FACULTEIT
RECHTSGELEERDHEID

Spionage en activiteiten van inmenging door buitenlandse inlichtingendiensten.

De reactie van de Belgische inlichtingen - en veiligheidsdiensten onderzocht.

Masterproef neergelegd tot het behalen van
de graad van Master in de criminologische wetenschappen
door (00805081) **ANTUNOVIC Kresimir**

Academiejaar 2013-2014

Promotor :
Prof. dr. Marc COOLS

Commissarissen :
Prof. dr. Gert VERMEULEN
Msc. Veerle PASHLEY

"He that will not apply new remedies must expect new evils; for time is the greatest innovator."

Francis Bacon , "Of Innovations"

Trefwoorden :

- Spionage
- Inmenging
- Counterintelligence
- Inlichtingen – en veiligheidsdiensten

Verklaring inzake toegankelijkheid van de masterproef criminologische wetenschappen

Ondergetekende,

ANTUNOVIC Kresimir (00805081

geeft hierbij aan derden,

zijnde andere personen dan de promotor (en eventuele co-promotor), de commissarissen of leden van de examencommissie van de master in de criminologische wetenschappen,

[de toelating] ~~[geen toelating~~] *(schrappen wat niet past)*

om deze masterproef in te zien, deze geheel of gedeeltelijk te kopiëren of er, indien beschikbaar, een elektronische kopie van te bekomen, waarbij deze derden er uiteraard slechts zullen kunnen naar verwijzen of uit citeren mits zij correct en volledig de bron vermelden.

Deze verklaring wordt in zoveel exemplaren opgemaakt als het aantal exemplaren waarin de masterproef moet worden ingediend, en dient in elk van die exemplaren ingebonden onmiddellijk na het titelblad.

Datum: 15/08/2014

Handtekening: ……

VOORWOORD

Deze masterproef kwam tot stand met het oog op het behalen van het masterdiploma in de Criminologische wetenschappen aan de Universiteit van Gent. De verwezenlijking van deze thesis kon niet tot stand gekomen zijn zonder de steun en bereidwilligheid van de volgende personen.

In de eerste instantie gaat mijn oprechte dank uit naar de heer prof. dr. Marc Cools wie fungeerde als mijn promotor en mij als eerste liet kennismaken met de wereld van de inlichtingen – en veiligheidsdiensten. Zijn kennis en raad hebben mee vorm gegeven aan de fundering en ontwikkeling van deze thesis evenals zijn feedback en steun. Het is een enorme eer geweest hem als promotor te hebben en ik heb ook zeer veel van hem geleerd.

Een bijzonder woord van dank gaat naar de leden van de Algemene Dienst Inlichtingen en Veiligheid & de Veiligheid van de Staat evenals het federaal parket. Ook een persoonlijke dank aan Kristof Clerix die zijn visie en kennis over de inlichtingendiensten wou delen.

Ten slotte wens ik mijn ouders te bedanken voor hun onvoorwaardelijke steun in mijn studies. Met name mijn moeder die een enorme steun was en mij heeft geleerd dat volharding loont. Ongeacht de tegenslagen die men soms in het leven ervaart.

INHOUDSOPGAVE

LIJST VAN AFKORTINGEN

ADIV/GRS	Algemene Dienst Inlichtingen en Veiligheid
ACOS - IS	Assistant Chief of Staff Intelligence and Security
AIVD	Algemene Inlichtingen - en Veiligheidsdienst
BIM	Bijzondere Inlichtingenmethoden
BISC	Belgian Intelligence Studies Centre
CIA	Central Intelligence Agency
CIV	College voor Inlichtingen en Veiligheid
COMINT	Communication Intelligence
ELINT	Electronic Intelligence
EYES	Samenwerkingsverband tussen buitenlandse inlichtingendiensten
FAPSI	Speciale Communicatie en Informatie Dienst v/d Russische Federatie
FSB	Federale Veiligheidsdienst van de Russische Federatie
GCHQ	Hoofdkwartier voor Regeringscommunicatie
GRU	Russische Militaire Inlichtingendienst
HUMINT	Human Source Intelligence
IMINT	Imagery Intelligence
KGB	Comité voor Staatsveiligheid van de Russische Federatie
MASINT	Measurement and Signature Intelligence
MCIV	Ministerieel comité voor inlichtingen en veiligheid
MI5	Military Intelligence, Section 5
MI6	Military Intelligence, Section 6
MSS	Ministerie voor Staatsveiligheid van de Volksrepubliek China
NOC	No Operational Cover
NSA	National Security Agency
OSINT	Orgaan van de Coördinatie en de Analyse van de Dreiging
SIGINT	Signal Intelligence
SVR	Dienst Buitenlandse Veiligheid van de Russische Federatie
TECHINT	Technical Intelligence
VSSE	Veiligheid van de Staat

LIJST VAN FIGUREN

INLEIDENDE BESCHOUWINGEN

1. INLEIDING

Sinds mensenheugenis bestaat spionage en buitenlandse inmenging. Volgens het Boek van Joshua is spionage het tweede oudste beroep van de mensheid. Vanaf het Hittitische rijk tot de Oudheid, de Middeleeuwen en iedere opeenvolgende geschiedkundige periode vinden we het gebruik van spionnen terug.[1] Weliswaar werden spionnen voornamelijk op militair vlak ingezet om informatie in te winnen over de zwaktes of sterktes van vijandige legers. Hun nut en inzet wordt nooit onderschat en wordt zelfs nauwkeurig beschreven in 'De Kunst van het Oorlogsvoeren' van de Chinese strateeg en wijsgeer Sun Tzu.[2]

"Wees tactvol! Werkelijk tactvol! Spionage kan overal worden gebruikt." […]"Het is belangrijk erachter te komen wie de vijand als agent heeft gestuurd om u te bespioneren. Koop hem om zodat hij u dient. Zorg voor hem en geef hem instructies. Zo kunnen dubbelagenten worden gerekruteerd en ingezet."

Toch zal er een evolutie en verbreding komen in het inwinnen van informatie door spionnen vanaf de 16de eeuw. Enerzijds zal het inwinnen van inlichtingen van de economische productie en ontwikkeling ook een belangrijke doelstelling worden voor spionnen van het andere kamp. Anderzijds zullen ook de eerste vormen van politieke en economische inmenging voor het eerst zichtbaar worden in Italië, Zwitserland en het Vaticaan. Spionage zal blijven evolueren, zowel op het vlak van inzet als het gebruik van middelen. Het wordt een professioneel beroep met volwaardige opleidingen en zal zijn hoogtepunt kennen tijdens de Koude Oorlog. De hoofdstad Brussel zal een zeer belangrijke rol op zich nemen als smeltkroes voor verschillende buitenlandse inlichtingenofficieren en agenten. Brussel is, na Genève en New York, immers de derde stad met het grootste aantal diplomaten en is het centrale punt van Europa, de thuiszetel van de NAVO en talrijke Europese instellingen. [3]

Na de Koude Oorlog is het zeer lang stil geweest rond deze op 'James Bond' gelijkende toestanden. De hedendaagse moderne tijd met zijn wereldwijde samenwerkingsverdragen zouden het beeld scheppen dat dergelijke feiten niet meer zouden voorvallen.

---

[1] LERNER, L. en LERNER, B., *Encyclopedia of Espionage, Intelligence & Security,* III, Detroit, Gale, 2004, p.317-351

[2] GRIFFITH, S.B., *Sun Tzu. De Kunst van het oorlogsvoeren,* Kerkdriel, Librero, 2010, p.231-239

[3] CLERIX, K.,*Spionage in het hart van Europa*, België, Wereldmediahuis, 2006, p.3

Niets is minder waar want "*The Great Game*", zoals Kipling het ooit noemde[4], is nooit uitgespeeld. Spionage en inmenging zijn nog nooit op dergelijk grote schaal gebeurd als nu. De hedendaagse actualiteit en media getuigen hiervan nadat vele inlichtingenoperaties zijn geopenbaard door klokkenluiders zoals Julian Assange, Chelsea Manning en Edward Snowden. Het enige verschil met het verleden is het gebruik van hoogtechnologisch digitaal vernuft dat een extra dimensie heeft gecreëerd in het spel. De spelregels zelf zijn nooit veranderd en de inzet om informatie is nog steeds even hoog.

1.1. Situering onderwerp & motivering

De laatste jaren heeft de actualiteit nog nooit zo veel gepubliceerd over spionage als tijdens de Koude Oorlog; "Europa pikt spionage door VS niet meer"," Is privacy dood?", "De cultuur van het geheim neemt toe". "Meer bijzondere inlichtingen methoden ingezet in spionage-onderzoeken", "Klokkenluider Snowden bezit geheime documenten over cyberaanvallen in China", "NSA vooral geïnteresseerd in buitenlandbeleid EU", "Slecht rapport voor Winants", "Merkel werd bespioneerd vanuit VS-ambassade in Berlijn", "Britse geheime dienst bespioneerde Belgacom", "Kwaadaardige software NSA op 50.000 netwerken" enz. Al deze krantenkoppen zijn slechts het topje van de ijsberg van gerapporteerde gebeurtenissen van spionage en activiteiten van inmenging in de media. En dit in slechts in enkele jaren tijd.

Onze maatschappij begint zich meer en meer bewust te worden van het fenomeen van spionage en buitenlandse inmenging. Ook is er een digitale evolutie bezig die deze activiteiten vergroot en nieuwe dimensies geeft. Maar hoe kunnen inlichtingen – en veiligheidsdiensten zich hiertegen wapenen? We krijgen de indruk dat deze diensten in ons land hier niet effectief in kunnen optreden ondanks de vergroting van bewegingsruimte die door de Bijzondere Inlichtingen Methoden (BIM) wetgeving is geregeld. Doch mogen we niet vergeten dat we niet precies weten hoe deze diensten opereren en hoe omvangrijk de effectieve opsporing en vervolging is waaruit inlichtingenstudies zijn voortgevloeid.

Het doel van inlichtingenstudies is het bestuderen van de geschiedenis en werking van inlichtingendiensten evenals de veiligheidsdiensten die met inlichtingendiensten samen werken.

[4] KIPLING, K., *Kim*, Hertfordshire, Wordsworth classics, 1993, p.213

In de jaren zeventig richt men het Centrum voor Politiestudies (CPS) op dat zich inzet tot het organiseren van studiedagen, het publiceren van Cahiers Politiestudies evenals wetenschappelijk onderzoek naar de entiteit van de politie. Hierna werd het Belgium Intelligence Studies Association (BISA) opgericht dat het eerste initiatief was door de Veiligheid van de Staat zelf. Door dit initiatief trachtte de Veiligheid van de Staat de inlichtingendiensten en de wetenschappelijke gemeenschap met elkaar in contact te brengen. Dit met het oog op het samenwerken aan oplossingen van maatschappelijke vraagstukken die verband houden met het verzamelen van inlichtingen. Na een korte bestaansperiode wordt het Belgium Intelligence Studies Centre (BISC) in het leven geroepen. Het Belgium Intelligence Studies Centre organiseert op regelmatige basis, en al dan niet in samenwerking met het Centrum voor Politiestudies, studiedagen en Cahiers over onderzoeken naar de werking van de inlichtingendiensten. Inlichtingenstudies hebben oog voor een brede waaier aan specifieke fenomenen zoals spionage, inmenging, extremisme en radicalisme, proliferatie, terrorisme, criminele organisaties, het behoud van het Wetenschappelijk, Economisch en Politiek potentieel (WEP) en sekten.

Inlichtingenstudies baseren zich juridisch op twee belangrijke wetgevingen. Enerzijds de wet van 18 juli 1991 die de regeling van het toezicht op de politie – en inlichtingendiensten, evenals het Coördinatieorgaan van de Dreigingsanalyse (CODA), bepaalt. De bevoegdheid van controle op de juiste naleving van deze wetten ligt in bij het Comité I. Hiernaast is er de wet van 30 november 1998 inzake de houdende regeling van de inlichtingen en veiligheidsdienst. Sinds 2010 is deze wet uitgebreid met de Bijzondere Inlichtingen Methode (BIM) en de wet op de veiligheidsmachtigingen.

Als we de organisatorische aspecten van inlichtingenstudies in België naderbij bekijken, zien we dat er twee actoren binnen de ‘Belgium Intelligence Community‘ een belangrijke rol spelen. Enerzijds is er het ‘Ministerieel Comité voor Inlichtingen en Veiligheid’ (MCIV) dat de algemene politiek inzake het verzamelen en verwerken van inlichtingen vastlegt. Eveneens coördineert het de Veiligheid van de Staat en de Algemene Dienst Inlichtingen en Veiligheid, waarbij ze hun prioriteiten bepaalt. Als laatste bepaalt ze de politiek inzake de bescherming van gevoelige informatie en geeft ze advies over politieke en legislatieve initiatieven op het vlak van inlichtingen en veiligheid. Anderzijds is er het ‘College voor inlichtingen en Veiligheid’ (CIV). Dit college voert de beslissingen uit van het ‘Ministerieel Comité voor Inlichtingen en Veiligheid.

Inlichtingenstudies bevindt zich binnen een deeldomein van de criminologie. Daarom levert deze thesis een belangrijke meerwaarde op voor de criminologie. De klemtoon van deze bijdrage is het beschrijven, exploiteren en constateren van enerzijds het fenomeen spionage en buitenlandse inmenging in België. Anderzijds tracht het de mogelijke formele en informele reacties, die zowel Belgische inlichtingen - en veiligheidsdiensten als het Federaal Parket ondernemen bij constatering van inbreuken van spionage en buitenlandse inmenging, te schetsen.

Zelf is mijn interesse in inlichtingenstudies opgewekt toen ik, na de middelbare school, werd toegelaten tot de Voorbereidende Divisie van de Koninklijke Militaire School. Hier kreeg ik les van prominente leerkrachten, en één van hen was de heer Jean-Louis Hoëz. Deze man gaf (Krijgs)geschiedenis en vertelde tijdens de lessen vaak over de verschillende militaire diensten waaronder de inlichtingendiensten. Dit heeft mijn interesse zodanig opgewekt dat ik mijzelf ben gaan verdiepen in de werking van de Algemene Dienst Inlichtingen en Veiligheid. Hierna ben ik begonnen met mijn studies criminologie waar ik in het derde jaar het vak 'Politiële en Gerechtelijke studies' kreeg. Dit werd onderricht door Prof. dr. Paul Ponsaers, Dr. Antoinette Verhaege en mijn promotor Prof. dr. Marc Cools. De boeiende lessen van professor Cools verschaften mijn medestudenten en ikzelf een brede en duidelijke inleiding over de werking van de Belgische en buitenlandse inlichtingen- en veiligheidsdiensten. Dit heeft mijn interesses en kijk op inlichtingen – en veiligheidsdiensten zodanig verbreed waardoor ik tot dit onderwerp ben gekomen.

1.2. Doel en situering van het onderzoek.

Het gekozen onderzoeksdoel is vele malen breder dan het eerst doet vermoeden. De hoofddoelstelling in dit onderzoek is tweezijdig. Enerzijds tracht deze bijdrage het fenomeen van spionage en buitenlandse inmenging in België te beschrijven, te exploiteren en constateren.[5] Anderzijds tracht het de mogelijke formele en informele reacties, die zowel Belgische inlichtingen - en veiligheidsdiensten als het Federaal Parket ondernemen bij constatering van inbreuken van spionage en buitenlandse inmenging, te schetsen. . Rekening houdend met de omvang en de tijdsduur waarin deze thesis geschreven is, is het niet mogelijk om exhaustief te werk te gaan.

[5] MARSHALL, C., en ROSSMAN, G.B., *Designing qualitative research,* Thousand Oaks, Sage, 1999, p.38

Vertrekkend vanuit een beschrijvend kader zal langzaam de hedendaagse aanpak en reactie opgebouwd worden en naar het einde toe een kritische visie gevormd worden omtrent de knelpunten waar verbetering aangewezen is.

Niet alleen het beschrijven van de verschillende concepten komt uitgebreid aan bod maar ook de doelwitten, de herkenning van spionagepraktijken of spionnen, technologische vooruitgang, praktijkwerking en de toetsing hiervan aan de bestaande Belgische wetgeving. Het realiseren van deze doelstellingen zal gebeuren door een eigen gevormde structuur te volgen.

Allereerst zal er een beeld geschetst worden van de huidige vormen van spionage en buitenlandse inmenging en hun manier van werken. Dit zal worden ondersteund door een vergelijking te maken van internationale definities en theorieën. Hierdoor krijgt de lezer inzicht in de moeilijkheden van de opsporing van deze misdrijven. Hierna volgt een opsomming van de verschillende soorten Belgische inlichtingen – en veiligheidsdiensten met ieders doelen, werking, specialisaties, sterktes en zwaktes. Dit zowel in het verleden als het heden, gebruik makend van historisch onderzoek en hedendaagse (praktijk) handboeken Wat ook zeer belangrijk is, en verder in de thesis aan bod zal komen, is de gehele wetgevende context waarbinnen de opsporing, vervolging en straftoemeting valt. Dit alles zal gecontroleerd worden door het bevragen van sleutelfiguren van de inlichtingen – en veiligheidsdienst evenals deze van het Federaal Parket.

We weten nu dat spionage en inmenging terug heel actueel zijn. Ook de technologische vooruitgang en ontwikkelingen spelen hierin een belangrijke rol. Technologie heeft immers de strijd om inlichtingen verlegd naar een totaal andere dimensie. Maar een belangrijke vraag die men nog steeds kan stellen is; waarom gebeurt spionage en buitenlandse inmenging in de 21ste eeuw en waarom gebeurt dit in het bijzonder in België?

Door de vele internationale verdragen, diplomatieke samenwerkingen en supranationale wetten zou men toch verwachten dat spionage en buitenlandse inmenging slechts nog een kleine rol vervullen. Hierbij kunnen de volgende vragen worden gesteld. Welke informatie tracht men te verzamelen door spionage? Welke bedrijven of organisaties zijn het doelwit? Welke personen of beroepen worden vooral in het vizier genomen op dit moment? Over welke middelen beschikt men om deze inlichtingen te verzamelen? Waarom nu nog inmenging door buitenlandse mogendheden? En hoe verloopt dit heden ten dage?

Om een adequaat antwoord te formuleren op deze vraag moeten we vooral kijken naar de werking van de contraspionage in ons land en de aanpak van deze criminele feiten. Daarbij moeten we ook de onderlinge samenwerking bestuderen van de contraspionagedienst van ADIV, VSSE en het Federaal parket. Ook mogen we niet vergeten dat deze diensten een nauwe samenwerking hebben met de buitenlandse inlichtingen – en veiligheidsdiensten. De werking van deze diensten en de samenwerking van deze diensten met andere diensten moeten eerst door grondige case studies onderzocht worden.

Na deze studie moeten ze, in de mate van het mogelijke, vergeleken worden met de hedendaagse werking van de inlichtingen – en veiligheidsdiensten. Het zijn immers diensten die voor vele buitenstaanders gehuld zijn in een wazige nevel en waarover concrete informatie vaak schaars is. Het doel van deze thesis is er in de eerste plaats niet op gericht om een volledig gedetailleerde beschrijving te geven van opleidingen, tactische opstellingen en werkwijzen. Doch zullen er methoden en manieren van opereren beschreven worden die noodzakelijk zijn om een beter zicht te krijgen op de feitelijke werking van de diensten. Dit zal van belang zijn om deze werking te toetsen aan het wettelijk kader waarbinnen deze plaatsvindt in zoverre de wetgeving hiertoe strekt.

1.3. Onderzoeksvraag en deelvragen

De thesis zal opgebouwd zijn uit één centrale vraag die uiteenvalt in verschillende deelvragen.[6] De hoofdvraag onderzoekt *'de reactie van de Belgische inlichtingendiensten – en veiligheidsdiensten op spionage en activiteiten van inmenging door buitenlandse inlichtingendiensten'*.

De deelvragen die hieruit voortvloeien zijn;

§1 Wat houdt spionage en inmenging in en welke soorten vormen van spionage en inmenging bestaan er?

Bij deze vraag wordt er dieper ingegaan op de vele verschillende vormen van spionage en inmenging in de 21ste eeuw waarin technologische vooruitgang een steeds belangrijkere rol inneemt.

[6] Goethals, J., Pauwels, L. (2008). Onderzoeksvragen. In: Goethals J., Pauwels L. (Eds.), *Kwantitatieve en kwalitatieve criminologische onderzoeksmethodes: een introductie.*. Leuven: Acco, 46-68.

§2. Welke buitenlandse inlichtingen - en veiligheidsdiensten vormen de grootste bedreiging in België en wat voor specifieke informatie zoeken zij?

Met deze deelvraag wordt er dieper ingegaan op de doelwitten ban buitenlandse inlichtingendiensten waaronder personen, bedrijven, technologieën worden verstaan en mogelijk aantrekkelijker zijn voor buitenlandse mogendheden om inlichtingen over in te winnen. Allereerst zal er specifieker gekeken worden naar de manier van werken om informatie in te winnen. Werken ze met een bepaald 'cover' zoals diplomaten of NOC's?[7] Welke methoden passen ze toe om mensen te overtuigen en in welke mate is dit succesvol? Ook zullen de verschillende soorten buitenlandse inlichtingendiensten besproken worden om erna aan te tonen hoe men deze tegengaat.

§3. VSE, ADIV en het wettelijk kader – Wie zijn ze? Wat zijn hun opdrachten en hun bevoegdheden?

Deze vraag schetst een beeld van hedendaagse Belgische inlichtingen - en veiligheidsdiensten en hun opdrachten. Na een korte reflectie van het verleden zullen de huidige diensten gedetailleerd en gestructureerd aan bod komen.

§4. Wat is counterintelligence?

"If the spy is the sword, the counterspy is the shield"[8]. Counterintelligence is de reactie op buitenlandse dreigingen van spionage en inmenging. Een nauwkeuriger beeld wordt ervan geschetst bij punt 3 - uitleg van de begrippen. In de thesis zal de werking van counterintelligence aan bod komen.

En wat houdt de Belgische counterintelligence in?

Dit deel vervolledigt het deel over de counterintelligence. Er zal getracht worden een vergelijking te maken met de Belgische counterintelligence, in die mate dat er informatie over bestaat en door middel van interviews mag medegedeeld worden.

[7] NOC ', uitgesproken als 'knock', betekent 'No Operational Cover'.
[8] BURTON, B., *Top secret : A Clandestine Operator's Glossary of Terms*, Boulder, Paladin Press, 1986, p.30

§5. Hoe verloopt de samenwerking tussen ADIV, VSSE en het Federaal Parket?

Tenslotte staan we nog even stil bij de samenwerking tussen de drie belangrijke diensten en hoe zij uiteindelijk reageren als er voldoende bewijs is van individuen die een misdrijf plegen met betrekking tot spionage of inmenging.

1.4. Onderzoekstechnieken

Zoals in de vorige paragrafen werd aangegeven, zal de thesis gebruik maken van drie soorten onderzoekstechnieken.[9] We onderscheiden de literatuurstudie, de casestudy en kwalitatieve interviews. De redenen voor de gekozen technieken zullen hier worden uiteengezet en beargumenteerd. Het gekozen thesisonderwerp is qua concept moeilijk te onderzoeken door de discretie die gehanteerd wordt door de inlichtingen – en veiligheidsdiensten. De onderzoekspopulatie, namelijk spionnen, inlichtingen – en rekruteringsofficieren, contra-agenten en de diensten zelf van deze onderzoekspopulatie leven in grootste anonimiteit. Deze anonimiteit is immers hun bescherming en instrument. Dus het vinden van dergelijke respondenten is zo goed als uitgesloten.

Bedrijven of diensten die het slachtoffer zijn geweest van spionage, zullen hierover zo goed als geen informatie vrijgegeven. Bedrijven willen immers geen imagoschade lijden en de kans bestaat dat ze hierover niet mogen praten omdat het onderzoek nog steeds loopt door de Veiligheid van de Staat. Hierdoor is een grondig kwantitatief en kwalitatief onderzoek uitgesloten. Ook roepen de weinige bestaande en concrete buitenlands empirische gegevens de gedachte op dat het realiseren van een kwantitatief of kwalitatief onderzoek zo goed als niet mogelijk is, en dit zeker in een masterjaar. Daarom is er geopteerd voor een bronnentriangulatie om zo veel mogelijk uit het onderzoek te kunnen halen.

Al deze argumenten leiden in de eerste plaats tot de keuze van het bureauonderzoek, en specifieker het literatuuronderzoek. De kennisbronnen zullen voornamelijk bestaan uit buitenlandse wetenschappelijke literatuur, historische literatuur en bibliografieën met betrekking tot het onderzoeksdoel. Door middel van bevindingen uit de literatuurstudie kan een kritische reflectie worden gemaakt over de counterintelligence en of het al dan niet een nuttige tool kan vormen in de bestrijding van spionage en activiteiten van inmenging.

[9] DECORTE, T. (2011). Methoden van onderzoek: ontwerp en dataverzameling. Gent: Academia Press, 265p.

Het gebruik van buitenlandse literatuur is te wijten aan het weinige bestaande Belgisch onderzoeken op vlak van counterintelligence. Er bestaan gespecialiseerde boeken over bedrijfsspionage maar vertellen niets meer over de werking van de inlichtingen - en veiligheidsdiensten. Voorts mogen we niet vergeten dat België reeds in het verleden is beïnvloed geweest door de Duitse, Engelse, Franse & Amerikaanse manier van counterintelligence.

Als tweede techniek is er geopteerd voor de casestudy. [10] De casestudy zal een diepgaand en integraal inzicht geven in een klein domein en zal zich richten tot enkele gekozen cases. De cases gaan over Belgische gebeurtenissen op het gebied van spionage en inmenging; het dossier Kolonel Binet, het dossier Rainer Rupp, het dossier Krupka, enz. Door vooral te werken in de diepte zal er vooral een holistisch beeld geschetst worden van de beweegredenen die hebben geleid tot het plegen van deze activiteiten. De details van de "hunt for intelligence" en de counterintelligence op Belgische bodem spelen een cruciale rol om de literatuurstudie aan te vullen en te beargumenteren.

Het interview is de derde techniek in dit onderzoek. Het feit dat deze techniek uitermate geschikt is om te peilen naar extra informatie[11], evenals verzamelde informatie te toetsen aan de realiteit, maakt het een geschikte keuze. We opteren voor het open - of diepte-interview. De respondenten zullen voornamelijk bestaan uit selectief gekozen sleutelfiguren die open staan voor een interview. De gekozen sleutelfiguren van de onderzoekspopulatie zijn Kristof Clerix (journalist) alsook medewerkers van de ADIV, de VSSE en het federaal parket. Zij zullen fungeren als knowledgeable agents en hopelijk zeer specifieke en gedetailleerde antwoorden (mogen) geven die de laatste hiaten in de thesis zullen opvullen. Verder kunnen ze mij ook in contact brengen met mogelijke andere sleutelfiguren.

Gezien de kleinschaligheid van deze thesis, de korte tijdspanne en de grote delicate gevoeligheid van informatie is het onmogelijk om de volledige populatie van counterintelligence agenten te interviewen. Dit in het achterhoofd houdende is het belangrijk een planning bij te houden en al vroeg contact te zoeken met deze personen. Het interviewen zal afgenomen worden op een wederzijds afgesproken tijdstip en de vragen zullen op voorhand overgemaakt worden.

[10] VANDERHALLEN, M., VERVAEKE, G., OPDEBEECK, A., GOETHALS, J. (2002). Het ontwerp van een gevalsstudie. In: *Criminologie in actie*. Brussel: Politeia, 419-444.
[11] DECORTE, T., ZAITCH, D. (eds.), *Kwalitatieve methoden en technieken in de criminologie*, Leuven-Den Haag, Acco, 2010, p. 204-205.

Zodoende kunnen de respondenten hun antwoorden voorbereiden en mogelijk gedetailleerde informatie geven. Hierbij zullen de respondenten ook geïnformeerd worden over het doel van het onderzoek. Wel is het belangrijk om de correcte ethische regels te hanteren inzake het afleggen van een interview.[12]

Zo zal er eerst op verbale wijze een informed consent bekomen worden van de gekozen respondenten. Dit zal samen gaan met een verduidelijking over wat het onderzoek precies inhoudt en dat de vertrouwelijkheid gegarandeerd wordt. Anonimiteit is uiterst belangrijk op het gebied van inlichtingen - en veiligheidsdiensten. Maar de geselecteerde respondenten zijn enerzijds publiekelijk gekende personen die eerder al interviews hebben afgelegd zonder enige vorm van anonimiteit. Als één van bovenstaande respondenten, of mogelijke nieuwe respondenten, wenst dat het interview gedeeltelijk anoniem moet gebeuren, zal enkel de rang/functie en zijn of haar initialen gebruikt worden. Bij volledige anonimiteit zal de letter 'X' gebruikt worden. Gedurende elk moment van het interview kunnen de respondenten hun medewerking stopzetten.

[12] X, (2010/11/01) Economic and Social Research Council. [WWW]. CBPR Ethics Guide: Framework for Research Ethics 2010 Updated September 2012, http://www.esrc.ac.uk/_images/Framework-for-Research-Ethics_tcm8-4586.pdf.[05/11/2013]

DEEL I : SPIONAGE

“But I don’t want to go among mad people," Alice remarked.
"Oh, you can’t help that," said the Chesire Cat: "we’re all mad here. I’m mad. You’re mad."
"How do you know I’m mad?" said Alice.
"You must be or you wouldn’t have come here.”

Lewis Carroll, Alice in Wonderland

1. INLEIDING

Spionage is een zeer ruim begrip. Als we spionage in zijn volledigheid willen omvatten kunnen we stellen dat; *alle pogingen en handelingen die gericht zijn op het opzoeken, het verstrekken, te weten komen van nuttige, gevoelige of geclassificeerde informatie, gebruik makende van clandestiene methoden, teneinde een voordeel over anderen te verwerven*. [13]Dit in het bijzonder politieke informatie maar ook militaire, economische, technologische of wetenschappelijke informatie.[14] In de thesis zal zowel militaire, wetenschappelijke als economische spionage aan bod komen. Militaire spionage handelt over alle activiteiten van spionage die de werking, strategieën, kracht en/of het Belgisch militair geheim in gevaar kunnen brengen. Wetenschappelijke spionage handelt over activiteiten van spionage die betrekking hebben tot het stelen van vertrouwelijke en geheime technologische ontwikkelingen. Deze ontwikkelingen kunnen zich situeren over verschillende doelgebieden zoals geneeskunde, chemie, fysica, elektronica, enz. Als laatste volgen de activiteiten van economische spionage.[15]

We onderscheiden spionage tussen twee concurrerende (Belgische) bedrijven of spionage door inlichtingendiensten of vreemde mogendheden om bepaalde kennis in handen te krijgen. Deze kennis dient om het landsbelang van de buitenlandse inlichtingendienst of mogendheid te ondersteunen. In deze thesis zullen deze laatste ontwikkelingen besproken worden. De drie vormen van spionage zullen betrekking hebben op gebeurtenissen en de huidige problemen van deze activiteiten in België. De hedendaagse technologische vooruitgang zal ook een belangrijke rol gaan spelen, in het bijzonder over de nieuwe dimensie die is gecreëerd onder de vorm van cyberspionage.

[13] GOULDEN, J.C., T*he dictionary of espionage. Spyspeak into English*, New York, Dover Publications, 2012, 256 p.
[14] X, *Brochure : De Veiligheid van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.18
[15] NASHERI, H., Economic espionage and industrial spying, Cambridge, Cambridge university press, 2005, 270p.

