weggegeven maar binnenshuis vernietigd, juist om dit soort zaken te voorkomen', aldus de justitiewoordvoerder."

(Telegraaf, 15 april 2010)

In deze casus is de harde schijf niet of onjuist gewist. De computer is vervolgens aan een goed doel gegeven, maar toen deze gebruiker de computer afdankte bleek dat de harde schijf nog gerubriceerde of gevoelige informatie bevatte. Daarom is het correct wissen van digitale gegevensdragers van belang. Dat kan zowel door middel van software als met behulp van hardware, elektronisch (magnetisch) door het gebruik van een degausser of mechanisch door de gegevensdrager te versnipperen (Vir-bi, 2004:42). Het lekincident uit casus 11 was eenvoudig te voorkomen door de computer van een nieuwe harde schijf te voorzien voordat deze aan het goede doel werd gegeven.

5.4 Organisatorische maatregelen tegen lekken

5.4.1 Bewustwording

Bij bewustwording gaat het vaak om een campagne naar aanleiding van een incident. Alle medewerkers moeten dan naar een workshop, men krijgt een folder en een 'gimmick' en wordt dan geacht 'bewust' te zijn. Het is echter veel belangrijker dat er een goede structuur aanwezig is waar medewerkers weten waar men terecht kan voor informatie, de juiste middelen en het melden van incidenten. Belangrijk is ook een cultuur waar leidinggevenden het goede voorbeeld geven, men elkaar kan aanspreken en het mogelijk is om incidenten of inbreuken te melden (een 'meldcultuur' zoals beschreven door Reason, zie ook paragraaf 2.4.1).

Bewustwording betekent ook dat medewerkers zich realiseren wat hun eigen rol is binnen de organisatie en de mogelijke gevolgen van het individuele handelen: "Eén van de aandachtspunten is medewerkers te wijzen op de ongewenstheid van het lekken van vertrouwelijke informatie en de negatieve gevolgen daarvan voor de gehele organisatie en de directe collega's" (Lemstra et al., 2005:34). Daarnaast spelen zaken als politiek-bestuurlijke sensitiviteit en de omgang met media (de pers), Het Nieuwe Werken en social media een rol (Maat, 2011:34).

Dit begint al bij de indiensttreding door het afleggen van de ambtseed of -belofte. Dit is verplicht ingevolge artikel 51 van het Algemeen Rijksambtenarenreglement (hierna: ARAR). In de eed en belofte is ook een passage opgenomen die betrekking heeft op de geheimhouding (zie paragraaf 3.3.1). Het doel van het doen afleggen van de ambtseed of -belofte bij indiensttreding door ambtenaren is het nog eens duidelijk wijzen op en bewust maken van hun speciale positie en de gevolgen daarvan voor hun integriteit. Het is hierbij verstandig de ambtseed of -belofte opnieuw af te laten leggen bij indiensttreding bij een ander bestuursorgaan en hier jaarlijks aandacht aan te besteden in het functioneringsgesprek. Daarnaast dient men een geheimhoudingsverklaring te tekenen (Vir-bi, 2004:31).

5.4.2 Procedures

De maatregelen zoals genoemd in de paragrafen 5.2 en 5.3 hebben alleen zin als ze ook gebruikt worden. Daarvoor zijn procedures noodzakelijk, bijvoorbeeld voor het rubriceren zelf, het registreren van gerubriceerde informatie, het melden van incidenten. Deze procedures dienen echter niet zo complex te zijn dat het verschijnsel van 'practical drift', zoals beschreven in paragraaf 2.6 optreedt: "the slow, steady uncoupling of local practice from written procedure" (Snook, 2000:220).

Procedures kunnen ook bijdragen aan de bewustwording, waarbij een bepaald gewenst gedrag, zoals 'clean desk' (gerubriceerde informatie is onder toezicht of deugdelijk opgeborgen), onderdeel is van de organisatiecultuur:

> Toen ik in de jaren zeventig als jonge ambtenaar bij Algemene Zaken werkte behoedde de schaamtecultuur je voor fouten. Je schaamde je enorm als je betrapt werd bij het overtreden van het clean desk beleid. Dat je je spullen moest ophalen bij de SG. Algemene Zaken is een kleine organisatie en je bent trots dat je voor de premier mag werken. Je wilt dan het gevoel hebben dat je het waard bent. Dat culturele kenmerk van de organisatie moet je pakken, het aanzien van de organisatie. Je moet je bij dit soort acties goed bedenken wat werkt, wat spreekt aan binnen de organisatie. (Interview J.W. Holtslag, 11-01-2011)

Een ander voorbeeld van een procedure is het werven en selecteren van medewerkers. Al tijdens het sollicitatiegesprek kan met de kandidaat gesproken worden over de omgang met gerubriceerde en gevoelige informatie. Ook kunnen referenten benaderd worden om te vragen hoe de kandidaat in het

verleden hiermee omging. Dit is een vorm van pre-employment screening. Wanneer medewerkers omgaan met staatsgeheimen, dienen ze een Verklaring van Geen Bezwaar voor het vervullen van een vertrouwensfunctie te hebben (Vir-bi, 2004:31). Deze wordt afgegeven nadat een veiligheidsonderzoek op basis van de Wet veiligheidsonderzoeken (hierna: WVO) positief is afgerond (artikel 4, derde lid, WVO). Het aanwijzen van een vertrouwensfunctie is vanwege de inbreuk op de persoonlijke levenssfeer van de betreffende functionarissen echter wel het sluitstuk van de beveiliging. De organisatie dient al de nodige andere maatregelen te hebben toegepast om de exclusiviteit van staatsgeheimen te beschermen (Leidraad Aanwijzing Vertrouwensfuncties, 2006:9). Voorbeelden hiervan zijn functiescheiding (ook een procedurevorm), fysieke compartimentering en ICT-maatregelen. Gezien de kwetsbaarheid van vertrouwensfuncties is het ook van belang dat er bij reorganisaties en gedwongen ontslagen extra aandacht is voor medewerkers met een vertrouwensfunctie.

5.4.3 Sanctioneren

Naast het faciliteren en bewustmaken van medewerkers zodat deze op een juiste wijze met gerubriceerde en gevoelige informatie om kunnen gaan, dient er ook ruimte te zijn om in voorkomende gevallen over te gaan tot het sanctioneren van ongewenst gedrag. "Indien een organisatie duidelijke regels stelt en het belang onderstreept dat medewerkers zich aan deze regels houden, past het dat medewerkers worden aangesproken op vergissingen, slordigheden en het onopzettelijk niet naleven van die regels" (Lemstra et al., 2005:32-33). Hierbij valt te denken aan functionerings- en beoordelingsgesprekken waarbij gewezen kan worden op de kwalijke gevolgen van lekken voor de medewerker als individu en de organisatie of samenleving als geheel. Indien nodig kan het bevoegd gezag overgaan tot disciplinaire maatregelen of ontslag wegens ongeschiktheid voor de functie. Dit is geregeld in de artikelen 50, 80, 81, 82, 83 en 84 ARAR.

Het bewuste gedrag van mensen wordt beïnvloed door intrinsieke motivatie (van binnenuit) en door extrinsieke motivatie (belonen en straffen). Nu wordt wel gesteld dat de invloed van straffen op het gedrag overschat wordt (Overbeek, Roos Lindgreen & Spruit, 2005:69). Daarom is ook aan de respondenten gevraagd of straffen een preventieve werking heeft.

- "Dat is betrekkelijk. De kans op ontdekking is gering, dan neem je het risico makkelijker. Men denkt dan niet aan de mogelijke straf." (Interview A. Nieuwpoort, 27-01-2011)
- "Je moet straffen. Straffen heeft een generale preventie, je stelt een voorbeeld." (Interview C.R. Niessen, 26-01-2011)
- "Strenger straffen is een manier, net als uniformiteit, consequentheid en publiekelijk melden van incidenten. Ik denk dat bewustwording het belangrijkste is." (Interview H.G. Geveke, 17-06-2010)
- "Ik heb nooit gestraft bij lekken. Stel dat een secretaresse een fout maakt met een Staatsgeheim, moet ik haar dan ontslaan? Je moet eerder denken aan confronteren en handhaven. We hebben wel eens een clean desk campagne gedaan, vertrouwelijke documenten werden dan in beslag genomen en dit werd dan gerapporteerd. Als SG moet je zo'n campagne natuurlijk wel dekken. Ik ben een voorstander van voorbeeldstellend handhavend optreden." (Interview J.W. Holtslag, 11-01-2011)

5.4.4 Klokkenluidersregeling

Zowel in de literatuur (Bovens, Geveke & De Vries, 1993:66, Lemstra et al., 2005:81) als tijdens de interviews (subparagraaf 4.5.6) kwam geregeld de noodzaak van een goed functionerende klokkenluidersregeling aan bod als een voorwaarde om lekken – vanuit het algemeen belang – tegen te gaan. Professor Niessen, die de Ien Dales Leerstoel bekleedde, gaf hierover aan:

> Ik constateer verder dat anoniem lekken effectiever is dan het gebruik maken van de klokkenluidersregeling. Dan kan je óf iedereen adviseren door te gaan met anoniem lekken óf je kan de klokkenluidersregeling nog eens doorlichten. Zorgen dat ook daar anonimiteit gegarandeerd is, want dat is nu niet zo. Er wordt nu heel weinig gebruik gemaakt van de klokkenluidersregeling Rijksdienst, vier of vijf keer sinds hij bestaat. En wie weet er nou dat er een Criminele Inlichtingeneenheid binnen de Rijksrecherche is waar je net zoveel anoniem kunt lekken als je wilt? (Maat & De Graaf, 2005:15)

Ook de Commissie Lemstra komt tot een vergelijkbare conclusie: "Weliswaar is anoniem klagen niet de chicste vorm om onvrede te uiten, maar zolang anoniem lekken naar de media minder belastend is dan het volgen van voorgeschreven klachtenprocedures, zal de overheid niet verbaasd moeten zijn dat er gelekt wordt" (Lemstra et al., 2005:71). Ook voor zaken die geen misstanden zijn, maar die wel

tot onvrede binnen de organisatie leiden dient men oog te hebben om lekken te voorkomen: “De belangrijkste les is dat je moet kijken naar de medewerker tevredenheid.” (Interview J.J.J.M. van den Hout, 19-01-2011).

5.5 Restrisico’s

Op basis van het voorgaande kan gesteld worden dat het risico van intentionele en verwijtbare compromittering van gerubriceerde en gevoelige informatie gereduceerd kan worden. Echter, lekken helemaal uitsluiten is niet mogelijk: “Iemand die toegang heeft tot gerubriceerde of gevoelige informatie en de intentie heeft deze naar buiten te brengen zal hier in slagen, welke beveiligingsmaatregelen de organisatie ook treft” (Lemstra et al., 2005:12). Ook parlementair verslaggever Wester benadrukte dit: “Welke maatregelen je ook neemt, tegen lekken is geen kruid gewassen. Er bestaat een natuurlijke behoefte om informatie te delen. Dat betekent natuurlijk niet dat je helemaal geen maatregelen kunt nemen, zoals het afschermen van systemen” (Interview F. Wester, 03-02-2011).

Dit is belangrijk om in gedachten te houden bij het treffen van de beveiligingsmaatregelen. Deze kosten namelijk geld. Toch mogen de directe kosten voor beveiliging niet leidend zijn, niet voor niets kan gesteld worden: ‘If you think security is expensive, try an incident’, zoals de Commissie Lemstra ook al opmerkte:

> Met name de immateriële kosten in verband met het lekken van vertrouwelijke dan wel geheime informatie zijn al spoedig hoger dan die van de investeringen in beveiligingstechnologie. Eveneens moet hierbij de geloofwaardigheid van de organisatie in aanmerking worden genomen. Indien investeringen in beveiligingstechnologie te duur worden gevonden, moet men niet verbaasd staan dat de […] organisatie door bondgenoten niet serieus wordt genomen. Dit kan ertoe leiden dat Nederland, zonder dat dit gezegd wordt, geen deelgenoot wordt gemaakt van belangrijke informatie. (Lemstra et al. 2005:36)

Aan de andere kant leveren beveiligingsmaatregelen ook beperkingen in de bedrijfsvoering op. Dit kan vervolgens weer leiden tot practical drift. Proportionaliteit hierbij is dan ook van belang:

> Als iemand bewust informatie naar buiten wil brengen, dan kan dat altijd. Je moet veel doen aan bewustwording, maar je kunt er niets aan doen als iemand slordig is. Je kunt de kans reduceren, maar terugbrengen naar nul is onmogelijk bij dit soort informatie. Je maatregelen moeten ook proportioneel zijn. Laten we wel wezen, er vallen geen doden als de Rijksbegroting een week eerder bekend raakt. (Interview A. Nieuwpoort, 27-01-2011)

Verder kan het ontbreken van een integrale benadering van informatiebeveiliging, ondanks alle investeringen, leiden tot blijvende gevallen van lekken:

> In het algemeen wordt er te weinig geïnvesteerd in informatiebeveiliging. Ad hoc beleid is typisch voor de overheid, er is vaak geen groter plan. De ene afdeling houdt zich bezig met awareness, de andere afdeling met technische zaken als firewalls. Verantwoordelijkheden en budgetten zijn verspreid, er wordt soms heel veel geïnvesteerd in bijvoorbeeld die firewalls maar dan weer nauwelijks iets in bewustwording. De beveiliging is vaak slecht georganiseerd. Of het wordt als een technisch iets geplaatst onder ICT, of het wordt een verantwoordelijkheid van iemand die ook over de fysieke beveiliging gaat maar niets te zeggen heeft over de ICT. (Interview R. Prins, 31-12-2010)

Dat het maken van informatiebeveiligingsbeleid eenvoudiger is dan het ook te implementeren heeft ook de Amerikaanse president Barack Obama ondervonden. Op 29 december 2009 vaardigde hij een zogenoemde ‘Executive Order’ aangaande ‘Classified National Security Information’ uit:

> This order prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism. Our democratic principles require that the American people be informed of the activities of their Government. Also, our Nation’s progress depends on the free flow of information both within the Government and to the American people. Nevertheless, throughout

> our history, the national defense has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, our homeland security, and our interactions with foreign nations. Protecting information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification standards and routine, secure, and effective declassification are equally important priorities. (Executive Order, 2009:707)

Deze 'Executive Order' is wat inhoud betreft te vergelijken met het Nederlandse Vir-bi. De toezichthouder hierop, de Information Security Oversight Office, kwam op 15 april 2011 in het jaarverslag met de nodige kritiek op de implementatie van het informatiebeveiligingsbeleid. Zo hadden – ondanks de deadline van de President – slechts 19 van de 41 organisaties het voorschrift geïmplementeerd (Report to the President 2010, 2011:2).

5.6 Integraal overzicht dreigingen, kwetsbaarheden, maatregelen en restrisico's geheimen

Op basis van het voorgaande is in de volgende figuur (5.3) het integrale overzicht van dreigingen, kwetsbaarheden, maatregelen en restrisico's gecompleteerd.

	Dreigingen, achtergrond van handelen	Kwetsbaarheden, het is mogelijk om	Maatregelen, kunnen bestaan uit	Restrisico's
INTENTIONEEL HANDELEN	Persoonlijk, gericht op: • beloning in de vorm van geld, goederen of diensten • versterken van de eigen positie of het verzwakken van de positie van een tegenstander • het vergroten van de eigen status, bijv. om te laten zien dat men een insider is (opscheppen) • wrok of frustratie jegens een persoon of organisatie	• inzage te geven tijdens een gesprek, direct of indirect ('even weglopen') • fysieke overdracht van papieren documenten of digitale gegevensdragers te realiseren, al dan niet tijdelijk ('uitlenen') • digitale overdracht van bestanden te realiseren, al dan niet via een omweg om sporen te vermijden • mondelinge overdracht in persoon of telefonisch (eventueel anoniem) te realiseren, waarbij de informatie exact wordt gegeven of juist 'off the record' of omschreven in de vorm van 'achtergrond-gesprekken'	• beter personeelsbeleid, waaronder selectie (veiligheidsonderzoek i.k.v. vertrouwensfunctie) • geheimhoudingsverklaring • aandacht voor (emoties) medewerkers bij reorganisaties • gerichte en a-selecte controle van opslag en transport van gerubriceerde informatie • merkingen in tekst • kopieerbeveiligd papier (herleidbaarheid) • kopieerbeveiliging (restricted content detection)	• kwade opzet
	Institutioneel, al dan niet geautoriseerd, gericht op het strategisch belang zoals het voortbestaan van het eigen onderdeel, te onderscheiden in: • mobiliseren • antagonistisch (hinderen) • conditioneren (quid pro quo)		• aandacht voor politiek-bestuurlijke sensitiviteit	
	Publiek belang, gericht op het melden van misstanden (de dreiging is in dit kader relatief)		• klokkenluidersregeling (veilig intern melden van misstanden mogelijk maken)	• gebrek aan vertrouwen in regeling, bijv. door slechte ervaringen in het verleden
VERWIJTBAAR HANDELEN	• Slordigheid • Onbekendheid met regels • Onderschatting risico of belang • Gebrek aan bewustzijn • Gebrek aan motivatie • Gebrek aan kennis en vaardigheden om op juiste wijze met gerubriceerde of gevoelige informatie om te gaan	• binnen organisatie vat te krijgen op dreigingen uit linkerkolom	• bewustwording • sanctioneren	• gebrek aan betrokkenheid top- en lijnmanagement
		• ongeautoriseerde toegang tot gerubriceerde informatie te verkrijgen	• access control • digital rights management • audit-based access control	
		• een te grote kring van geïnformeerden te laten ontstaan	• het toepassen van het 'need-to-know' beginsel	• 'nice-to-know'
		• zich te vergissen in de aard van de gevoelige informatie	• duidelijk rubricering aanbrengen, inclusief termijn	
		• zich te verspreken tegenover niet gerechtigde (bijv. door social engineering, gebruik bewustzijnsverminderende middelen als alcohol en drugs)	• sociale controle (aanspreken) • penetratietesten gericht op social engineering	• sociale druk, gebrek aan ondersteuning door collega's en leidinggevende
		• mee te lezen of te luisteren op openbare plaats (terras, OV, congres, vliegtuig, horeca)	• bewustwording	• ambtenaar wordt geacht zich tijdens reis voor te bereiden in het OV
		• digitale gegevensdragers te verliezen	• beveiligde gegevensdragers verstrekken en verplicht stellen	
		• papieren documenten te verliezen	• transportmiddelen beschikbaar en verplicht stellen	
		• op onjuiste wijze op te bergen (niet afgesloten, gedeelde wachtwoorden, onjuist sleutelbeheer)	• bergmiddelen beschikbaar en verplicht stellen	
		• op onjuiste wijze digitale bestanden te verzenden (verkeerd e-mailadres, onversleuteld)	• versleutelprogramma's beschikbaar en verplicht stellen	• sleutel is eenvoudig te achterhalen of meegezonden
		• e-mailberichten automatisch door te zenden (auto-forwarden)	• auto-forwarden uitschakelen	
		• op onjuiste wijze papieren documenten te verzenden	• veiligheidsenveloppen beschikbaar en verplicht stellen	
		• de informatie onjuist te verwerken door een rubriceringsgebrek	• opleiding • rubricering vaststellen door steller en leidinggevende (vier ogen principe)	
		• de informatie op onjuiste wijze te vernietigen (wegwaaien, 'dumpsterdiving', onvolledig wissen)	• apparatuur voor correcte vernietiging beschikbaar en verplicht stellen	

Figuur 5.3: Integraal overzicht dreigingen, kwetsbaarheden, maatregelen en restrisico's geheimen

6. CONCLUSIES EN AANBEVELINGEN

6.1 Inleiding

In deze thesis stond de volgende onderzoeksvraag centraal:
'Welke factoren spelen een rol bij het intentioneel en verwijtbaar compromitteren van gerubriceerde en gevoelige informatie?'

Met behulp van een viertal deelvragen is getracht hier een antwoord op te formuleren:

a. *Waarom zijn er geheimen?*
   Geheimen zijn er om belangen te beschermen. Er is dan sprake van gevoelige informatie, waarbij kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van – in het kader van deze thesis – de Staat, van zijn bondgenoten of van één of meer ministeries. Het belang van geheimen kan vanuit een ethische, een juridische en een politiek-bestuurlijke dimensie beschouwd worden.
b. *Waarom worden geheimen gelekt?*
   Geheimen kunnen worden gelekt om persoonlijke, institutionele of publieke belangen te dienen. Er is dan sprake van intentioneel handelen (opzet). Daarnaast kunnen geheimen gelekt worden vanwege bijvoorbeeld onachtzaamheid, onkunde of onprofessioneel handelen. Er is dan sprake van verwijtbaar handelen (schuld), de actor heeft namelijk de (reële) mogelijkheid zich anders te gedragen. Hiervan is bijvoorbeeld sprake wanneer de actor geen gebruik maakt van de middelen die ter beschikking staan om geheimen te beschermen (zie figuur 5.3, kolom 1). Geheimen kunnen ook uitlekken door niet verwijtbaar handelen (zoals overmacht), maar dat valt buiten het kader van deze thesis.
c. *Hoe worden geheimen gelekt?*
   Intentioneel lekken geschiedt door bewuste mondelinge, fysieke en digitale overdracht van informatie. Verwijtbaar lekken geschiedt niet bewust, maar bijvoorbeeld door het verlenen van ongeautoriseerde toegang, zich te verspreken, mee te laten lezen of luisteren, het verliezen van documenten en digitale gegevensdragers en een onjuiste wijze van verwerken, opbergen, verzenden of vernietigen van gevoelige informatie (zie figuur 5.3, kolom 2).
d. *Welke maatregelen zijn mogelijk tegen het lekken van geheimen?*
   De mogelijke maatregelen zijn technisch en organisatorisch van aard. Technische maatregelen bestaan uit hard-copy en digitale maatregelen. Organisatorische maatregelen bestaan onder andere uit bewustwording, procedures, sanctioneren en een goed werkende klokkenluidersregeling. Door het toepassen van een gelaagdheid aan onafhankelijk van elkaar werkende maatregelen kan het risico op 'lekken' teruggedrongen worden. Er blijven echter restrisico's bestaan, de mens is gebleken de zwakste schakel te zijn (zie figuur 5.3, kolommen 3 en 4).

Als antwoord op de centrale onderzoeksvraag kan derhalve gesteld worden dat de factoren die een rol spelen bij het intentioneel en verwijtbaar compromitteren van gerubriceerde en gevoelige informatie bestaan uit zowel de belangen om de informatie te beschermen, als uit de belangen om de informatie buiten de kring van gerechtigden te brengen. Daarnaast spelen de factoren van zowel de juiste wijze van rubriceren, derubriceren en openbaren van informatie, als de juiste wijze van beschermen van de informatie door het treffen van technische en organisatorische maatregelen een rol.

6.2 Conclusies

Op basis van het onderzoek naar intentionele en verwijtbare compromittering van gerubriceerde en gevoelige informatie binnen de Rijksoverheid zijn de volgende conclusies te trekken:

1. Als (al dan niet) gevoelige informatie correct gerubriceerd is (het staat er letterlijk op) kan men spreken van een 'formeel geheim'. Als gevoelige informatie niet correct gerubriceerd is (het staat er letterlijk niet op) maar de houder van de informatie begreep of had behoren te begrijpen dat de informatie gevoelig is en openbaarmaking een afbreukrisico vormt, dan kan men spreken van een 'materieel geheim' (paragraaf 2.7).