2. DEFINITIE

Een algemene definitie voor spionage bestaat niet. Artikel 8, 1°, a. van de organieke wet van 30 november 1998, die de werking van de inlichtingendiensten bepaalt omschrijft spionage als ; *" het opzoeken of het verstrekken van inlichtingen die voor het publiek niet toegankelijk zijn en het onderhouden van geheime verstandhoudingen die deze handelingen kunnen voorbereiden of vergemakkelijken*."[16]. Deze enge definitie dekt niet de volledige lading. Om het concept spionage in zijn volledigheid te kunnen omvatten, moet er gesteld worden dat; "*alle pogingen en handelingen die gericht zijn op het opzoeken, het verstrekken, te weten komen van nuttige, gevoelige of geclassificeerde informatie, gebruik makende van clandestiene methoden, teneinde een voordeel over anderen te verwerven. Dit in het bijzonder politieke informatie maar ook militaire, economische, technologische of wetenschappelijke informatie".*[17]

3. INLICHTINGEN ALS HET DOEL VAN SPIONAGE

Er bestaan geen internationale verdragen die spionage verbieden. Volgens het VN verdrag is het verzamelen van informatie niet gebonden aan landgrenzen. Wel is het zo dat alle nationale wetgevingen bepalingen hanteren die informatieoverdracht aan banden legt wanneer er nationale - en veiligheidsbelangen worden geschaad. [18] Of de spionage gericht is tegen een bondgenoot of een vijandig gezind land speelt geen beduidende rol. Het enige wat altijd een belangrijke rol speelt is informatie. Door de eeuwen heen zijn inlichtingendiensten immers altijd de ogen en oren geweest van legers en staatsleiders.[19] En de diensten zelf dienen in de eerste plaats het land waar ze trouw aan zijn. Andere landen zijn hedendaagse of toekomstige mogelijke vijanden en daarom is het belangrijk steeds de potentiele militaire slagkracht alsook het wetenschappelijk, economisch en politiek potentieel (WEP) [20] te weten. Deze verrijkte informatie wordt inlichting of 'intelligence information' genoemd[21]. Hierdoor is het mogelijk om toekomstige plannen of acties van deze landen uit te stippelen. Ook is het voor het landsbelang steeds interessant te beschikken over nieuwe informatie die de grootsheid of groei van het andere land ten goede komt.

---

[16] Art. 17 & art. 26 Internationaal Verdrag inzake Burgerlijke en Politieke Rechten van 1966
[17] X, *Brochure : De Veiligheid van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.18
[18] Bedrijfsspionage is ook een vorm van spionage maar gebeurt noodzakelijkerwijs niet in opdracht van een inlichtingendienst. De meeste bedrijfsspionage gebeurt door bedrijven in dezelfde branche. In de thesis zal dit onderdeel aan bod komen maar vanuit het oogpunt dat de spioange in opdracht is van een inlichtingendienst of overheid.
[19] GRIFFITH, S.B., Sun Tzu. De Kunst van het oorlogsvoeren, Kerkdriel, Librero, 2010, p.239
[20] X, *Brochure : De* Veiligheid *van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.28
[21] HASTEDT, G.P., *Espionage. A reference handbook.*, Californië, ABC CLIO, 2003, p.52

Gelijktijdig is het van enorm groot belang dat het land zijn eigen inlichtingen of de ingewonnen informatie voor zichzelf houdt. Dit met uitzondering dat het land de informatie doorgeeft met het oog op internationale samenwerking. Zelf zal een spion nooit informatie uitwisselen op één uitzondering na; *"Arguably, one of the rules of thumb of espionage is to never give away a piece of information – instead, sell it or trade it for information that is of equal or greater value".*[22]

4. VAN INFORMATIE TOT INLICHTING

4.1. Inlichtingenbronnen

De inlichtingenwereld kent een waaier aan soorten inlichtingenbronnen en hun kwaliteiten in het voortbrengen van ruwe informatie. Het is aangewezen om deze diverse bronnen gedetailleerder te bespreken om zodoende een beter zicht te krijgen op de daadwerkelijke werking van inlichtingen – en veiligheidsdiensten en hoe zij informatie verzamelen. Dit zal ook de werking van de inlichtingencyclus verduidelijken die later nog aan bod komt. Hieronder bespreken we de belangrijkste bronnen die te onderscheiden zijn;

4.1.1. OSINT

OSINT, alias *Open Souce Intelligence*, is de benaming voor alle activiteiten waarbij informatiebronnen publiekelijk openstaan en er vrij informatie uit geput mag worden. Onder OSINT vallen magazines, kranten, radio, televisie, internet berichten, films, (informatie)brochures, publieke lezingen of vergaderingen, interviews, IP adressen, telefoonnummers, enz.[23] Een onderdeel hiervan is Web Intelligence (WEBINT) dat alle vrije informatie haalt uit het gebruik van internetzoekmachines zoals Google. Als een bron niet openlijk te raadplegen valt is het een gesloten bron. We noemen dit type van bron voor de gemakkelijkheid '*Close Source Intelligence'* of 'CSINT'. CSINT omvat met andere woorden alle private, vertrouwelijke en op verborgen manier verkregen bronnen. Het onderscheid is strafrechtelijk belangrijk omdat het bewust verzamelen van CSINT enkel opzettelijk en op illegale manier kan gebeuren, wat strafbaar is binnen de Europese Unie als tenzij men de wettelijke bevoegdheid hiervoor heeft.[24]

[22] PRUNCKUN, H., *Counterintelligence. Theory and practice*, Maryland, Rowman & Littlefield Publishers, 2012, p.20
[23] SMITH JR, W.T., Enc*yclopedia of the Central Intelligence Agency*, New York, Facts On File, 2003, p.9
[24] Artikel 18/16 §1 W.I&V en artikel 3, 10° W.I&V.

4.1.2. HUMINT

HUMINT is de afkorting voor Human Intelligence. Het omvat activiteiten waarbij informatie (mondeling) is verkregen. Dit via informanten of spionnen, ondervraging van (krijgs)gevangenen, diplomatieke vluchtelingen en burgers maar evengoed via vertaling van verkregen documenten of individuen die technische (of digitale) middelen gebruiken.[25] Met andere woorden; we spreken over inlichtingen die voortkomen uit menselijke activiteiten.

'*Human Intelligence'*-activiteiten kunnen informatie verzamelen op open of clandestiene manier, al dan niet met een dekmantel.[26] Als er wordt gesproken over '*Open Human Intelligence*' mag dit niet verward worden met '*Open Source Intelligence'*. Het verschil ligt in de vertrouwelijkheid en de toegankelijkheid van de open Human Intelligence bronnen. Het inwinnen van informatie vloeit dan voort uit conversaties, ondervragingen, correspondentie of officiële contacten met militaire of politieke diplomaten en attachés.[27]

Door middel van een dekmantel als diplomaat, journalist of vertegenwoordiger kan men zonder argwaan te wekken een bepaald persoon interviewen of uithoren omtrent bepaalde zaken. Ook wordt er onderling informatie geruild tussen inlichtingen – of veiligheidsdiensten. Dit kan gebeuren zonder cover; bv. als er sprake is van informatieruil tussen inlichtingenofficieren van twee verschillende diensten.[28]

Clandestiene informatie inwinning, al dan niet met een dekmantel, is de andere en meest gekende manier van informatie inwinning. We herkennen het vooral aan het oude Franse woord '*spy'* waarbij undercover agenten worden ingezet om informatie te verzamelen door 'observatie'. Observatie mag hier niet verward worden met 'verkenning', wat eerder een militaire term is met een ander doel. In deze thesis staat observatie voor informatieverzameling wat al reeds ver terug gaat. Zo getuigt het vierde boek van het Oude Testament, hoofdstuk 13, het gebruik van spionnen die door Mozes gezonden werden naar de twaalf stammen in Kanaän om hun populatie, militaire kracht en vruchtbaarheid van de grond te observeren.

---

[25] HITZ, F., 'Human Source Intelligence' in *Handbook of intelligence studies*, JOHNSON, L.K, (ed.), London, Routledge, 2009, p.127-128.
[26] DE VALK, G., *Dutch Intelligence: Towards a quantitative framework for analysis*, Den Haag, Boom Juridische Uitgevers, 2005, p.19
[27] DEPARTMENT OF DEFENSE PERSONNEL, *Unit 3. Intelligence Productions*, in *Operations Intelligence Journeyman (1N051A)*, Goodfellow, 2004, p.5
[28] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 98

Sindsdien is de term spion blijven bestaan en is ze zeer populair in de media en literatuur. Maar wat houdt die term precies in? Spionnen kunnen als persoon onderscheiden worden in drie categorieën, namelijk als; inlichtingenofficier, rekruteringsofficier of agent.

- Een inlichtingofficier die operationele opdrachten uitvoert inzake het verkrijgen van inlichtingen wordt ook wel een '*operation officer'* of '*field officer'* genoemd. Zij opereren voornamelijk vanuit hun eigen land of ambassade, ondervragen (krijgs)gevangenen en trekken achtergrondgegevens na. Soms krijgen ze ook een specifieke rol toegedeeld zoals observatieagent of counterintelligence speurder.[29]

- De rekruteringsofficier, ook wel gekend onder de benaming van "*recruiteerder*", "*handler*" of '*case officer'*, rekruteert agenten om vertrouwelijke en geheime informatie te verkrijgen in naam van de dienst. Zelf is dit type officier zeer diplomatisch, charismatisch en bovenal zeer geduldig. Hij herkent en rekruteert potentiële agenten en leidt hen op met bepaalde vaardigheden. Vaardigheden die vooral het verzamelen en kopiëren van inlichtingen omvatten, als het gebruiken van '*death letter boxen'* of contact leggen met de rekruteringsofficier. [30] Een '*death letter box'*, of dode brievenbus, wordt gebruikt om anoniem en discreet informatie uit te wisselen zonder elkaar persoonlijk te ontmoeten. Dit op geheime locaties die enkel de personen in kwestie weet.[31]

- Een agent is iemand die in naam van een ander individu of agentschap werkt. Een agent kan dus werken voor een inlichtingen – of rekruteringsofficier of een privaat bedrijf. De rol van een agent is zichzelf in een dergelijke positie te plaatsen die hem in staat stelt vertrouwelijke of geheime informatie bijeen te krijgen. Dit door te kijken, afluisteren, het participeren in discussies of door andere middelen waardoor de verlangde informatie kan verkregen worden. Zijn vaardigheden van coderen, achtervolgers afschudden, ondervraginsprioriteiten, observatie, dode brievenbussen en communicatie worden aangeleerd door de rekruteringsofficier.

[29] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.18-19
[30] HEADQUARTERS : DEPARTEMENT OF THE ARMY, FM2-22.3 (34-52) *HUMAN INTELLIGENCE COLLECTOR OPERATIONS, Field manual, Washington DC*, 2006, p. 14-17
[31] GOULDEN, J.C., T*he dictionary of espionage. Spyspeak into English*, New York, Dover Publications, 2012,p.56

> Een agent, die niet op zelfstandige basis werkt, is zich er meestal van onbewust dat hij gebruikt of gemanipuleerd wordt om dit te doen. [32] Of hij is zich hiervan wel bewust maar dan werkt de agent vrijwillig mee of onder dwang. We onderscheiden naast de standaard agent ook nog de 'dummy-agent' en de dubbelagent. Een dummy agent heeft als taak voor afleiding te zorgen bij de counterintelligence dienst zodoende deze dienst tijd verdoet met een vals spoor. Een dubbelagent echter is een al dan niet vrijwillig overgelopen agent, die werkt voor een andere dienst of inlichtingenofficier. Hij blijft informatie doorgeven aan zijn oorspronkelijke rekruteringsofficier. Maar deze informatie is op voorhand bepaald door de andere dienst waardoor ze nutteloos is. Dit is een andere manier om een dwaalspoor te creëren of een dienst bezig te houden, maar vanuit het counterintelligence oogpunt.[33]

Een ander belangrijk onderscheid is het al dan niet hebben van een dekmantel of 'cover' als inlichtingen – of rekruteringsofficier. Deze 'legalen' hebben een dekmantel die het best wordt beschreven al een plausibel verhaal dat de officier gebruikt om een alternatief verleden en leven op te bouwen. Voorbeelden van dekmantels zijn die van een ambassadeur, diplomaat of afgezant van een consulaat. Dit geeft hem ineens het ideale excuus om op bepaalde (voor het grote publiek ontoegankelijke) plaatsen te zijn of bepaalde activiteiten te ondernemen. [34] Werkt hij zonder een officiële cover dan is de kans groot dat hij werkt met een commercieel cover. Deze personen worden vaak 'illegalen' genoemd of 'NOC's'[35]. Hij werkt dus met andere woorden voor een spookbedrijf of organisatie. Dit bedrijf bestaat slechts enkel op papier en is speciaal gecreëerd en onderhouden door een inlichtingendienst. Hij kan de identiteit aannemen van een rijsthandelaar, onderzoeker, freelance fotograaf en veel meer.[36]

De ontwikkeling van menselijke bronnen kan extreem riskant zijn en kan inlichtingen en rekruteringsofficieren compromitteren. Het is nu éénmaal geweten dat individuen die bereidwillig zijn om familie, bloed, land of andere bondgenootschappen te verraden, moeilijker te hanteren zijn. Omdat ze sneller hun eigen agenda volgen, zelf informatie verzinnen of dubbelspion worden.

---

[32] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.19-20
[33] CAROLL, T.P., Syllabus section 1. *Human intelligence: From sleepers to walk-ins*, 2006, p.1-29
[34] SMITH JR, W.T., Enc*yclopedia of the Central Intelligence Agency*, New York, Facts On File, 2003, p.57
[35] *'NOC' (uitgesproken als 'knock') staat voor 'No Operational Cover'*
[36] WALLACE, R., MELTON, H.K. & SCHLESINGER, H.R., *Spycraft. The secret history of the CIA's spytech from communism to Al-Qaeda*, New York, Dutton, 2008, p. xvii

Ze kunnen een afkeer krijgen om verder te doen in wat mogelijk het vuilste gedeelde is van alle soorten inlichtingenbronnen.[37] Toch is ze essentieel voor het inwinnen van informatie en speelt een belangrijke rol in de beveiliging of het inlichtingenapparaat. Satellieten, afluisterapparaten of andere technische middelen leveren zeer waardevolle informatie maar ze zijn niet in staat om politieke intenties weer te geven zoals een menselijke bron.

Men mag dan ook niet vergeten dat niet alle landen even ver staan op technologisch vlak en gebruik kunnen maken van enorm geavanceerde apparatuur waardoor spionnen en informanten soms de enige (goedkope) keuze is. En ze zijn echter in staat om gevoelsmatig bepaalde zaken af te tasten en details of onbekende informatie te sprokkelen, waartoe een technisch hulpmiddel niet in staat toe is. [38] Het is zoals de oude romantische uitdrukking het aangeeft: *" Cloak and dagger"*. Dit verwijst naar de spion die, slechts gewapend met mantel en dolk zijn clandestiene opdrachten uitvoert.[39]

4.1.3. TECHINT

TECHINT of *'Technical Intelligence'* is de derde grote categorie van inlichtingenbronnen.
De benaming is afkomstig van de verzameling en analyse van mogelijke dreigingen, verzamelde documenten, datagegevens en buitenlandse militaire en burgerlijke uitrusting, evenals hiermee geassocieerd materiaal. Ook omvat *'Technical Intelligence'* materiaal met het doel het voorkomen van technologische verrassingsaanvallen (detectieapparatuur) en bijdragen tot buitenlands wetenschappelijke en technische mogelijkheden. Deze mogelijkheden krijgen in het vakjargon de benaming '*Scientific and technical intelligence'* (S&TI). Het bestudeert niet alleen de uitrusting en mogelijkheden, maar ook het ontwikkeling- en productieproces. Als laatste bezit het ook alle ontwikkelingen op vlak van tegenmaatregelen ontworpen om de technologische voordelen van een opponent te neutraliseren. [40] Er kan aangenomen worden dat Technical Intelligence een zeer ruim begrip is en verduidelijkt wordt door zijn deelcategorieën; SIGINT, MASINT & IMINT.

---

[37] WEST, N., *Historical dictionary of international intelligence in Historical dictionaries of intelligence and counterIntelligence*, IV, United Kingdom, Scarecrow Press, 2009, p.129
[38] UNITED STATES MARINE CORPS COMMAND STAFF COLLEGE, *Projecting organic intelligence, surveillance, and reconnaissance: A critical requirement of the Stryker Brigade Combat Team, Quantico, Rand, 2003, p.6*
[39] SMITH JR, W.T., Enc*yclopedia of the Central Intelligence Agency*, New York, Facts On File, 2003, p.59
[40] X., *B-GL-352-001/FP-001 : Intelligence, surveillance, target acquisition and reconnaissance (ISTAR)*, Canada, Land force Canada, 2004, p.61-64

ONDERVRAGINGSPRIORITEITEN ONDERVERDEELD BIJ POTENTIËLE KENNIS

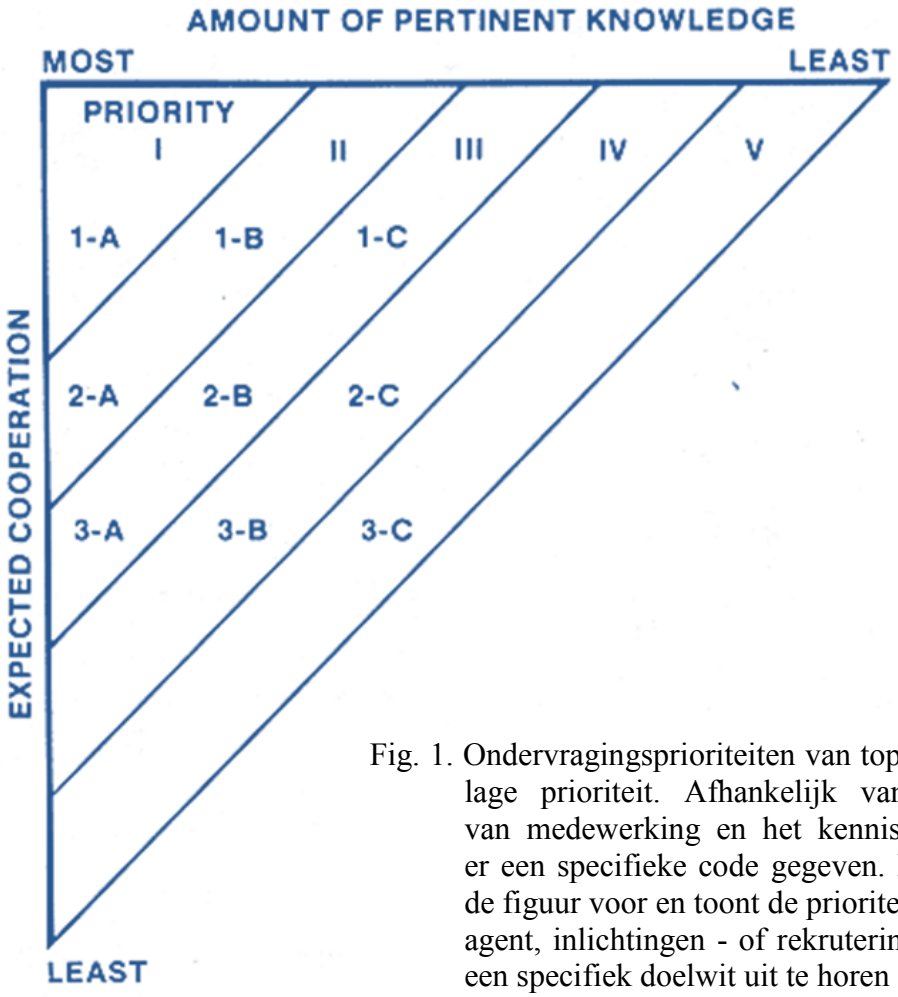


Fig. 1. Ondervragingsprioriteiten van topprioriteit naar lage prioriteit. Afhankelijk van het niveau van medewerking en het kennisniveau wordt er een specifieke code gegeven. Deze komt in de figuur voor en toont de prioriteit aan van een agent, inlichtingen - of rekruteringsofficier om een specifiek doelwit uit te horen over bepaalde kennis.

NIVEAU VAN MEDEWERKING		
Antwoordt direct op de vragen	Antwoordt aarzelend op de vragen	Antwoordt niet op de vragen
CODE VAN MEDEWERKING		
1	2	3
KENNISNIVEAU		
Zeer waarschijnlijk in bezit van bruikbare informatie	Mogelijk in bezit van bruikbare informatie	Onwaarschijnlijk in het bezit van bruikbare informatie
CODE VAN KENNISNIVEAU		
A	B	C

4.1.3.1. SIGINT

SIGINT, beter gekend als *Signals Intelligence*, is een discipline dat communicatie, het onderscheppen van berichten en signalen, gecodeerde berichten ontcijfering en signaalanalyse inhoudt. Sinds de eerste dag dat data en informatie via de radio kon worden doorgezonden, trachten (buitenlandse) vijandige elementen deze te onderscheppen. En niet alleen de signalen worden onderschept, maar ook wie, vanwaar en hoe vaak ze worden verstuurd. Dit is uiteindelijk wat 'spoken' van inlichtingendiensten doen. Het zijn eerder 'voyeurs' dan *James Bond look-a-likes*. De term 'Signalen' is zeer breed en kan op zichzelf COMINT (*Communication Intelligence*), dat voornamelijk gesprekken onderschept, en ELINT (*Electronic Intelligence*) als inlichtingenbron omvatten.[41]

Naast het onderscheppen van signalen, omvat het ook het gebruik van afluister - en toezichtsapparatuur. Deze apparatuur is een goede hulp om eventuele dreigingen en veiligheidsniveaus van individuen te evalueren in verschillende situaties. Een draadloze microfoon of afluisterapparatuur zendt private conversaties uit naar een radio – of communicatieontvanger. Dit gaande van verborgen elektronische en telefonische 'bugs' (zeer kleine afluisterzenders) tot telefoontaps en zenders. We onderscheiden vijf soorten apparatuur[42] ;

- **Verbergbare zender**: Met deze zender is men in staat alle conversaties in een ruimte te surveilleren wanneer het moeilijk is toegang tot deze ruimte te verkrijgen met (draagbare) afluisterapparatuur. Deze zenders zijn zelfstandig, vrijstaand en bijna onvindbaar met het blote oog**.** Hierdoor kunnen ze op voorhand in (nabijheid van) de ruimte geplaatst worden en is de kans op ontdekking zeer klein.

  Gecamoufleerde of ingebouwde zender: Dit type van zenders wordt gebruikt voor geheime surveillance door het plaatsen en installeren van afluisterapparatuur in alledaagse voorwerpen zoals een klok, lamp, stopcontact, enz. die aanwezig zijn in ruimte of woonst die gesurveilleerd wordt. Sommige van deze zenders worden gegoten of geïnstalleerd in een perfecte replica van het gebruiksvoorwerp om betere signalen te ontvangen of de kans op ontdekking drastisch te verkleinen.

[41] WEST, N., *Historical dictionary of international Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, IV, United Kingdom, Scarecrow Press, 2009, p.230
[42] X, (2013/07/05) SigInt: Types of electronic eavesdropping devices, [WWW]. StratRisks : http://stratrisks.com/geostrat/13756 [05/11/2013]

- **Digitale surveillance zenders (DTM**): Deze moderne afluisterapparatuur onderscheidt zich van zijn voorgangers door zijn mogelijkheid om op afstand bestuurd en geactiveerd te worden, geluidsfragmenten op te nemen, te coderen en door te zenden evenals toezicht te houden op digitale datagegevens.

- **Telefoon zenders**: Dit type zender is special ontworpen om telefoongesprekken van beide zijden af te luisteren. Ze worden op de telefoonkabel aangesloten waarbij deze toestellen via de kabel onbeperkte energie verkrijgen. Dit in tegenstelling tot bovenstaande opgesomde apparatuur die gebruik maakt van een (lithium) batterij

- **Stroom aangedreven zender**: Als laatste zender hebben we afluisterapparatuur dat voor overmatig en lang gebruik wordt ingezet. Ze hebben geen eigen stroombron maar hebben een eigen stroomkabel dat met een stroombron moet verbonden worden. Dit type kan bij wijze van spreken in muren ingemetseld worden en aangesloten op een interne stroomkabel en zolang het gebouw bewoond word informatie doorsturen.

In tegenstelling tot *Human Intelligence* is *Signal Intelligence* soms betrouwbaarder door de onvoorspelbare aard die sommige informanten hebben. Een onofficieel motto van het Amerikaans National Security Agency (NSA) laat hier ook geen onduidelijkheid over bestaan; *"In God we trust. Everything else we monitor".*[43]

4.1.3.2. MASINT

MASINT staat voor *Measurerement and Signature* Intelligence en omvat alle informatie - bronnen uit datastudies afkomstig van een specifiek doelwit en veranderingen die er gebeuren in tijd. Het omvat een reeks aan gebruiksmogelijkheden zoals het traceren van raketten en satellieten, surveilleren van grote oppervlakten tot het gebruik maken van infrarode sensoren en het detecteren van nucleaire explosies.[44] Het omvat hiernaast ook nog ACINT (*Acoustical Intelligence*), OPTINT (*Optical Intelligence*), IRINT (*Infrared intelligence*), LASINT (*Laser Intelligence*), NUCINT (*Nuclear Intelligence*) en RINT (*Radiation Intelligence*).[45]

[43] BAMFORD, J., *Body of secrets. Anatomy of the ultra secret national security agency*, New Yokrk, Anchor Books, 2002, p.8
[44] RICHELSON, J., 'The technical collection of intelligence' in *Handbook of intelligence studies*, JOHNSON, L.K,
(ed.), London, Routledge, 2009, p. 108-110
[45] LERNER, L. en LERNER, B., *Encyclopedia of Espionage, Intelligence & Security,* III, Detroit, Gale, 2004, p.304

4.1.3.3. IMINT

IMINT, of *Imagery Intelligence*, zijn informatie en inlichtingen die verzameld zijn door het bestuderen van gemaakte afbeeldingen waaronder foto's en satelliet – of warmtebronbeelden. In theorie zouden de foto's van de 'target site', en van mogelijk (staf) personeel, genomen moeten worden in de voorbereidende fase die afhankelijk is van de aard van betrokkenheid in een situatie. Een onderdeel van *Imagery Intelligence* is *Photographic Intelligence* (PHOTINT) dat zich concreet en alleen bezighoudt met het inwinnen van informatie uit foto's. Goede fotografie mag als inlichtingenbron zeker niet onderschat worden. Zijn bruikbaarheid en voordelen hebben in de loop der geschiedenis steeds een belangrijke rol gespeeld. [46] Een mooi voorbeeld hiervan waren de luchtfoto's die genomen werden boven Cuba tijdens de Koude Oorlog en aanleiding hebben gegeven tot de Cubaanse rakettencrisis.[47]

4.1.4. CYBINT

Dit is het tijdperk van een nieuwe vorm van spionage en informatieverzameling, namelijk die van de digitale wereld. CYBINT is een nieuwe term als inlichtingenbron en staat voor '*Cyber Intelligence'*. Het omvat eigenlijk alle vormen van informatieverzameling die gebeuren door middel van personen, computers en software om informatie te verzamelen die digitaal wordt opgeslagen. [48] Deze inlichtingenbron wordt door velen gezien als een onderdeel van '*Signal Intelligence'*. Doch is dit niet zo door de enorme diversiteit en omvang die het inneemt.

Cyber Intelligence maakt gebruik van '*Human Intelligence', 'Signal Intelligence'* en *'Technological Intelligence'*.[49] Een subcategorie van '*Cyber Intelligence'* is '*Digital Network Intelligence'* (DNINT)[50] en verwijst naar inlichtingen afkomstig van onderschepte digitale data communicatie of gebruikers onderling, op een netwerk van computers. Een militaire toepassing hiervan is het '*Computer Network Exploitation'* (CNE) [51]

---

[46] ALLSOP, W., *Unauthorised access. Physical penetration testing for IT security teams*, United Kingdom, WILEY, 2009, p.19
[47] ROBERTS, P., *Cuban missiles crisis. The essential reference guide*. California, ABC-Clio, 2012, p.56
[48] CARR, J., *Inside Cyber Warfare: Mapping the Cyber Underworld*, Sebastopol, O'Reilly Media, 2012,p.86-88
[49] REED, J., (2011/01/03) Cyber Intelligence, [WWW]. DefenseTech : http://defensetech.org/2011/01/03/cyber-intelligence [05/02/2014]
[50] Digital Network Intelligence wordt door de National Securty Agency afgekort tot DNI. Om geen verwarring te scheppen met DNI als Director of Naval Intelligence wordt hier geopteerd voor de afkorting DNINT.
[51] MINISTERIE VAN DEFENSIE, *Jaarverslag : Militaire Inlichtingen – en Veiligheidsdienst*, Nederland, Bestuurstaf/Militaire Inlichtingen en Veiligheidsdienst Defensie, 2012, p.19

Verder omvat Cyber Intelligence een heel gamma aan toepassingen en werkgebieden zoals [52];

- het decrypteren van digitale steganografische berichten en foto's waarin verborgen boodschappen zitten die niet zichtbaar zijn zonder ze eerst te coderen via een programma.[53]

- De betrachting van het creëren van voordelen bij een mogelijke cyberoorlog. Dit door het verzamelen van informatie over de nieuwste uitvindingen en dreigingen op gebied van computers, software en internet.

- De verzameling en regelmatige vernieuwing van alle mogelijke inlichtingenbronnen alsook de dreigingsanalyse en verzameling van persoonsprofielen die mogelijk een potentiële dreiging vormen.
- Het opsporen van misbruik door zowel '*social engineering'* als '*social networking'*, als het gebruik ervan voor activiteiten van spionage.

- Het surveilleren via de computer van mogelijk potentiële dreigingen, hun surfgedrag, sociale netwerken, activiteiten op forums en zelfgemaakte websites evenals hun contacten. In bepaalde gevallen kan men overgaan tot het verzamelen van informatie door middel van hacken of een '*Computer Network Operation'* (CNO).

- Het is ook duidelijk te merken dat er een hedendaagse trend aan de gang is die landen aanzet om zich meer te bewapenen tegen digitale vijanden met cyberwapens. Zo is '*Cyber Warfare'* en *'Cyber Defense'* een belangrijke evolutie in dit digitaal tijdperk.[54] Het deel Cyber weapons zal door zijn toepassingsgebied later uitvoerig besproken worden. '*Cyber Warfare'* en '*Cyber Defense'* zijn beide zeer interessant als opkomend fenomeen maar dit zou ons te ver doen afdwalen van de doelstelling van deze thesis.

Tenslotte zal een doeltreffende '*Cyber Intelligence'* in staat zijn nieuwe cyberdreiging activiteiten te voorspellen en ervoor te waarschuwen, alsook betere risicoanalyses van de dreiging uit te voeren.

---

[52]HURLEY, M.M., For and from Cyberspace. Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance., *Air & Space Power Journal (ASPJ*), 2012, 12-33
[53] PELTIER, R.T., PELTIER, J. en BLACKLEY, J., *Information security fundamentals*, Boca Raton, Auerbach Publications, 2005,p. 155
[54] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 29

Dit alles om effecten van een cyberaanval beter in te schatten, de handelingsbekwaamheid te vergroten en daardoor cybersecurity meer te stroomlijnen in een efficiënte en kostenbesparende beveiliging. [55]

4.1.4.1. Social engineering

Er zijn talrijke manieren om als een fysiek persoon aan informatie te komen. In deze moderne tijd bestaan er '*social engineering'* technieken waarbij er wel op vijf manieren informatie kan verzameld worden zonder enig echt fysiek contact te hebben met het slachtoffer. '*Social engineering'*, ook wel sociaal hacken vertaald, is een vorm van hacken die zich richt op het verzamelen van specifieke informatie via een computer van een individu. Deze technieken worden hoofdzakelijk gebruikt door criminelen en criminele organisaties om bankgegevens, identificatiegegevens en wachtwoorden te verzamelen.[56]
Dit belet echter bepaalde buitenlandse inlichtingendiensten niet deze technieken te gebruiken voor hun doeleinden. Dit geldt evengoed voor sociale netwerken.[57] Als men immers in staat is bankgegevens en wachtwoorden uit een persoon te ontlokken, waarom dan geen andere gegevens of andere data? We onderscheiden volgende hedendaagse methoden van social engineering[58];

- '*Phish(ing*)' : Er wordt een gelijkaardige of perfecte namaak email vervaardigd die bij het slachtoffer een indruk van legitimiteit opwekt. Onwetend haalt het slachtoffer kwaadaardige codes en inhoud binnen op zijn computer. Deze codes en programma's bezorgen de verstuurder alle nodige informatie die hij wil. Een vaak voorkomende '*phish'* mail handelt over '*online banking'*. Welke spion is niet geïnteresseerd in iemands bankgeheimen en de daaruit voortvloeiende chantagemogelijkheden of bijvoorbeeld kwetsbaarheid voor online gokken?