2. Idealiter is de verzameling gerubriceerde informatie gelijk aan de verzameling gevoelige informatie. Deze passen dan naadloos over elkaar heen. In de praktijk is dit niet volledig het geval, er is zowel informatie die ten onrechte gerubriceerd is, als informatie die ten onrechte niet gerubriceerd is (Eclips Model, figuur 2.5, paragraaf 2.7). Beide kunnen leiden tot het lekken van geheimen. Het proces van rubriceren is dan ook een kunde (subparagraaf 4.5.3).
3. Een geheim verliest de betekenis en beschermbaarheid als deze binnen een grote kring bekend of toegankelijk is (paragraaf 4.2, subparagrafen 3.3.2, 4.4.2 en 4.4.1).
4. Practical drift – the slow, steady uncoupling of local practice from written procedure – is een van de oorzaken van het niet volgen van maatregelen ter bescherming van gevoelige en gerubriceerde informatie (subparagraaf 2.6.2). Uiteindelijk leidt dat tot een situatie waarbij er sprake is van 'an incident waiting to happen': er wordt gelekt.
5. De mogelijkheid tot lekken is de afgelopen vijftien jaar toegenomen door de ontwikkelingen in de technische infrastructuur zoals e-mail, internet, goedkope digitale gegevensdragers met grote capaciteit, gepaard gaande met onvoldoende en verkeerde technische middelen en onvoldoende aandacht voor bewustwording (paragraaf 4.2 en subparagraaf 4.5.1). De ontwikkeling van ‘Het Nieuwe Werken’ kan met name de mogelijkheid tot verwijtbaar lekken verder doen toenemen als hier vanuit het perspectief van security onvoldoende op wordt ingespeeld (paragraaf 4.6).
6. Een gelaagdheid aan onafhankelijk werkende maatregelen helpt om het risico op lekken beheersbaar te krijgen (paragrafen 2.4, 2.5 en 2.6). Hierbij kan geleerd worden van het Error Management in High Reliability Organisations (subparagraaf 2.4.4).
7. Ingrijpende bezuinigingen, reorganisaties en een (gevoel van) onheuse bejegening kunnen lekken uit frustratie en wrok in de hand werken (subparagraaf 4.5.4).
8. Op basis van het onderzoek kan gesteld worden dat de veelgenoemde uitspraak ‘Het Schip van Staat is het enige schip dat van boven lekt’ de lading niet helemaal dekt (subparagraaf 4.5.5). Op basis van het onderzoek kan gesteld worden dat lekken zowel vanuit het stuurhuis als het vooronder geschiedt. Wellicht is daarom het gezegde ‘Geen schuit zo dicht of er komt wel een lek in’, beter van toepassing.

6.3 Aanbevelingen

Naar aanleiding van de conclusies worden de volgende aanbevelingen gedaan om intentionele en verwijtbare compromittering van gerubriceerde informatie binnen de overheid terug te dringen:

1. Laat het topmanagement bepalen dat medewerkers met een vertrouwensfunctie op grond van de toegang tot gerubriceerde informatie bij aanvang van hun functie en vervolgens periodiek verplicht voorgelicht (bewustwording) worden over het belang van gerubriceerde informatie (aan de hand van casuïstiek, zoals in deze thesis gebruikt, als het kan ook uit de eigen organisatie), het bepalen van het rubriceringsniveau en de omgang met gerubriceerde informatie (regels, procedures en middelen voor een juiste verwerking, opslag en transport).
2. Zorg dat de middelen voor de omgang met gerubriceerde informatie (zoals bergmiddelen, usb-sticks, versleutelprogramma’s, veiligheidsenveloppen, GSM-cryptotelefoons) functioneren en daarbij eenvoudig en ruimschoots beschikbaar zijn.
3. Voorkom practical drift door de maatregelen af te stemmen op de belangen, de dreigingen en de kwetsbaarheden van de gerubriceerde informatie van de organisatie. Zorg voor actieve handhaving en onderdruk de neiging om bij de eerste ernstige inbreuk op de maatregelen zwaardere maatregelen in te voeren dan de maatregelen die toch al niet gevolgd werden.
4. Laat het vaststellen van een rubricering op het niveau Staatsgeheim Confidentieel/Geheim/Zeer Geheim altijd accorderen door een leidinggevende (vier ogen principe). Dit om het onnodig (te hoog) rubriceren van informatie te voorkomen. Voor bepaalde informatie kan dit categoriaal geschieden.
5. Laat gerubriceerde informatie op het niveau Staatsgeheim Confidentieel/Geheim/Zeer Geheim uitsluitend afdrukken op kopieerbeveiligd en genummerd papier (zoals bijlage VII).
6. Voorkom het lekken van gerubriceerde informatie door deze periodiek te herzien en deze – indien mogelijk – vervolgens actief openbaar te maken conform de Wet openbaarheid van bestuur.
7. Zorg voor een goed werkende klokkenluidersregeling voor het intern en extern melden van vermoedens van misstanden.
8. Sanctioneer verwijtbare compromittering via een disciplinair traject. Sanctioneer intentionele compromittering via een strafrechtelijk én disciplinair traject.

BIJLAGEN

Bijlage I Lijst van geïnterviewde personen

Naam	Functie en organisatie	Reden interview	Gesprek d.d.
Dr. J.J.G. van der Bruggen	Onderzoeker Technische Universiteit Delft	Als secretaris van de Commissie van onderzoek besluitvorming Irak (Commissie Davids, 2009) o.a. verantwoordelijk voor de interne organisatie van de Commissie	10-01-2011
Drs. H.G. Geveke	Directeur Nationale Veiligheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Expertise lekonderzoeken en lijnmanager organisatie met veel gerubriceerde informatie	17-06-2010
E.P. Grobbe	Beveiligingsambtenaar Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Verantwoordelijk voor o.a. beleid informatiebeveiliging departement	20-12-2010
Drs. J.W. Holtslag	Lid Wetenschappelijke Raad voor het Regeringsbeleid, voormalig Secretaris-Generaal Ministerie van Binnenlandse Zaken en Koninkrijksrelaties	Als SG destijds eindverantwoordelijk voor o.a. beleid informatiebeveiliging departement	11-01-2011
J.M.M.M. van den Hout	Sub-Beveiligingsambtenaar Algemene Inlichtingen- en Veiligheidsdienst	Verantwoordelijk voor o.a. beleid informatiebeveiliging AIVD	19-01-2011
H. Hummel	Plaatsvervangend directeur Rijksrecherche	Expertise lekonderzoeken	28-12-2010
Prof. mr. C.R. Niessen	Emeritus hoogleraar 'Overheid als arbeidsorganisatie', Ien Dalesleerstoel, Universiteit van Amsterdam	Als lid Commissie Lemstra belast met onderzoek naar oorzaken van het lekken van vertrouwelijke informatie bij het Ministerie van Defensie (2005)	26-01-2011
Dr. A. Nieuwpoort	Beveiligingsambtenaar, Ministerie van Financiën	Verantwoordelijk voor o.a. beleid informatiebeveiliging departement	27-01-2011
R. Prins, MSc	CEO Fox-IT IT Security	Gespecialiseerd in informatiebeveiliging	31-12-2010
F. Wester	Parlementair verslaggever RTL Nieuws	Wist bij herhaling de hand te leggen op Prinsjesdagstukken	03-02-2011

Alle geïnterviewde personen hebben ingestemd met opname in bovenstaande lijst en het opnemen van citaten in deze thesis. Afgesproken is dat de integrale gespreksverslagen alleen in te zien zijn door de examencommissie.

Bijlage II Vragenlijst met totaalantwoorden 'Lekken bij de Rijksoverheid'

	Vragen:	Antwoordmogelijkheden:	Geantwoord door 13 departementen:
1.	Is binnen uw departement[1] sprake geweest van lekken[2] in de periode 2004-2009?	a. Ja b. Nee	a. 7 x ja b. 6 x nee
2.	Is het aantal voorvallen van lekken[2] bijgehouden?	a. Ja b. Nee	a. 6 x ja b. 1 x nee
3.	Om hoeveel bekende gevallen van lekken[2] gaat het in de periode 2004-2009?	… gevallen, exact/bij benadering	39 x
4.	Is er onderzoek gedaan naar deze lekken[2]?	a. Ja b. Nee	a. 7 x ja b. 0 x nee
5.	Zijn deze lekken[2] onderzocht door (meerdere antwoorden mogelijk):	a. Interne partij? b. Externe commerciële partij? c. Rijksrecherche? d. Andere partij…?	a. 7 x intern b. 1 x comm. c. 4 x RR d. 1 x ander
6.	Zijn er uitspraken te doen over de oorzaak van lekken[2] op basis van deze onderzoeken?	a. Ja b. Nee	a. 7 x ja b. 0 x nee
7.	Was er sprake van (meerdere antwoorden mogelijk):	a. Bewust handelen? b. Onbewust handelen? c. Technisch falen? d. Anders …	a. 4 x bewust b. 7 x onbewust c. 1 x techn. falen d. 2 x anders
8.	Zijn naar uw oordeel binnen uw departement[1] voldoende maatregelen beschikbaar op het terrein van regelgeving (Vir-bi, departementale regelingen) om lekken[2] tegen te gaan?	a. Ja b. Nee	a. 13 x ja b. 1 x nee
9.	Zijn naar uw oordeel binnen uw departement[1] voldoende maatregelen beschikbaar op het terrein van technische voorzieningen (cryptomiddelen, kluizen, bijzonder papier, enveloppen) om lekken[2] tegen te gaan?	a. Ja b. Nee	a. 10 x ja b. 3 x nee
10.	Zijn naar uw oordeel binnen uw departement[1] voldoende maatregelen beschikbaar op organisatorisch terrein (procedures en gespecialiseerde functionarissen) om lekken[2] tegen te gaan?	a. Ja b. Nee	a. 10 x ja b. 3 x nee
11.	Is naar uw oordeel binnen uw departement[1] een voldoende niveau van informatie-beveiligingsbewustzijn (men kent de regels en handelt ernaar) om lekken[2] tegen te gaan?	a. Ja b. Nee	a. 8 x ja b. 5 x nee
12.	Bent u beschikbaar voor een interview in het kader van het onderzoek 'Lekken bij de Rijksoverheid'?	a. Ja b. Nee	a. 9 x ja b. 4 x nee
13.	Ruimte voor opmerkingen		

De vragenlijst is op 26 mei 2010 verspreid onder de Beveiligingsambtenaren van de dertien departementen. De verwerking van de antwoorden is afgesloten op 16 juni 2010.

[1] Onder het departement wordt verstaan: het departement zelf en de daaronder ressorterende organisaties inclusief diensten, bedrijven, instellingen en agentschappen (bijv. AIVD en KLPD bij BZK; RIVM bij VWS).

[2] Onder 'lekken bij de Rijksoverheid' wordt verstaan: het compromitteren (kennisname door niet gerechtigden) van bijzondere informatie (departementaal vertrouwelijk en staatsgeheim confidentieel/geheim/zeer geheim, alsmede bijzondere informatie van internationale herkomst als genoemd in art. 4 Vir-bi)

Bijlage III Lijst van gehanteerde afkortingen

ABAC	Audit-Based Access Control
AC	Acces Control
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
ARAR	Algemeen Rijksambtenarenreglement
AW	Ambtenarenwet
BVA	Beveiligingsambtenaar
BZK	Binnenlandse Zaken en Koninkrijksrelaties, (ministerie van)
DRM	Digital Rights Management
EHRM	Europees Hof voor de Rechten van de Mens
EVRM	Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden
HNW	Het Nieuwe Werken
HRO	High Reliability Organisations
LiFT	Li Frequency Trap
SAM	Screen Angle Modulation
Sr	Wetboek van Strafrecht
Stg.	Staatsgeheim
Vir	Voorschrift informatiebeveiliging rijksdienst 2007
Vir-bi	Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004
Vir-gi	Voorschrift informatiebeveiliging rijksdienst – gerubriceerde informatie (is men voornemens in 2011 in te voeren)
VPN	Virtual Privat Network
Wbs	Wet bescherming staatsgeheimen
Wiv	Wet op de Inlichtingen- en Veiligheidsdiensten
WOB	Wet openbaarheid van bestuur
WVO	Wet veiligheidsonderzoeken

Bijlage IV Lijst van gehanteerde begrippen

Actieve fouten	een directe en gewoonlijk kortdurende impact op de integriteit van de maatregel, bewust of onbewust veroorzaakt door de direct betrokken actor
Bijzondere informatie	staatsgeheimen en overige bijzondere informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van de Staat, van zijn bondgenoten of van één of meer ministeries (artikel 1 onder a Vir-bi)
Compromittering	de kennisname dan wel de mogelijkheid tot kennisnemen door een niet gerechtigde van bijzondere informatie (artikel 1 onder g Vir-bi)
Departementaal (Dep.) Vertrouwelijk	vereiste rubricering voor bijzondere informatie die geen staatsgeheim is indien kennisnemen door niet gerechtigden nadeel kan toebrengen aan het belang van één of meer ministeries (artikel 5, tweede lid, Vir-bi)
Dreiging/bedreiging	een gebeurtenis of een proces die in potentie een verstorende invloed heeft op de betrouwbaarheid van een object
Dumpsterdiving	het bewust zoeken naar – niet of onjuist vernietigde – gerubriceerde en vertrouwelijke informatie in afvalcontainers
Formeel geheim	hiervan is sprake als (al dan niet) gevoelige informatie correct gerubriceerd is (het staat er letterlijk op)
Gegevens	de objectief waarneembare weerslag van feiten op een drager
Gerubriceerde informatie	informatie die als Departementaal Vertrouwelijk of Staatsgeheim Confidentieel/Geheim/Zeer Geheim is aangeduid
Gevoelige informatie	informatie waarvan kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van – in dit geval – de Staat, van zijn bondgenoten of van één of meer ministeries, al dan niet gerubriceerd
Het Nieuwe Werken	plaats- en tijdonafhankelijk werken, ondersteund door de laatste technologieën zoals social media, cloud computingdiensten en mobiele communicatie
High Reliability Organisations	complexe organisaties die moeten opereren onder grote mentale druk in een gevaarlijke en interactieve omgeving waarbij weinig foutmarge toegestaan is, zoals vliegdekschepen, kerncentrales en luchtverkeersleidingcentra (Reason, 2000:770)
Informatie	de betekenis die de mens aan de hand van bepaalde afspraken toekent aan gegevens
Informatiebeveiliging	het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen (artikel 1 onder a Vir)
Intentioneel handelen	de actor is zich bewust wat deze wilde, er is sprake van opzet (dolus)

Kwetsbaarheid	de mate waarin het betreffende object voor deze (be)dreiging gevoelig is
Latente condities	systeemfouten die gecreëerd zijn door beslissingen van de ontwerpers, de bouwers en het hogere management
Lekken	het intentioneel of verwijtbaar compromitteren van gerubriceerde of gevoelige informatie door een persoon die hiervan gerechtigd houder is of anderszins toegang heeft
Li Frequency Trap	een rastervervanger die beschermt tegen kleurkopieën, in de kopie verschijnt een tekst die duidelijk maakt dat dit geen origineel is
Materieel geheim	hiervan is sprake als gevoelige informatie niet correct is gerubriceerd (het staat er letterlijk niet op) maar de houder van de informatie begreep of had behoren te begrijpen dat de informatie gevoelig is en openbaarmaking een kwetsbaarheid vormt
Merking	aanduiding die een bepaalde wijze van behandelen van bijzondere informatie aangeeft (artikel 1 onder d Vir-bi)
Rubriceren	vaststellen en aangeven dat een gegeven bijzondere informatie is en het bepalen en aangeven van de mate van beveiliging die aan deze informatie moet worden gegeven (artikel 1 onder c Vir-bi)
Screen Angle Modulation	beveiliging tegen kopiëren, de kopie vertoont een tekst of verstoring van het beeld, waardoor duidelijk blijkt dat het om een kopie gaat
Staatsgeheim	bijzondere informatie waarvan de geheimhouding door het belang van de Staat of zijn bondgenoten wordt geboden (artikel 1 onder b Vir-bi)
Staatsgeheim (Stg.) Confidentieel	vereiste rubricering indien kennisnemen door niet gerechtigden schade kan toebrengen aan het belang van de Staat of zijn bondgenoten (artikel 5, eerste lid, onder c Vir-bi)
Staatsgeheim (Stg.) Geheim	vereiste rubricering indien kennisnemen door niet gerechtigden ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten (artikel 5, eerste lid, onder b Vir-bi)
Staatsgeheim (Stg.) Zeer Geheim	vereiste rubricering indien kennisnemen door niet gerechtigden zeer ernstige schade kan toebrengen aan het belang van de Staat of zijn bondgenoten (artikel 5, eerste lid, onder a Vir-bi)
Verwijtbaar handelen	de actor heeft de (reële) mogelijkheid zich anders te gedragen, er is sprake van schuld (culpa)
Virtual Privat Network	digitale verbinding met ‘kantoor’ waarbij de medewerker een virtuele digitale werkplek heeft die (vrijwel) gelijk is aan die op kantoor

Bijlage V Vergelijking van diverse (inter)nationale beveiligingsrubriceringen

Nederland	Stg.[1] Zeer geheim	Stg.[1] Geheim	Stg.[1] Confidentieel	Dep.[2] Vertrouwelijk
EU-rubricering	Trés Secret UE EU TOP Secret	Secret UE	Confidentiel UE	Restreint UE
NAVO-rubricering	Cosmic Top Secret	Nato Secret	Nato Confidential	Nato Restricted
WEU-rubricering	Focal Top Secret	WEU Secret	WEU Confidential	WEU Restricted
België	Zeer Geheim Très Secret	Geheim Secret	Vertrouwelijk Confidentiel	Beperkte verspreiding Diffusion restreinte
Duitsland	Streng Geheim	Geheim VS	Vertraulich VS	Nur für den Dienstgebrauch
Frankrijk	Très Secret	Défense Secret	Défense Confidentiel	Défense Diffusion restreinte
Luxemburg	Très Secret	Secret	Confidentiel	Diffusion restreinte
Verenigd Koninkrijk	Top Secret	Secret	Confidential	Restricted
Verenigde Staten	Top Secret	Secret	Confidential	For official use only

Bron: Bijlage 1, Vir-bi (p. 25)

[1] Stg. kan ook uitgeschreven worden als Staatsgeheim.
[2] Dep. kan ook uitgeschreven worden als Departementaal.

Bijlage VI Schema voorbeelden van rubriceringen

	Compromittering kan leiden tot:			
	Stg. Zeer geheim	***Stg. Geheim***	***Stg. Confidentieel***	***Dep. Vertrouwelijk***
Gegevens met betrekking tot het Koninklijk Huis	Aantasting van de eenheid van de Kroon	Kwetsbare gegevens met betrekking tot het Koninklijk Huis	Gegevens met betrekking tot reizen van het Koninklijk Huis	
Gegevens met betrekking tot de krijgsmacht	Buitengewoon ernstige aantasting van de slagkracht of de veiligheid van de strijdkrachten	Ernstige aantasting van de slagkracht of de veiligheid van de strijdkrachten	Schadelijke gevolgen voor de slagkracht de veiligheid van de strijdkrachten	Nadelige gevolgen voor de slagkracht of de veiligheid van de strijdkrachten
Gegevens met betrekking tot de Inlichtingen- & Veiligheidsdiensten (I&V-diensten)	Zeer ernstige schade aan de effectiviteit van de I&V-diensten	Ernstige schade aan de effectiviteit van I&V-diensten (i.v.m. bron-bescherming)	Schade aan de effectiviteit van de I&V-diensten	
Openbare orde	Directe aantasting van de interne stabiliteit	Ernstige en grootschalige aantasting van de openbare orde		
Vertrouwelijke gegevens van derden onder berusting van de Rijksdienst				Verstrekking is in strijd met afspraak met derden om de vertrouwelijkheid te waarborgen
Non-proliferatie		Proliferatierisico met betrekking tot kernenergie/NBC-wapens	Proliferatierisico (overig)	
Internationale betrekkingen	Buitengewoon ernstige schade in de relatie met bevriende landen	Toename van internationale spanningen Verstoring van de relaties met bevriende landen	Schade aan diplomatieke relaties (formeel protest)	Nadelige gevolgen voor de diplomatieke relaties
Economische/Financiële schade	Zeer langdurige schade aan de economie	Wezenlijke materiële schade aan de financiële monetaire, economische en handelsbelangen	Schadelijke gevolgen voor de financiële economische en commerciële belangen van de Staat	Ongerechtvaardigde verrijking of voordeel voor natuurlijke personen of bedrijven
Gegevens m.b.t onderzoek zware criminaliteit	Zeer ernstige schade aan belangen van informanten	Schade toebrengen aan de opsporing, van en de opsporingsmethodieken inzake ernstige inbreuken op de rechtsorde	Schadelijke gevolgen voor het onderzoek naar de zware misdaad	
Gegevens met betrekking tot de beveiliging			Schadelijke gevolgen voor de effectiviteit van beveiligingsplannen van vitale objecten	Nadelige gevolgen voor de effectiviteit van beveiligingsplannen van vitale objecten
Onderhandelingen			Schadelijke gevolgen voor internationale onderhandelingen	Nadelige gevolgen voor onderhandelingen
Gegevens m.b.t. de ministerraad	Notulen Ministerraad		Besluitenlijst Ministerraad persoonlijke zaken met betrekking tot bewindslieden	

Bron: Bijlage 2, Vir-bi (p. 26)

Bijlage VII Voorbeeld kopieerbeveiligd papier

1. Linksboven, links in het midden en rechtsonder uniek nummer, tweezijdig gedrukt.
2. Rijkslogo
3. Zichtbaar gedrukt de tekst: *"Dit document bevat gerubriceerde informatie. Reproductie is alleen toegestaan na toestemming conform de regelgeving."*
4. Rijkslogopapier met signaalkleur (lichtgeel), voorzien van SAM-techniek, bij kopiëren verschijnt tekst: *"KOPIE – Dit document bevat gerubriceerde informatie. Reproductie is alleen toegestaan na toestemming conform de regelgeving."*
5. Door SAM-techniek verschijnt bij kopiëren in het midden de tekst: "KOPIE".

BIJLAGE VIII Aanbevelingen Commissie Lemstra

Onderstaande aanbevelingen zijn afkomstig uit het rapport 'Cultuur, ondersteund door structuur: hét wapen tegen het lekken van vertrouwelijke informatie' van de 'Commissie Lemstra' in opdracht van de minister van Defensie.