- '*Phone phising'* : Het verloop is hetzelfde als bij gewone '*pish'*, met het verschil dat de e-mail een vals telefoonnummer bevat waar het slachtoffer naar moet bellen in

[55] FAST, B., JOHNSON, M., SCHAEFFER, D., Cyber Intelligence : Setting the landscape for an emerging discipline. *Intelligence and national security alliance*, 2011, 13
[56] DEIBERT, R., MANCHADA, A., ROHOZINSKI, R., VILLENEUVE, N., WALTON, G., GOWAN, J., BRUCE, B. en TAY, J., Tracking GhostNet : Investigating a cyber espionage network*, Information warfare monitor,* 2009*,* p.39.
[57] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 68
[58] BEAVER, K., *Hacking for dummies*, Hoboken, Wiley Publishing, 2010, p.61-74

verband met zijn account. Aan de lijn wordt dan gevraagd naar zijn account gegevens, wachtwoorden en additionele informatie die normaal nooit via mail wordt gevraagd.

- '*Pretexting'* : Het misleiden van het doelwit door hem te laten geloven dat hij te maken heeft met een autoritair figuur als IT beveiliging, politieagent, auditor of gerechtelijk onderzoeker. Hierdoor zal het doelwit de gevraagde informatie direct geven uit angst en onwetendheid.

- '*Baiting'* : Hierbij worden fysieke apparaten en opslagmedia gebruikt die geïnfecteerd zijn met verborgen '*malware'*. Eenmaal als dit is gegeven of uitgedeeld aan een doelwit, bestaat er een grote kans dat dit individu het ook gaat gebruiken om documenten er op te zetten. Wat het doelwit niet weet is dat bij gebruik, de verborgen '*malware'* zich installeert en zijn computer alsook zijn interne netwerk probleemloos gehackt wordt. Dit is gebeurd op de G20 in 2013. Op deze Europese top hebben (vermoedelijk) Russische agenten besmette USB sticks uitgedeeld waarop onzichtbare spyware was geïnstalleerd. Dit werd ontdekt door EU president Herman Van Rompuy.[59] Een andere manier van *'baiting'* is telefonisch of digitaal contact maken, onder valse voorwendselen, om informatie van individuen te achterhalen. Deze informatie kan gaan van gebruikersnamen tot wachtwoorden.[60]

- '*Quid or quo'*: dit is het Latijns voor; "Ik geef wat, jij geeft wat". Het doelwit krijgt zogezegd geld of een cadeau aangeboden als hij in ruil zijn wachtwoorden, identiteit of andere informatie doorgeeft.

4.1.4.2. Hacken

Hacken als term omvat een zeer brede dreigingscategorie en een groot pallet aan activiteiten die een grote impact hebben op een organisatie. De rode draad hier is het individu, of groepering, die gebruik maakt van persoonlijke computers om toegang te verkrijgen tot het netwerk en de servers van een organisatie. Dit met het oog op het verstoren, onthullen of beschadigen van informatie gerelateerd aan de organisatie of de informatiestrucuur an sich.

[59] MTM (2013/10/29), Rusland probeerde Herman Van Rompuy te bespioneren met USB-stick, [WWW]. DeStandaard: http://www.standaard.be/cnt/dmf20131029_00815482 [02/11/2013]
[60] X,(z.d.) Assessment spionage-weerbaarheid. Hoe weerbaar bent u tegen spionage?, [WWW]. Fox-It: www.fox-it.com/nl/wp-content/uploads/2012/02/Assessment-Spionageweerbaarheid-v3.pdf [02/11/2013]

Dit gebeurt aan de hand van volgende methoden[61] ;

- '*Scanning'*: Deze techniek wordt aangewend door hackers om opzoek te gaan, via het internet of bepaalde organisaties, naar systemen die mogelijk bepaalde zwakheden vertonen om uit te buiten. Er is een hele reeks aan scaninstrumenten beschikbaar die bliksemsnel een individueel systeem, of alle systemen op een bepaald netwerk, kan controleren en de resultaten opslaan voor later gebruik of misbruik. Visueel kan het scannen gezien worden als de verkenners van de hacker die erop uit zijn gestuurd om gemakkelijke doelwitten te vinden.

- '*Defacen'* of '*Website defacements'* : vloeit voort uit de ontdekking en uitbuiting van een zwak punt, door een hacker, op de webserver van een organisatie. Na ontdekking kan de hacker de server controleren en de inhoud verwisselen met zijn eigen inbreng. Naargelang de motivatie kan de hacker zelfs lasterlijke documenten of foto's plaatsten op de webserver van de eigenaar. Dit kan gebeuren uit persoonlijk plezier, om een bepaalde organisatie te schaden of om te eigenaar van de website te chanteren. Chantage is een van de beweegredenen die mensen hebben om over te gaan tot spionage voor een bepaald land of dienst.

- Informatie stelen is de meest voorkomende vorm van hacken. Meestal trachten hackers gemakkelijk verhandelbare informatie te stelen zoals bankkaartencodes, maar ook private informatie zoals Rijksregisternummers en persoonsgegevens. Bankkaart codes kunnen gemakkelijk verkocht worden aan criminele organisaties. Persoonsgegevens en nummers kunnen verkocht worden aan individuen of groeperingen die gespecialiseerd zijn in identiteitsdiefstal. Dit ziet men vooral bij '*script kiddies'* en meer ervaren hackers. [62] Maar de experten en elite hackers, die een meer economische of politieke spionage motivatie hebben, zullen elke soort aan informatie stelen dat kan gevonden worden op webservers of op andere systemen binnen organisaties.

[61] GREGORY, P., *Enterprise information security. Information security for non-technical decision makers*. Groot Brittanië, Pearson Eduction Limited, 2003, p.13-15
[62] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 116-117

- *'Denial of service attack* '(DOS) is een digitale blokkade opgericht in de cyberwereld. De aanvallende hacker creëert een vloedgolf aan internetverkeer naar een website of server. De vloedgolf maakt het systeem totaal onbereikbaar voor de eigenaar van de website of netwerk als de gebruikers ervan. In het ergste geval zal het aangevallen systeem '*roll over and die'*. Met andere woorden, de website of server crasht of slaagt intern door omdat het de grote hoeveelheden internetverkeer niet aankan.

- '*Distributed denial of service attack'* (DDOS) wordt wel de grote broer genoemd van '*Denial of service'* en is ook vele malen schadelijker en gesofisticeerder. Met een '*distributed denial of service attack'* kan de hacker een masterprogramma gebruiken om honderden tot duizenden onbewuste (zombie)computersystemen op te roepen. Zombiecomputers zijn computers die geïnfecteerd zijn en gebruikt worden door de hacker om grote hoeveelheden internetverkeer op te wekken. De eigenaars van de computers zijn er zich niet van bewust dat hun toestel voor dergelijke zaken wordt gebruikt. Deze zullen allen gelijktijdig geïnstrueerd worden om hetzelfde doelwit 'aan te vallen'. De computers die hiervoor gebruikt worden zijn niet enkel geïnfecteerde zombie computers maar ook doodgewone bedrijfscomputers en servers die in het verleden eens succesvol zijn besmet met een virus, wormvirus of Trojaans paard.

Naast de methode van hacken bestaat er ook een vorm van digitale "lockpicking". Door middel van redelijk geavanceerde computersoftware en een blanco keycard kan een gevorderde hacker toegang verkrijgen tot alle fysieke ruimtes die zijn beveiligd door een digitaal codeslot en/of keycard. Door het slot en/of de blanco kaart te manipuleren en te cryptograveren is hij in staat ongemerkt kluizen, hotelkamerdeuren, enz. te openen zonder een onopzettelijk spoor achter te laten. [63]

4.1.4.3. Cyber weapons

Zoals hierboven reeds is vermeld, houdt Cyber Intelligence zich ook bezig met cyberwapens die gebruikt worden voor digitale oorlogsvoering. Cyber Intelligence verzamelt op twee soorten vlakken informatie. Enerzijds is ze bezig op met het inwinnen van informatie over de identificatie en de opsporing van individuen of organisaties die digitale 'wapens' ontwikkelen, verkopen en gebruiken op grote basis.

[63]KERR, I., Digital Locks and the Automation of Virtue. in *Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda,* GHEIST, M., (eds.), Ottowa, University of Ottawa, 2010, 247-303

Anderzijds tracht ze door de inzet van eigen ontwikkelde cyberwapens informatie in te winnen. Volgens '*Cyber Warfare'* experten Thomas Rid en Peter McBurney kunnen we digitale wapens definiëren als; "*Een computer code die wordt gebruikt, of is ontworpen, met het doel om te bedreigen of fysieke, functionele of mentale schade te berokken aan gestructureerde systemen of levende wezens*." [64]

Met andere woorden heeft men het over zeer schadelijke, specifiek en welgeschreven virussen en '*malware'* die zowel defensief als offensief kunnen ingezet worden. Voorbeelden van dergelijke virussen en '*malware'* zijn Stuxnet, Wiper, Duqu en Flame. [65] Het doel van deze cyberwapens is drievoudig [66], namelijk;

- Surveilleren van systemen of zijn operatoren evenals gevoelige en vertrouwelijke informatie zoals wachtwoorden en asymmetrische cryptografie sleutels.

- Diefstal van intellectuele eigendom waaronder; vertrouwelijke informatie van de overheid of defensie evenals bedrijfseigen informatie van een privaat bedrijf of organisatie.

- Vernietiging van één of meerdere specifieke datagegevens of uitvoerbestanden op een systeem of een ander hieraan verbonden systeem. Evengoed maar minder frequent voorkomend is de beschadiging of vernietiging van computer hardware. Dit laatste kan gebeuren door de koeling uit te schakelen en gelijktijdig de processorsnelheid te verhogen waardoor oververhitting ontstaat en bepaalde interne siliciumchips kunnen smelten. Ook kan het bepaalde veiligheidssystemen overschrijven van extern verbonden hardware en elektromechanische toepassingen. Indien gelijktijdig het stuurprogramma wordt gewijzigd, kan dit leiden tot een mechanisch defect. Als dit gebeurt bij elektromechanische processen of veiligheidssystemen, op industrieel niveau, kan dit leiden tot het verlies van mensenlevens of eigendommen. [67]

[64] PAGANINI, P., 'Cyber weapon', *The Hacker News*, 2012, 3-8
[65] X, (2012/08/29) Kaspersky looks at the wreckage of Wiper malware, [WWW]. Inforsecurity : http://www.infosecurity-magazine.com/view/27869/kaspersky-looks-at-the-wreckage-of-wiper-malware [06/02/2014]
[66] MELE, S., '*Cyber weapons : legal and strategic aspects'*, Edizioni Machiavelli, 2013, 8-15
[67] MELE, S., *Cyberwarfare and its damaging effects on citizens*, Milan, 2010, p.10-14

Als er over de inzet van cyberwapens '*out of the box* ' nagedacht word, kan er gesteld worden dat naast surveilleren en inwinnen van informatie, dergelijke cyberwapens ook kunnen gebruikt worden door landen als sabotage of inmenging middel. Zo is het Stuxnet virus als defensief cyberwapen ingezet tegen Iran door de Amerikaanse en Israëlische inlichtingendiensten. Amerika en Israël wilden zich inmengen in het Iraanse atoomprogramma. Het virus had als opdracht de Iraanse ultracentrifuges te saboteren die nucleaire brandstof maken. Dit leidde tot het verlies van controle over de snelheid en de stopzetting van de aanmaak van brandstof.[68]

Het bovengenoemde is een schoolvoorbeeld van sabotage en inmenging door buitenlandse inlichtingendiensten en een mogelijke toepassing van een cyberwapen. Er wordt een wapen ingezet tegen bepaalde economische productiewijzen om schade aan te richten aan elektromechanische processen. Dit zou tot gevolg hebben dat het land de financiële markt van vraag en aanbod tijdelijk kan bespelen of verzwakken.

Naast deze vorm van economische inmenging is ook politieke inmenging mogelijk. Hierbij behoort volgend scenario tot één van de mogelijkheden; Als een vereniging of partij in een bepaald land wil opkomen met de verkiezingen kunnen vijandige (buitenlandse) elementen, door inzet van een cyberwapen, de vereniging of partij tijdelijk uitschakelen en andere partijen bevoordelen. Door het cyberwapen in te zetten op het hoogtepunt van een verkiezingsstrijd kunnen de datagegevens van leden, toespraken, printklaar drukwerk (brochures, boeken, banners, flyers, affiches, enz.) vernietigd worden. Zowel materiaal en gegevens die veel tijd en energie hebben gekost om te creëren en verzamelen zijn dan verloren. Dit op zowel de centrale partijcomputer, als de hieraan verbonden computers van leden. De partij is niet meer in staat om te wedijveren met de andere propaganda van de concurrerende bedrijven waardoor de partij veel stemmen zal verliezen. De andere partijen echter zullen dan veel stemmen verkrijgen.

4.1.5. Andere bestaande inlichtingenbronnen

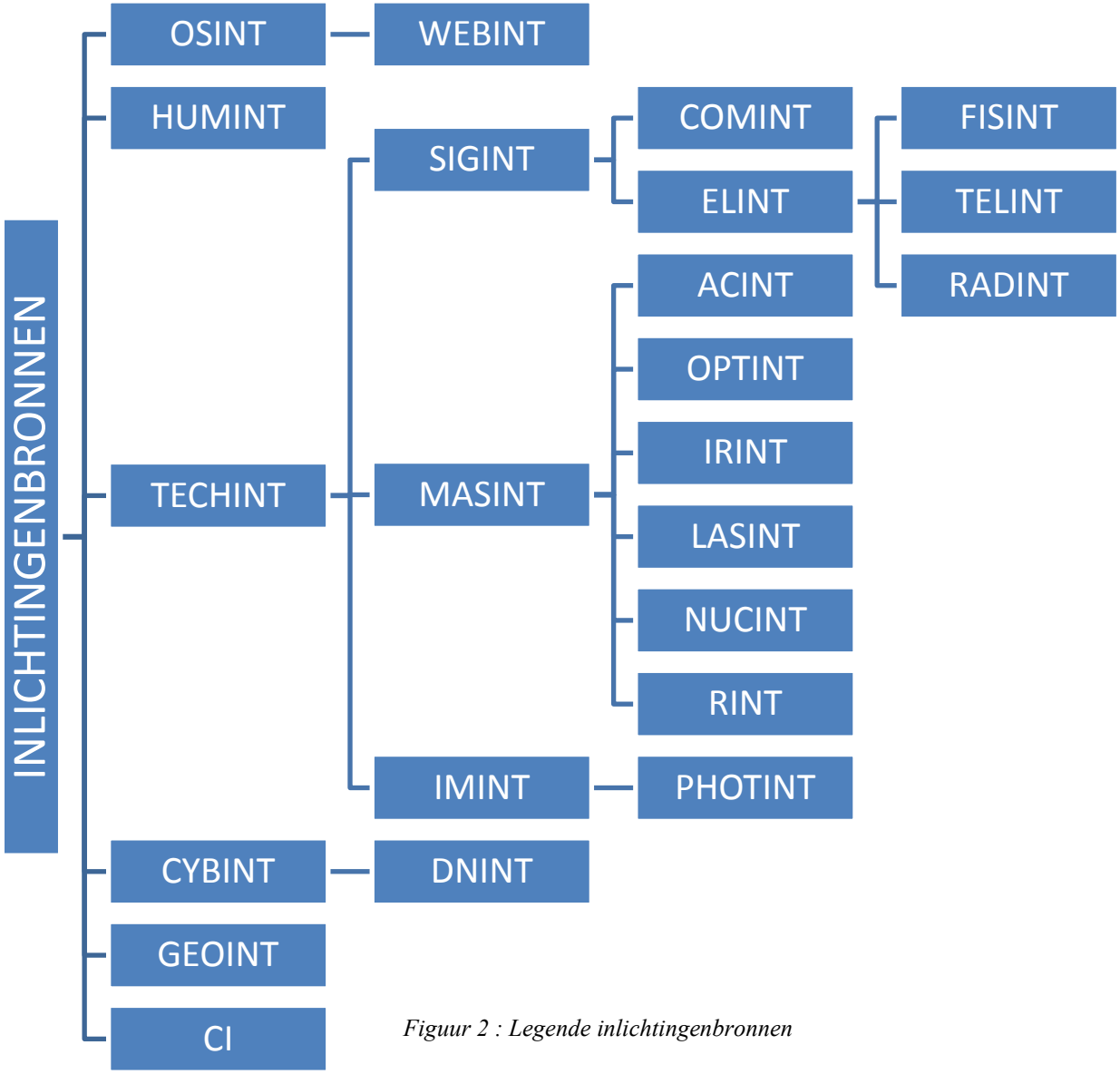
GEOINT of '*Geospatial Intelligence'* is informatie afkomstig van verschillende soorten inlichtingenbronnen.

[68] SHAKARIAN, P., SHAKARIAN, J. & RUEF, A., Introduction to cyber-warfare. A Multidisciplinary approach, Waltham, Elseviers, 2013, p.224-235.

Aan de hand van het analyseren en verkennen van foto's, beelden en elektronische kaarten tracht het een grondlaag te vormen. Op deze grondlaag worden vervolgens meerdere informatielagen, aangebracht. Deze informatielagen bestaan uit menselijke bronnen, telefoon, radio - en internetverkeer en open bronnen. Op deze manier ontstaan nieuwe en correctere inzichten, en dit na het in elkaar puzzelen van zeer grote datagegevens en bestanden die een duidelijke geografische duiding (coördinaten) bevatten. [69]

CI of '*Counterintelligence'*. Hiervoor wordt u vriendelijk verwezen naar Deel III waar '*Counterintelligence'* is zijn geheel wordt uiteengezet.

[69] MINISTERIE VAN DEFENSIE, *Jaarverslag : Militaire Inlichtingen – en Veiligheidsdienst*, Nederland, Bestuurstaf/Militaire Inlichtingen en Veiligheidsdienst Defensie, 2012, p.16



Figuur 2 : Legende inlichtingenbronnen

INLICHTINGENBRONNEN

LEGENDE

OSINT : Open Source Intelligence
HUMINT : Human Intelligence
TECHINT : Technical Intelligence
SIGINT : Signal Intelligence
COMINT : Communication Intelligence
ELINT : Electronic Intelligence
FISINT : Foreign Instrumentation Signals Intelligence
TELINT : Telemetry Intelligence
RADINT : Radar Intelligence
MASINT : Measurement and Signature Intelligence
ACINT : Acoustical Intelligence
OPTINT : Optical Intelligence
IRINT : Infrared intelligence
LASINT : Laser Intelligence
NUCINT : Nuclear Intelligence
RINT : Radiation Intelligence
IMINT : Image Intelligence
PHOTINT : Photo intelligence
CYBINT : Cyber intelligence
DNINT : Digital Network Intelligence
GEOINT : Geospatial Intelligence
CI : Counterintelligence

4.2. Inlichtingencyclus

Spionage en het inwinnen van inlichtingen gebeurt niet spontaan of op eigen initiatief. Er bestaan natuurlijk uitzonderingen hierop van 'Einzelgängers' die op hun eentje informatie proberen in te winnen op malafide manieren, doch is dit zeer beperkt.[70] Spionage op zich is niets meer dan een instrument voor informatie-inwinning alsook een specifiek onderdeel van een inlichtingencyclus. Spionage en inlichtingen zijn dus niet simultaan. In een inlichtingencyclus kunnen er 5 belangrijke onderdelen onderscheiden worden.[71]

Planning en sturing

Het eerste onderdeel van de inlichtingencyclus omvat het voorbereidend werk en planning nadat er een specifieke opdracht is gegeven. Deze opdracht kan door een minister, inlichtingen – of veiligheidsdienst gegeven worden. Het moet in ieder geval van hoger af gegeven worden. Als dit niet zo is, moet de commandant of teamleider hiervan op de hoogte gebracht worden. Er kan immers een vijandige mogendheid mee gemoeid zijn die andere diensten het vuile werk wil laten opknappen of afleiden. Centraal staat het bespreken en bediscussiëren van de mogelijke manieren om de nodige inlichtingen te verzamelen. Er wordt gewerkt in een bepaalde richting om de doelstelling te volbrengen. Dit met voorkennis over de geschikte persoon die de opdracht moet uitvoeren, actoren en/of obstakels die mogelijk het pad zullen of moeten kruisen en wat er allemaal verzameld moet worden. Hierbij wordt rekening gehouden met de beschikbare manschappen, middelen en vooral tijd.

Inwinnen en verzamelen

Het inwinnen van informatie begint nadat de opdracht is gegeven om specifieke, belangrijke en al dan niet geheime informatie in te winnen. Deze opdracht wordt gegeven aan inlichtingenofficieren, rekruteringsofficieren of slapende agenten.[72] Deze trachten informanten te oogsten via hun bronnen. Het verzamelen van informatie hangt ook in grote mate af van de aard van de informatie die verzameld moet worden. Is met andere woorden de informatie openbaar en voor iedereen toegankelijk (OSINT) of is de informatie eerder vertrouwelijk of geheim (CSINT)? [73]

---

[70] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 194
[71] HASTEDT, G.P., *Espionage. A reference handbook.*, Californië, ABC CLIO, 2003, p.52-54
[72] VOLKMAN, E., Spies. *The Secret agents who changed the course of history*, Amerika, Wiley 1996, p.1-2
[73] DEPARTMENT OF DEFENSE PERSONNEL., *Unit 3. Intelligence Productions*, in *Operations Intelligence Journeyman (1N051A)*, Goodfellow, 2004, p. 5-6

Een andere manier waarop overheden en diensten informatie of inlichtingen kunnen verkrijgen is via andere overheden en diensten die dit mededelen, voortvloeiend uit bondgenootschap, onderlinge samenwerking of in ruil voor andere inlichtingen. Alsook kunnen overlopende informanten of agenten van andere mogendheden informatie en geheimen prijs geven in ruil voor asiel of bescherming[74]

Tegenwoordig wordt er ook veel gebruik gemaakt van I.C.T. specialisten die werken voor een inlichtingendienst en gerekruteerde hackers. Veel informatie tegenwoordig is digitaal en opgeslagen op een elektronisch medium. Het gebruik van 'I.*C.T. skilled'* personen zorgt ervoor dat men niet meer fysiek het veld op moet gaan om informatie in te winnen. Een tekort aan bewijzen van mogelijk gekopieerde digitale informatie, evenals weinig tot geen gevoerde controle, zorgen ervoor dat er geen traceerbaarheid mogelijk is. Dit in het achterhoofd houdende dat het digitaal hacken of spioneren niet hoeft te gebeuren door een virus en kan gebeuren door een waakzaam moment van de eindgebruiker.[75]

Verwerken en exploiteren

Het derde onderdeel van de inlichtingencyclus handelt over de verwerking van de verzamelde 'ruwe' informatie. Het heeft een dubbele functie in de verwerking. Allereerst filtert het alle niet-belangrijke informatie weg tot slechts de noodzakelijke informatie overblijft. Deze informatie is dan verrijkt en gebruiksklaar en wordt keurig neergeschreven in een inlichtingenrapport.[76]

Analyseren en produceren

Het inlichtingenrapport wordt hierna geanalyseerd en de mogelijke bestaande hiaten worden opgevuld met reeds verkregen informatie of hypothetische veronderstellingen. Het vervolledigen van het inlichtingenrapport levert een bijdrage aan het onderzoeksdoel, namelijk het beantwoorden van de vragen: wat en waarom is er iets aan het gebeuren, wat kan er nog gebeuren en welke rol speelt het onderzoekende land hierin.[77]

---

[74] MELTON,. H.K., *Ultimate spy. Inside the secret world of espionage*, New York, DK Publishing, 2009, p.11
[75] CARR, J., *Inside Cyber Warfare: Mapping the Cyber Underworld,* Sebastopol, O'Reilly Media, 2012, p.86-87
[76] CIA (z.d.), The Intelligence Cycle, [WWW]. Office of Public Affairs
Central Intelligence Agency: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html [25/12/2013]
[77] SHULSKY, A. & SCHMITT, G., *Silent Warfare. Understanding the world of intelligence*., Virginia, Potomac Books, 2002, p.1-2

Verbreiding

Het einde van de cyclus wordt gekenmerkt door het doorgeven van het vervolledigde en gedetailleerde inlichtingenrapport aan diegenen die de opdracht hebben gegeven. Nadat er geoordeeld is over de kwaliteit van het inlichtingenrapport zullen, als de noodzaak zich voordoet, daar de nodige gevolgen aan gegeven worden. Dit kan gaan tot opsporing en arrestatie tot tegenaanvallen of een preventieve aanval. In de meeste gevallen zal men de inlichtingen gebruiken als richtlijn om meer specifieke informatie in te winnen over het onderwerp. Het is niet onlogisch dat een inlichtingenrapport telkens nieuwe vragen oproept die beantwoord moeten worden. Hierdoor start het gehele proces opnieuw.[78]

Figuur. 3 : De inlichtingencyclus

[78]CIA (z.d.), The Intelligence Cycle, [WWW]. Office of Public Affairs Central Intelligence Agency: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html [25/12/2013]

5. DE ROL VAN INLICHTINGEN

De befaamde strateeg Carl Von Clausewitz schreef in zijn boek Vom Kriege [79]

"*Solange ich den Gegner nicht niedergeworfen habe, muß ich fürchten, daß er mich niederwirft, ich bin also nicht mehr Herr meiner."*

Von Clausewitz wijst hier naar het belang van het onderwerpen van een mogelijke gelijke of sterkere opponent. Hij leidt er uit af dat het van het grootste belang is niet alleen de opponent zijn mogelijkheden van aanval te vermorzelen maar ook zijn motivatie. En door steeds tijdig zijn aanval af te slaan, evenals direct te kunnen anticiperen op iedere zet die de opponent neemt, zal het pas mogelijk zijn de opponent te demotiveren. Maar om steeds een zet of meerdere zetten voor te staan op de opponent, moet je meer te weten komen over hoe hij denkt en wat zijn daadwerkelijke troeven zijn. Hiervoor spelen inlichtingen een belangrijke rol.

Het is dus duidelijk dat het verlangen om inlichtingen te verzamelen zo oud is als de straat. De materie van inlichtingen is zeer complex en uitgebreid. Daarom is het belangrijk dat de focus hier gelegd zal worden op de kern van het soort inlichting. Dit zou anders kunnen leiden tot misverstanden. Inlichtingen kunnen eenvoudig in drie soorten groepen[80] geclassificeerd worden;

- Strategische inlichtingen: De etymologie van het woord strategie is afkomstig uit de Griekse woorden 'strategia' en 'strategos'. Met ander woorden, strategie is de kunst en wetenschap van het tewerkstellen van de, psychologische, politieke, economische en militaire machten van een natie of een coalitie van naties. Dit om de maximale ondersteuning te bekomen bij het overnemen van politieke koersen die streven naar oorlog of vrede. De aard van dit type inlichtingen kan technisch, sociologisch, wetenschappelijk, diplomatisch of een combinatie van beiden zijn. Strategische inlichtingen leggen de nadruk op brede kwesties. Dit kan gaan van nationale of globale economie, intenties van buitenlandse(sub) naties, politieke afweging en opdrachten tot militaire middelen en mogelijkheden.

[79] VON CLAUSEWITZ, C., *Vom Krieg*,Berlijn, Ferdinand Dümmler, 1832, boek 1, Hoofdstuk I, parafgraaf 4
[80] GRAGIDO, W. & PIRC, J., *Cybercrime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, p. 91-96

- Tactische inlichtingen: De focus bij tactische inlichtingen ligt bij het leveren van steun op het tactische niveau. Dit wordt meestal gelinkt aan de inzet van militaire gevechtstroepen en gespecialiseerde eenheden die verkenningsmissies uitvoeren.
  De verkenningsmissies leveren de informatie op die terecht zal komen in de inlichtingencyclus. Strategen kunnen dan operationele objectieven behalen van gegeven opdrachten door gebruik te maken van stipte, doelgerichte en accurate inlichtingen over mogelijke vijandig gezinde opponenten en (gevechts)zones.

- Operationele inlichtingen: Deze vorm van dataverwerving is zowel noodzakelijk voor de inlichtingenwereld als voor de militaire organisaties. Dit voor het welslagen van de planning, uitvoering en verwezenlijking van een missie. Deze missie kan zowel tactisch als strategisch zijn. Operationele inlichtingen, alias OPTINEL, focust op het leveren van ondersteuning aan expeditionaire eenheidofficiers en haar band met hoofdkwartiereenheden. Dit is zeer belangrijk omdat het activiteiten van strategische en tactische inlichtingen ondersteunt. Operationele inlichtingen maken gebruik van Elektronische inlichtingenbronnen (ELINT) omdat deze zich concentreren op de interceptie van niet-communicatiegerelateerde signalen over elektronische golven (met uitzondering van signalen die afkomstig zijn van nucleaire ontploffingen). Hiernaast gebruiken operationele inlichtingen ook vaak *'Measurement and Signature Intelligence'* (MASINT) en *'Foreign Instrumentation Signals Intelligence'* (FISINT) bronnen. Het mag echter niet vergeleken worden met de activiteiten die gerelateerd zijn met bedrijfsprocesmanagement hetgeen soms ook OPTINEL genoemd wordt.

Wanneer deze drie categorieën worden gesynthetiseerd kan er algemeen gesteld worden dat inlichtingen steun en kennis leveren aan een scala van taken en opdrachten. Inlichtingen dragen bij aan; [81]

- Het leveren van stipte, accurate, gedetailleerde en significante kennis van de omliggende omgeving.

- Het leveren van steun aan de diplomatieke betrekkingen en handelingen van een natie.

[81] LERNER, L. en LERNER, B., *Encyclopedia of Espionage, Intelligence & Security,* II, Detroit, Gale, 2004, p.117-127

- Het leveren van steun en kennis aan counterintelligence diensten van bevriende bondgenootschappen. Dit met het oog op wederzijdse bescherming en onderliggende samenwerking.

- Het leveren van kennis over andere landen, regio's, staten en naties en de politieke, wetenschappelijke en economische standpunten die ze dragen.
  Ook leveren inlichtingen een kijk op de invloed van bepaalde actoren, die deze standpunten al dan niet ondersteunen. Dit laatste is interessant wanneer een land zich politiek wil inmengen in buitenlandse politiek, economie of wetenschappelijke vooruitgang.

- Het leveren van ondersteuning en toezicht bij correcte opvolging van verdragen en overeenkomsten tussen naties.

- Het leveren van steun bij militaire operaties en de verdediging van het wetenschappelijk, economische of politiek potentieel (WEP) van het eigen land of natie, evenals de bescherming tegen mogelijke (buitenlandse) dreigingen.

- Ondersteuning aan het Federaal Parket en de navolging van de wetgeving.

Men kan het voor de eenvoud vergelijken met de weerman of - vrouw op televisie. Zijn 'voorspelling' van de volgende dagen is niets meer dan de interpretatie van verzamelde en geanalyseerde informatie of inlichtingen door meteorologen, die klimaatwijzingen in kaart brengen van zowel het binnenland als het buitenland. Deze voorspellingen kunnen aanzet geven tot wijziging van plannen of afspraken die men heeft gemaakt. Of het nemen van voorzorgsmaatregelen (in dit voorbeeld een paraplu, winterbanden, zonnecrème, enz.).

We concluderen dat inlichtingen voornamelijk steun leveren aan de politieke, gerechtelijke en militaire beleidsmakers en actoren. Maar inlichtingen kunnen in veel gevallen ook zaken aan het licht brengen van mogelijke dreigingen, potentiële problemen of veranderingen in het buitenland. Hierdoor zijn veiligheids - en inlichtingendiensten in staat om voorzorgsmaatregelen te treffen.

6. BEWEEGREDENEN TOT SPIONAGE

Waarom zou een individu overgaan tot spionage van zijn vaderland? Soms kan het gebeuren dat men door onwetendheid onbewust informatie geeft aan een spion. Dit is in het verleden al vaak gebeurd. Meestal gaat dit over informatie die eerder toegankelijk is voor iedereen (*'Open Source'*) of misschien iets gespecialiseerder is maar niet gericht naar het brede publiek. We spreken dan nog niet van informatie die geklasseerd is als; *'Confident'* (vertrouwelijk), *'Secret'* (geheim) of *'Top Secret'* (uiterst geheim). [82]

Maar alle andere informatie die wel vertrouwelijk of geheim is kan men niet onbewust doorgeven aan een inlichtingenofficier of tussenpersoon van een vreemd land. De wettelijke straffen op spionage zijn immers zeer hoog en kunnen in bepaalde landen zelfs tot de levenslange eenzame opsluiting of de doodstraf leiden. Om dit te begrijpen zijn er een zestal beweegreden die rekruteringsofficieren gebruiken om specifiek geselecteerde individuen te overtuigen voor hem en zijn land te spioneren.[83]

Sommige van deze beweegredenen kunnen de indruk wekken dat ze enkel kunnen gebeuren bij personen die naïef, hebzuchtig of slordig zijn. Maar het is belangrijk om te weten dat iedere geheime dienst hetzelfde stramien toepast op vlak van rekrutering. [84]

- 1ste fase: in de beginfase voert de inlichtingen - of rekruteringsofficier gangbare en banale gesprekken met zijn doelwit. Weliswaar soms op een hoog intellectueel niveau maar genoeg om de interesse op te wekken van het doelwit om een vertrouwensband op te bouwen. Deze band kan nog evolueren naar een hechte vriendschapsband. Het doel van deze band berust vooral op het inwinnen van privégegevens. Deze gegevens handelen over het ego, geldgebreken, verslavingen, professionele frustraties, tekorten en dergelijke meer. De eerste fase kan maanden tot jaren duren maar 'geduld is een schone zaak' is hier de boodschap.

- 2de fase: Deze treedt in werking wanneer er een vriendschapsband aan het groeien is. Deze kan verdiept worden door geschenken te geven aan het doelwit; een dure fles alcohol, boeken, een pen, een restaurantbezoek, etc.

[82] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.138
[83] HITZ, F. P., *Why spy? Espionage in an Age of Uncertainty*, New York, Thomas Dunne Books, 2008, 212p .
[84] CLERIX, K., S*pionage. Doelwit Brussel*, Antwerpen, Manteau, 2013, p. 204

Ook is het belangrijk om nieuwe veranderingen in het leef - en gedragspatroon nauwlettend in het oog te houden.

- 3de fase: De officier schuift zijn doelwit ongevraagd geld toe. Als het doelwit toe hapt door het geld aan te nemen, trapt hij in de val. Want wie eenmaal het geld heeft aangenomen, is vanaf dat moment chanteerbaar en ziet geen weg terug. Deze derde fase hoeft niet noodzakelijkerwijs met geld te gebeuren. Ook chantagefoto's, informatie of andere drukmiddelen kunnen voor deze fase gebruikt worden. Maar het is zo dat geld in sommige gevallen als bijkomend 'motivatie - en drukmiddel' wordt gebruikt.

6.1. Ideologie en toewijding

Een welgekend motief is het spioneren uit ideologische beweegredenen voor een politiek gedachtegoed of toewijding voor een bepaald land of leider. Ze delen dus een ideologie met het land of zetten zich af tegen de ideologie van hun eigen land. Bij dit laatste trachten ze door hun spionageactiviteiten de koers van hun land te veranderen of op een goed blaadje te komen staan bij het land waar ze voor spioneren. Dit met het oog op toekomstige emigratie naar het land.

6.2. Geld en materiële goederen

Hebzucht is altijd een zwakte geweest van veel personen om te spioneren of informatie te overhandigen. Zo kan informatie geruild worden voor geld of materiële goederen. Materiële goederen kunnen gaan van een etentje of enkele flessen alcohol tot een stereoketen of auto. Dit wordt door vele counterinlichtingendiensten met aversie gezien door de sterke christelijke achtergrond die hieraan hangt. Het was namelijk Judas die Christus heeft verraden voor dertig zilverlingen. Anderzijds is het wel de meeste voorkomende beweegreden die aanleiding heeft gegeven tot spionage. De inlichtingendiensten zelf vinden dit totaal niet erg. Want in tegenstelling tot iemand die spioneert uit ideologie, kan iemand die spioneert voor geld niet zomaar stoppen. De voormalige KGB wist dit maar al te goed. Iemand die spioneert voor geld, alias '*chuzhoi'* genoemd in het Russisch, heeft zichzelf blootgesteld aan mogelijke toekomstige chantagepraktijken wanneer hij op een bepaald moment wil stoppen met zijn activiteiten.

Zelfs als zijn geweten of angst om gepakt te worden te groot is, zal de '*case-officer'* nog altijd druk kunnen uitoefenen om te blijven spioneren totdat hij bewijs heeft dat de agent al geld heeft ontvangen.

6.3. Wraak en vergelding

Spionage uit wraak of vergelding komt zelden voor maar is niet onbestaand. Meestal gebeurt dit uit een sluimerend gevoel om zichzelf te bewijzen tegenover collega's, familie of vrienden. Meestal gaat het over individuen die al op een jonge leeftijd een grens bereiken in hun carrière waardoor ze niet verder kunnen doorgroeien of promoveren. Deze individuen zijn ook vaak het mikpunt van spot, worden uitgesloten door hun collega's of zijn ondergewaardeerd door hun superieuren. Doordat hun kennis of professionaliteit niet wordt erkend, gaan ze zich wreken op de dienst of het bedrijf door informatie te lekken. Deze vorm van bittere sabotage komt de werkomgeving niet ten goede en straft mede zijn collega's. Geld of ideologie is hier nooit aan de orde.

6.4. Seks, intimidatie en afpersing

Het liefdes/seksueel aspect gebruiken om bepaalde individuen te verleiden om voor hen te spioneren is een zeer vaak gebruikte techniek van rekruteringsofficieren. '*Romeos'* of '*Ravens'* (mannelijke verleidende agenten) en '*Swallows'* (vrouwelijke verleidende agenten) hebben vaak hun reputatie waargemaakt als de ultieme verleider. Ze zijn altijd uiterst doeltreffend en slagen erin zeer veel informatie in te winnen van hun slachtoffers. De relatie die ze hebben met hun slachtoffer kan ook gebruikt worden als drukmiddel (foto's of beelden van een geënsceneerde affaire) als de spion later ineens van gedachte veranderd en weigert nog verdere informatie te verstrekken. Dit is zeer doeltreffend als het slachtoffer getrouwd is of een hoge reputatie geniet.

Geen enkele persoon met een hooggeplaatste functie zou graag foto's uitgelekt zien van zijn avontuurtjes of 'ongewone' levenswijze. Naast deze vorm van chantage kan een inlichtingenofficier of rekruteringsofficier het slachtoffer chanteren. Dit met het feit dat hij al informatie heeft geleverd als spion, en er al dan niet voor betaald is geweest, waardoor hij een zware misdaad heeft begaan. Hij is met andere woorden in de val gelokt.

Als het slachtoffer dan niets onderneemt om dit te melden aan zijn superieuren of inlichtingendienst van zijn land, zal hij vastzitten in een neerwaartse spiraal. Om te voorkomen dat het slachtoffer toch publiek zijn acties kenbaar maakt, zullen inlichtingenofficieren of rekruteringsofficieren de spion intimideren. Het bedreigen van zijn/haar familie is meestal het laatste drukkingsmiddel dat kan gebruikt worden om iemand zover te krijgen om verder te doen met de spionageactiviteiten.

6.5. Redenen van vriendschap, etniciteit of religieuze solidariteit

Een krachtige motivatie voor het plegen van spionage, die vaak ook ondergewaardeerd wordt, is simpele naïeve vriendschap. Uit onwetendheid kan een individu een goede band opbouwen met een rekruteringsofficier. Deze band kan uitgroeien tot echte vriendschap en als vriendendienst spioneert het individu of geeft hij belangrijke informatie door. En op dit moment is de gemeenschappelijke etniciteit, culturele afkomst of religieuze band tussen een spion en het land dat hem rekruteert een opkomende sterke motivatie om over te gaan tot spioneren.[85] Het aanwakkeren van patriotisme is zijn comeback aan het maken in de inlichtingenwereld en dit dan voornamelijk in Amerika en het Midden-Oosten.

6.6. '*The Spy Game'* en omwille van het spel

Zowel in de eerste wereldoorlog als tijdens de Koude Oorlog kon men rekenen op spionnen en inlichtingenofficieren die spioneerden omwille van het spel. Spion zijn, wat voor velen zelfs nu nog steeds een romantisch beeld oproept, is voor sommige de beste voldoening die men kan krijgen. Er bestaan in de literatuur enkele 'excentrieke' spionnen die geen andere beweegreden nodig hadden. In de meeste gevallen echter ontvingen de spionnen nog een financiële vergoeding of deed men het ook vanuit een bepaalde ideologie als secundaire beweegreden.

Ondanks dat spionage tegen het eigen land nog steeds op veel afkeer kan rekenen, kan het voor counterintelligence agenten een bepaalde vorm van respect opbrengen. Juist omwille van de sterke persoonlijkheid en professionaliteit dat een individu spionage pleegt, kan hij nog steeds achtbaar zijn.

[85] HUBAND, M., *Trading secrets. Spies and Intelligence in an Age of Terror*, New York, I.B. Tauris, 2013, p.56-69

7. CASESTUDY: "DE RODE KOLONEL" ALIAS DE ZAAK BINET

"Op dinsdag 6 september 1988 verscheen er op de voorpagina van de Belgische krant Le Soir volgend bericht;[86]

" Colonel espion arrêté : il vendait des secrets militaires à l'U.R.S.S." […] "un officier supérieur de la Force aérienne, le colonel Guy Binet (54 ans), est arrêté et au secret jusqu'à ce mardi, inculpé d'atteinte à la sûreté de l'État. Il a avoué avoir vendu depuis deux ans au moins à l'Est, pour des millions de francs, des documents et des informations sur l'armée belge et la stratégie de l'O.T.A.N "

Deze aanhouding zal, hoe ironisch het ook mag klinken, leiden tot een van de mooiste en bekendste voorbeelden van spionage in België. Dit vooral door de omvang van de zaak zelf. De 'brave' Belgische burgers werden toen met de neus op de feiten gedrukt van het reële gevaar van spionnen zoals men voordien enkel gelezen had in stationsromans of stripverhalen.

Kolonel Gustave "Guy" Binet heeft het als officier bij de toenmalige Belgische Krijgsmacht ver geschopt. Na zijn studies aan het atheneum in Dinant ging hij zijn dienstplicht vervullen. Doordat hij al van jongs af aan een hoge dosis aan intellect bezat, werd hij al snel opgemerkt door zijn oversten. Hij begon aan een echte blitzcarrière wanneer hij binnen ging als vrijwilliger zodat hij de toelatingsexamens van de Koninklijke Militaire school niet (opnieuw) moest afleggen. Als jonge matroos zal hij snel doorgroeien via het kader van onderluitenant om vervolgens op de administratiedienst te werken.

Hieruit zal hij op de telecommunicatiedienst van de luchtmacht terechtkomen. Door specialisaties in telecommunicatie - en versleutelingstechnieken te volgen, evenals een bijkomende opleiding in militaire administratie, wordt hij definitief overgeplaatst naar de generale staf van het Koningin Elisabethkwartier te Evere. Hij wordt beschouwd als een harde betrouwbare werker, steeds vriendelijk en correct. Evenals staat hij bekend bij zijn collega's als een charmeur die gemakkelijk aan het flirten slaat. [87]

[86] HAQUIN, R. & MATHIL, P., Colonel espion arrêté, Le Soir, 6 maart 1988, p.1
[87] VAN DAMME, G., Cour militaire., Le Soir, 10 juni 1989 , p.7

Op 26 september 1983 organiseert de Vriendschapvereniging België - USSR een thema-avond vond die een lezing inhoudt over de negentiende-eeuwse Russische schrijver Ivan Toergenjev. Binet, die opgegroeid was tijdens de Koude oorlog, had altijd een bepaalde interesse voor wat er aan de andere kant van het "IJzeren Gordijn" lag. En een dergelijke thema-avond, georganiseerd door deze "vriendschapskring", brengen Belgen en burgers uit de Sovjet Unie dichter bij elkaar. Het is aannemelijk dat deze interesse is voortgevloeid uit het feit dat Binet was opgegroeid tijdens de Koude Oorlog, een grijze naoorlogse periode gekenmerkt met grote politieke en militaire spanningen tussen Oost en West. Hij wil als het ware het denken van deze Sovjet-Unie inwoners beter leren kennen. Iets wat zeker niet ongepast is als hoog officier. Het gezegde 'ken je vijand' zal zeker door zijn hoofd hebben gespookt.

Op deze avond ontmoet hij Piotr die zichzelf voorstelt als "adjunct van de militaire attache van de Sovjet Unie. Wat Binet niet realiseert is dat Piotr een alias is van Petr Prokoptsov. Podpolkovnik[88]. Petr Prokoptsov werkt als rekruteringsofficier voor de Russische geheime dienst die beter gekend is onder de benaming GRU. Zoals dit eerder in deze thesis aan bod kwam, zijn rekruteringsofficieren van vitaal belang om de juiste potentiële personen te vinden en hen te rekruteren als agent.[89]

'Piotr' komt gedurende achttien maanden regelmatig op bezoek bij het thuis van Binet. Zeer geduldig verzamelt hij stukje voor stukje informatie over Binet zelf. Hiermee is de rekruteringsofficier in staat om een duidelijk profiel van zijn doelwit te schetsen, evenals de methode voor te bereiden om zijn doelwit te overhalen voor hem te werken. Er zijn immers zes verschillende soorten motivaties waardoor iemand kan overhaald worden zijn land te 'verraden'. Dus het is van het grootste belang om achter iemand zijn zwaktes te komen om zo de juiste strategie te hanteren.[90]

Al snel wordt het duidelijk dat Binet niet meteen ideologisch te overtuigen is voor de zaak. Hij is wel tegen de imperialistische houding van Amerika en het zwart-wit kijken naar de wereld. Piotr en Binet bespreken en bediscussiëren vaak de internationale geopolitiek evenals de zoektocht naar een vreedzame oplossing naar de toekomst toe. Piotr wil Binet graag voorstellen aan een andere collega die in Wenen vertoeft.

[88] Russische rang voor Luitenant-Kolonel
[89] X, (2011/08/21), De KGB in België (5): De rode kolonel[WWW.] Apache : /http://www.apache.be/2011/08/21/de-kgb-in-belgie-5-de-rode-kolonel/ [18/03/2014]
[90] CLERIX, K., Spionage. Doelwit Brussel, Antwerpen, Manteau, 2013, p. 43-60

Hij tracht Binet te overtuigen voor een rendez-vous om een gedachtewisseling te doen. Maar Binet is hier niet gerust op. Hij voelt aan dat hij dit voor zijn carrière beter niet doet. Hij weet niet wie deze zogenaamde 'vriend' is dus slaagt hij het aanbod af. De rekruteringsofficier heeft nog maar twee manieren om hem te overtuigen, namelijk; chantage en druk uitoefenen of hem omkopen met geld. Hij besluit om druk uit te oefenen door middel van foto's die genomen zijn op de thema-avond in Sint-Joost van de vriendschapskring. Subtiel toont Piotr de foto's en vertelt hem dat hij ze wil publiceren in het tijdschrift van de vereniging.

De foto's op zich zijn gewoon momentopnamen van ontmoetingen maar dan wel met hoge Sovjet officieren. Dergelijke ontmoetingen kunnen een hoog officier als Binet in nauwe schoentjes brengen. Men is in die periode zeer achterdochtig en de kans bestaat dat men Binet al gaat zien als pro-Russisch, iets wat hij absoluut wil vermijden. Ook heeft hij de ontmoetingen met Pjotr en anderen nooit bij zijn oversten gemeld waardoor hij militaire voorschriften heeft overtreden. Deze overtredingen kunnen een zware blaam en/of een mogelijke overplaatsing veroorzaken.[91]

Op 20 augustus 1986 vindt de ontmoeting plaats te Wenen. Door op voorhand afgesproken codezinnen weten ze elkaar te herkennen. De man die Binet ontmoet is een zekere Valère, die de graad van Polkovnik[92] draagt binnen het Rode leger. Maar ook hier is dit maar een schertsvertoning want Valère blijkt niemand minder te zijn dan de adjunct-chef van het eerste GRU directoriaat in Moskou ; General-Polkovnik[93] Glazkov.Glazkov wil graag dat Binet hem informatie bezorgt over nucleaire aangelegenheden in het Westen, maar dit wordt door Binet geweigerd. De generaal kan tot een compromis komen met Binet over het bezorgen van een aantal bepaalde geclassificeerde NAVO-documenten. Binet denkt dat Glazkov voor de Conferentie voor Veiligheid en Samenwerking werkt, maar vermoedt ook dat er iets niet klopt. Vooral niet als hij een zwart Minox EC fototoestel toegestopt krijgt en Afgapan filmrolletjes. Het fototoestel is gemanipuleerd zodoende het brandpuntafstand is aangepast van tachtig naar tweeënveertig centimeter terwijl de lens ook schuin staat. Dit om foto-opnames aan een bureau te vergemakkelijken. De fotorolletjes zijn ook abnormaal doordat ze flinterdun zijn en tot 110 opnames kunnen bedragen.

[91] CLERIX, K., Spionage. Doelwit Brussel, Antwerpen, Manteau, 2013, p. 43-60
[92] Russische rang voor Kolonel
[93] Russische rang voor Generaal

De val wordt duidelijk en Binet zit er middenin. Glazkov stopt Binet nog een enveloppe in de handen om de 'reiskosten' te dekken. Deze enveloppe bevat 200.000 Belgische Frank en een biljet van 500 dollar. Als laatste krijgt Binet een dreigement; "Wees voorzichtig en denk aan je familie". Woorden die Binet heel ernstig neemt. Een prachtige strategie van een rekruteringsofficier om een belangrijke pion eigen te maken. Binet zit nu al diep in de problemen. Hij is in een typische val gelokt en heeft zijn eer, door het geld en de camera aan te nemen, verkocht aan een buitenlandse agent. Hier bovenop weet hij dat het verkeerd kan aflopen met zijn dierbare familie als hij niet op zijn tellen let.

Doch is de zaak op dit moment nog niet verloren. Hij heeft een beschrijving van twee mogelijke buitenlandse agenten evenals bewijsmateriaal (geld, camera, etc.) en een lijst van documenten die ze zoeken. Als hij hiermee naar de militaire inlichtingendienst zou stappen, of zijn oversten in zou lichten wat hem is overkomen, zou hij de rollen hebben kunnen omdraaien. Maar in plaats daarvan houdt hij het geld in een buitenlandse kluis en koopt met de dollars een radio ontvanger. [94] Het is nu wel duidelijk dat zijn aanblik niet kon weerstaan aan de inhoud van de envelop evenals bereidwillig te verklaren zijn land, eer en geweten te verkopen voor geld. Menselijke hebzucht is nu eenmaal diep geworteld.

In het najaar van 1986 neemt hij voor het eerst geclassificeerde NAVO documenten mee naar huis en legt alles vast op foto met zijn gekregen fototoestel. Deze documenten op fotorol zal hij in de tweede week van het nieuwe jaar persoonlijk bezorgen aan Glazkov. Maar door de slechte kwaliteit van de opnames verhoogt de Rus zijn dreigementen aan Binet en zijn dochters. Binet weet dat hij niet meer terug kan en dat hij een brug te ver is gegaan. Om zijn geweten te sussen stelt hij een samenwerkingsakkoord voor; bruikbare foto's van belangrijke documenten in ruil voor een bedrag van tien miljoen Belgische Frank. Dit bedrag zal herleid worden tot vijf miljoen Belgische Frank en een compromis wordt bereikt. Binet zal diezelfde avond nog genieten van een snelcursus in GRU-technieken om de camera beter te hanteren.[95]

Binet leert radioboodschappen ontcijferen met coderingstabellen. Een van deze tabellen, gedrukt op een fijn rolletje papier dat verborgen zit in een Snowman viltstift, bestaat uit reeksen van steeds vijf cijfers. Een andere tabel staat dan weer voor de geplande radiofrequenties voor de rest van het jaar waarlangs versleutelde radioboodschappen zullen verstuurd worden.

[94] CLERIX, K., Vrij spel. Buitenlandse geheime diensten in België, Antwerpen, Manteau, 2007, p. 149-156
[95] CLERIX, K., Spionage. Doelwit Brussel, Antwerpen, Manteau, 2013, p. 43-60

Hij kan zelf ook versleutelde boodschappen versturen als hij in contact wenst te komen met de Glazkov of één van zijn collega's. Dan moet hij een brief, geschreven in onzichtbare inkt, versturen naar een zekere *"heer W. Treusch, Am Schöpfwerk 29/14/34 te Wenen"*. [96] Dan leert hij de werking van het dode brievenbus principe. Iets wat tot de hedendaagse tijd in gebruik is.

De dode brievenbussen zijn niets meer dan een holle (bak)steen, spelonk of holte op een vooraf gesproken plek waar men bepaalde documenten of voorwerpen achterlaat. De plekken kunnen via radio, telefoon, krant met 'persoonlijke toets' of op mica velletjes worden afgesproken. Bij Binet waren dit mica velletjes die door middel van eosine hun onzichtbare boodschap weergeven. Iets wat ook later zal gebruikt worden tegen hem in zijn proces. Eenmaal er 'post' in de dode brievenbus is, zal de zender door middel van een krijttekening dit kenbaar te maken aan de bestemmeling.

De dode brievenbussen van de Russen stonden toen ook steeds in een straal van dertig kilometer rond de Sovjetambassade waar Sovjet diplomaten vrij mogen bewegen. Want zouden ze buiten deze zone gaan, dan moesten ze dit melden aan Buitenlandse Zaken. Wel stonden ze dan meestal in stille landelijke gebieden om observaties van de Belgische inlichtingendiensten, zoals deze van de VSSE of de ADIV en haar SDRA III dienst, te bemoeilijken. Als men toch betrapt wordt, kan men nog steeds vertellen dat men aan het wandelen is, paddenstoelen zit te zoeken of een mooi picknick plekje zoekt.

Vooraleer ze afscheid nemen krijgt hij een Cavalet aktetas mee die een dubbele bodem bevat en met een druk op een verborgen knop een geheim mechanisme opent. Hiermee is Binet in staat documenten te smokkelen. Hij zal er al meteen dankbaar gebruik van maken om zijn 1,8 miljoen frank, die hij gekregen heeft van zijn nieuwe Russische partners, te smokkelen naar België. In het voorjaar van 1987 zal hij nog een som van één miljoen Belgische Frank ontvangen, die verstopt is in het kattenluik onder de stenen trap van zijn huis. Niet veel later komt SDRA III erachter, na een tip van de Amerikaanse '*Defense Intelligence Agency'* (DIA) , dat Binet contacten heeft met Glazkov die gekend is als Sovjet agent.[97]

[96] CLERIX, K., Spionage. Doelwit Brussel, Antwerpen, Manteau, 2013, p. 43-60
[97] X, (2011/08/21), De KGB in België (5): De rode kolonel[WWW.] Apache : (/http://www.apache.be/2011/08/21/de-kgb-in-belgie-5-de-rode-kolonel/ [18/03/2014]

Een speciaal opgerichte taskforce zal het begin inluiden van '*Operation Ostrich'*, alias Operatie Struisvogel. Binet wordt geschaduwd en geobserveerd. Iedereen met wie hij in contact komt wordt nagetrokken. Zijn reilen en zeilen worden tot in de kleinste details nauwkeurig bijgehouden. De observaties leveren niet veel op. Hij weet dat SDRA III hem observeert doordat een collega hem vertelde dat deze dienst hem vragen had gesteld over Binet zelf. Binet leeft in angst en dit zowel voor SDRA III als voor de Russen en hun mogelijke vergeldingsacties tegen zijn familie.

Nadat hij zijn situatie heeft uitgelegd aan de GRU, die alweer kloegen over overbelichte en onduidelijke foto's, krijgt hij nog een som van driehonderdduizend Belgische Frank. Dit zal ook zijn laatste omkopingssom zijn geweest. Niet veel later ondervragen twee commissarissen Binet aan de hand van foto's, genomen in Wenen waarop hij te zien is met Glazkov. Na een lang verhoor zwicht hij en bekent hij alles. Hij vraagt wel om bescherming voor zijn familie en zichzelf tegen mogelijke wraakacties van de Russen. Er worden huiszoekingen gedaan op zijn bureau en in zijn huis in samenwerking met West-Duitse specialisten op aanvraag van de onderzoeksrechter. Deze specialisten hebben immers veel meer ervaring op dat vlak dan onze eigen diensten. Snel vonden ze alles terug, voornamelijk doordat Binet zijn materiaal zeer slordig verstopte. [98]

Binet had voor zijn arrestatie nog contact gehad met de GRU, die een ontmoeting gepland hadden met hem. Hij moest hierbij drie pasfoto's meebrengen en moest deze geven aan een nieuwe contactpersoon. Misschien dat ze hem een Russisch paspoort wouden geven waardoor hij, in geval van nood, naar de Sovjet Unie zou kunnen vluchten. De ontmoeting zal nu, ondanks de aanhouding van Binet, toch doorgaan. Maar een dubbelganger zal zijn plaats innemen. De dubbelganger zal de nieuwe Russische contactpersoon, een diplomaat, in de val laten lopen en hem de keuze geven tussen werken voor de SDRA III of arrestatie. De diplomaat kiest om te wisselen van kamp en wordt een dubbelspion. Een mooi voorbeeld van hoe Sun-Tsu's visie en strategie van dubbelspionnen in de praktijk omgezet. In 1989 wordt Binet veroordeeld tot twintig jaar dwangarbeid, militaire degradatie en verliest hij op te koop toe de meer dan vier miljoen Belgische Frank die hij had gekregen als omkoopsom van de Russen. Na vijf jaar komt hij vervroegd vrij en verdwijnt hij in de anonimiteit.[99]

[98] Persoonlijk interview met X, één van de twee commissarissen die het onderzoek heeft geleidt.
[99] HAQUIN, R. & MATHIL, P., Colonel espion arrêté, Le Soir, 06 maart03 1988, p.6

8. BESLUIT

In dit eerste deel is er een uiteenzetting gedaan van de term spionage in haar volledigheid. Deze verduidelijking toont de complexiteit en variatie aan die de term inhoudt. Er bestaat enorm veel literatuur maar het is belangrijk de term tegen een hedendaagse achtergrond te zien. Ondanks dat er niet veel veranderd is in het principe van inlichtingenwerk, is er veel veranderd in de manier waarop men aan inlichtingenwerk doet. En dit manifesteert zich vooral in de OSINT, TECHINT en CYBINT zijde. Er is nog nooit zo veel informatie beschikbaar geweest en kan met enkele muisklikken al opgevraagd worden.

Het wordt ook duidelijk hoe vaak deze informatie een vertrouwelijk karakter bevat en achteloos op het wereldwijde net wordt geplaatst. Dit deel gaat niet verder in op het gebruik van deze methoden door de Belgische inlichtingendiensten. Het is niet direct eenvoudig te zeggen welke methoden ze wel of niet toepassen. De jaarverslagen van de inlichtingendiensten wekken wel de indruk op dat alle vormen, in die mate van het (financieel) mogelijke, worden toegepast. Vooral CYBINT is actueel door de vele recente cyberaanvallen alsook de oprichtingen van een ‘coördinatiecentrum rond cyberveiligheid’ om beter in te spelen op de toekomst.

Spionage als term omvat een waaier aan technieken om informatie in te winnen. Elke gespecialiseerde techniek omvat specifieke eigenschappen. Nadat er voldoende informatie is ingewonnen doorloopt ze de inlichtingencyclus. Het belang van deze cyclus is ook naar voren gebracht in dit deel. Het zorgt immers dat de verwerkte en geëxploiteerde informatie nog geanalyseerd dient te worden. Deze filters vormen de ruwe informatie om tot bruikbare inlichtingen. Hierna komt de verbreiding die zal uitmaken of de verkregen inlichtingen nog bijgestuurd moeten worden of niet. Deze inlichtingen zijn altijd enorm waardevol geweest voor inlichtingen - en veiligheidsdiensten. Door deze kennis zijn deze diensten in staat om mogelijke toekomstige plannen of acties van bepaalde landen uit te stippelen. En niet alleen daarom, maar het is voor het landsbelang steeds interessant te beschikken over de nieuwste informatie. Immers, deze informatie draagt bij tot de eigen grootsheid of groei.

Na deze interessante uiteenzetting is er nauwer ingegaan op de beweegredenen om aan spionage te doen. Vooral de twee nieuwe bijgevoegde beweegredenen geven een meerwaarde aan het onderzoek naar spionage. HUMINT blijft de meest gebruikte bron om informatie uit te verkrijgen.

Ondanks enkele nadelen is deze inlichtingenbron essentieel voor het inwinnen van informatie en speelt het een belangrijke rol in de beveiliging van het inlichtingenapparaat. Satellieten, afluisterapparaten of andere technische middelen leveren zeer waardevolle informatie. Althans zijn deze technische middelen niet in staat om bepaalde emoties of intenties op te vangen zoals een menselijke bron.

Om te eindigen is er nauwer ingegaan op de zaak Binet. Deze zaak toonde aan hoe spionage in de praktijk verloopt. Het is een weliswaar een oude zaak tijdens een hoogtepunt in de Koude Oorlog, Desalniettemin is ze nog steeds het ideale voorbeeld van hoe spionage via menselijke bronnen heden ter dage zou verlopen.

Het reële gevaar van spionage is terug aangewakkerd na de vele berichtgevingen in de media en de bekentenissen van klokkenluider Edward Snowden. Amerika en Engeland die aan 'spionagewaan' leiden en al haar bevriende landen bespioneren. Duitsland neemt wraak door aan contraspionage te doen op Amerika naast haar vaste contraspionage op andere grootmachten. De vrees voor cyberspionage gaat zo ver dat zowel Rusland als Duitsland het gebruik van ouderwetse typmachines voor interne communicatie gebruiken.

Het conflict in Oekraïne doet de spionage activiteiten van Rusland drastisch toenemen. Ook België is al vele malen het doelwit geweest van buitenlandse (Russische) cyberaanvallen. Dit alles, alsook het toenemend verlies van privacy en angst voor een daadwerkelijk oorlog, doet de burger het gevoel opleven dat er een nieuwe Koude Oorlog aan de gang. Een gevoel dat voor sommigen als beklemmend en angstaanjagend wordt ervaren en door anderen dan weer als een melancholisch en romantisch gevoel naar oude vervlogen tijden.

DEEL II. (BUITENLANDSE) INMENGING

"I don't see why we need to stand by and watch a country go communist due to the irresponsibility of its people. The issues are much too important for the Chilean voters to be left to decide for themselves."