1. Inventariseer alle (inter)departementale regels. Schaf de overbodige en in de praktijk niet uitvoerbare regels af en kom tot één beperkt integraal regelcomplex met betrekking tot (document)beveiliging.
2. Start een voorlichtingscampagne om de nieuwe regels inzake documentbeveiliging op grond van het Besluit voorschrift informatie – beveiliging rijksdienst – bijzondere informatie, onder de aandacht van alle medewerkers van Defensie te brengen. Hanteer daarvoor een beperkt aantal gedragsregels (maximaal tien), die alle betrokkenen direct aanspreken.
3. Evalueer jaarlijks het aantal gerubriceerde stukken per vaststeller. Stel daarbij de vraag naar nut en noodzaak en pas vervolgens de praktijk zo nodig aan.
4. Stel in de rubriceringsvoorschriften duidelijke inhoudelijke rubriceringscriteria en hanteer daarbij de criteria van de Wet openbaarheid van bestuur en de daarop ontwikkelde jurisprudentie van de Afdeling Bestuursrechtspraak van de Raad van State.
5. Benoem een functionaris die uitleg kan geven over het Beleidskader Beveiliging Defensie in het algemeen en de uitwerking in de praktijk van de nieuwe rubriceringsregels in het bijzonder, mede in het licht van de WOB, en die adviseert (in voorkomend geval: beslist) over de hoogte van rubricering van een bepaald document.
6. Laat uit het rubricering blijken hoe lang een document gerubriceerd is. Maak een (electronisch beveiligd) rubriceringssysteem voor electronische documenten.
7. Bepaal dat de vaststeller van de rubricering van een document in een functionerings- of beoordelingsgesprek verantwoording aflegt voor zijn aandeel inzake de handhaving van de documentbeveiligingsregels, zoals beperkte verspreiding, need to know-beginsel en dergelijke.
8. Kom tot een effectieve controle bij het verlaten van het Ministerie of (militair of burger) complexen op het meenemen van vertrouwelijke of geheime informatie, opdat medewerkers zich bewust worden van het belang van (document)beveiligingsregels.
9. Voer bij een ernstige verdenking van opzettelijk lekken een integriteitstest uit, als in het rapport beschreven.
10. Bepaal dat de Beveiligingsautoriteit met zijn staf en de veiligheidscoördinatoren een aanjaagfunctie op het punt van de handhaving van en de controle op (document)-beveiligingsregels hebben.
11. Hou vast aan (regelmatige) screening van alle medewerkers op vertrouwensfuncties.
12. Voorkom dat (document)beveiligingsregels een obstakel zijn voor snelle besluitvorming.
13. Neem het zich houden aan (document)beveiligingsregels op als vast onderdeel van functionerings- en beoordelingstrajecten.
14. Kom tot een geloofwaardig sanctiebeleid met betrekking tot hen die zich opzettelijk of onopzettelijk niet houden aan (document)beveiligingsregels, waarbij ongeschiktheidsontslag en disciplinaire bestraffing als ultieme correctiemiddelen niet worden geschuwd.
15. School (militaire) medewerkers regelmatig in beveiligingsbewustzijn en in bewustzijn van de negatieve gevolgen van lekken voor de organisatie, maar ook voor de directe collegae.
16. School (militaire) medewerkers, die in contact zouden kunnen komen met journalisten, in de omgang met de media.
17. Investeer in beveiligingstechnologie.
18. Implementeer de aanbevelingen van het 'Beleidsplan KMar 2010' en het rapport van de commissie-Staal over de cultuur en de integriteit van de KMar.
19. Kom tot meer en betere voorlichting aan medewerkers omtrent de noodzaak van reorganisaties en inkrimpingen.
20. Kom tot een politieke (middel)lange termijnvisie voor Defensie waardoor medewerkers enig zicht wordt geboden omtrent het perspectief voor hun organisatie.
21. Maak de spelregels voor medezeggenschapsorganen om naar de politiek en media te stappen binnen de organisatie uitvoeriger bekend.
22. Kom tot een actief voorlichtingsbeleid, gedragen door het uitgangspunt dat alles wat niet geheim is, openbaar kan worden gemaakt (artikel 8, eerste lid van de Wet openbaarheid van bestuur).

23. Ga minder krampachtig met contacten tussen (militaire) topambtenaren en Kamerleden om.
24. Besteed structureel aandacht aan een herkenbare positie van Defensie binnen de samenleving (zie bijvoorbeeld de Notitie van de CDA-fractie van de Tweede Kamer).
25. Kom tot een samenvloeiing van militaire opleidingen, daar waar dit mogelijk is (met name de initiële militaire opleiding).
26. School (militaire) medewerkers zo vroeg mogelijk in politieke en bestuurlijke gevoeligheden en de positie van de (militaire) ambtenaar ten opzichte van de politiek (grondrechten, klokkenluiden, (niet) lekken).
27. Neem mediatraining op in de opleiding van (militaire) medewerkers, die in contact kunnen komen met journalisten.
28. Neem topmilitairen op in de Algemene Bestuursdienst.
29. Zorg voor een evenwichtige verdeling van militairen en burgers binnen het bestuursdepartement.
30. Maak van de Commandant der Strijdkrachten 'een bekende Nederlander' die als boegbeeld van de militaire organisatie een eigenstandige rol vervult in het publieke en politieke debat om het militaire belang in het publieke en politiek debat uit te dragen en te verdedigen.
31. Geef de Commandant der Strijdkrachten de nodige ruimte om in contact te treden met de media en de politiek.
32. Investeer structureel in samenwerking binnen de staf van de Commandant der Strijdkrachten.
33. Betrek de operationele commandanten bij politieke besluitvorming.
34. Leg de verantwoordelijkheid voor interne onderzoeken naar een lekincident bij een daartoe adequaat uitgeruste Beveiligingsautoriteit.
35. Schakel de Koninklijke Marechaussee in bij een lek van vertrouwelijke informatie.
36. Houd een register bij met aanbevelingen naar aanleiding van een onderzoek van lekincidenten.
37. Laat onderzoeken naar lekincidenten uitmonden in aanbevelingen tot verbetering en zorg ervoor dat de Beveiligingsautoriteit deze borgt.
38. Geef meer bekendheid aan de Regeling klachtenprocedure ongewenst gedrag en melding vermoedens van misstanden bij Defensie (KOGVAM-regeling) en aan de rol van de vertrouwenspersoon op grond van deze regeling.
39. Maak het mogelijk dat een misstand anoniem kan worden gemeld.
40. Zorg dat het ieder binnen de Defensie-organisatie duidelijk is dat de opzettelijke lekker de grote kans loopt op disciplinaire straf van ontslag.

(Lemstra et al., 2005:76-82)

GERAADPLEEGDE LITERATUUR

Alberdingk Thijm, C. & Antic, M. (2010, 9 december). *Tien Wikileaks-stellingen ontkracht.* Geraadpleegd op http://webwereld.nl/opinie/68068/tien-wikileaks-stellingen-ontkracht--opinie-.html, 3 januari 2011.

Ale, B. (2009). *Risk: An introduction. The concepts of risk, danger and chance.* Abingdon: Routledge.

Antonio, L.A.M. & Nascimento, L.P.R. (2010). *Careless Talk Costs Revenue: The perils of sharing confidential corporate information with family and friends*, Geraadpleegd op http://www.datalossbarometer.com/14720.htm, 2 januari 2011.

Asma, J. (2010). *Portable Media: Sometimes your biggest problems are little ones.* Geraadpleegd op http://www.datalossbarometer.com/14708.htm, 2 januari 2011.

Assange, J. (2010, 8 december). WikiLeaks doet wat alle media doen. *NRC Next,* 21.

Asscher, L.F. (2002). *Communicatiegrondrechten: een onderzoek naar de constitutionele bescherming van het recht op vrijheid van meningsuiting en het communicatiegeheim in de informatiesamenleving* (dissertatie UvA). Amsterdam: Otto Cramswinkel.

Avermaete, J. van (2002). Latente condities, niet latente fouten. Interview met James Reason. *HUFAG Nieuwsbrief.* Herfst, 2-4. Geraadpleegd op http://www.hufag.nl/archief/huf05.pdf, 5 maart 2011.

Balkenende berispt Kabinet der Koningin (2007, 30 mei). *NRC Handelsblad*. Geraadpleegd op http://vorige.nrc.nl/binnenland/article1802011.ece/Balkenende_berispt_Kabinet_der_Koningin, 24 april 2011.

Barnum, S. & Gegick, M. (2005). *Defense in Depth.* Geraadpleegd op https://buildsecurityin.us-cert.gov/bsi/articles/knowledge/.../347-BSI.pdf, 14 januari 2011.

Bastiaans, M.H. (2001). *Leidraad voor juridische auteurs.* Deventer: Kluwer.

Becker, M. (2007). *Bestuurlijke ethiek.* Assen: Van Gorcum.

Bedaf, A. van (2010). Beveiligingsbewustzijn en de factor mens. Méér dan alleen de medewerker. Security Management, 11, 14-16.

Beenakkers, E.M.Th., & Grapendaal, M. (1995). *Lekken en lekkers: Een verkennend onderzoek naar het lekken van vertrouwelijke informatie naar de pers.* Den Haag: WODC.

Bemmelen, J.M. van, Veen, Th.W. van, Jong, D.H. de & Knigge, G. (1998). *Het materiële strafrecht.* Deventer: Gouda Quint.

Biesheuvel-Vermeijden, J. (2010). Embargo op Prinsjesdagstukken. *Nederlands Juristenblad.* 6, 367.

Blankesteijn, H. (2010, 9 december). Diplomaten zeggen A, denken B en doen C. *NRC Next,* 20-21.

Boekhout van Solinge, T. (2010, 19 november). Het Nederlandse drugsbeleid en de wet van de remmende oorsprong. *Nederlands Juristenblad.* 40, 2583.

Boer, W.Th. de (1996). *Koenen Woordenboek Nederlands*, Utrecht: Koenen Woordenboeken.

Boogaard, R. van den (2005, 8 november). Op defensie is veel te veel geheim. *NRC Handelsblad,* 3.

Bovens, M.A.P. (2006). *Analysing and Assessing Public Accountability. A Conceptual Framework.* European Governance Papers (EUROGOV) No. C-06-01.

Bovens, M.A.P., Geveke, H.G., & Vries, J. de, (1993). Strikt vertrouwelijk: lekken in het openbaar bestuur. *Beleid & Maatschappij.* 2, 61-80.

Bovens, M.A.P., Hart, P. 't & Twist, M.J.W. van (2007). *Openbaar bestuur.* Alphen aan de Rijn: Kluwer.

Bruggen, J.J.G. van der (2010). Met de kennis van nu. Reflecties van een Irak-onderzoeker. *Vrede en veiligheid,* 1/2, 83-95.

Buruma, Y. (2011, 14 januari). WikiLeaks: wat leert het ons echt? *Nederlands Juristenblad,* 2, 1.

Canon-printer censureert tekst (2010, 14 oktober). *NRC Handelsblad.* Geraadpleegd op http://vorige.nrc.nl/economie/article2631485.ece/Canon-printer_censureert_tekst, 15 oktober 2010.

Chernick, D. (2010). *Staff Vetting: Keep a closer eye on your employees.* Geraadpleegd op http://www.datalossbarometer.com/14719.htm, 2 januari 2011.

Code voor Informatiebeveiliging. NEN-ISO/IEC 27002 (2007). Delft: NEN.

Coolsma, J.C. & Schuiling, K.F. (1995). *De kleine scriptiegids: Stappenplan met schrijftips voor juristen en bestuurswetenschappers.* Bussum: Countinho.