Henry A. Kissinger

1. INLEIDING

De reden dat inmenging nog steeds een containerbegrip is, komt door het veelzijdig karakter ervan. Hierdoor moet er een duidelijke afbakening komen. In deze thesis ligt de focus vooral op inmenging door buitenlandse inlichtingendiensten en de schending van het Belgische soevereiniteitsbeginsel. Inmenging ondermijnt ook de democratische rechtsorde en tast de politiek ambtelijke integriteit aan. Er bestaat ook inmenging binnen de Belgische politiek en al dan niet met betrokkenheid van industriëlen. Maar dit zou ons enerzijds te ver afleiden van het onderzoeksdoel en anderzijds is het zeer moeilijk een grens de onderscheiden. Het is immers in België en Europa toegestaan om te lobbyen. Dit is de grijze zone waardoor inmenging opsporen soms moeilijk gaat.

Hier zal dit begrip vooral handelen over politieke inmenging door buitenlandse inlichtingendiensten of mogendheden. Dit met het doel om buitenlandse agendapunten of doelstellingen erdoor te krijgen en politieke beslissingen te beïnvloeden. Het is zeer moeilijk om dit deel af te bakenen. Aan de ene kant bestaat er weinig literatuur over. Aan de andere kant is er, zoals eerder aangehaald, slechts een dunne lijn tussen inmenging en lobbyen waardoor het moeilijk is om spionnen evenals verboden activiteiten op te sporen. [100]

2. DEFINTIE

Een mogelijke definitie kan gevonden worden in artikel 8, 1°, g. van de organieke wet van 30 november 1998 die de werking van de inlichtingendiensten bepaalt;

[100] X, *Brochure : De* Veiligheid *van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.28

"De poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden". [101] De reden dat inmenging nog steeds een containerbegrip is, komt door het veelzijdig karakter ervan en de door de wetgever omschreven vaagheid van het begrip.

3. AGENT OF INFLUENCE

Wanneer een buitenlandse natie of organisatie bepaalde publieke opinies of beslissingen wil beïnvloeden op politiek, wetenschappelijk, economisch of militair vlak, dan maakt men vaak gebruik van een *'agent of influence'*. De term *'agent of influence'* is, in tegenstelling tot de Franse vertaling *'agent d'influence'*, niet gekend in het Nederlands. Er wordt enkel gesproken over (vijandige) agenten. Daarom zal voor de eenvoud ook hier gesproken worden van agenten, maar verschillend van de reeds beschreven agenten in het vorige deel gaande over spionage.

E. Howard Hunt, een voormalig CIA officier en gekend uit het Watergate schandaal, definieert een beïnvloedingsagent die zich bezighoudt met inlichtingen als;

"Either a government official so highly placed that he can exercise influence on government policy or an opinion molder so influential as to be capable of altering the attitudes of an entire country" [102]

De voormalige KGB maakte gretig gebruik van hun actief beïnvloedingsprogramma dat ze zelf de onopvallende naam *'aktivnyye meropriyatiya'* gaven. Deze term diende om hun echte activiteiten te verdoezelen. Dit programma had tot doel tweedracht te zaaien in de Westerse politiek en publieke opinie. Hierin slaagde ze door onder andere desinformatie, manipulatie, het verlenen van financiële aan bepaalde politieke partijen of verenigingen, het uitzenden van radioprogramma's en de namaak of het verdelen van valse propaganda. De meest doeltreffende manier was het gebruik van agenten, *'agent vlyiyania'*, om minder significante (*'lower key'*) publieke opinies te beïnvloeden. Door het feit dat ze minder significant zijn, betekent niet dat ze minder belangrijk zijn. Een pion in een schaakspel staat ook soms sterker dan een andere pion en draagt bij tot de overwinning van het gehele spel.[103]

[101] Organieke wet van 30 november 1998, artikel 8, 1°, g. , Belgisch Staatsblad, 18 december 1998
[102] GOULDEN, J.C., T*he dictionary of espionage. Spyspeak into English*, New York, Dover Publications, 2012, p. 3-5
[103] ROMERSTEIN, H., *Soviet Active Measures and Propaganda: "New Thinking" & Influence*

De Russen hadden al opgevangen dat de Amerikanen langzaam de Russische desinformatie - en beïnvloedingsstrategieën gewaar werden. Wat ook later echt aan het licht kwam na de openbaring van de Russische overloper Stanislav Levchenko.[104]

Een agent die zich bezig houdt met inmenging is een individu die een bepaalde hoge of invloedrijke status of functie bekleedt. Dit kunnen journalisten, professoren, politici, senators en parlementsleden, bedrijfsvertegenwoordigers, religieuze leiders of diplomaten zijn. Genietend van zijn status of functie, is de beïnvloedingsagent in staat de publieke opinie of beslissing in een land te beïnvloeden zodoende de uitkomst in het voordeel is van de inlichtingendienst voor wie de agent werkt. Hun status en functie permitteren hen immers te lobbyen of in discussie te treden over bepaalde gevoelige standpunten met andere hooggeplaatste individuen. Een etentje tussen twee hooggeplaatste personen, waarvan één agent is, is zeker niet ongewoon.[105]

Dergelijke agenten behoren daardoor tot de meest effectieve middelen om buitenlands beleid om te zetten naar de eigen hand van een andere natie. Ze hebben al een grote carrière gemaakt in het land, worden vertrouwd door hun omgeving en hebben een grote hooggeplaatste vriendenkring waardoor ze regelmatig contact hebben met belangrijke sleutelfiguren. Nietsvermoedende personen weten ook in de meeste gevallen niet dat ze beïnvloed worden door een agent, die zelf bespeeld wordt door een buitenlandse inlichtingendienst.[106]

Beïnvloedingsagenten doen zelden aan spionage of informatieverzameling, noch hebben ze echte beweegredenen zoals bij spionnen. Ze krijgen weliswaar van een inlichtingenofficier eens 'kleine' relatiegeschenken zoals een zilveren vulpen, een visum voor een bepaald land, een dure fles wijn, enz. Ook gebeurt het vaak dat hun vereniging, organisatie of publicaties (digitaal en drukwerk) onbewust financieel gesteund worden met donaties van een inlichtingenofficier. Dit alles versterkt de 'vriendschapsband' tussen elkaar evenals de invloed die de officier uitoefent op de agent. Dit alles maakt het de counterintelligence dienst meestal onmogelijk om proactief op te sporen of genoeg bewijs te verzamelen.[107]

Activities in the Gorbachev Era , Toronto, Mackenzie Institute for the Study of Terrorism, Revolution, and Propaganda, 1989, p.5

[104] FEDERAL BUREAU OF INVESTIGATION, *Soviet Active Measures in the United States: 1986–1987,* Washington, FBI, 1987, p.1-2

[105] SHULTZ, R.H. en GODSON, R., *Dezinformatsia: Active Measures in Soviet Strategy,* New York, Pergamon Brassey's, 1984, p. 133

[106] MITROKIN, V., (ed*.) KGB Lexicon: The Soviet Intelligence Officer's Handbook*, Groot Brittanie, Frank Cass & co, 2002, p.33.

[107] SCHOEN, F., en LAMB, C.J., *Deception, disinformation, and strategic communications. How one interagency group made a major difference,* Washington, National Defense University Press, 2012,p.18-20 .

Er zijn drie vaak voorkomende soorten agenten die gebruikt worden bij inmenging.[108]

- Eerst hebben we de agent die direct gerekruteerd en gecontroleerd wordt door een buitenlande inlichtingendienst. Dit wil zeggen dat hij letterlijk alle doorgegeven teksten en standpunten krijgt van andere diensten. Hij doet dit meestal uit een ideologische en/of financiële motivering.

- Als tweede categorie is er de agent die goede contacten heeft met een inlichtingenofficier. Hij collaboreert vaak met de inlichtingenofficier om bepaalde standpunten te laten doorschemeren aan de publieke opinie. Zelf is hij niet gerekruteerd of gecontroleerd door een buitenlandse dienst waardoor hij steeds onafhankelijk blijft in zijn schrijven en spreken. Vaak vermoeden dergelijke agenten dat ze bewust beïnvloed worden, maar zien het eerder als een verrijking van kennis en een verfrissende andere kijk op de huidige maatschappij. Ze weten tot in welke mate hun handelingen gevolgen hebben voor een buitenlandse natie.

- De derde soort is de agent die totaal onbewust is dat hij beïnvloed wordt. Door zijn naïviteit heeft hij geen enkel idee wat de gevolgen zijn van zijn acties. Hij ziet de inlichtingenofficier als een goede vriend of collega.

Als laatste punt is het belangrijk aan te halen dat een agent niet alleen hoeft te slaan op een natuurlijk persoon, maar evengoed een rechtspersoon kan zijn. Met andere woorden kunnen ook bedrijven, partijen, organisaties of verenigingen als agent functioneren.

4. SOORTEN INMENGING EN HUN DOEL

Ons 'klein' land ligt geografisch tussen grootmachten met vele internationale instellingen, buitenlandse gemeenschappen en bedrijven. Het is dan ook niet ondenkbaar dat België vaak het doelwit is van andere landen, bedrijven en organisaties die interne beslissingsprocessen willen beïnvloeden. We onderscheiden politieke inmenging, ideologische inmenging, economische inmenging en religieuze inmenging.

[108] SHULTZ, R.H. en GODSON, R., *Dezinformatsia: Active Measures in Soviet Strategy,* New York, Pergamon Brassey's, 1984, p. 193-194

Ook kan inmenging handelen over de beïnvloeding of het verwerven van controle over; buitenlandse gemeenschappen en etnische minderheden[109] die aanwezig zijn in dit land.[110]

4.1. Politieke inmenging

Politieke inmenging kan gericht zijn tegen een staatshoofd van een land, regeringen of specifieke politiekers en hun partijen. [111] Zo kan opzettelijke rondcirculerende desinformatie bepaalde politieke individuen of staatshoofden in diskrediet brengen. Als deze georganiseerde 'lastercampagnes' door vijandige buitenlandse elementen slagen in hun opzet, kan dit leiden tot het ontslag of afzetting van het staatshoofd of regering. Anderzijds kunnen buitenlandse agenten ervoor zorgen dat, door het verspreiden van desinformatie, staatshoofden of regeringen een andere politieke koers gaan varen en hun bondgenootschappen veranderen. Deze verandering van bondgenootschap komt dan ten goede van het buitenlands land wiens agenten de desinformatie hebben geplaatst.

4.2. Economische inmenging

Door bepaalde economische standpunten te veranderen, geheime samenwerkingsakkoorden of afspraken te maken, is men in staat de economische markt te beïnvloeden naar eigen voordeel. Vooral economische inmenging is moeilijk op te sporen doordat er een vage grens bestaat tussen het wettelijk toegestane lobbyen enerzijds en spionage en inmenging anderzijds.

4.3. Ideologische inmenging

Ideologische inmenging is zeer vergelijkbaar met politieke inmenging omdat het ook de politieke context van het land omvat. Het verschil ligt in het feit dat ideologische inmenging de gehele ideologie en beleid dat een land hanteert omvat en niet enkel de beleidsbeslissingen. Zo kan een buitenlands land zijn ideologie proberen opleggen in een bepaald land.

---

[109] NASHERI, H., *Economic espionage and industrial spying*, Cambridge, Cambridge university press, 2005, p.127.
[110] CLERIX, K., S*pionage. Doelwit Brussel*, Antwerpen, Manteau, 2013, 262 p.
[111] HAYNES, J.E, en KLEHR, H., *Early cold war spies. The Espionage trials that shaped American politics,* Cambridge, Cambridge university press, 2006, p.232

Dit om sterke bondgenootschappen te creëren en samen dezelfde strafrechtelijke, economische of religieuze te ideeën te delen. De landen die trachten deze ideologie op te leggen, willen en mogen door hun ideologie geen bondgenootschappen sluiten met landen die niet dezelfde ideologie hanteren.

4.4. Religieuze inmenging

De laatste jaren is religieuze inmenging gestegen en dit voornamelijk in Westerse en Oosterse landen. Door de toename van fundamentalisten en radicalen, neemt ook de toename van religieuze inmenging toe. Zij trachten hun geloofsovertuiging op te leggen aan bepaalde bevolkingsgroepen door hun te wijzen op hun foute levensstijl, de mogelijke gaten in hun denken en vooral door angst en desinformatie te verspreiden. Religieuze inmenging leunt ook zeer dicht aan bij politieke en ideologische inmenging doordat het tracht de scheiding tussen staat en geloof te vervagen.

4.5. Inmenging in bevolkingsgroepen en gemeenschappen

Naast deze vormen van inmenging bestaat er ook het zogenaamde 'entrisme'[112]. Dit is de betrachting om zich in te werken in een private onderneming, publieke instelling of overheidsdienst met als doel het van binnenuit sturen van beslissingsprocessen of standpunten. Misleidende campagnes, desinformatie, aanzetten tot geweld en haat of het creëren van spanningen door buitenlandse elementen behoren tot 'entrisme'. Dit om bepaalde negatieve gedachten te voeden en te versterken over de staat, hetgeen aanleiding kan geven tot machtsovername door het volk of sabotage.

5. CASESTUDY : KRUPKA, AGENT D'INFLUENCE

Inmenging is steeds een moeilijk te onderzoeken feit omdat het moeilijker te bewijzen valt en het in veel gevallen gaat om subtiele beïnvloeding en het financieren van wel uitgekozen personen wegens hun ideologie of daden door buitenlandse agenten. Een wel beschreven en gedetailleerd voorbeeld van inmenging in België is de zaak van geheim agent Jan "Krupka" Braňka.

[112] X, *Brochure : De Veiligheid van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.29

Dit voorbeeld is enkel en uitvoerig beschreven door Kristof Clerix in zijn boek "Spionage. Doelwit Brussel". Clerix heeft 26.000 archiefdocumenten over Krupka bestudeerd evenals hem geïnterviewd. Dit uniek gegeven maakt het daarom boeiender deze case aan de hand van dit boek te bestuderen dat enorm veel authentieke en correcte gegevens bevat. [113]

Tijdens de Koude Oorlog probeerde vele landen van de Sovjet Unie de publieke opinie te bespelen. Dit met het oog op het promoten van; het communistische gedachtegoed en het Warschaupact, de gevaren en zelfdestructie van het Westerse kapitalisme aan te kaarten evenals een positief beeld te schetsen van de lidstaten van de Sovjet Unie. Eén van deze landen die zich met deze activiteit in België bezig hield was het voormalige Tsjecho-Slowakije. De '*Zpravodasjská Správa Generálního Štabu'*, alias de Tsjecho-Slovaakse militaire inlichtingendienst was net zoals haar burgerlijke variant, de '*Státní Bezpečnost'*, geïnfiltreerd in Belgische politieke milieus. De ambassade was zoals voor vele agenten hun uitvalsbasis en gebruikte hun deelname aan het diplomatieke korps als dekmantel. Deze dekmantel wordt tot op vandaag nog vaak gebruikt door inlichtingen - en rekruteringsofficieren.[114]

In december 1985 arriveert Jan Braňka in Brussel waar hij zal werken op de Tsjecho-Slovaakse ambassade als 'persattaché'. Hoewel hij hiervoor is opgeleid is hij niets minder dan een geheim agent wiens opdracht de inmenging in de Belgische politiek inhoudt. Op 30 oktober 1986 ontmoet hij Jean Verstappen tijdens een lunchafspraak. Jean Verstappen, een gewezen senator van de Communistische Partij in België, is lid van het voorzitterschap van de '*Conseil Mondial de la Paix'*. Deze organisatie wordt gedirigeerd door de Sovjet Unie en is in een honderdtal landen aanwezig. Een belangrijk detail omtrent deze organisatie is dat er nooit daadwerkelijk bewijs is geweest dat de Sovjet Unie deze organisatie ook financieel steunde. Het kwam vaak voor dat buitenlandse organisaties en partijen, die op de 'socialistische' - of 'communistische' leer waren gestoeld, vaak gecreëerd waren door Sovjets die hun propaganda en ideologie in de Westerse landen trachtten te verspreiden. Bovendien steunde men deze organisaties vaak financieel, wat in veel gevallen leidde tot inmenging op politiek en economisch vlak. Deze organisaties fungeerden als dekmantels en hadden als doel om gelijkgestemden, die al dan niet het Leninistisch gedachtengoed navolgden, te rekruteren.[115]

---

[113] Interview met Kristof Clerix , onderzoeksjournalist en schrijver
[114] HAYNES, J.E, en KLEHR, H., *Early cold war spies. The Espionage trials that shaped American politics,* Cambridge, Cambridge university press, 2006, 265 p.
[115] SERVICE, R., *Comrades!: a history of world communism,* Cambridge, Harvard University Press 2007, p. 107-118

Sinds zijn pensioen neemt Verstappen regelmatig deel aan buitenlandse vredescongressen waaronder deze in satellietstaten van de Sovjet Unie. Hier komt hij in contact met Sovjetdiplomaten - en inlichtingenofficieren en wisselt hij gedachten uit over de anti-imperialistische machtsstrijd in Europa. Verstappen zal toen al opgemerkt zijn door de inlichtingendiensten als potentiële buitenlandse beïnvloedingsmogelijkheid. Hij kan niet aan geclassificeerde en geheime documenten en informatie komen maar vervult onrechtstreeks nog een politieke rol. Verstappen kan een bepaald aantal kiezers beïnvloeden door zijn gewezen politieke carrière en zijn Belgische bijdrage aan de '*Conseil Mondial de la Paix'*.

Zelf schrijft Jan Verstappen nog vele betogen en visies over geopolitieke thema's voor het boekje '*Rencontres pour la Paix'*. Deze thema's handelen over de wapenindustrie, het militair - industriële complex, de NAVO, de Westerse militaire superioriteit, de Sovjet-Unie, mensenrechten, de vredesbewegingen, etc. Sommige artikels zijn ook geschreven aan de hand van unieke informatie afkomstig van Braňka. Deze informatie kon best foutief zijn, maar droeg bij tot het propaganderen van de Sovjet Unie en Tsjecho-Slovakije zelf. Het was toen zo goed als onmogelijk dergelijke informatie te toetsen aan de waarheid. Dit zal ertoe bijdragen dat Jan Verstappen in 1988 voor het eerst een grote som geld zal toegestopt krijgen van Braňka als steun voor het drukken van het boekje. Dit gebeurt thuis bij de zoon van Jan verstappen die over een eigen drukpers beschikt. Verstappen zelf ziet geen probleem met financiële steun afkomstig uit Tsjecho-Slovakije.

In de volgende twee jaar zullen er nog vaak enveloppen met geld onder de tafel worden doorgegeven aan Verstappen. . De Staatsveiligheid schaduwt Braňka en Verstappen maar treft zo goed als geen bewijs aan. Tijdens de Fluwelen revolutie in de jaren negentig worden Branka's opdrachten opgeschort en keert hij terug naar zijn thuisland. Dit zal het einde betekenen van de financiële steun voor het boekje 'Rencontres pour la Paix', evenals het verzamelen van voldoende juridisch bewijs door de Staatsveiligheid.

6. BESLUIT

In dit tweede deel wordt inmenging in zijn geheel beschreven. Inmenging, als onderzoeksonderwerp, is niet zo uitgebreid als spionage. Maar beiden worden nu eenmaal altijd samen bestudeerd. Het handelen over politieke inmenging door buitenlandse inlichtingendiensten en mogendheden is nog steeds een zeer actueel thema.

Vele landen proberen bepaalde buitenlandse politieke kringen en partijen te beïnvloeden voor zowel politieke als economische redenen. Rusland poogt nog steeds invloed uit te oefenen op de voormalige satellietstaten van de Sovjet Unie. Echter Amerika tracht hetzelfde te doen met Europa, terwijl Amerika zelf beïnvloed wordt door Israël en het Israëlisch-Palestijns conflict. De terroristische groepering ISIS is bezig met de politiek van landen op ideologische wijze te beïnvloeden door geïmmigreerde moslims en bekeerlingen in opstand te laten komen tegen hun eigen staat waar ze vertoeven. Hiermee tracht ISIS een internationaal, dictatoriaal en moslimfundamentalistisch Kalifaat te stichten.

De studies naar het beroep van beïnvloedingsagent is zeer boeiend. Enkel het gebrek aan literatuur bemoeilijkt het onderzoek ernaar. In de meeste literatuur staan enkel (vage) beschrijvingen over hun doel en de werkwijze.

Het gebruik van propaganda met het oog op inmenging bestaat al even. Sinds Goya's etsen en de opkomende anti-monarchistisch literatuur tijdens de renaissanceperiode, is propaganda enkel maar toegenomen. Fysieke propagandamiddelen, zoals flyers en films, zijn gemakkelijk op te sporen en kunnen gebruikt worden als bewijs an sich. Maar wat als inmenging vooral mondeling tot stand komt tijdens een etentje? Zoals eerder is aangehaald, is de lijn tussen inmenging en lobbyen zeer dun wat de aanpak ervan juist bemoeilijkt.

DEEL III. INLICHTINGENDIENSTEN, VEILIGHEIDSDIENSTEN EN HET FEDERAAL PARKET

"In addition to being right most of the time, a good intelligence officer must also have two other qualities to help him sublimate the ugly aspects of his calling: a deep love of his country and an unshakable belief in his principles. To be a master of spies, a man must be above all a master of himself and must be convinced of the intrinsic goodness of his cause."

František Moravec, Master of Spies

1. INLEIDING

In België bestaan er twee soorten inlichtingendiensten. We onderscheiden de civiele binnenlandse inlichtingendienst, namelijk de Veiligheid van de Staat (VSSE) die zich uitsluitend bezig houdt met defensieve binnenlandse opdrachten. Hiernaast bestaat er ook een militaire inlichtingendienst, namelijk de Algemene Dienst Inlichting en Veiligheid (ADIV) die zich zowel bezig houdt met binnenlandse en buitenlandse offensieve opdrachten. Beide inlichtingendiensten zijn gebonden aan de wetgeving en zijn bovendien onderworpen aan een parlementaire controle.

Hiernaast kan de parlementaire controle beroep doen op een onafhankelijk controleorgaan zoals het 'Vast Comité I van Toezicht op de Inlichtingen - en Veiligheidsdiensten' (alias Comité I). Dit controleorgaan gaat na of de VSSE en ADIV zich beiden aan de wettelijke bepalingen houden. Het is in staat om als gerechtelijke instantie op te treden wanneer er voldoende bewijzen zijn van onwettelijkheden. Omdat het niet de bedoeling is om in deze thesis een volledige uiteenzetting te doen van alle controleorganen van de inlichtingendiensten¸ zullen enkel de VSSE en ADIV besproken worden.

Ook zal er een korte uiteenzetting gehouden worden over de onderlinge samenwerking en met het Federaal parket. Dit met het oog op de wettelijke bestrijdingsmogelijkheden van spionage en inmenging beter te begrijpen.

1.1. De Veiligheid van de Staat (VSSE)

Op 15 oktober 1830, tijdens het Voorlopig Bewind in België, werd de' Openbare Veiligheid', of in het Frans de '*Sûreté'* opgericht. Hierdoor behoort ze tot een van de oudste instellingen van België. Dit ministerie was één van de vijf directies die elk onder leiding stond van een Administrateur-Generaal. De overige directies waren Oorlog, Binnenlandse Zaken, Financiën en Justitie. In tegenstelling tot de andere vier diensten, die zijn uitgegroeid tot volwaardige diensten met een minister, is de 'Openbare Veiligheid' onder leiderschap gebleven van een Administrateur-Generaal. Daardoor viel de Openbare Veiligheid op sommige momenten onder het Ministerie van Justitie, dan weer het Ministerie van Binnenlandse zaken of het Ministerie van Landverdediging. [116]

De aanwezige buitenlandse dreiging van de Orangisten onder Willem I zorgde ervoor dat dit ministerie zeer ruime bevoegdheden toegekend kreeg waaronder; de binnenlandse veiligheid handhaven, het afleveren van paspoorten, controleren van de invalswegen, toezicht op fabrieken en hun arbeiders, etc. Daardoor werd in de schoot van de Openbare Veiligheid een directie 'Veiligheid van de Staat' opgericht. Onder deze dienst viel ook de 'Vreemdelingenpolitie', die nieuwkomers en vreemdelingen in de jonge Belgische staat moest observeren. [117]

In 1940 werd het 'Hoog commissariaat voor de Veiligheid van de Staat' opgericht dat bevelen kreeg van de Minister van Landsverdediging. Dit commissariaat zal na de oorlog nog enkel in naam blijven voortbestaan. De dienst Openbare Veiligheid werd door de Duitse bezetter ontbonden, op de 'Vreemdelingenpolitie' na.[118] Na de tweede wereldoorlog kreeg de 'Dienst voor Openbare Veiligheid' een andere benaming, namelijk 'Administratie voor de Staatsveiligheid'. [119] Sinds dan wordt de Staatsveiligheid geleid door een administrateur generaal onder de bevoegdheid van het Ministerie van Justitie. Ze richtte zich vanaf toen op zowel extreem-links als extreem-rechts. Haar bevoegdheden werden nog uitgebreid tot subversie, contraspionage, inmenging en sabotage en zo is ze geëvolueerd tot de hedendaagse dienst.

---

[116] VAN OUTRIVE, L., CARTUYVELS, Y., en PONSAERS, P., *Sire, ik ben ongerust. Geschiedenis van de Belgische politie 1794-1991*, Leuven, Kritak, 1992, 52.
[117] AMEZ, F., Un aspect oublié de la réforme de l'Etat : le régime des cultes, in *Journal des Tribunaux*, 2002, p. 529-537.
[118] LAUREYS, E., *Het Bevrijde België (1944–1945). Feiten, opinies en voorstellingen*. Brussel, Soma, 1998, 81 p.
[119] CARPENTIER, C., en MOSER, F., *De staatsveiligheid, geschiedenis van een destabilisatie*, Leuven, Kritak, 1994, 293p.

1.1.1. Opdrachten VSSE

De opdrachten van de VSSE zijn geregeld in *artikel 7 van de wet van 30 november 1998, houdende regeling van de inlichtingen-en veiligheidsdienst die de werking van de VSSE regelt*. De opdrachten kunnen in vier categorieën onderscheiden worden[120] ;

- De inlichtingenopdracht

Het inwinnen, verwerken en analyseren van informatie is het hoofddoel van de VSSE. De Veiligheid van de Staat wint informatie in over activiteiten van personen of groeperingen die de fundamentele belangen en waarden van het land bedreigen of zouden kunnen bedreigen. In de wet wordt een onderscheid gemaakt tussen de waarden die beschermd dienen te worden. De VSSE heeft als opdracht om volgende waarden te beschermen; "*de inwendige veiligheid van de staat en het voortbestaan van de democratische en grondwettelijke orde, de uitwendige veiligheid van de staat en de internationale betrekkingen en het wetenschappelijk of economisch potentieel"*.[121]

Het beschermen van de Belgische Staat is geen sinecure en er blijft een interpretatiemarge bestaan voor de soorten dreigingen die de VSSE moet opvolgen. De wet voorziet een opsomming van deze dreigingen; "*elke individuele of collectieve activiteit ontplooid in het land of vanuit het buitenland die verband kan houden met spionage, inmenging, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties en criminele organisaties*".[122]

- De veiligheidsonderzoeken

Ieder natuurlijk - of rechtspersoon dat omgaat met geclassificeerde (vertrouwelijke of geheime) informatie wordt, op vraag van de Nationale Veligheidsauditoriteit, gescreend door de VSSE. Dit geldt ook voor personen die werken in een 'gevoelige' omgeving en in aanraking komen met bepaalde soorten druk van buitenaf. De regels omtrent de veiligheidsonderzoeken zijn vastgelegd in *de wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen*. Risicovolle profielen kunnen de toegang tot gevoelige gegevens of plaatsen ontzegd worden, na een negatief veiligheidsonderzoek.

[120] WINANTS, A., *Veiligheid van de Staat. Jaarverslag 2010*, Brussel, Winants A., 2010, p. 11-15
[121] Art. 7, Wet houdende regeling van de inlichtingen – en veiligheidsdienst, B.S., 18 december 1998
[122] Art. 8, Wet houdende regeling van de inlichtingen – en veiligheidsdienst, B.S., 18 december 1998

- De bescherming van personen

De VSSE kan, op verzoek van de Minister van Binnenlandse Zaken, bescherming bieden aan buitenlandse staats - en regeringhoofden alsook hun leden. Hiernaast kan ze ook bescherming bieden aan bepaalde belangrijke personen die (mogelijk) bedreigd worden. Dit soort van beschermingsopdrachten vallen onder de bevoegdheid van een sectie van buitendiensten, die bij de uitoefening van hun opdrachten beschikken over zowel beperkte als specifieke politionele bevoegdheden. Dit laat de veiligheidsofficieren toe om tussen te komen wanneer de fysieke integriteit, of het leven, van de te beschermen persoon in het gedrang komt.

- De opdrachten die door of krachtens de wet aan de Veiligheid van de Staat toevertrouwd worden.

De ruime interpretatiemogelijkheden bij deze laatste opdracht van de VSSE vloeien voort uit het feit dat deze opdracht zeer vaag is beschreven. De wetgever heeft met voorbedachten rade de interpretatie zo ruim mogelijk gehouden zodat er 'bewegingsruimte' is voor de VSSE. Anders zou de wetgever bij iedere nieuwe dreiging onmiddellijk een nieuwe wet moeten vervaardigen.

1.1.2. Structuur VSSE

De werking van de VSSE wordt geregeld wordt geregeld door de wet van 30 november 1998 betreffende de regeling van de inlichtingen-en veiligheidsdienst. Toch zijn er ook algemene beleidslijnen en algemene richtlijnen die mee vorm geven aan de structuur en werking van de VSSE. De algemene beleidslijnen van de dienst worden door het Ministerieel Comité voor inlichtingen en veiligheid bepaald. In dit comité zetelt de Eerste Minister als voorzitter en de Ministers van Justitie, Defensie, Binnenlandse Zaken, Buitenlandse Zaken, Financiën en Mobiliteit als comitéleden. [123]

De voorbereide algemene richtlijnen van het Ministerieel Comité worden na beslissing veraanschouwelijkt door het College voor inlichtingen en veiligheid, waarin onder andere de Administrateur-generaal van de VSSE zetelt.

[123] VAST COMITE VAN TOEZICHT OP DE INLICHTINGENDIENSTEN, *Codex inlichtingendiensten: werking,*
bevoegdheden en controle, Brugge, Die Keure,1996

De VSSE, ressorterend onder de bevoegdheid van de Minister van Justitie, wordt nog steeds geleid door een Administrateur-Generaal.
Deze wordt bijgestaan door een adjunct Administrateur Generaal die van een andere taalrol is. De Administrateur-Generaal en zijn adjunct vormen de Directie-Generaal.[124]

Figuur 4 : Embleem VSSE

De Directie-Generaal wordt ondersteund door een cel met specialisten. Deze cel is de ondersteuningscel van de VSSE maar speelt volgens een audit van Comité I een ruimere rol dan de Belgische regering haar oorspronkelijk had toegekend in haar Koninklijk Besluit. En sinds 2007 wordt van de VSSE verwacht dat ze een vierjaarlijks strategisch plan opstelt waarin de prioriteiten en operationele strategieën uitgeschreven staan en hoe ze deze prioriteiten tot stand zouden brengen. Hiernaast zou er ook een jaarlijks actieplan moeten opgesteld worden. Iets wat tot nu toe nog niet goed geïmplementeerd wordt door mogelijk een gebrek aan juist management. [125]De samenwerking tussen die cel en de directie verloopt informeel en ongestructureerd. Hiernaast word de Directie-Generaal bijgestaan door een Cel Informatie en Communicatie die de interne en externe communicatiedoorstroom regelt. Het Directiecomité geeft leiding aan de drie diensten die de onderbouw vormen van de VSSE, namelijk de Algemene diensten, de Buitendiensten en de Analysediensten. Er wordt meestal gewoon gesproken over de binnendiensten[126] waaronder de Analysediensten en de Algemene diensten vallen, en de buitendiensten.[127]

- de Algemene diensten

Deze binnendiensten omvatten alle logistieke en informatica/technische diensten alsook andere diensten die ondersteuning geven aan de Directie-Generaal en aan de anderen diensten. Ook is er sinds enkele jaren binnen de VSSE een stafdienst opgericht die zowel de administratieve diensten omvatten, alsook de diensten personeel en organisatie en de diensten juridische en financieel beheer omvat.