Corruptiebrief Bijleveld komt hard aan. (2009, 27 februari). *Radio Nederland Wereldomroep.* Geraadpleegd op http://static.rnw.nl/migratie/antilliaans.caribiana.nl/politiek/

car20090227_bijleveld-corruptie-redirected, 12 december 2010.
Daalder, E. (2011, 7 januari). In afwachting van een regeringsstandpunt over Tromsø. *Nederlands Juristenblad,* 1, 10-11.
Davids, W.J.M. (2010). *Ketelaar-lezing 7 oktober 2010. Gerubricerd staatsgeheim: ZEER GEHEIM, GEHEIM, CONFIDENTIEEL, VERTROUWELIJK.* Geraadpleegd op http://www.archief.nl/sites/default/files/docs/ketelaarlezing_2010.pdf, 10 januari 2011.
Davids, W.J.M., Boer, M.G.W. den, Fasseur, C., Koopmans, T., Schrijver, N.J., Schwegman, M.J., & Walsum, A.P. van (2010). *Rapport Commissie van Onderzoek besluitvorming Irak.* Amsterdam: Boom.
Dekker, M., Veugen, T. & Etalle, S. (2006, december). Audit-based Access Control in de Zorg. *Informatiebeveiliging,* 19-23. Geraadpleegd op https://www.pvib.nl/download/?id=6474160&download=1, 1 maart 2011.
Delaere, M. (2007, 12 oktober). Gelekt wordt er toch. *Binnenlands Bestuur,* 26-29.
Den Haag reageert onderkoeld op nieuws WikiLeaks (2011, 15 januari). *NRC Handelsblad,* 2.
Diehl, E. (2008, maart). Content Protection. In this digital age, protecting your assets is essential. *Broadcast Engineering World*, 10-13. Geraadpleegd op http://eric-diehl.com/index.php?lang=En&page=publi, 1 maart 2011.
Diplomatieke post voor en na WikiLeaks (2010, 30 november). *NRC Next,* 19.
Dommering, E.J. (2007). Annotatie bij EHRM 25 april 2006 (Dammann/Zwitserland) en EHRM 25 april 2006 (Stoll/Zwitserland. *NJ,* 2007-11, nr. 126 en 127, 1262-1263. Geraadpleegd op http://www.ivir.nl/publicaties/dommering/Annotatie_NJ_2007_126_127.html, 8 januari 2011.
Doorduyn, Y. & Sommer, M. (2007, 18 mei). De communicatiestaat. *Volkskrant.*
Drenthen, M., Willems, J., & Zwart, H. (2005). *Ethiek van de wetenschapscommunicatie.* Amsterdam: Boom.
Driver, J. (2007). *Ethics: the fundamentals*. Malden, MA, USA: Blackwell.
Fransman opgepakt om opzetten WikiLeaks-site (2011, 7 januari). *NRC Next,* 6.
Freedman, W. (1967). *Legal theory.* London: Stevens & Sons.
Graaf, J. van der Graaf & Kuitert, H. (2009, 6 juni). Dalai Lama bedreigd. *De Telegraaf.* Geraadpleegd op http://www.telegraaf.nl/binnenland/4074385/__Dalai_lama_bedreigd__.html, 14 juni 2010.
Handleiding Kwetsbaarheidsanalyse spionage (2011). Den Haag: Algemene Inlichtingen- en Veiligheidsdienst.
Handreiking Risicoanalyse (2009). Den Haag: Nationaal Adviescentrum Vitale Infrastructuur.
Hanson, K.O. & Ceppos., J. (2006, October 6). The Ethics of Leaking. *Los Angeles Times.* Geraadpleegd op http://www.scu.edu/ethics/publications/ethicalperspectives/leaks.html, 23 juli 2010.
Heij, H. de (2010). *Banknote design for retailers and public.* Amsterdam: De Nederlandsche Bank.
Heijmans, T. (2009, 15 januari). Lekken?, *De Volkskrant.*
Hero Brinkman zet Rijksrecherche aan het werk (2011). *RTL Nieuws.* Geraadpleegd op http://www.rtl.nl/(/actueel/rtlnieuws/binnenland/)/components/actueel/rtlnieuws/2011/03_maart/09/verrijkingsonderdelen/Hero_Brinkman_zet_rijksrecherche_aan_het_werk.xml, 9 maart 2011.
Het grote Haagse lekken (2007, 22-29 oktober) [Web log post]. Geraadpleegd op http://www.communicatieonline.nl/opinie/bericht/het-haagse-lekken/, 2 februari 2011.
Heuvel, J.H.J. van den, Huberts, L.W.J.C., & Verberk, S. (2002). *Het morele gezicht van de overheid. Waarden, normen en beleid.* Utrecht: Lemma.
Hins, W. (2008). Eens openbaar, altijd openbaar? Over de status van uitgelekte informatie. In N. van Eijk & B. Hugenholtz (Red.), *Dommering-bundel, Opstellen over informatierecht aangeboden aan prof. mr. E.J. Dommering* (p. 149-159). Amsterdam: Otto Cramwinkel. Geraadpleegd op http://www.ivir.nl/publicaties/hins/Dommering_bundel_Hins.pdf, 25 maart 2011.
Huberts, L.W.J.C. & Nelen, J.M. Nelen (2005). *Corruptie in het Nederlands openbaar bestuur: omvang, aard en afdoening*. Amsterdam: Vrije Universiteit. Geraadpleegd op http://www.wodc.nl/images/1065_volledig%20rapport_tcm44-58675.pdf, 26 maart 2011.
Huff, P. (2010, 29 december). Iedereen prijst zijn eigen waarheid aan. *NRC Next,* 18.
Hulsebos, M. (2011, 24 februrari). *Omgaan met gevoelige informatie. Eerst de mensen, dan pas DLP.* Geraadpleegd op http://www.whitepaperlibrary.nl/categorie/7-security.html, 10 maart 2011.
Janssen, R. (2007, 18 mei). Iedere minister heeft wel iets moois in de aanbieding. *NRC Next.*
Jensma, F. (2010, 18 december). De stelling van Alex Brenninkmeijer: WikiLeaks is een breekijzer voor meer openheid door de overheid. *NRC Handelsblad,* 10-11.

Jeurissen, R.J.M. (2001). *Bedrijfsethiek: Een goede zaak.* Assen: Van Gorcum.
Jippes, H. (2009, 9 april). Britse antiterreurchef Quick weg na blunder. *NRC Handelsblad.* Geraadpleegd op http://vorige.nrc.nl/buitenland/article2208648.ece/Britse_antiterreurchef_Quick_weg_na_blunder, 19 januari 2011.
Jong, J. de, & Vries, M.S. de (2007). Toward unlimited transparency?: Morals and facts concerning leaking to the press by public officials in the Netherlands. *Public administration and development.* 27, 215–225. doi: 10.1002/pad.457
Jongbloed, L. (2009, 31 maart). Politierechter raakt dossiers kwijt. Geraadpleegd op http://www.telegraaf.nl/binnenland/3604951/__Politierechter_raakt_dossiers_kwijt__.html, 31 maart 2009.
Jongen vindt gevangenis-pc op straat (2010, 15 april). *De Telegraaf*. Geraadpleegd op http://www.telegraaf.nl/binnenland/6530289/__Jongen_vindt_gevangenis-pc__.html, 24 april 2011.
Kabinet heeft reactie op Irak-rapport bijna af. (2010, 4 februari 2010), *De Volkskrant,* Geraadpleegd op http://www.volkskrant.nl/binnenland/article1345656.ece/Kabinet_heeft_reactie_op_Irak-rapport_bijna_af, 14 juni 2010.
Kamervragen over uitlekken afschaffing pc-privé-regeling (2004, 31 augustus). *NU.nl.* Geraadpleegd op http://www.nu.nl/internet/390164/kamervragen-over-uitlekken-afschaffing-pc-prive-regeling.html, 26 januari 2011.
Karssing, E. & Spoor, S. (2009). Integriteit 3.0: Naar een derde generatie integriteitsbeleid. In E. Karsing en M. Zweegers (red.), *Jaarboek Integriteit 2010* (pp. 72-81), Den Haag: CAOP.
Ketelaar, T. (2010, 25 oktober). Hij is nergens meer welkom. *NRC Next,* 4.
Klaver, M.-J. (2007, 28 november). Mens is zwakste schakel bij databeveiliging. *NRC Handelsblad.*
Kleiweg, M. (2010, 23 maart). Embargoregeling niet meer van deze tijd [Web log post]. Geraadpleegd op http://www.dktv.nl/wordpress/?page_id=27, 27 januari 2011.
Klompenhouwer, L. (2011, 6 januari). Nee, geen pennen. Er zijn weer gegevens gestolen. *NRC Next,* 12-13.
König, E. (2010, 7 december). Deze onderzeese telecomkabel is van vitaal belang. *NRC Next,* 6-7.
König, E. (2011, 21 april). In z'n nieuwe cel mag hij zelfs tv kijken. *NRC Next,* 7.
Kooistra, J. (2006, 15 augustus). Extra stappen om begroting geheim te houden. *Elsevier.* Geraadpleegd op http://www.elsevier.nl/web/1087267/Nieuws/Politiek/Extra-stappen-om-begroting-geheim-te-houden.htm, 27 januari 2011.
KPMG (2010, November). *Data Loss Barometer. Insights into lost and stolen information*. Geraadpleegd op http://www.datalossbarometer.com/docs/KPMG_Data_Loss_Barometer_-_Issue_3_-_November_2010.pdf, 2 januari 2011.
Kranenburg, M. (2010, 30 november). Leve de Beslotenheid. *NRC Next,* 5.
Kuiper, R. & Groen, P. (2005, juli). Zijn Staatsgeheimen te beveiligen? *Informatiebeveiliging,* 16-21.
Kuipers, M. & Schoof, D. (2010). Kwetsbaarheidsanalyse spionage: Alles van waarde is weerloos. *Magazine nationale veiligheid en crisisbeheersing.* Mei/juni, 46-47.
Kuitenbrouwer, J. (2011, 29 januari). U luidt de klok, WikiLeaks doet de marketing. *NRC Handelsblad,* Opinie & Debat 7.
Kwetsbaarheidsanalyse spionage (2010). Den Haag: Algemene Inlichtingen- en Veiligheidsdienst.
Lekken. (g.d. a). In *Van Dale*. Geraadpleegd op http://www.vandale.nl/vandale/opzoeken/woordenboek/?zoekwoord=lekken, 11 april 2010.
Lekken. (g.d. b). In *Woorden.org.* Geraadpleegd op http://www.woorden.org/woord/lekken, 11 april 2010.
Lemstra, W., Brouwers, E., Niessen, C.R., Wuisman, G.P.I.M., Schouten, M. (2005). *Cultuur ondersteund door structuur: hét wapen tegen het lekken van vertrouwelijke informatie.* Den Haag: Ministerie van Defensie.
Lintel, P. van (2009, 17 september). Vrouwen kunnen echt geen geheim bewaren. *Nu.nl.* Geraadpleegd op http://www.nu.nl, 9 juli 2010.
Lovink, G. & Riemens, P. (2010, 11 december). Voor WikiLeaks telt slechts de banaliteit van het spektakel. *NRC Handelsblad, Opinie & Debat,* 1-2.
Luyendijk, J. (2010). *Je hebt het niet van mij, maar …. Een maand aan het Binnenhof.* Amsterdam: Podium.
Lynn, J. & Jay, A. (1994). *Yes Minister.* London: BBC Books.
Maat, J.H. & Graaf, H. (2005, 14 juli). 'Anoniem lekken is effectiever dan klokkenluiden'. Ron Niessen, hoogleraar Ien Dales leerstoel UvA. *PM, hét magazine voor de overheid*, 14-16.
Maat, J.H. (2011). 'Het Nieuwe Werken of De Nieuwe Kwetsbaarheid?'. *Security Management*, 1/2, j anuari/februari, 32-34.