---

[124] WINANTS, A., *Veiligheid van de Staat. Jaarverslag 2010*, Brussel, Winants A., 2010, p. 11-15
[125] BOVE, L., (2010/08/10) *De staatsveiligheid op de rooster* [WWW.] De Tijd : http://blogs.tijd.be/zaakjustitie/2010/08/de-staatsveiligheid-op-de-rooster.html [21/04/2014]
[126] Art. 99-112 KB van 19 november 1998 betreffende de verloven en afwezigheden toegestaan aan de personeelsleden van de Rijksbesturen en Omzendbrief nr. 476 van 28 mei 1999 van de minister van Ambtenarenzaken
[127] Art. 184 en 187 KB van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat en de dienstnota's van 20 februari 2007 en 7 december 2007 van de VSSE

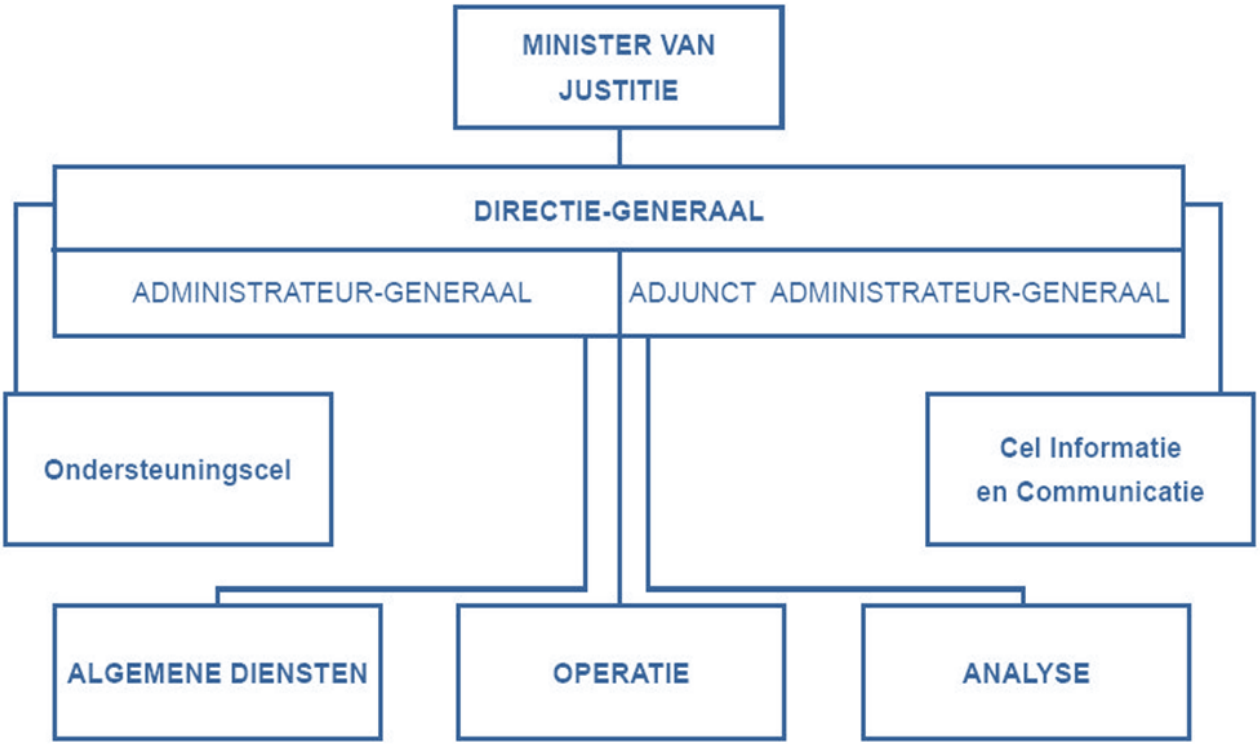
- Analysediensten.

Aan het hoofd van deze binnendiensten staat een ‘directeur Analyse’. Deze diensten, analyseren de door de buitendiensten verkregen informatie en inlichtingen. Ook analyseren zij informatie en inlichtingen verkregen van buitenlandse (bevriende) naties en hun inlichtingendiensten evenals zelf gevonden open source informatie.

- de Buitendiensten

De diensten die zich vooral buiten op het terrein afspelen worden geleid door de ‘directeur Operaties’. Ze zijn onderverdeeld in eenheden en teams die ieders hun specialisatie en bevoegdheden hebben. Ze staan in voor de bescherming van (belangrijke) personen, het inwinnen van human intelligence op het terrein evenals het uitvoeren van veiligheidsonderzoeken.

Om te eindigen is er het Directiecomité van de Veiligheid van de Staat dat bestaat uit de Administrateur-Generaal, de adjunct Administrateur-Generaal, de Directeur van de dienst Operaties en de Directeur van de dienst Analyse. Dit alles toont aan dat de VSSE een burgerlijke en defensieve inlichtingendienst is.



Figuur 5 : Organisatiestructuur Veiligheid van de Staat

1.2. De Algemene Dienst Inlichtingen en Veiligheid (ADIV)

In 1915 zal door wereldoorlog I een 'Veiligheidsdienst van het Leger' gecreëerd worden die belast wordt met de bestrijding van misdaden en delicten gepleegd in het militaire milieu, in het bijzonder spionage, en dit voor de gehele duur van de oorlog.[128] Deze dienst, die een jaar later omgevormd wordt tot de 'Militaire Veiligheidsdienst', is samengesteld uit commissarissen en inspecteurs die bij het leger de bevoegdheid uitoefenden van officieren van de gerechtelijke politie. Deze dienst zal alweer ontbonden worden in 1919 bij een besluit tot oprichting van de 'Militaire Veiligheid in bezet Duitsland'. In 1920 zal dan bij het ministerie van Landsverdediging een dienst in het leven geroepen worden die belast is met de taken van contraspionage in al haar vormen evenals het toezicht op subversieve groepen binnen de Belgische Krijgsmacht.

In 1947 zal, na de Utrecht-affaire, de Generale Staf van het leger de militaire inlichtingen, de militaire contraspionage en de verwerking van rapporten van de militaire attachés alsook de Belgische officieren in het buitenland opnieuw in handen krijgen. Enige tijd later zal in 1963 een Koninklijk Besluit verschijnen dat de algemene structuur van het ministerie van Landsverdediging en van de Krijgsmacht bepaalt. Hierbij krijgt de Stafchef de verantwoordelijkheid voor de opsporing, de verwerking en de verspreiding van inlichtingen alsook voor de toepassing van de regels betreffende de militaire veiligheid en contraspionage.[129] Een jaar later zal dan, na de reorganisatie van de Krijgsmacht, de Algemene Dienst Inlichtingen- en Veiligheid (ADIV) opgericht worden.

1.1.3. Opdrachten ADIV

Ook hier zijn de opdrachten geregeld door *artikel 11 van de wet van 30 november 1998 betreffende de regeling van inlichtingen en veiligheidsdiensten*. Volgens deze organieke wet is de Minister van Defensie de voogdijminister van de ADIV zoals de Minister van Justitie de voogdij heeft over de VSSE. De opdrachten van de militaire inlichtingen- en veiligheidsdiensten worden onderverdeeld in twee categorieën, namelijk het inwinnen van inlichtingen en de militaire veiligheid.

[128] K.B. van 1 april 1915 houdende de oprichting van een militaire veiligheidsdienst voor de duur van de oorlog
[129] K.B van 3 december 1963 tot de vaststelling van de algemene structuur van het ministerie van Landsverdediging en van de Krijgsmacht, vastlegging van de bevoegdheden van bepaalde autoriteiten en de machtiging van de ministervan landsverdediging om een gedeelte van zijn bevoegdheden over te dragen

De eerste categorie omvat "het inwinnen, analyseren en het verwerken van inlichtingen" en dit met betrekking tot;

- *activiteiten die de onschendbaarheid van het nationaal grondgebied bedreigen of zouden kunnen bedreigen. Het betreft hier elke uiting van het voornemen om met middelen van militaire aard, het gehele grondgebied of de territoriale wateren, in te nemen, te bezetten of aan te vallen, of de bescherming of het voortbestaan van de bevolking, het nationaal patrimonium of het economisch potentieel van het land in gevaar te brengen.*[130]

- *activiteiten die de militaire defensieplannen bedreigen of kunnen bedreigen*

- *activiteiten die de vervulling van de opdrachten van de strijdkrachten bedreigen of kunnen bedreigen*

De tweede categorie omvat "de militaire veiligheid" en dit met betrekking tot;

- *het behoud van de militaire veiligheid, de bescherming van het militair geheim en de veiligheidsonderzoeken.*

In het *K.B van 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Defensie en tot vastlegging van de bevoegdheden van bepaalde autoriteiten* [131] worden er ook meerdere bijkomende taken aan de onderstafchef inlichtingen en veiligheid van de VSSE gegeven;

- *Hij is belast met de organisatie van de steun inlichtingen en veiligheid aan operaties;*

- *Hij is bevoegd voor het ten laste nemen van de in België geaccrediteerde buitenlandse defensieattachés en voor de relaties met de buitenlandse strijdkrachten voor dewelke ze geaccrediteerd zijn;*

- *Hij stelt de voorschriften op betreffende de geclassificeerde archieven van Defensie en*

[130] Door de nieuwe BIM wetgeving van 4 februari 2010 wordt er een uitbreiding voorzien. Het wetenschappelijk en economisch potentieel van de defensie-industrie, alsook de cyberaanvallen op de militaire informatica-systemen worden toegevoegd aan de eerste categorie van activiteiten van de ADIV

[131] K.B van 21 December 2001 tot bepaling van de algemene structuur van het ministerie van Defensie en tot vastlegging van de bevoegdheden van bepaalde autoriteiten, *B.S.*

controleert de naleving ervan;

- *Hij beheert de defensieattachés en de militaire raadgevers bij de ambassades en gezantschappen van België;*

- *Hij adviseert de chef Defensie betreffende het beheer van het personeel tewerkgesteld in het domein 'inlichtingen en veiligheid'.*

1.1.4. Structuur ADIV

Zoals het al aan bod kwam, valt de ADIV onder de voogdij van de Minister van Defensie. Onder het Ministerie van Landsverdediging ressorteert een Chef Defensie die samen de Defensiestaf vormen. Ze staan aan het hoofd van tien militaire stafdepartementen en directies. Een van deze stafdepartementen is het stafdepartement Inlichting en Veiligheid. Dit departement wordt geleid door een Onderstafchef Inlichtingen en Veiligheid, alias '*Assistant Chief of Staff Intelligence and Security' (*ACOS IS) genoemd.[132].

Figuur 6 :
Embleem ADIV

De ACOS IS is chef van de ADIV die beschikt over vier ondergeschikte divisies, met ieder hun specialisaties, om haar opdrachten te vervullen, namelijk; de Divisie Inlichtingen, de Divisie Veiligheid, de Divisie Veiligheidsinlichtingen en de Divisie Beleidsondersteuning. [133]

- **Divisie Veiligheidsinlichtingen:** Het inwinnen, analyseren en verwerken van alle inlichtingen die de belangen van Defensie, de uitvoering van de opdrachten van de Krijgsmacht of de militaire defensieplannen bedreigen of zouden kunnen bedreigen onder de vorm van spionage, sabotage, terrorisme en subversie vallen onder de bevoegdheid van deze divisie. Ze voert deze opdracht, net zoals de VSSE, ook op nationaal niveau uit maar dit voor het militaire aspect. Dit is geregeld in de wetgeving en het protocolakkoord tussen de ADIV en de VSSE.

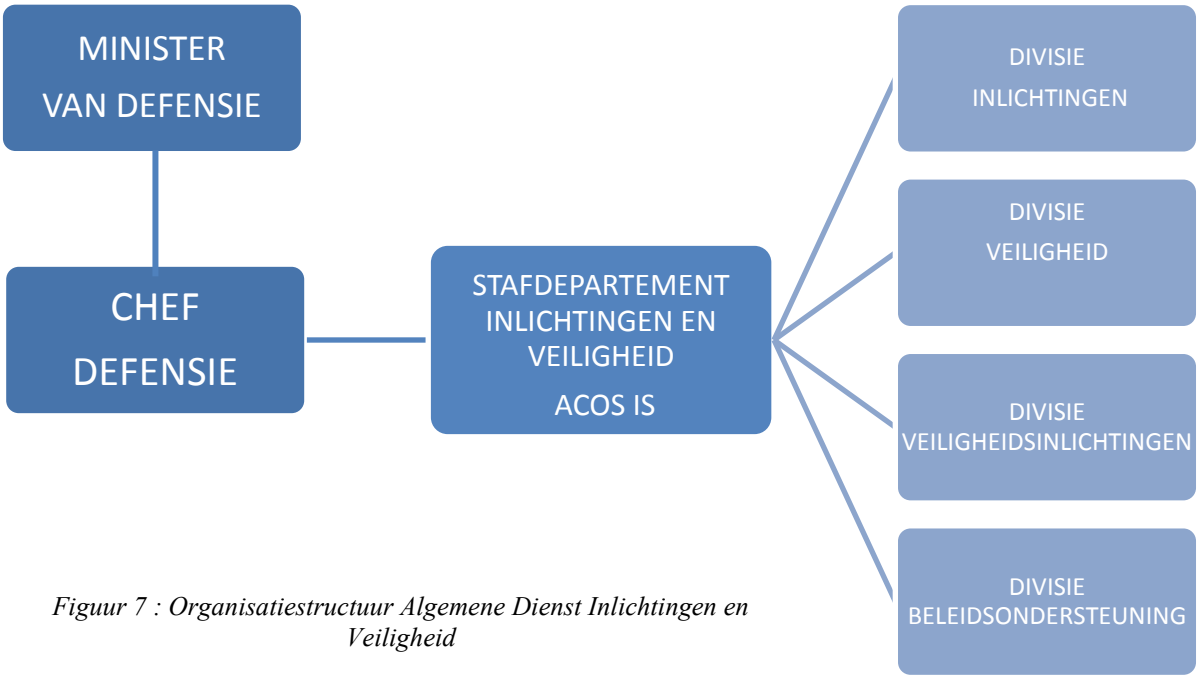
[132] STEVENS, D., 'De Algemene Dienst Inlichtingen en Veiligheid van de Krijgsmacht: actuele analyse' in *Geheime diensten in Benelux,Israël, en de Verenigde Staten*, MATTHIJS, H., (ed.), Brugge, die Keure, 2005, 27-47

[133] CLERIX, K., (2014/03/14) Militaire Inlichtingendienst treedi uit de schaduw [WWW]. MO : http://www.mo.be/interview/militaire-inlichtingendienst-treedt-uit-de-schaduw [23/06/2014]

- **Divisie Inlichtingen**: Deze divisie verzamelt strategische en operationele inlichtingen en dit in het bijzonder buitenlandse opgespoorde inlichtingen. De strategische inlichtingen dienen ter ondersteuning van de politiek militaire besluitvormers. De wetgeving regelt de inlichtingenverstrekking aan de bevoegde ministers door de ADIV en verleent aan de ADIV, op verzoek van de regering, advies bij de omschrijving van haar buitenlands defensiebeleid. De ADIV stelt ook inlichtingenanalyses op die bestemd zijn voor hooggeplaatste personen, organisaties of autoriteiten zoals in België. De operationele inlichtingen zijn bestemd voor de militaire componenten evenals voor commandanten en officieren van de eenheden die opereren in het buitenland.

- **Divisie Veiligheid:** Ze handhaaft de militaire veiligheid van het personeel dat ressorteert onder de minister van Defensie. Ook handhaaft het de veiligheid bij; militaire installaties, wapen - en munitietransporten, de militaire uitrusting, strategische - en tactische plannen, informatica, communicatiesystemen en militaire documenten. Dit zowel voor binnenlandse als buitenlandse Belgische strijdkrachten. De handhaving omvat ook de bescherming van de geheimhouding krachtens de internationale verbintenissen van België of teneinde de vervulling van de opdrachten van Defensie te verzekeren. Deze divisie voert, voorafgaand aan het verlenen van een veiligheidsmachtiging, ook veiligheidsonderzoeken uit. Deze veiligheidsmachtigingen worden afgegeven aan militair of burgerlijk personeel van het departement va Landsverdediging evenals aan personeel van firma's indien men dit nodig acht in het kader van contractuele leveringen van materiaal of diensten. Als laatste opdracht verzorgt de Divisie Veiligheid de voorschriften op betreffende de geclassificeerde archieven van de Krijgsmacht evenals de controle op de naleving ervan.

- **Divisie beleidsondersteuning: Deze dienst levert** de steun op het vlak van personeel en financiën, interne veiligheid, opleiding en training, logistiek, informatica- en communicatie(verbindings)systemen. Ze leggen en houden contacten met de Belgische en de buitenlandse defensieattachés, leveren praktische steun, organiseren de planning, de programmering en de controle van de financiële middelen en toelagen die aan de ADIV zijn toegekend.



Figuur 7 : Organisatiestructuur Algemene Dienst Inlichtingen en Veiligheid

2. DE ONDERLINGE SAMENWERKING TUSSEN DE VSSE, DE ADIV & HET FEDERAAL PARKET

Nu de opdrachten en de structuur van de VSSE en de ADIV duidelijker zijn geworden, is het ook belangrijk om te zien hoe de onderlinge samenwerking verloopt. Dit deel zal zich voornamelijk toespitsen op de samenwerking op nationaal niveau. Het is al zeer moeilijk om vertrouwelijke informatie te verkrijgen over de onderlinge samenwerking tussen de beiden inlichtingendiensten en het federaal parket binnen België, laat staan op internationaal niveau. Weliswaar brengt de wetgeving en haar Koninklijke Besluiten een omschrijving van de samenwerking, doch is de realiteit op vlak van samenwerking totaal anders. Zo werd in de zomer van 2011 voor de eerste keer, in de hele geschiedenis van de VSSE, openlijk een spionagedossier overgemaakt aan het parket. Dit onder artikel 19 van de 'wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten' (alias BIM wet). Dit was een zeer vreemd gebeuren omdat in het verleden dergelijke spionagedossiers in stilte werden geregeld door de Belgische inlichtingendiensten. Door deze actie van samenwerking stuurde de VSSE een krachtig signaal door naar Rusland. Door dit spionagegeval publiek te maken zullen andere landen hun relaties met Russische diplomaten immers herzien. [134]

[134] CLERIX, K., (2012/11/05) *Belgische diplomaat verdacht van spionage* [WWW]. MO: http://www.mo.be/artikel/belgische-diplomaat-verdacht-van-spionage [01/08/2014]

2.1. Samenwerking tussen ADIV en VSSE

Over de samenwerking tussen de ADIV en de VSSE bestaat er sinds 12 november 2004 een protocolakkoord dat door de ministers van Justitie en Landsverdediging werd geratificeerd. Naargelang de realisatie van dit akkoord zijn een aantal samenwerkingsplatforms opgezet die rond bepaalde nationale en internationale thema's werken. Hiernaast vinden regelmatig vergaderingen plaats tussen de diensthoofden wat bevorderend werkt voor de communicatie en samenwerking. Alsook de condities voor de informatie uitwisseling worden in dit akkoord nader omschreven. [135]

Een voorbeeld van zo een conditie is wanneer een VSSE dossier niet onder de bevoegdheid valt van de ADIV maar er toch een duidelijke link is met Defensie. Dan wordt er samengewerkt tussen beide diensten. Een ander voorbeeld van een conditie is wanneer een dossier wel onder de bevoegdheid valt van de ADIV maar er een 'onbekend' natuurlijk - of rechtspersoon in voorkomt. Dan kan er samengewerkt met de VSSE door hen te vragen of de natuurlijke - of persoon bij hen gekend is.[136]

2.2. Samenwerking tussen het federaal parket en de Belgische inlichtingendiensten

Omtrent de samenwerking tussen de inlichtingendiensten en het parket bestaat er sinds 17 december 2012 een dienstnota die de schriftelijke informatieverstrekking door de inlichtingendiensten aan het Openbaar Ministerie en omgekeerd regelt. Deze dienstnota is gebaseerd op de omzendbrief COL 9/2012 van 21 juni 2012 van het College van procureurs-generaal betreffende de wet van 30 november 1998 houdende regeling van de inlichtingen –en veiligheidsdienst. Een van de nieuwigheden aan deze nota liggen hem in de verduidelijking van de principes die het gebruik evenals de bewaring van geclassificeerde documenten op het federaal parket vastlegt.[137]

De activiteiten van buitenlandse inlichtingendiensten op Belgisch grondgebied spelen zich meestal net af binnen de grenzen van de wet of in een grijze zone. Echter wanneer de VSSE of ADIV vermoedens heeft van illegale activiteiten gepleegd door buitenlandse inlichtingenofficieren, zal de inlichtingendienst dit meedelen aan het federaal parket volgens art. 29 van het Wetboek van Strafvordering.

---

[135] *Parl. St.,* Senaat , nr. 5-1226, 8 februari 2011
[136] Interview met afdelingscommissaris X, Hoofd Operaties CI ADIV
[137] OPENBAAR MINISTERIE, Jaarverslag federaal parket 2012, Brussel, 2012, p.124 289

Maar wanneer er tijdens de aanwending van specifieke of uitzonderlijke inlichtingenmethoden ernstige aanwijzingen of vermoedens zijn van een misdrijf, dan wordt dit volgens art. 19 van de BIM wetgeving gemeld aan de BIM-commissie. De BIM-commissie is de bestuurlijke commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen - en veiligheidsdiensten.[138] Deze commissie kan inlichtingen overmaken aan het federaal parket voor verdere opvolging. Dit doet ze door een proces verbaal op te stellen wanneer inlichtingendiensten een BIM maatregelen toepassen. Dit wordt doorgegeven aan het federaal parket die dan een BOM maatregel machtigen.[139]

Na gesprekken met een federaal parket[140] is het gebleken dat er in België bitter weinig HUMINT spionagedossiers overgemaakt worden aan het federaal parket. Dit wil niet zeggen dat er geen spionage is in België. Het veelvuldig gebruik van de BIM wetgeving wordt in de eerste plaats gebruikt voor spionagezaken. De enige dossiers waar van het parket direct weet van heeft zijn de vele dossiers omtrent '*hacking'*.

Deze dossiers worden meestal door de sectie georganiseerde criminaliteit van het federaal parket behandeld. Deze sectie is het gewend om zware dossiers van informaticacriminaliteit te bestuderen en slagen hier ook vaak in dankzij hun eigen technische kennis inzake deze materie. Het '*dark number'* van gevallen waar bedrijfsspionage gepleegd is zou ook vele malen groter zijn dan gedacht. Veel bedrijven trachten dit stil te houden en intern op te lossen wegens de vrees voor reputatieverlies.

In de meeste gevallen worden de Belgische inlichtingendiensten gevraagd om technische bijstand te verlenen in dossiers. [141] Technische bijstand verleent hen de mogelijkheid om specifieke informatie vrijblijvend te delen zonder enige verplichting. Door op te treden als technisch expert hebben ze ook inzage in het dossier waardoor er een wisselwerking kan ontstaan van andere dossiers of beschikbare informatie evenals het vinden van mogelijke connecties.

---

[138] VAN DAELE, D. en VANGEEBERGEN, B., "De BIM-wet in vogelvlucht" in VAN DAELE, D., VANGEEBERGEN, B., en VAN LAETHEM, W. (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, p. 29-64
[139] *Parl. St*., Senaat, nr. 5-6060, 11 april 2012
[140] Interview met X, Federale Parketmagistrate
[141] VAN DAELE, D. & VAN GEEBERGEN, B., "De verhouding tussen de inlichtingen- en veiligheidsdiensten en de gerechtelijke overheden" in VAN DAELE, D., VANGEEBERGEN, B., & VAN LAETHEM, W. (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, p. 207-233

Wanneer het federaal parket een dossier doorstuurt met de vraag om technische bijstand, krijgen ze steeds een antwoord terug. Iets wat niet bij andere doorgestuurde zaken het geval is. Dit antwoord vermeldt kort en duidelijk of ze al dan niet bereid zijn en vermeldt er de desbetreffende contactpersonen bij waarmee het parket contact kan opnemen bij hoogdringendheid. Tegenwoordig zet ADIV naast hun antwoord er ook bij of ze over informatie beschikken aangaande het dossier.

De achterliggende bedoeling is, zoals reeds gezegd, dat er een wisselwerking[142] is, wat niet altijd het geval blijkt te zijn. De Belgische inlichtingendiensten hebben altijd een afwachtende houding gehad. Met andere woorden, ze krijgen wel het schrijven toe van het federaal parket inzake een dossier maar zijzelf zullen hierover geen informatie meedelen totdat het federaal parket zelf persoonlijk contact met hen opneemt. Het federaal parket weet niet of de inlichtingendiensten daadwerkelijk met het dossier bezig zijn alsook de betreffende inlichtingendienst er informatie over heeft, of het dossier nog behandeld moet worden en op een stapel is terechtgekomen bij andere dossiers. Hetzelfde geldt voor nieuwe elementen die opduiken en belangrijk zijn voor het dossier. Worden deze tijdig medegedeeld of niet?

Gelijktijdig vernemen de inlichtingendiensten niet wat er uiteindelijk met het dossier is gebeurd dat ze hebben overgemaakt of technische bijstand aan hebben geleverd. Is de zaak geseponeerd of is er vervolging ingesteld en is het tot een veroordeling gekomen? Ergens is het wel begrijpelijk dat er langs beide kanten een hoge werklast aanwezig is, gecombineerd met een mogelijk gevoel van argwaan tegenover elkaar. Ook hoeven ze niet aan elkaar te rapporteren wat enerzijds bewegingsruimte oplevert maar hen ook in het ongewisse laat over de opvolging.

Een ander kritisch maar onvermijdelijk punt is het afschermen van de bronnen. Het federaal parket heeft een andere visie dan de inlichtingendiensten op gebied van de bronnen in een zaak. Het parket ziet er vaak minder graten in welke bronnen in het open dossier zouden mogen komen omdat ze dit gewoon zijn door dossiers waar ze samenwerkt met politie en informanten. Het belang ligt in de classificatie van de bronneninformatie als steunbewijs of volbewijs. [143]

[142] Artikel 20 Organieke Wet 1998.
[143] VAN DAELE, D. & VAN GEEBERGEN, B., 'Geheime (?) diensten. Over de noodzaak van een ernstig debat over de bijzondere inlichtingenmethoden en de rol van de inlichtingen- en veiligheidsdiensten in de opsporing" in *Orde van de dag* 2008, afl. 42, 33.

In het kader van een eerlijk proces is er noodzaak aan een zo groot mogelijke openheid van informatie. Paradoxaal wordt de door de inlichtingen- of veiligheidsdienst verzamelde informatie zo veel mogelijk afgeschermd tijdens een zo open mogelijke procedure. Doch is er een positieve evolutie bezig door de vele vergaderingen waar zowel federaal parket als de inlichtingendiensten aanwezig op zijn. Door de vele vergaderingen verbetert het onderlinge contact en ontstaat er meer een collegiale sfeer. En dit is ook zo ten opzichte van andere landen waar er soms amper samenwerking is door de interne politiek.

Zo stelt de VSSE tegenwoordig zelf een vertrouwelijke nota op voor het federaal parket. Deze nota bevat een opsomming van alle informatie die ze hebben over bepaalde elementen in een dossier. Deze aanpak zorgt ervoor dat het parket slechts nog moet aanduiden over welke *targets* ze informatie willen voor het open dossier en zal de VSSE op haar beurt trachten de informatie over te maken in de mate ze dit kan.

3. BUITENLANDSE INLICHTINGENDIENSTEN

België is altijd al een 'aantrekkingspunt' geweest voor buitenlandse inlichtingenofficieren en agenten. Voornamelijk door de hoge concentratie aan grote instellingen zoals de NAVO en de Europese Unie. Brussel alleen al telt momenteel rond de 150 Russische diplomaten en meer dan dertig procent is een inlichtingenofficier. Dit aantal overstijgt zelfs het gekende aantal Russische inlichtingenofficieren tijdens de Koude Oorlog. [144]

Om een duidelijk zicht te krijgen op de buitenlandse inlichtingendiensten worden de drie sterkst vertegenwoordigende inlichtingendiensten binnen België in dit hoofdstuk naderbij bekeken, alsook hun interesse van informatie inwinning binnen ons land. Het is echter ook belangrijk om niet te denken dat alleen Rusland, China en Amerika of andere grootmachten vijandelijke agenten inzetten in Brussel. In de hoofdstad zijn inlichtingenofficieren aanwezig afkomstig uit talloze landen, zoals Engeland, Israël, Congo, Marokko, Iran, Pakistan, Colombia en vele anderen. De keuze van deze drie landen ligt hem in het feit van het aantal dossiers dat men erover heeft aangelegd in de laatste jaren[145].

[144] CLERIX, K.,*Spionage in het hart van Europa*, België, Wereldmediahuis, 2006, p.3
[145] Interview met afdelingscommissaris X, Hoofd Operaties CI GSR van ADIV

Ook hebben deze buitenlandse inlichtingendiensten door hun toenemende spionageactiviteiten ook veel persbelangstelling gekregen binnen België en in de wereld. Andere inlichtingendiensten hebben zeker ook een belangrijke rol gespeeld binnen België maar hier bestaat noch concrete bewijslast, noch weinig daadwerkelijke informatie over. Hiernaast zijn veel van de dossiers vertrouwelijk of geheim. Dus is het moeilijk in te schatten in welke mate ze spionage - en inmengingactiviteiten hebben ondernomen in dit land.

3.1. RUSSISCHE INLICHTINGENDIENSTEN

Rusland heeft altijd een zeer sterke en uitgebouwde inlichtingendienst gehad dat zijn hoogtepunt heeft gekend tijdens de Koude Oorlog met de inzet van KGB agenten in diverse landen. Onder meer op ons grondgebied zijn de Russische inlichtingendiensten actief en richten hun activiteiten, naast op de klassieke politieke inlichtingen, op het vergaren van informatie over militaire technologieën. Deze vijandige activiteiten zijn het werk van de buitenlandse Russische inlichtingendiensten en hoofdzakelijk van de militaire inlichtingendienst GRU. Het voornaamste politiek - militaire doelwit van de Russische inlichtingendiensten blijft de Noord-Atlantische Verdragsorganisatie (NAVO). Toch neemt hun belangstelling voor technologieën die militaire toepassingen hebben binnen Belgische privébedrijven toe.[146]

Ook door het conflict in Oekraïne is Rusland geïnteresseerd in de geclassificeerde en 'gevoelige' documenten die België en de NAVO in hun bezit hebben. Naar aanleiding van dit conflict was mogelijk Rusland verantwoordelijk voor het hacken van de computersystemen van het Ministerie van Buitenlandse Zaken. Russische hackers, in dienst van de Russische inlichtingendienst, zijn hierin geslaagd via het zogenaamde '*Snake virus'* en zijn opgemerkt na een tip van de Amerikaanse' *Central Intelligence Agency'*.[147] Ook de ADIV heeft lange tijd problemen gehad met het verwijderen van een stuk hardnekkige *'malware'* van Russische origine.

Rusland heeft enerzijds een burgerlijke defensieve binnenlandse inlichtingendienst, namelijk de Federale Veiligheidsdienst van de Russische Federatie ("*Federalnaja sloezjba bezopasnosti Rossijskoj Federatsii'* - FSB).

[146] *Parl. St.* Senaat, nr. 5-8727, 16 april 2013
[147] X, (2014/05/16)Russisch Spionagevirus op computers overheid [WWW]. Gelderlander: http://www.gelderlander.nl/algemeen/buitenland/russisch-spionagevirus-op-computers-overheid-belgi%C3%AB-1.4362573 [28/05/2014]

Hiernaast heeft ze zowel een burgerlijke als een militaire offensieve inlichtingendienst. De 'Dienst Buitenlandse Veiligheid van Rusland' en de 'Russische Militaire Inlichtingendienst'. Deze diensten zullen, doordat ze ook actief zijn op Belgisch grondgebied op vlak van spionage en inmenging, naderbij besproken worden.

1.1.5. Russische Militaire Inlichtingendienst

De 'Russische Militaire Inlichtingendienst' *('Glavnoje Razvedyvatelnoje Oepravlenie'* - GRU*)* ressorterend onder het Russisch ministerie van Defensie, is nooit zo bekend geweest als het toenmalige 'Comité voor Staatsveiligheid ' (KGB). Desalniettemin heeft zij meer geheime buitenlandse operaties en opdrachten dan eender welke Russische inlichtingendienst. De GRU krijgt haar opdrachten van het centrale orgaan binnenin de Generale Staf van de militaire inlichtingendienst.

Haar opdrachten lopen evenredig met de totaalsom van alle opdrachten die alle departementen van een militaire inlichtingendienst, zoals die van Amerika, omvatten. Dit maakt van haar een geduchte en grote dienst. Ze heeft tot vijf maal meer inlichtingenofficieren in een buitenlands grondgebied ingezet dan de Dienst Buitenlandse veiligheid van Rusland. Dit is niet zo moeilijk als men ongeveer 12000 medewerkers in dienst heeft.[148] De GRU verzamelt informatie via hoofdzakelijk HUMINT bronnen van militaire attaches en buitenlandse agenten. Hiernaast gebruikt het ook SIGINT en IMINT. Eén van de prioriteiten van deze organisatie is spionage van het WEP van een land alsook de politieke standpunten of posities die een land heeft ten opzichte van Rusland op politiek militair en economisch vlak.[149]

Figuur 8 : Embleem GRU

1.1.6. Dienst Buitenlandse veiligheid van De Russische Federatie

De 'Dienst Buitenlandse Veiligheid van de Russische Federatie' ('*Sloezjba Vnesjnej Razvedki'* - SVR) is in feite de belangrijkste Russische inlichtingen - en veiligheidsdienst die actief is in het buitenland en heeft rond de 13000 medewerkers in dienst.

[148] WEST, N., *Historical dictionary of international Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, IV, United Kingdom, Scarecrow Press, 2009, p.118-119
[149] ANDREW, C. & MITROHHIN, V., The sword and the shield. The Mitrokhin archive and the secret history of the KGB, New York, Basic Books, 1999, 700 p.

Ze is ontstaan na de val van de Berlijnse muur. De hoofdopdracht van deze dienst bestaat uit het verzamelen en onderzoeken van alle zaken waarbij de Russische staat mogelijk belang bij heeft. Dit kan gaan over mogelijke existerende dreigingen waaronder acties en (strategische)plannen van andere staten, organisaties en personen.

Ze onderhoudt ook contacten met verschillende inlichtingen - en contraspionage diensten van voormalige Sovjet landen en werkt ook met hen samen. Dit op vlak van; massa-destructiewapens, terrorismebestrijding, drugshandel, georganiseerde misdaad, witwaspraktijken, illegale wapenhandel en vermiste/ontvoerde Russische staatsburgers in het buitenland.

Deze samenwerking uit zich in het uitwisselen van informatie, opleidingen en technische assistentie. [150] Er zou mogelijk ook een geheim verdrag tussen China en Rusland bestaan sinds 1992 omtrent de samenwerking op vlak van inlichtingen. Dit verdrag handelt over de SVR alsook de GRU en hun samenwerking met het Chinees Volksbevrijdingsleger. Ook geeft deze dienst ondersteuning aan de concretisering van staatsmaatregelen met betrekking tot de veiligheid van de Russische staat. [151]

Figuur 9 :
Embleem SVR

Er bestaat bewijs dat de SVR, in samenwerking met andere diensten, vooral geïnteresseerd is in het buitenlandse militair, wetenschappelijke en economische potentieel. Hierdoor is deze dienst vooral bekend door haar betrokkenheid in industriële militaire spionage en dit sinds 1996, toen de toenmalige President van Rusland Boris Jeltsin de kloof tussen de Sovjet-Unie en het Westen wou dichten.[152]

Naast het verzamelen van informatie over het buitenlands WEP, tracht ze Human Intelligence informatie te verzamelen over buitenlandse inlichtingen - en veiligheidsdiensten door agenten te rekruteren.[153]

---

[150] X, *(2009/01/01) Службы внешней разведки Российской Федерации* [WWW] CBP: http://svr.gov.ru/ [03/07/2014]
[151] SUIB, S., *Inside Russia's SVR. The Foreign Intelligence Service* , The Rosen Publishing Group, New York, 2003, p. 45-51 (65p.)
[152] Interview met de directeur van de Dienst Buitenlandse veiligheid van Rusland 'Vyacheslav Trubnikov' door Andrey Poleshchuk verschenen in NEZAVISIMAYA GAZETA (1996/12/18), p. 1- 2
[153] BENNET, G., The SVR. Russia's Intelligence Service in *Conflict Studio's Research Center*, Royal Military Academy Sandhurst, Camberley, 2000, 26p.

1.1.7. Speciale Communicatie en Informatie Dienst van de Russische Federatie

'De Speciale Communicatie en Informatie Dienst van de Russische Federatie' ('*Spetssvya'* - FAPSI) is een zeer gesloten gespecialiseerde inlichtingendienst die gespecialiseerd is in SIGINT, ELINT en COMINT. Deze dienst is voornamelijk bezig met verzameling en de (de)cryptografie van buitenlandse SIGINT alsook de bescherming en het onderhoud van de informatiebeveiliging van de Russische Federatie.

Figuur 10 :
Embleem FAPSI

Ze is op decreet in 2003 ontbonden en grotendeels verdeeld is onder de FSB en de GRU. [154] Doch is het van beland deze dienst naderbij te bekijken wegens haar werking. Ze is op veel vlakken het equivalent van de Amerikaanse Nationale Veiligheidsdienst die later nog aan bod zal komen. Haar hoofdopdracht is het beschermen van de Russische Federatie op vlak van de digitale wereld, satellietnetwerken en transmissies tussen de Russische overheden alsook haar inlichtingendiensten. [155]

Een eigenaardigheid aan deze dienst is dat ze meer FAPSI officieren had dan alle andere Russische inlichtingendiensten. De ontbinding en verdeling hebben ervoor gezorgd dat de FSB en de GRU efficiënter zijn geworden en over meer directe middelen beschikken. Dit zou aan de basis kunnen liggen van de Russische militaire expansie en wapenwedloop op digitaal en elektronisch vlak waarbij deze dienst een zeer speciale rol speelt op gebied van hacken. Activiteiten van hacken zijn in België en vele andere landen toegenomen en vaak wordt Rusland als mogelijke dader aangeduid. De dienst heeft zelf geen directe interesses van informatie en levert eerder bijstand aan andere Russische (en mogelijke Chinese) veiligheids - inlichtingendiensten en Russische staatsbedrijven. Deze dienst wordt ook verantwoordelijk gehouden voor de grootschalige '*cyberattacks'* op bepaalde wel uitgekozen landen. Deze aanvallen hebben enorme economische schade veroorzaakt aan de financiële wereld en toonde ook aan hoe zwak landen staan zonder hun digitale communicatie - en verbindingsmiddelen.[156]

---

[154] ANDREW, C. & MITROHHIN, V., *The sword and the shield. The Mitrokhin archive and the secret history of the KGB*, New York, Basic Books, 1999, p.354
[155] MELTON,. H.K., *Ultimate spy. Inside the secret world of espionage*, New York, DK Publishing, 2009, p.62.
[156] BLOCH, J., & TODD, P., *Global Intelligence: The World's Secret Services Today,* ,Londen, Zed Books, 2003, p.146-150

3.2. CHINESE INLICHTINGENDIENST

Het 'Ministerie voor Staatsveiligheid van de Volksrepubliek China' ('*Guójiā Ānquán Bù'* - MSS), wiens hoofdkwartier gelegen is in Beijing, is één van de grootste en meest effectieve inlichtingendienst ter wereld. Het MSS ressorteert onder de Staat van de Volksrepubliek China en houdt zich zowel bezig met binnenlandse als buitenlandse dreigingen binnen de republiek.

De primaire doelstelling van deze dienst ligt in de continue paraatheid tegen dreigingen die gericht zijn tegen de Chinese Volksrepubliek. Om aan potentiële dreigingen hoofd te bieden wint deze dienst informatie in over de veiligheid van haar staat evenals informatie over internationale affaires. Deze verzamelde informatie wordt, na het doorlopen van de inlichtingencyclus, overhandigd aan de Secretaris-Generaal van de 'Commissie voor Politiek en Wetgeving' die evenals de Minister van Publieke Veiligheid is.

Figuur 11 : Embleem MSS

Het uiteindelijke doel van de dienst is de totale veiligheid te garanderen ten opzichte van potentiële dreigingen zoals (buitenlandse) spionnen en agentschappen, staatsvijanden, terrorisme, antirevolutionaire gedachten en activiteiten evenals sabotage of het ondermijnen van het gezag. Doch hecht ze enorm veel belang aan het gebruik van inlichting - en rekruteringsofficieren in het buitenland, met meestal een diplomatieke dekmantel, om agenten en 'vertrouwelijke) informatie te verwerven van andere landen.

Naast een diplomatieke dekmantel maakt de dienst ook gretig gebruik van zakenlui, bedrijven en studenten om aan HUMINT te doen, evenals clandestiene buitenlandse operaties. Ze is vooral geïnteresseerd in militaire ontwikkelingen en technologie die ze daarna doorgeeft voor analyse aan het 'Militaire Inlichtingen departement' en de 'Nationale Defensie Commissie voor Wetenschap, Technologie & Industrie'. [157] De Chinese inlichtingendiensten hebben ook enorm veel belangstelling voor onze industriële ontwikkelingen.

[157] HANNAS, W.C., MULVENON, J., & PUGLISI, A.B., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* ,Abingdon , Routledge, 2013, 320p.

In 2005 werd een groep Chinese studenten ervan verdacht, werkend onder het mom van 'De Chinese Studenten en Wetenschappers associatie van Leuven', zich geïnfiltreerd te hebben in de Katholieke Universiteit Leuven. Dit stelde hen in staat industriële spionageactiviteiten te doen om rapporten en gegevens van nieuwe ontwikkelingen en onderzoeken te bemachtigen.[158]

3.3. NOORD - AMERIKAANSE INLICHTINGENDIENSTEN

Door klokkenluider Edward Snowden en zijn onthullingen is de doos van Pandora geopend voor de Amerikaanse inlichtingendiensten. Niet alleen zijn vele geheimen gelekt maar ook is de wereldbevolking zich meer gaan realiseren welke spionagedreigingen heden ter dage aanwezig zijn. Amerika is altijd al een trouwe bondgenoot geweest van België en van spionage is er normaal geen sprake in dit land. Alleszins toch niet uitgevoerd door Amerikaanse inlichtingenofficieren van de 'Centrale Inlichtingendienst'. Als ze hier aanwezig zijn in ons land, dan is het om andere buitenlandse inlichtingenofficieren in het oog te houden of met toestemming.

Het grote probleem van Amerika is haar 'spionagewaan'. Ze wil de hele wereld in het oog houden omdat ze overal mogelijke spionnen en terroristen ziet. In het monitoren van grote delen van de wereld is ze dan ook zeer goed geslaagd. Dit met behulp van hun 'Nationale Veiligheidsdienst'. Deze dienst is erin geslaagd, samen met haar Britse tegenhanger (GCHQ), nietsvermoedende en onschuldige burgers in grote delen van de wereld te monitoren en hun gegevens te verzamelen. [159]

België is hier vermoedelijk vaak het slachtoffer van geworden Ze onderschept(e) ook dataverkeer van Europese leiders - en instanties in Brussel. De reden dat deze inlichtingdiensten hier worden besproken ligt niet aan het feit dat ze indirect vertrouwelijke informatie hebben gestolen maar in het ethisch aspect. Hun spionagedaden hebben het vertrouwen van landen en staten in de Verenigde Staten geschonden evenals het recht op privacy van de Belgische bevolking.

---

[158] AMKREUTZ, R., (12//04/18) Als studenten maar geen spionnen zijn [WWW]. De Morgen : http://www.demorgen.be/dm/nl/1344/Onderwijs/article/detail/1425069/2012/04/18/Als-studenten-maar-geen-spionnen-zijn.dhtml [03/07/2014]

[159] PERMAN, S., *Spies, Inc. Bussiness Innovation from Israel's Master of Espionage*, Upper Sadle River, Pearson Education, 2005, p.107-109

1.1.8. Centrale Inlichtingendienst

Er zijn weinig personen die nog nooit van de 'Centrale Inlichtingendienst' van de Verenigde Staten van Amerika *('Central Intelligence Agency*' - CIA) hebben gehoord. Ze spelen vaak een duistere en sinistere rol in Amerikaanse films en series met ongelimiteerde bevoegdheden. Doch weten niet veel mensen wat deze dienst echt inhoudt. De CIA is de grote centrale buitenlandse inlichtingendienst van de Verenigde Staten. [160]

Figuur 12 : Embleem CIA

Ze is verantwoordelijk voor het verkrijgen en analyseren van informatie over individuen, bedrijven, organisaties en staten die verwerkt worden in de inlichtingencyclus. Hierna worden de verkregen inlichtingen doorgegeven aan verschillende overheidsdiensten en politieke instanties. Ze leidt een defensieve en offensieve inlichtingen en - counterintelligence dienst. Een van haar afdelingen, namelijk de *'Special Activities Division'* houdt zich bezig met het beïnvloeden van buitenlandse regeringen en politiek[161].

Dergelijke vormen van inmenging zullen waarschijnlijk ook in België zijn gebeurd hoewel er nooit echt iets over is gepubliceerd. Momenteel is het uitgelekt dat er '*undercover'* CIA agenten aanwezig zijn Europese landen waaronder in Nederland en Duitsland. Deze agenten voeren spionageopdrachten uit en zijn mogelijk ook in België actief. Ze hebben geen bepaalde doelwitten maar zijn eerder globaal geïnteresseerd in de geclassificeerde dossiers van landen.

1.1.9. Nationale Veiligheidsdienst

'De Nationale Veiligheidsdienst' ('*National Security Agency'* -NSA) valt onder de bevoegdheid van het Ministerie van Defensie en is gespecialiseerd in SIGINT en ELINT. Ze houdt zich met andere woorden bezig met het globaal verwerven, afluisteren en analyseren van elektronische informatie afkomstig uit communicatiemiddelen. Hiernaast houdt ze zich ook bezig met (de)cryptoanalyses. De dienst is ontstaan uit de angst voor te globale evolutie van elektronica en digitale communicatiemiddelen.

---

[160] TURNER, M.A., *Historical dictionary of United States Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, II, United Kingdom, Scarecrow Press, p.22-25
[161] JOHNSON, L.K. (ed.), *Handbook of intelligence studies*, London, Routledge, 2009, 382p

Haar oorspronkelijk doel lag in de bescherming van het de Verenigde Staten tegen mogelijke cyberaanvallen die desastreuze gevolgen konden hebben. De prioriteiten veranderde in elektronische oorlogsvoering door de toename van digitale dreigingen. Daardoor is ze ook bevoegd voor het gebruik van clandestiene methoden om haar opdrachten te vervullen. De middelen kunnen gaan van afluisterapparatuur, '*hacking'* en sabotage door subversieve software.[162]

Althans dit waren haar oude prioriteiten. Momenteel doet ze ook aan '*data-captatie'* en -'*mining'* en politieke spionage. De geheime informatie die Edward Snowden heeft onthuld, toonde aan dat de NSA, via zijn divisie '*International Securities Issues Build Out'*, informatie vergaart over het beleid van 'bevriende' landen. Landen die nauwe banden hebben met de VS op het vlak van economie, handel en defensie.[163]

Volgens een gelekt document verzamelt de NSA sinds 2006 informatie over het buitenlands beleid en buitenlandse handel van België. Vermoedelijk heeft ze dit gedaan door verschillende malen binnen te hacken op de computerinfrastructuur van Binnenlandse Zaken. Ook op de computers van ADIV zijn sporen van gesofisticeerde '*malware'* teruggevonden. Ook andere Belgische burgers en instellingen zoals professor Quisquater en BICS, het zusterbedrijf van Belgacom, zijn gehackt door een buitenlandse inlichtingendienst. De professionaliteit en manier van werken komt op veel vlakken overeen met de werkwijze van de NSA.[164]

Figuur 13 : Embleem NSA

4. BESLUIT

In dit derde gedeelte is er dieper ingegaan op de structuur en werking van de binnenlandse en buitenlandse inlichtingendiensten. In dit hoofdstuk komen de Belgische inlichtingen - en veiligheidsdiensten eerst aan bod. Eerst wordt er dieper ingegaan op hun ontstaansgeschiedenis. Vanuit deze geschiedenis is het simpeler om de huidige structuur van de diensten te begrijpen en onder wiens autoriteit ze ressorteren.

[162] BAMFORD, J., *Body of secrets. Anatomy of the ultra secret national security agency*, New Yokrk, Anchor Books, 2002, 654p.
[163] X, (z.d.)Snowden en België [WWW]. Datapanik : http://www.datapanik.org/dossiers/snowden-files/snowden-en-belgie/[03/07/2014]
[164] HARDING, L., *The Snowden Files : the inside story of the world's most wanted man*, Amsterdam, Nieuw Amsterdam, 320 p.

De wetgeving van 1998 en 2004, houdende regeling van de inlichtingen – en veiligheidsdienst, duiden de verschillende taken en bevoegdheden van beiden inlichtingendiensten aan. De VSSE is een burgerlijke defensieve dienst, terwijl de militaire tegenhanger, ADIV, zowel defensief als offensief is. Dit verschil geeft iedere dienst ook andere taken en bevoegdheden. Wat direct opvalt, is de soms 'vage' omschrijving door de wetgever over de bevoegdheden en werking van de inlichtingendiensten regelt.

De wetgever had hier mogelijk een dubbel doel voor ogen. Zo kon er 'speelruimte' zijn voor de inlichtingen - en veiligheidsdiensten in het vervullen van hun opdrachten. Het is al zeer moeilijk om dergelijke diensten volledig in het gelid te laten lopen als zij moeten waken over de veiligheid van het Belgisch grondgebied. Comité I en de BIM-commissie houden toezicht op de werking van deze diensten en tikken hen zeer snel op de vingers als ze hun 'boekje' te buiten gaan. Hierdoor kan een inlichtingendienst perfect functioneren binnen een democratie.

Verder in dit hoofdstuk kwam de onderlinge samenwerking aan bod evenals de samenwerking met het federaal parket. Het valt enorm op hoe goed de onderlinge samenwerking wettelijk is uitgewerkt. Opvallend is ook de feitelijke onbekendheid van spionagedossiers bij het federaal parket op het gebied van HUMINT of TECHINT. CYBINT dossiers, over gehackte computers, zijn eerder schering en inslag op dit moment. Het federaal parket stuurt dit type dossiers door naar hun afdeling georganiseerde misdaad, omdat deze afdeling over meer expertise beschikt. Maar de andere spionage en inmenging dossiers zijn zo goed als onbekend. Daardoor zijn er vragen gaan rijzen waar het misloopt.

Tijdens een interview met ADIV kwam er een spionagedossier ter sprake dat doorgegeven was aan het federaal parket. Dit dossier, zonder in detail te treden, ging over de omkoping van een hooggeplaatste industrieel door een agent van een niet nader genoemde buitenlandse inlichtingendienst. De ADIV had een overdaad aan bewijs verzameld en dit hebben doorgegeven. Na een periode van een jaar zou het parket nog steeds geen acties bevolen hebben. Zowel de VSSE, als ADIV, zullen niet te snel naar het federaal parket stappen. Dus de onderlinge samenwerking op dat vlak is nog niet optimaal. De samenwerking is wel goed wanneer de VSSE of ADIV gevraagd worden om technische bijstand. Daar is een positieve evolutie bezig door toenemend onderling contact en wederzijds vertrouwen. Nadat de binnenlandse inlichtingendiensten nader zijn bestudeerd, kwam de beurt aan de buitenlandse inlichtingendiensten.

Bijna ieder land ter wereld heeft een goed functionerende en uitgebouwde inlichtingendienst. Vele agenten van deze diensten zijn ook in Brussel actief door de aanwezigheid van de NATO en andere belangrijke Europese instellingen.

Het doel van deze thesis ligt niet in de volledige opsomming en bestudering van deze diensten. Daarom is er gefocust op drie landen wiens diensten volop bezig houden met activiteiten van spionage en inmenging op Belgisch grondgebied. Deze drie landen en hun diensten zijn; Rusland, China en Amerika. Andere landen hebben ook veel agenten in België maar van spionage of inmenging hoeft er niet direct sprake te zijn.

De aanwezigheid en doelstellingen van deze diensten tonen niets meer aan dan het belang dat spionage en inmenging niet minder belangrijk is dan terrorisme of subversie binnen België. Het is een actueel onderwerp en moet ook de nodige aandacht krijgen. Daarom is het ook van het grootste belang dat de Belgische inlichtingendiensten meer financiële middelen krijgen om spionage en inmenging te detecteren en te neutraliseren.

DEEL IV. COUNTERINTELLIGENCE

"An ideal counterintelligence system anticipates the enemy's move, notionally satisfies his needs, and indeed operates a notional intelligence service for him"

Eric W. Timm, "Countersabotage: A CI Function"

1. INLEIDING

Zoals gezegd is counterintelligence de verdedigingslinie om aanvallen af te weren van buitenlandse elementen en (criminele) groeperingen die trachten informatie te verzamelen door het gebruik van spionage. Hierdoor is zij verantwoordelijk voor de bescherming van het wetenschappelijk, economisch en politiek potentieel (WEP). Naast spionage tracht counterintelligence ook activiteiten van inmenging op te sporen en reactief te handelen. Zij doet dit door gebruik te maken van systematische observatie van belangrijke WEP sleutelfiguren, diplomaten, criminele groeperingen en van spionage verdachte individuen of bedrijven. Ook kan deze dienst op haar beurt informatie verzamelen door infiltratie of geheime operaties. Dit laatste wordt voornamelijk toegepast door militaire inlichtingendiensten zoals ADIV, maar ook de VSSE houdt zich hier mee bezig.

Deze diensten zullen ook, door middel van desinformatie, trachten spionnen om te tuin te leiden of in een val te lokken om hun identiteit bloot te geven. Naast spionage zorgt ook de CI dienst voor opsporing en bescherming tegen inmenging, de zogenoemde contra - inmenging. De counterintelligencedienst analyseert alle ingewonnen en door observatie verkregen informatie en zal deze inlichtingen dan verder aanvullen met bijkomende gezochte informatie. Eenmaal de inlichtingen 'vervolledigd' zullen ze worden geclassificeerd en opgevolgd, of doorgestuurd naar het federaal parket.

Als laatste luik in deze thesis zullen de principes van counterintelligence uiteengezet worden. Door het begrijpen van deze principes is het ook mogelijk om de preventieve en reactieve handhaving te bestuderen evenals de reactie van de Belgische inlichtingendiensten op voornamelijk spionage. Inmenging zelf is zo goed als onmogelijk preventief aan te pakken tenzij er sprake zou zijn van een kliklijn of klokkenluiderssysteem. Reactief optreden is wel mogelijk maar nog steeds zeer moeilijk. Immers, waar zit de grens tussen vriendschappelijk lobbyen en politieke inmenging.

Zolang er geen voldoende bewijslast is zoals fraude of duidelijke grote omkopingssommen kan er niet veel tegen ondernomen worden. Counterintelligence als inlichtingenstudie is in mijn ogen één van de meest interessante maar ook een van de moeilijkste onderwerpen om te bestuderen. Als men immers weet heeft van de actie - en reactiemogelijkheden van een land, dan vindt men ook zeer snel de zwaktes in haar systeem.[165] Inlichtingendiensten zullen hierover nooit iets concreet meedelen. Daarom zal dit hoofdstuk zowel academisch als praktijkgericht besproken worden aan de hand van globale standaard gekende elementen en handboeken.

2. SITUERING

Vooraleer de term '*counterintelligence'* (CI) te definiëren, is het belangrijk om te weten waar het begrip zich precies situeert. We hebben in de vorige hoofdstukken gezien wat inlichtingen precies inhoudt. Inlichtingen kunnen verdeeld worden in vier brede zuilen[166]; spionage, onderzoek en analyse, observatie en geheime operaties. De zuil spionage en de zuil observatie ondersteunen de zuil onderzoek en analyse. De combinatie van deze drie zuilen ondersteunt dan weer de zuil geheime operaties. In deze structuur vormt *counterintelligence* het verbindingsstuk tussen deze zuilen. [167]

In het eerste hoofdstuk werd spionage helemaal uiteengezet net zoals onderzoek en analyse in de paragraaf over de inlichtingencyclus. Observatie refereert naar bepaalde methoden voor het vergaren van informatie door middel van kijken. Deze methoden verschillen van HUMINT en zijn eerder gericht op TECHINT zoals afluisterapparatuur, radiofrequentie apparatuur en speciale fotografie zoals het gebruik van satellieten. Het gebruik van observatiemiddelen kan informatie opleveren op vlakken waar andere middelen falen. Toch zal een inlichtingendienst niet snel de HUMINT verwaarlozen. Het gebruik van observatie staat in grote mate gelijk aan het gebruik van open source bronnen. Per slot van rekening wordt er vaak geobserveerd in het publiek domein.

In de grijze zone van inlichtingenwerk liggen de geheime operaties, ook wel '*covert ops'* of '*black ops'* genoemd.

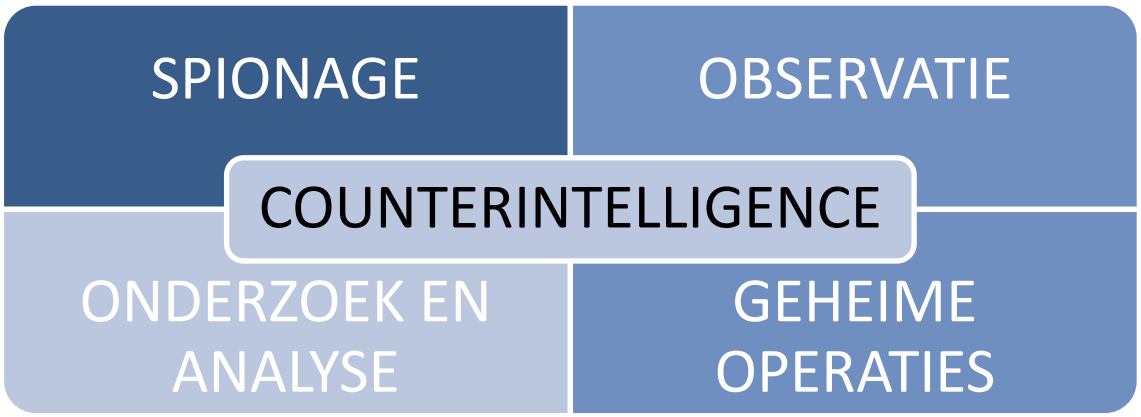
---

[165] JOHNSON, W.R., T*hwarting Enemies at Home and Abroad. How to Be a Counterintelligence Office*, Whasington, Georgetown University Press, 2009, p.149-150

[166] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.18-22

[167] EHRMAN, J.," Toward a Theory of CI**:** What are We Talking About When We Talk about Counterintelligence?", in *Studies in Intelligence,* Washington, Government printing office, 5-23

Dit zijn operaties waar de indringer de verkregen informatie via de drie zuilen gebruikt om bondgenootschappen te versterken en voor het verzwakken (en zelfs vernietigen) van zijn opponenten. De effectiviteit van geheime operaties hangt af van hoe goed de betrokkenheid van de indringer geheim blijft of ontkend wordt.



Figuur 14 : De bouwstenen van counterintelligence

3. DEFINTIE

Counterintelligence als term wordt vaak verward met operationele beveiliging gericht op de bescherming van gebouwen en personen. In de praktijk zou men kunnen beargumenteren dat ze beiden gerelateerd zijn aan elkaar maar niet identiek zijn. Immers, beveiliging is een belangrijk aspect van inlichtingenwerk dat ook counterintelligence omvat, maar moet gezien worden in een ruimere betekenis. In dit hoofdstuk zal ook vaak de generale term tegenstander of opponent worden gebruikt als verzamelnaam voor spionnen, agenten, inlichtingen - en rekruteringsofficieren.

Operationele beveiliging is een manier van leven die hoort bij alle geheime activiteiten ongeacht het over counterintelligence, spionage, overspel of poker gaat. Het staat tegenover deze activiteiten zoals stijl staat ten opzichte van een schrijver of kunstenaar, en staat niet op zichzelf zoals een verhaal of kunstwerk. En zoals alle beveiliging is het doel 'profylactisch' want het sluit 'schadelijke' en 'toxische organismes' uit. Dit komt er dus op neer om te zwijgen en het beschermen van geclassificeerde en vertrouwelijke documenten. Het komt neer op de ' *Need-to-Know'* wet. [168]

[168] JOHNSON, W.R., T*hwarting Enemies at Home and Abroad. How to Be a Counterintelligence Office*, Whasington, Georgetown University Press, 2009, p. 1-5.

Dit wil zeggen dat enkel mensen die bepaalde gevoelige en vertrouwelijke informatie moeten weten daar toegang tot hebben.[169] Het grote verschil nu tussen operationele beveiliging en CI ligt in de betekenis van CI zelf. Het is een actieve bescherming van inlichtingen tegen zowel preventief als reactief vijandige pogingen en activiteiten van inwinning en dit door verschillende technieken te hanteren waaronder operationele beveiliging. Al deze technieken zijn gericht op het frustreren van vreemde mogendheden die aan spionage en inmenging doen.

Counterintelligence kan verdeeld worden in een defensieve en offensieve strategie. Defensief zal afschrikking en detectie inhouden. Afschrikking is het in staat zijn om te voorkomen dat een potentiële indringer toegang verkrijgt tot informatie. In deze context kan het twee betekenissen hebben. Het kan gebeuren door de indringer te ontmoedigen om binnen te dringen. Evenwel kan het ook de stopzetting van de informatieverzameling van de indringer inhouden nadat hij reeds is binnengedrongen.[170]

- Afschrikking: Dit bestaat uit drie componenten die allen aanwezig moeten zijn om van haar doel te kunnen bereiken. Afschrikking moet een dreiging inhouden die een onaanvaardbare schade kan aanrichten bij een indringer. De dreiging moet waarneembaar zijn voor de indringer. En als laatste moet de dreiging geloofwaardig zijn en in staat zijn om onaanvaardbare schade te kunnen en willen aanrichten

- Detectie: Dit houdt in dat men een gebeuren opmerkt en dat dit gebeuren in verband kan staan met een mogelijke (potentiële) binnendringing of lek van vertrouwelijke informatie. Hierbij zijn vijf belangrijke acties van belang na een detectie;

    - Het identificeren van een gebeuren of gebeurtenis.
    - Het identificeren van de personen die hierbij betrokken waren.
    - Het identificeren van de organisatorische banden van mogelijke verdachten. Met andere woorden, voor wie werkt hij of zij?
    - Het identificeren van de huidige locatie van de mogelijke verdachten
    - Het verzamelen van bewijs (en feiten) dat een persoon schuldig is aan het gebeuren.