Machiavelli, N. (1995). *De heerser.* Amsterdam: Athenaeum-Polak & Van Gennep (Il Principe, 1513, vertaald door F. van Dooren).
Many people, many solutions… (z.j.). Haarlem: Joh. Enschedé Security Solutions.
Meeus, T.-J. (2010, 29 november). Wat wereldleiders écht van elkaar vinden. *NRC Next,* 4-5.
Meeus, T.-J. (2011, 11 januari). De klokkenluider zit in een kale isoleercel. *NRC Next,* 4.
Mentens, J. (2009, 6 februari). Nieuwe rel Aruba na lekken geheim rapport. *De Volkskrant.* Geraadpleegd op http://www.volkskrant.nl/binnenland/article1144582.ece/Nieuwe_rel_Aruba_na_lekken_geheim_rapport, 14 juni 2010.
Mil, B.P.A. van, Dijkzeul, A.E., & Pennen, R.M.A. van der (2006). *Zicht op risico's. Handboek Risicoanalysemethodieken.* Utrecht: Berenschot.
Miljoenennota opnieuw uitgelekt. (2010, 12 september). *De Pers.* Geraadpleegd op http://www.depers.nl/binnenland/336512/Miljoenennota-opnieuw-uitgelekt.html, 14 juni 2010.
Miljoenennota weer uitgelekt (2005, 13 september). *NU.nl.* Geraadpleegd op http://www.nu.nl/algemeen/591521/miljoenennota-weer-uitgelekt.html, 27 januari 2011.
Miller, S., Blackler, J. & Alexandra, A. (2006). *Police Ethics.* Crows Nest, Australia: Allen & Unwin.
Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 (2010). Den Haag: GOVERT.NL
Nierop, L. van (2010, 28 december). Anoniem lekken is zo simpel nog niet. *NRC Next,* 9.
Oltshoorn, R. (2011, 11 januari). Assange heeft nooit van Manning gehoord, zegt hij. *NRC Next,* 5.
Onderzoek naar lek Belastingdienst (2010, 7 december). *NU.nl.* Geraadpleegd op http://www.nu.nl/economie/2396541/onderzoek-lek-belastingdienst.html, 26 januari 2011.
Oranje, J. (2010, 11 januari). Den Haag wacht met spanning op Irak-onderzoek. *NRC Handelsblad.* Geraadpleegd op http://www.nrc.nl/binnenland/article2456068.ece/Den_Haag_wacht_met_spanning_op_Irak-onderzoek, 14 juni 2010.
Overbeek, P., Roos Lindgreen, E.R., & Spruit, M. (2005). *Informatiebeveiliging onder controle*. Amsterdam: Pearson Education.
Patel, H. & Morrison, D. (2010). *Information Theft: Are nervous employees sizing up your data?* Geraapleegd op http://www.datalossbarometer.com/14737.htm, 2 januari 2011.
Perlow, J. (2010, 1 december). Wikileaks: How our Government IT Failed Us [Web log post]. Geraadpleegd op http://www.zdnet.com/blog/perlow/wikileaks-how-our-government-it-failed-us/14988, 6 december 2010.
PVV'er Brinkman tipte Rijksrecherche (2011). *RTL Nieuws.* Geraadpleegd op http://www.rtl.nl/(/actueel/rtlnieuws/binnenland/)/components/actueel/rtlnieuws/2011/03_maart/09/binnenland/brinkman-tipgever-van-rijksrecherche.xml, 9 maart 2011.
Reason, J. (2000, March 18). Human error: models and management. *British Medical Journal.* Geraadpleegd op http://www.bmj.com/content/320/7237/768.full.pdf, 5 maart 2011.
Rijksrecherche (2005). *Jaarbericht Rijksrecherche 2004.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche (2006). *Jaarbericht Rijksrecherche 2005.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche (2007). *Jaarbericht Rijksrecherche 2006.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche (2008). *Jaarbericht Rijksrecherche 2007.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche (2009). *Jaarbericht Rijksrecherche 2008.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche (2010). *Jaarbericht Rijksrecherche 2009.* Geraadpleegd op http://www.om.nl/organisatie/rijksrecherche/publicaties/jaarberichten/, 28 november 2010.
Rijksrecherche onderzoekt lek ministerraad. (2010, 30 september). *Trouw*. Geraadpleegd op http://www.trouw.nl/nieuws/nederland/article2876769.ece/Rijksrecherche_onderzoekt_lek_ministerraad.html, 14 juni 2010.
Roelants, C. & Erdbrink, T. (2010, 30 november). Amerikaanse propaganda. Zo noemt Iran de documenten. *NRC Next,* 6-7.
Room, S. (2010). *Legal Developments: Living with a regulatory bear market,* Geraadpleegd op http://www.datalossbarometer.com/14781.htm, 2 januari 2011.
Rossum, M. van (2010, 31 januari). Focus op het triviale. *NRC Next,* 3.
Rutte, M. (2011, 14 januari). Wekelijkse persconferentie premier Rutte [Video file]. Geraadpleegd op http://www.rtl.nl/xl/#/u/215bd6cd-92f5-4860-8c55-d21a3db7e1b8/, 14 januari 2011.
Sala, L. (2011, 5 januari). Wikileaks; de ethiek mist in cuberspace. [Web log post]. Geraadpleegd op

http://www.amsterdampost.nl/wikileaks-de-ethiek-mist-in-cyberspace/, 8 januari 2011.
Salden, J. (2008, 8 november). Hoe meer dossiers, hoe meer lekt. *Nederlands Dagblad.*
Scharenborg, M.H.G. (2006a). *Fraude & Onderzoek.* Den Haag: Sdu.
Scharenborg, M.H.G. (2006b). *Integriteit & Ambtenaar.* Den Haag: Sdu.
Scharenborg, M.H.G. (2007). *Fraude & Preventie.* Den Haag: Sdu.
Schneier, B. (2003). *Beyond Fear.* New York: Copernicus.
Schoemaker, R. (2010, 29 november). 'Iedereen' heeft toegang tot 'geheim' netwerk. *Webwereld.* Geraadpleegd op http://webwereld.nl/nieuws/67940/-iedereen--heeft-toegang-tot--geheim--netwerk-vs.html, 10 maart 2011.
Schuijt, G.A.I. (1990). Hoge Raad niet meer bang voor de uitingsvrijheid? *Informatierecht AMI*, 1996-2, 23-30. Geraadpleegd op http://www.ivir.nl/publicaties/schuijt/HR1.doc, 8 januari 2011.
Schut, L.A.J. (2010). Ruimte voor klokkenluiden is kenmerk van democratie. In J.Th.J. van den Berg, E. Verhulp & R.K. Visser (red), *Zoals een goed ambtenaar betaamt* (pp. 193-203). Den Haag: Ien Dalesleerstoel.
Screen Angle Modulation (z.j.). Haarlem: Joh. Enschedé Security Printing.
Shirky, C. (2010, 16 december). WikiLeaks als Amsterdamse vrijbuiters uit de 16de-eeuw. *NRC Next*, 16-17.
Simon, C. (2010, 7 juli). Gij zult niet liegen, lekken en lokken. *NRC Next,* 20-21.
Singer, P. (1994). *Ethics.* Oxford, UK: Oxford University Press.
Sloot, B. van der (2011). WikiLeaks: te actief voor een webhoster, te passief voor een journalistiek medium. *Nederlands Juristenblad,* 12, 734-739.
Snook, S.A. (2000). *Friendly Fire. The Accidental Shootdown of U.S. Black Hawks over Northern Iraq.* Princeton (NJ): Princeton University Press.
Spionage bij reizen naar het buitenland (2010). Den Haag: Algemene Inlichtingen- en Veiligheidsdienst.
Staman, J. (2011, 18 januari). Julian Assange, de Robin Hood van deze tijd. *NRC Next*, 17.
Stoneburner, G., Hayden, C. & Feringa, A. (2004). *Computer Security*. Gaithersburg (MD): National Institute of Standards and Technology. Geraadpleegd op http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf, 5 maart 2011.
Swiss Cheese Model (2005). Geraadpleegd op http://patientsafetyed.duhs.duke.edu/module_e/swiss_cheese.html, 5 maart 2011.
Talbot, J. & Jakeman, M. (2008). *SRMBOK. Security Risk Management Body Of Knowledge.* Carlton South (Australia): Risk Management Institution of Australasia Limited.
Teeffelen, G.J. van (2009, 9 april). Hoofd Britse anti-terreurdienst weg na blunder. *Volkskrant.* Geraadpleegd op http://www.volkskrant.nl/vk/nl/2668/2009/article/print/detail/328415/Hoofd-Britse-anti-terreurdienst-weg-na-blunder.dhtml, 19 januari 2011.
Teffer, P. (2010, 13 december 2010, b). Vecht nú voor vrijheid. *NRC Next*, 8.
Teffer, P. (2010, 27 juli, a). De dramatische details van zes jaar oorlog. *NRC Next,* 6-7.
Tencer, D. (2011, 5 januari). *White House's 'insider threat' program targets federal employees for surveillance.* Geraadpleegd op http://www.rawstory.com/rs/2011/01/insider-threat-targets-employees-surveillance/, 12 februari 2011.
Tongeren, P. van & Becker, M. (2009) Integriteit als deugd. In E. Karsing en M. Zweegers (red.), *Jaarboek Integriteit 2010* (pp. 58-65), Den Haag: CAOP.
Tongeren, P. van (2003). *Deugdelijk leven: Een inleiding in de deugdethiek.* Amsterdam: SUN.
Udo de Haas, A. (2010, 18 december). Kroes: WikiLeaks dwingt tot open overheid. *Webwereld.* Geraadpleegd op http://webwereld.nl/nieuws/68160/kroes--wikileaks-dwingt-tot-open-overheid.html, 10 maart 2011.
Uitlekken. (g.d.) In *Wikipedia.* Geraadpleegd op http://nl.wikipedia.org/wiki/Uitlekken_(informatie), 11 april 2010.
Uniflow, Control scanning, printing and copying effectively with uniFLOW (2010). Bad Iberg: NT-ware.
Uniflow, Enhanced security (2010). Bad Iberg: NT-ware.
Vaartjes, E. (2008, 22 augustus). Filosofisch woordenboek. *Rechtsethiek.nl.* Geraadpleegd op http://www.rechtsethiek.nl, 7 augustus 2010.
Venetië, E. van & J. Luikenaar (2006). *Het Grote Lobbyboek.* Zutphen: Plataan.
Verkade, T. (2010, 30 november). Leve de Openbaarheid. *NRC Next,* 4.
VPRO Tegenlicht (2011, 24 januari). De wereld na WikiLeaks [Video file]. Geraadpleegd op http://tegenlicht.vpro.nl/afleveringen/2010-2011/de-wereld-na-wikileaks.html, 24 januari 2011.
Wallage, J. et al (2001). *In dienst van de democratie. Het rapport van de Commissie Toekomst Overheidscommunicatie.* Den Haag: Sdu.
Warning Signs: Is the credit crunch turning your employees into criminals? (2010). Geraadpleegd op

http://www.datalossbarometer.com/14694.htm, 2 januari 2011.
Werknemers lekken vaker informatie (2009, 22 oktober). Geraadpleegd op http://www.consultancy.nl/nieuws/kpmg-werknemers-lekken-vaker-informatie, 2 januari 2011.
Wester, F. (2008, 10 september). *Frits Wester over lekken.* Pauw & Witteman [Video file]. Geraadpleegd op http://pauwenwitteman.vara.nl/Archief-detail.113.0.html?&tx_ttnews%5Btt_news%5D=1163&tx_ttnews%5BbackPid%5D=111&cHash=ed8fa18d74, 2 februari 2011.
Westewoud, E.F.J. (2007). *EHRC caselaw on article 10 and journalism.* Geraadpleegd op http://www.issuu.com/westewoud/docs/echr_caselaw_art_10_efjw2007, 8 januari 2011.
Wijkerslooth de Weerdesteijn, J.L. de, Beaufort, W.H. de, Borst-Eilers, E. (2010). *Publiek geheim.* Den Haag: Tweede Kamer der Staten Generaal.
Wijnberg, R. (2011, 24 januari). De wereld na WikiLeaks. *NRC Next,* 10.
WikiLeaks. (g.d.). In *Wikipedia.* Geraadpleegd op http://nl.wikipedia.org/wiki/WikiLeaks, 18 december 2010.
Zwaap, R. (2010, 22 januari, a). De papieren draak. *PM*, 14-17.
Zwaap, R. (2010, 22 januari, b). Staatsgeheim gezocht. *PM,* 17-18.

Jurisprudentie

EHRM 10 december 2007, 69698/01 (Stoll v. Switzerland)
EHRM 25 april 2006, 77551/01 (Dammann v. Switzerland)
EHRM 9 februari 1995, 16616/90 (Bluf! v. The Netherlands)
EHRM 26 november 1991, 13166/87 (Sunday Times v. The United Kingdom)
EHRM 26 november 1991, 13585/88 (Observer and Guardian v. The United Kingdom, Spycatcher)
Hoge Raad 7 juli 2009, rolnummer 07/10741, LJN: BG7232 (AIVD-medewerker)
Hoge Raad 11 juli 2008, rolnummer C06/306HR, LJN: BC8421 (Telegraaf-zaak)
Hoge Raad 25 maart 2008, rolnummer 02387/06 B, LJN: BB2875 (Verschoningsrecht journalist)
Hof Amsterdam 23 december 2009, parketnummer 23-000759-08, LJN: BK7623 (Vancouver)
Hof 's-Gravenhage 4 maart 1999, Mediaforum 1999-4, nr. 21
Rechtbank Haarlem 14 juli 2010, rolnummer 15/700461-09, LJN: BN1195
Rechtbank Haarlem 14 juli 2010, rolnummer 15/700462-09, LJN: BN1191
Rechtbank 's-Gravenhage 19 juli 2007, rolnummer 06/7997, LJN: BK8847 (WOB)

Parlementaire stukken

WikiLeaks, *Kamerstukken II* 2010/11, 32 500 V, nr. 145
Kredietcrisis, *Kamerstukken II* 2009/10, 31 371, nr. 300, p. 1-2.
Regeling vertrouwelijke stukken, *Kamerstukken II* 2009/10, 32 391, nr. 3
Reglement van Orde van de Tweede Kamer der Staten-Generaal, *Kamerstukken II* 2009/10, 32 391

Aangehaalde wet- en regelgeving

Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (EVRM)
Ambtenarenwet (AW)
Wet bescherming staatsgeheimen (Wbs)
Wet op de Inlichtingen- en Veiligheidsdiensten (Wiv)
Wet openbaarheid van bestuur (WOB)
Wet veiligheidsonderzoeken (WVO)
Wetboek van Strafrecht (Sr)
Algemeen Rijksambtenarenreglement (ARAR)
Voorschrift informatiebeveiliging rijksdienst 2007 (Vir)
Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004 (Vir-bi)

Overige overheidsdocumenten

Aanwijzing taken en inzet rijksrecherche (2010, 13 december). Den Haag: College van procureurs-generaal (2010A033). Geraadpleegd op http://www.om.nl/organisatie/beleidsregels/overzicht/politie/@155174/aanwijzing-taken/, 26 maart 2011.

Besluit Melden vermoeden van misstand bij Rijk en Politie. (2009, 15 december). Staatsblad 2009, 572.

Besluit Vaststelling formulier eed/belofte rijksambtenaren (1998, 23 april). Minister van Binnenlandse Zaken, Staatscourant 1998, nr. 92:7. Geraadpleegd op http://wetten.overheid.nl/BWBR0009572/geldigheidsdatum_25-07-2010, 23 april 2011.

Brief van de minister van Financiën aan de Voorzitter Commissie Prinsjesdagstukken inzake de Commissie Prinsjesdagstukken (2009, 23 november), kenmerk BZ/2009/925 U.

Brief van de minister van Financiën aan de Voorzitter van de Tweede Kamer der Staten-Generaal inzake de stukkenstroom begrotingen (2009, 23 november), kenmerk BZ/2009/930 M.

Executive Order (2009, December 29). From the President of the United States of America] 13526, on Classified National Security Information. Geraadpleegd op http://www.archives.gov/isoo/pdf/cnsi-eo.pdf, 22 april 2011.

Leidraad Aanwijzing Vertrouwensfuncties (2006, 1 oktober). Minister van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd op https://www.aivd.nl/publish/pages/1398/leidraadvertrouwensfunctiesokt2006.pdf, 24 april 2011.

Memorandum from the Executive Office of the President (2011, January 3). Office of Management and Budget, for the Heads of Executive Departments and Agencies, on Initial Assessments of Safeguarding and Counterintelligence Postures for Classified National Security Information in Automated Systems, January 3, 2011 (reference M-11-08). Geraadpleegd op http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-08.pdf, 12 februari 2011.

Proces-verbaal van Bevindingen Feitenonderzoek 'Dieze' (2010, 23 augustus). Inzake notulen Ministerraad Dossier Westerschelde (proces-verbaalnummer 20090080); vrijgegeven door de voorzitter van het College van Procureurs-generaal namens de Minister van Veiligheid en Justitie op 7 maart 2011, kenmerk PaG/BJZ/35037, naar aanleiding van WOB-verzoek RTL Nederland. Geraadpleegd op http://media.rtl.nl/media/actueel/rtlnieuws/2011/WOBdocument2.pdf, 9 maart 2011.

Report to the President 2010 (2011, April 15). Washington (DC): Information Security Oversight Office. Geraadpleegd op http://www.archives.gov/isoo/reports/2010-annual-report.pdf, 22 april 2011.

SAMENVATTING

Wanneer publiekelijk bekend wordt dat er geheimen gelekt zijn, is dat vaak spannend. Spannend omdat het sensationeel kan zijn: men krijgt een inkijkje in een wereld die men niet zou mogen hebben. Het kan ook spannend zijn omdat er belangen op het spel staan: personen en organisaties kunnen schade oplopen door het lekken van geheimen. In deze thesis wordt een poging gedaan inzichtelijk te krijgen waarom er geheimen zijn, hoe en waarom deze gelekt worden en welke maatregelen hiertegen te nemen zijn: Welke factoren spelen een rol bij het intentioneel en verwijtbaar compromitteren van gerubriceerde en gevoelige informatie?

In het onderzoek lag de focus op de Rijksoverheid in de periode 2004-2010. Aan de hand van onder meer een literatuuronderzoek, het raadplegen van jurisprudentie, het uitvoeren van een enquête onder de Beveiligingsambtenaren van de departementen (strategisch verantwoordelijk voor informatiebeveiliging) en het afnemen van semi-gestructureerde interviews bij materiedeskundigen is geprobeerd bovenstaande vraagstelling te beantwoorden.

Op basis van het onderzoek kan gesteld worden dat geheimen er zijn om belangen te beschermen. Er is dan sprake van gevoelige informatie, waarbij kennisname door niet gerechtigden nadelige gevolgen kan hebben voor de belangen van – in het kader van deze thesis – de Staat, van zijn bondgenoten of van één of meer ministeries. Er kunnen zowel formele geheimen als materiële geheimen onderscheiden worden. Als (al dan niet) gevoelige informatie correct gerubriceerd is (het staat er letterlijk op) kan men spreken van een 'formeel geheim'. Als gevoelige informatie niet correct gerubriceerd is (het staat er letterlijk niet op) maar de houder van de informatie begreep of had behoren te begrijpen dat de informatie gevoelig is en openbaarmaking een afbreukrisico vormt, dan kan men spreken van een ‘materieel geheim’. Het belang van geheimen kan vanuit een ethische, een juridische en een politiek-bestuurlijke dimensie beschouwd worden. In alle drie de dimensies kunnen zowel argumenten voor als tegen lekken gevonden worden.

Geheimen kunnen worden gelekt om persoonlijke, institutionele of publieke belangen te dienen. Er is dan sprake van intentioneel handelen (opzet). Daarnaast kunnen geheimen gelekt worden vanwege bijvoorbeeld onachtzaamheid, onkunde of onprofessioneel handelen. Er is dan sprake van verwijtbaar handelen (schuld), de actor heeft namelijk de (reële) mogelijkheid zich anders te gedragen. Hiervan is bijvoorbeeld sprake wanneer de actor geen gebruik maakt van de middelen die ter beschikking staan om geheimen te beschermen. Geheimen kunnen ook uitlekken door niet verwijtbaar handelen (zoals overmacht), maar dat valt buiten het kader van deze thesis. Intentioneel lekken geschiedt door bewuste mondelinge, fysieke en digitale overdracht van informatie. Verwijtbaar lekken geschiedt niet bewust, maar bijvoorbeeld door het verlenen van ongeautoriseerde toegang, zich te verspreken, mee te laten lezen of luisteren, het verliezen van documenten en digitale gegevensdragers en een onjuiste wijze van verwerken, opbergen, verzenden of vernietigen van gevoelige informatie.

Er zijn meerdere omstandigheden die lekken in de hand kunnen werken. In de eerste plaats is dat de totstandkoming van gerubriceerde informatie. Idealiter is de verzameling gerubriceerde informatie gelijk aan de verzameling gevoelige informatie. In de praktijk is dit niet volledig het geval, er is zowel informatie die ten onrechte gerubriceerd is, als informatie die ten onrechte niet gerubriceerd is. In deze thesis wordt dit door middel van het Eclips Model beschreven. Beide kunnen leiden tot het lekken van geheimen. Daarnaast is geconstateerd dat een geheim de betekenis en beschermbaarheid verliest als deze binnen een grote kring bekend of toegankelijk is. Ook practical drift – the slow, steady uncoupling of local practice from written procedure – is een van de oorzaken van het niet volgen van maatregelen ter bescherming van gevoelige en gerubriceerde informatie. Voorts is de mogelijkheid tot lekken de afgelopen vijftien jaar toegenomen door de ontwikkelingen in de technische infrastructuur zoals e-mail, internet, goedkope digitale gegevensdragers met grote capaciteit, gepaard gaande met onvoldoende en verkeerde technische middelen en onvoldoende aandacht voor bewustwording. De ontwikkeling naar 'Het Nieuwe Werken' doet het aantal kwetsbaarheden aangaande verwijtbaar lekken toenemen als hier vanuit het perspectief van security onvoldoende aandacht voor is. Tot slot kunnen ingrijpende bezuinigingen, reorganisaties en een (gevoel van) onheuse bejegening lekken uit frustratie en wrok in de hand werken.

De mogelijke maatregelen zijn technisch en organisatorisch van aard. Technische maatregelen bestaan uit hard-copy en digitale maatregelen. Door middelen en technieken eenvoudig en ruimschoots ter beschikking te stellen zal men deze eerder gebruiken. Het kan hierbij gaan om zaken als bergmiddelen, usb-sticks, versleutelprogramma's, veiligheidsenveloppen en GSM-cryptotelefoons. Maar ook het uitsluitend laten afdrukken van bepaalde gerubriceerde informatie op kopieerbeveiligd en genummerd papier kan bijdragen aan het terugdringen van lekken. Organisatorische maatregelen bestaan onder andere uit bewustwording, procedures, sanctioneren en een goed werkende klokkenluidersregeling voor het intern en extern melden van vermoedens van misstanden. Procedures kunnen variëren van het toepassen van het 'vier ogen principe' ter voorkoming van overrubricering, waarbij de rubricering op bepaalde informatie alleen kan plaatsvinden na accordering door een leidinggevende, tot het periodiek herzien van gerubriceerde informatie en deze - indien mogelijk - vervolgens actief openbaar te maken conform de Wet openbaarheid van bestuur. Bewustwording dient primair gericht te zijn op de personen die toegang hebben tot gerubriceerde informatie. Deze groep zou bij aanvang van hun functie en vervolgens periodiek verplicht voorgelicht moeten worden over het belang van gerubriceerde informatie (bij voorkeur aan de hand van casuïstiek uit de eigen organisatie), het bepalen van het rubriceringsniveau en de omgang met gerubriceerde informatie (regels, procedures en middelen voor een juiste verwerking, opslag en transport). Vanuit organisaties kan ook meer aandacht besteed worden aan de achtergrond van het falen, zoals het Swiss Cheese Model - dat ingaat op de gelaagdheid van maatregelen - en practical drift. Deze maatregelen kunnen dan proportioneel afgestemd worden op de belangen, de dreigingen en de kwetsbaarheden van de gerubriceerde informatie van de organisatie.

Door het toepassen van een gelaagdheid aan onafhankelijk van elkaar werkende maatregelen kan het risico op lekken teruggedrongen worden. Verwijtbare lekken zijn vaak ook vermijdbare lekken. Intentionele lekken laten zich lastiger beteugelen, er blijven namelijk altijd restrisico's bestaan. Daarom is actieve handhaving van de maatregelen noodzakelijk en zou men de neiging kunnen onderdrukken om bij de eerste ernstige inbreuk op de maatregelen zwaardere maatregelen in te voeren dan de maatregelen die toch al niet gevolgd werden.