[169] JOHNSON, W.R., T*hwarting Enemies at Home and Abroad. How to Be a Counterintelligence Office*, Wahsington, Georgetown University Press, 2009, p.2-3
[170] FRANCQ, A., 'The Use of Counterintelligence, Security and Countermeasures' in *Managing Frontiers in Competitive Intelligence*, FLEISHER, C. & BLENKHORN, D. Westport, Greenwood, 2001, p.40-61

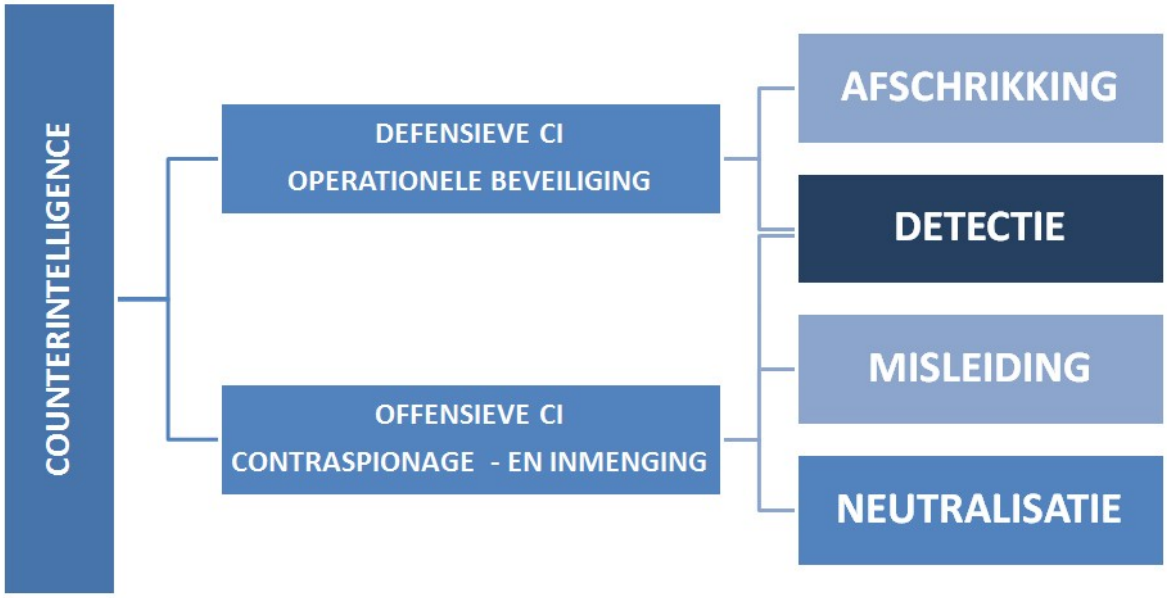
Contraspionage en contra-inmenging maken deel uit van het offensieve gedeelte waar misleiding en neutralisatie deel van uitmaken, alsook detectie in een bepaalde graad. Detectie is dus zowel passief defensief als actief offensief. Contraspionage en contra-inmenging verschillen van spionage en inmenging op vlak van wie het doelwit is. Er wordt over spionage gesproken als men informatie of geheimen van individuen, bedrijven, defensie, politiek of wetenschappelijke ontwikkelingen steelt.[171]

Contra-spionage is het stelen van informatie van inlichtingendiensten. Contra-inmenging houdt de opsporing van beïnvloedingsagenten in. Maar het kan evengoed contrapropaganda omvatten om verschenen negatieve propaganda te '*counteren*' door eigen propaganda te verdelen. Maar het kan ook gaan over het neerhalen van sites of haatzenders die oproepen tot radicalisme of terrorisme in België.

- Misleiding: Hierbij staat het misleiden van leidinggevende figuren van een oppositie centraal en dit over een bepaald aspect van de dienst of organisatie waarin ze is geïnteresseerd. Dit aspect kan gaan over de operaties, capaciteiten, middelen, intenties en beslissingen van deze dienst of organisatie. Ook het verbergen van de identiteit van de binnendringer valt hieronder. Het uiteindelijke doel van misleiding is de tegenstander acties laten ondernemen die vergeefs zijn of acties te doen stopzetten. Verwarring speelt hier soms ook een cruciale rol om de reactietijd van de tegenstander te doen verminderen. Dit alles maakt een tegenstander zwakker en geeft de eigen dienst de overhand.

- Neutralisatie: Als laatste is er de neutralisatie die de stopzetting van de informatieverzameling van de tegenstander als doel heeft. Het houdt het neerslaan van een aanval of lek in en kan zelfs de figuratieve vernietiging betekenen van een vijandig spionagenetwerk of organisatie.

[171] Interview met afdelingscommissaris X, Hoofd Analyse Counter Intelligence



Figuur 15 : Counterintelligence structuur

4. DEFENSIEVE COUNTERINTELLIGENCE

Defensieve counterintelligence zal zich dus focussen op het afschrikken en detecteren van potentiële indringers die trachten toegang te verkrijgen tot bepaalde geclassificeerde informatie. De afschrikking en detectie kunnen enkel efficiënt beoefend worden door fysieke beveiliging. Het woord 'fysiek' moet in deze context zeer ruim geïnterpreteerd worden. Immers, de huidige digitale en technologische evolutie heeft ervoor gezorgd dat ook digitale '*walls'* en barrières nodig zijn als bescherming. Er moet bescherming geboden worden aan (bijna) iedere bestaande potentiële dreiging. Om hierin te slagen moeten er verschillende hiërarchische soorten beveiliging aanwezig zijn. Als een indringer erin slaagt weg door de eerste barrière te breken zal hij steeds tegenover een nieuwe barrière komen te staan die steeds strikter en moeilijker te penetreren valt.

4.1. Risicomanagement

Vooraleer de defensieve counterintelligence naderbij wordt bekeken, is het belangrijk om te weten wat de omvang van de dreiging inhoudt. Om dit te weten moet men een risicoanalyse uitvoeren en uitmaken welke informatie hoge bescherming moet genieten en welke niet. Risico als term is afgeleid van het Latijnse woord '*Risicare'* wat 'durven' betekent. Durven winnen of falen. Bij een dreigingsanalyse onderscheidt men twee hoofdzaken. Er is enerzijds de persoon of entiteit die een dreiging vormt, de zogenaamde 'dreigingsagent'.

De term dreigingsagent, vrij vertaald uit het Engelse '*threat agent'*, hoeft niet direct specifiek te verwijzen naar een beroepsmatige agent of inlichtingenofficier maar kan alles en iedereen inhouden gaande van een buitenlandse organisatie tot een eigen werknemer tot een klein computervirus.[172] De soorten dreigingsagent worden gerangschikt volgens drie klassen;

- Klasse I: Deze klasse van dreigingsagent werkt voor een buitenlandse veiligheid - of inlichtingendienst. Deze kan burgerlijk, militair of privaat zijn en gaat zeer professioneel te werk.

- Klasse II: Onder deze klasse vallen dreigingsagenten die werken voor een georganiseerde misdaad - of terroristische groepering. Ook 'overijverige' journalisten en privédetectives vallen hieronder.

- Klasse III: De eerder 'amateuristische' klasse die het niet speciaal doet als opdracht of geld maar eerder uit eigen motief en ideologie zonder een bepaalde training of ervaring te hebben gehad. Vaak zijn dit activisten met een bepaalde ideologie.

Om te weten welke dreiging de dreigingsagent inhoudt, is het belangrijk om meer te weten te komen over zijn intenties en zijn bekwaamheid.[173] Dit gebeurt door risicomanagement en door meer te weten te komen over de informatie die hij begeert en zijn verwachtingen Op die manier is het mogelijk om de intenties van de potentiële indringer in te schatten. En door meer te weten te komen over de kennis en ervaring van de persoon alsook de middelen waarover hij beschikt, is het mogelijk in te schatten hoe bekwaam hij is.

Anderzijds is er ook het doel van de dreiging. Het doel is het mogelijke 'risico' dat een dreigingsagent vertrouwelijke informatie tracht te bekomen, gerelateerd met de kwetsbaarheid van een systeem dat dreigingsagenten tracht te ontdekken.[174] Naargelang de aantrekkelijkheid van vertrouwelijke informatie, de gemakkelijkheid van binnendringen en de impact die het heeft kan men de kwetsbaarheid achterhalen. Onder de term risico wordt er vaak in het risicomanagement gesproken over; de termen 'waarschijnlijkheid' en 'consequenties'. [175]

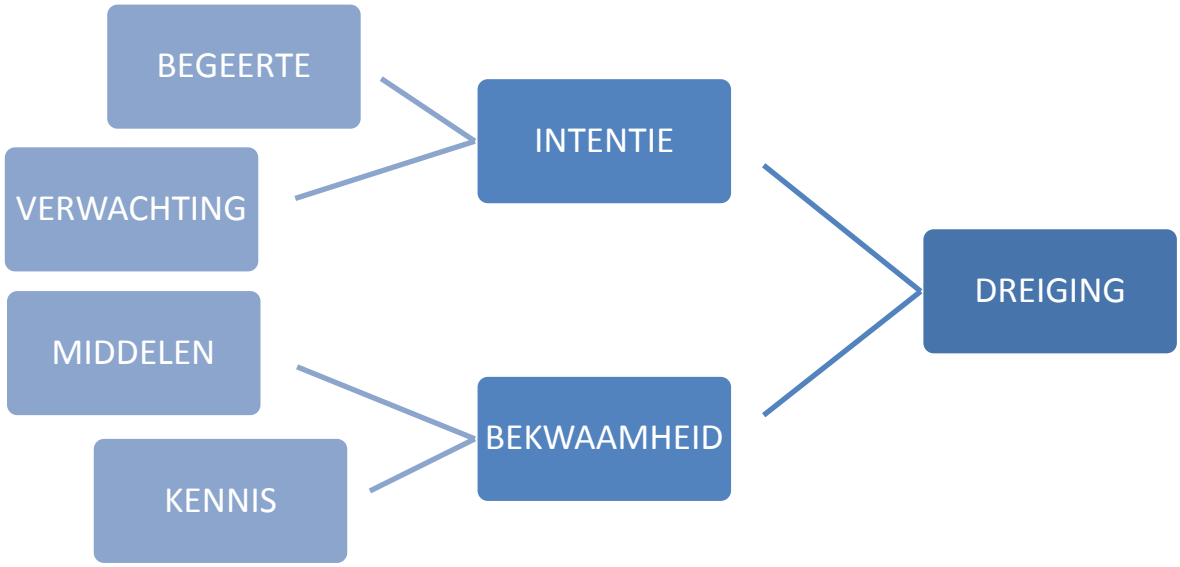
---

[172] TILLER, J.S., *The ethical hack. A framework for business value penetration testing, Boca Raton,* Auerbach, 2005, p.70-71

[173] GODLEWSKI, R.J, *"*Human Intelligence: Perceiving an Enemy's Thoughts*"* in *American Intelligence Journal,* COL.SPRACHER, W.C., 2009, p.29.

[174] X, ISO 31000 : Risk management. Risk assessment techniques., Genève, ISO, p. 13-15

[175] NICOLS, A., *A Perspective on Threats in the Risk Analysis Process,* SANS Institute, SANS Institute Reading Room, 2002, p.1-5



Figuur 16 : Dreigingsanalyse structuur

De term 'waarschijnlijkheid' gaat erover dat iets kan gebeuren, gecombineerd met de gevolgen die er uit kunnen voortvloeien. De term consequenties gaat over de implicaties die voortkomen wanneer vertrouwelijke informatie wordt gelekt. Met al deze informatie voorhanden zijn veiligheids - en inlichtingendiensten, waaronder de VSSE en de ADIV, in staat dreigingen tijdig op te sporen.

		Consequence				
		Trivial	**Minor**	**Moderate**	**Major**	**Severe**
Likelihood	Almost certain	L	H	H	E	E
	Likely	L	M	H	H	E
	Possible	L	M	M	H	E
	Unlikely	L	M	M	H	H
	Rare	L	L	M	M	H

E - Extreme risk, requiring immediate action.
H - High risk issue requiring additional research or some immediate action
M - Moderate risk issue that are likely to benefit from adaptation measures
L - Low risk issues that can be dealt with as and when they happen or they are considered acceptable should they happen

Figuur 17: Schema om het risiconiveau te berekenen door de factoren 'waarschijnlijkheid' en 'consequenties' in kaart te brengen

4.2. Afschrikking en Detectie

Als er gesproken wordt over beveiliging is het altijd handig om visueel een Romeins versterkt fort voor de geest te halen. Dergelijk bouwwerk bestaat uit; een houten palissade, een diepe greppel, een hoge muuromwalling met doorntakken en struiken bovenaan. Voor en achter de omwalling bevinden zich wachttorens, patrouilles en ganzen die bij het minste geluid alarm slaan. Eenmaal binnenin het fort is er een doolhof van diverse gebouwen aanwezig waarvan het belangrijkste gebouw de " PRINCIPIA" is. Dit is beter gekend als het hoofdkwartier dat zich pal in het midden bevond in het fort. In dit hoofdkwartier bevonden zich de archieven, orders en strategische plannen, de soldijen en de Aedas. Deze laatste kan men vergelijken met de regimentsvlag die troepen meenemen ter motivatie en geluk tijdens buitenlandse opdrachten. Dit hoofdkwartier werd extra bewaakt en vaak was er ook een zegel of rang nodig om bepaalde ruimtes te mogen betreden. [176]

Sinds dan zijn we een heel eind geëvolueerd maar het principe is hetzelfde gebleven. Er worden nog steeds omheiningen gebouwd, wachttorens worden vervangen door camera's, ganzen door bewegingsdetectoren, papieren boodschappen met geheimschrift zijn gecodeerde elektronische berichten geworden enzovoort. Het gebruik van dergelijke soorten beveiliging is niet absoluut maar geeft wel mee vorm aan het opbouwend afschrikkend effect. Des de dieper men binnendringt, des de groter de beveiliging. Weinigen zullen dan geneigd zijn over een hoge muur met scheerrmesjesprikkeldraad te klimmen.

Doen ze het toch zullen ze snel tegenover een volgende beveiligingsmaatregel staan zoals camera's, wachters, honden, toegangsdeuren, en vele andere detectiemiddelen. Potentiële indringers zullen daarom ook steeds nieuwe methodes trachten te bedenken en ontwikkelen. Methodes waar ook CI zal op anticiperen door (toekomstige) risico's te bestuderen en door aan offensieve CI te doen, wat later nog aanbod zal komen. Het is immers belangrijk om te weten welke nieuwe methoden buitenlandse inlichtingendiensten bezitten om een maximaal beveiligd gebouw of netwerk binnen te dringen om zo aan informatie te geraken. De verkregen kennis van nieuwe (mogelijke) ontwikkelde methoden van de tegenpartij kan dan gebruikt worden om hierop tijdig te anticiperen en maatregelen te nemen.

[176] MEIJER, F., *Het Romeinse leger. Handboek voor de generaal door Vegetius*, Amsterdam, Polak & Van Gennep, 2002, p. 175p.

4.2.1. Fysieke beveiliging

Onder fysieke beveiliging verstaan we alle soorten barrières zoals omheiningen rond gebouwen, de elektronische toegangscontroles en badges, kluizen en sloten, cameratoezicht, ramen en deuren maar ook complexe en gesofisticeerde computerbeveiliging. Ze worden hier even kort opgesomd. [177]

- Perimeter barrières: Dit zijn barrières die een bepaalde perimeter afbakenen door middel van afrastering, stalen hekken, muren. Deze muren zijn al dan niet uitgerust met een overklimbeveiliging zoals schrik - of (scheermesjes)prikkeldraad of stalen opstaande scherpe punten.

- Toegangspoorten: Onder toegangspoorten moeten alle plekken gezien worden waar men langs moet om een bepaalde plek te bereiken. Hier wordt een onderscheid gemaakt tussen externe en interne deuren, slagbomen en *'traffic control spikes'*. Deze poorten kunnen bemand zijn met een wachter die voor extra afschrikking en controle zorgt. Ook ramen kunnen voor een indringer als toegangspoort gezien worden en moeten daarom uitgerust worden met glasbreuksensoren gecombineerd met gelaagd veiligheidsglas of een raamhek. Om het afschrikeffect te vergroten kan de middelste laag van het veiligheidsglas bestaan uit spiegelglas. Dit effect zorgt ervoor dat potentiele indringers niet in staat zijn om binnen te kijken. Dus kunnen ze niet weten of er daadwerkelijk iemand aanwezig is en toezicht houdt of niet. Wat de angst om op heterdaad betrapt te worden vergroot.

- Detectiemiddelen: Camera's, paalverlichting, spots en bewegingssensoren vallen onder de detectiemiddelen omdat ze bijdragen tot het afschrikken en detecteren van abnormale gebeurtenissen of pogingen tot illegale binnendringing. Naast deze elektronische detectiemiddelen zijn er ook bewakers en/of patrouilles aanwezig die observeren, indringers detecteren en een enorm afschrikwekkend effect creëren. Een extra voordeel aan bewakers is dat ze handelen naargelang een situatie zich voordoet. Menselijke en technische detectiemiddelen worden: '*Trip wires'* genoemd omdat ze soms ongemerkt illegale acties kunnen observeren.

[177] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.73-85 & 109-111

- Computerbeveiliging: De beveiliging van een computer en computernetwerk is zeer complex. Het is ook zeer vaak een doelwit van buitenlandse inlichtingendiensten doordat ze niet in het gebouw aanwezig moeten zijn om binnen te dringen en informatie te stelen.[178] Bij computerbeveiliging zijn er drie belangrijke factoren die ervoor zorgen dat, als ze goed beveiligd zijn, er geen informatielek kan zijn van digitaal opgeslagen documenten. Deze drie factoren zijn de hardware van een computer (netwerk), de software van een computer(netwerk) en de digitale externe communicatie. Door veiligheidsmaatregelen te creëren voor deze factoren is de data veilig en beschermd. Maar wanneer er bijvoorbeeld geen afgeschermde communicatiekabels gebruikt worden, dus kabels waar geen isolatieschild rond zit van aluminium en koper, dan bestaat de kans dat het aangetast wordt door elektromagnetische straling of wordt onderschept en er illegaal informatie wordt van afgetapt. Of om het met de woorden van Martin C. Libicki in zijn boek "Cyberdeterrence and Cyberwar" te verduidelijken ;

  "As long as nations rely on computer networks as a foundation for military and economic power and as long as such computer networks are accessible to the outside, they are at risk."

4.2.2. Veiligheidsonderzoeken

Een veiligheidsonderzoek is noodzakelijk bij het aannemen van mensen voor bepaalde functies waar ze vaak in contact komen met gevoelige en vertrouwelijke informatie. Achtergrondscreening is van het allergrootste belang omdat het verleden voldoende voorbeelden bevat van infiltraties door tegenpartijen om aan informatie te geraken. Anderen zijn dan weer door bepaalde beweegredenen in hun carrière overgegaan tot spionage. Door een veiligheidsonderzoek is het mogelijk te zien of een persoon met vertrouwelijke informatie mag belast worden, bepaalde zwaktes heeft en of deze persoon loyaal zal blijven naargelang de tijd vordert. Hiervoor wordt zijn gehele levensgeschiedenis grondig onderzocht. Dit gaande van zijn geboorteplaats, opleiding, status, vorige werknemers, militair of politioneel verleden, financiën en bezit en natuurlijk ook zijn strafblad.

[178] SHAKARIAN, P., SHAKARIAN, J. & RUEF, A., *Introduction to cyber-warfare. A Multidisciplinary approach*, Waltham, Elseviers, 2013, p. 29-31.

4.2.3. Informatie - en communicatiebeveiliging

Als laatste wordt het gebruik en de verwerking van informatie en communicatie onder de loep genomen. Informatiebeveiliging legt zich toe op de observatie en de beveiliging van het gebruik van alle vormen van informatie en geclassificeerde documenten. Enkele van deze beveiligingen zijn[179];

- Classificatie: Documenten worden geclassificeerd naargelang de inhoud en de vertrouwelijkheid ervan. Hierdoor worden ze verdeeld in twee groepen, namelijk de geclassificeerde en ongeclassificeerde documenten. Binnen de geclassificeerde documenten bestaat er een onderverdeling van 'VERTROUWELIJK', 'GEHEIM' en 'TOP GEHEIM'. Ongeclassificeerde documenten worden onderverdeeld in 'GEVOELIG' en 'ONGECLASSIFICEERD'.

- Compartimering: Door deze gradaties is het mogelijk de documenten te compartimeren. Dit creëert een hiërarchie beginnende vanaf voor iedereen toegankelijk ongeclassificeerde documenten tot top geheime documenten, die slechts voor enkele 'ingewijden' toegankelijk zijn. Ook krijgen documenten, naargelang hun classificatie, vaak een ongerelateerde codenaam zoals 'Operatie Struisvogel' in de zaak Binet. Dergelijke benamingen zorgen ervoor dat buitenstaanders geen hint krijgen over wat het document mogelijk inhoudt.

Naast de informatieve beveiliging is er ook een communicatiebeveiliging waar de hoofdprioriteit het veilig communiceren zonder 'dat het contact wordt afgeluisterd door een derde persoon is. Hier gaat het zowel over telefoon - als internetcommunicatie en de nodige maatregelen die men neemt zoals het coderen van boodschappen.

5. OFFENSIEVE COUNTERINTELLIGENCE

Na het naderbij bestuderen van de defensieve vorm van CI komt nu de offensieve CI aan bod. Offensieve CI kan gezien worden als een ouderwets potje schaken en kan slechts gewonnen worden door de koning van de tegenstander schaakmat te zetten.

[179]BIDGOLI, H., *Handbook of Information Security. Key Concepts, Infrastructure, Standards, and Protocols*, Hoboken, John Wiley & Sons, 2006, p.27

Als speler moet je de tegenstander telkens twee zetten voor zijn. Mensenkennis speelt een grote rol alsook de kennis over de vaste strategieën van de tegenstander.Voert de tegenstander al zeer snel een 'rokade' uit door zijn koning in veiligheid te brengen of brengt hij liever al enkele pionnen in een aanvallende stelling? Naast kennis over de strategie, die ingewonnen kan worden door eerdere wedstrijden of video's van hem tegenover andere spelers, is het belangrijk om bepaalde pionnen uit te schakelen. Het neutraliseren kan gebeuren door een zeer goede aanval of door een aanval uit te lokken die uitmondt in een valstrik. Dit klinkt allemaal eenvoudiger dan het lijkt. De tegenstander weet waarschijnlijk dat je hem tracht in een val te laten lopen. Daarom is het belangrijk om de tegenstander ook te misleiden en schijnaanvallen te ondernemen. [180]

Verschilt een spel schaak nu zo hard van de realiteit? Neen, want zowel detectie, misleiding en neutralisatie komen hierin terug. Offensieve CI tracht ook eerst mogelijke toekomstige aanvallen en acties te detecteren door meer informatie over de tegenstander en zijn potentie in te winnen. Dergelijke CI tracht ook bepaalde acties uit te lokken bijvoorbeeld het plaatsen van '*honeypots'* om inlichtingenofficieren en agenten aan te trekken als wespen naar zoetigheid [181] Als laatste trachten CI officieren de dreiging te verlammen of te neutraliseren.

5.1. Detectie

Detectie is al kort besproken bij de defensieve aanpak. Het grote verschil met detectie bij de offensieve aanpak ligt in de ontdekking zelf. Detectie bij defensieve CI is een reactie die voortvloeit uit het betrappen van een indringer. Echter, bij offensieve CI is detectie de actie en moet er hierop een reactie op komen van de inlichtingendienst. Deze reactie bestaat uit een gerechtelijk (voor)onderzoek waar de inlichtingendiensten technische bijstand bij verlenen. Aan de hand van dit onderzoek zal, zoals een gerechtelijk onderzoek, gezocht worden naar alle mogelijke sporen die gelinkt kunnen worden aan de dader. Sporen zoals DNA, (digitale) vingerafdrukken en sporen, persoonsbeschrijving of camerabeelden, het *instrumentum sceleris* (het voorwerp waarmee het misdrijf is gepleegd), verloren of achtergelaten documenten of bewijslast. Het is wel belangrijk om te weten dat, ondanks de primaire focus nog steeds ligt op misleiding en neutralisatie als reactie, alles gecoördineerd wordt via het federaal parket.

---

[180] REAGAN, M.L., *Intro to U.S. Counterintelligence. CI 101 : A Primer.,* Amerika, HSDL, 2005, p.29-41.
[181] *Honeypots' zijn niet te verwarren met 'honeytraps' wat vrouwelijke seksuele ontmoetingen inhouden Deze ontmoeting worden dan gefotografeerd en gebruikt als chantage materiaal voor aan informatie te geraken.*

Er is tenslotte sprake van een gepleegd misdrijf dat onderzocht en vervolgd moet worden volgens de letter van de wet. [182]

5.2. Misleiding

Cognitieve psychologie bestudeert de mentale processen van een individu die in relatie staan tot zaken zoals kennis en kennisverwerking, herinneringen en het oplossen van problemen. Deze theoretische basis heeft gediend voor de toepassing van misleiding. Misleiding als CI tactiek tracht de cognitieve processen van (mogelijke) tegenstanders te beïnvloeden om zo zijn denken te manipuleren. Misleiding als tactiek kan door drie methoden[183] worden toegepast;

- Lokaas: Het plaatsen van een lokaas, '*honeypots',* heeft al vaak buitenlandse agenten en spionnen in de val doen lokken. Dit kan gebeuren door het subtiel laten uitlekken van bepaalde onwaarheden over de locatie van dossiers of nieuw ontwikkelde militaire technologie. De nietsvermoedende tegenstander gaat erop af en voor hij het weet is de indringer in de boeien geslagen of krijgt hij het aanbod om een dubbelagent te worden. Er bestaan ook computerlokeenden die fungeren als '*honeypots'* om hackers op het spoor te komen. Het gebruik van lokaas hoeft niet noodzakelijk te dienen om een persoon op heterdaad te betrappen maar kan evengoed als medium gebruikt worden om desinformatie te verspreiden. Foutieve informatie in de handen van de tegenstander zal hem op een tijdelijk dwaalspoor kunnen brengen. Tenslotte denkt de indringer dat hij zwaar beveiligde en geheime informatie heeft gestolen. Dus zal hij, zolang hij er niet snel achter komt, niet meer opnieuw trachten binnen te dringen opzoek naar dergelijke gevoelige informatie.

- Camouflage: Camouflage bij CI gaat over het opgaan in de omgeving. Het gebruik van denkmantels en nepbedrijven vallen ook hieronder als het helpt omstaanders en tegenstanders af te leiden.

  .

- List: Door voorwendsel en list te gebruiken is het mogelijk om tegenstanders te misleiden. Een oud maar zeer gekend voorbeeld is "Operation Mincemeat'.

[182] Interview met afdelingscommissaris X, Hoofd Operaties CI ADIV
[183] MELTHON, K.H. & WALLACE, R., *The Official CIA Manual of Trickery and Deception*, New York, Hardie Grant Books, 2009, p.88

- Hier werd een lijk van een soldaat aangekleed als hoog officier en kreeg de naam en rang van 'Majoor Martin'. Majoor Martin kreeg valse documenten toegestopt die de Duitsers op het verkeerde spoor moesten brengen als de geallieerden gingen binnenvallen. Majoor Martin werd 's nachts voor de Spaanse kunst gegooid en 's anderendaags opgevist door de Duitsers. De documenten die ze tot hun verwondering aantroffen heeft geleid tot de verandering van vele strategische plannen van de Duitse bezetting in Spanje. De veranderingen waren in het voordeel van de geallieerden die als enige wisten dat de papieren nep waren. Hierdoor konden ze in 1943, zonder al te veel tegenstand, Sicilië binnenvallen.

5.3. Neutralisatie

Het begrip 'neutralisatie' in deze context handelt niet over het liquideren van vijandige agenten zoals ze vaak beschreven staan in vele spionageromans. Liquidatie werd vroeger wel toegepast in bepaalde dictaturen. Doch gebeurde dit pas na de arrestatie, want men moest eerst de spion uithoren. Neutralisatie is de meest extreme tactiek van CI omdat het gebruik maakt van complexe strategieën die opzettelijk een eigen agent in direct contact plaatst met de het inlichtingenpersoneel van de tegenstander. Ongeacht het gaat over een kleinschalige spion of een hooggeplaatste inlichtingenofficier. Er zijn twee goede tactische redenen om over te gaan tot dergelijke handelingen. [184]

De eerste reden stelt een CI officier in staat om aan desinformatie te doen, door valse documenten continu en rechtstreeks te bezorgen aan een tegenstander. De tegenstander wordt zo misleid waardoor dit verwarringen en wijzigingen in hun plannen creëert. De tweede reden is van een andere aard. In plaats van desinformatie gaat men ineens over tot op heterdaad betrapping. Als de tegenstander gevat wordt zal hij gearresteerd worden of de keuze krijgen om dubbelspion te worden. In geval van TECHINT of CYBINT is het doel evenredig. Ofwel desinformatie via deze kanalen doorgeven of bij een cyberaanval een tegenaanval lanceren om het gevaar te neutraliseren.

Vooraleer over te gaan tot de daadwerkelijke desinformatie en neutralisatie moet er een tactiek bestudeerd worden om een opponent in de val de doen lokken.

[184] MORAVEJ, K. & DIAZ, G," Critical Issues in Contemporary Counter-Intelligence" in *UNISCI Discussion Papers,* UNISCI (eds.), Madrid, 2007, 53-70

Doch moet er rekening gehouden worden dat de tegenpartij er altijd vanuit zal gaan dat er mogelijk een valstrik is en uiterst behoedzaam te werk zal gaan. Daarom bestaat er een waaier aan tactieken die CI officieren kunnen toepassen om tot neutralisatie over te gaan. Door de uitgebreidheid zullen enkel de belangrijkste neutralisatietechnieken uitgelegd worden;

- Dubbelspion: Een dubbelspion is een individu die weg voor twee verschillende inlichtingendiensten werkt. Een inlichtingenofficier die voor een bepaalde buitenlandse dienst A werkt kan overlopen (op vrijwillige basis of als opdracht) of opgepakt worden door een andere inlichtingendienst B. Hij wordt volledig geanalyseerd en wordt gekeken of hij kan gebruikt worden voor dubbelspionage. Als het onderzoek positief is, en met zijn goedkeuren, gaat dat hij voor de B zijde werken. Dit betekent dat hij nu nog wel moet rapporteren aan zowel beiden diensten A en B, zonder dat A dit weet. Gelijktijdig is hij ook in staat te vertellen wie nog mede spionnen zijn. Dubbelspionnen zijn als het ware zowel een vloek als een zege voor CI officieren. Het gebruik ervan is ideaal om aan CI te doen maar zo denken de tegenstanders er ook over. En dan wordt het een enorme opgave om de dubbelspion te vinden. [185]

- Triple-spion: Een triple-spion verschilt niet veel van een dubbelspion. Het is vaak een dubbel spion die berouw heeft gekregen over zijn dubbelspel.[186] Door alles op te biechten aan zijn eerste werkgever kan deze beslissen hem in te zetten als triple-spion. Hij doet zich bij de andere zijde voor als dubbelspion maar werkt in feite terug voor de originele dienst die hem heeft opgeleid. Het houdt dus niets meer in dan een complexe verschuiving in het spionagespel. Sommige inlichtingendiensten hebben zelfs heuse strategieën uitgewerkt en agenten uitgekozen om triple-spion te worden.. De beste manier om dit uit te leggen is aan de hand van een duidelijk voorbeeld; Een CI officier van inlichtingendienst 'A' doet zich voor als een overloper of iemand die oneervol is ontslagen. Hij biedt zijn diensten aan een andere inlichtingendienst B. De dienst B ziet potentieel in het rekruteren van een ervaren inlichtingenofficier die kennis heeft over de werking van haar vorige inlichtingendienst A. Eenmaal aangenomen geeft de CI officier, zoals ervoor overeengekomen met de dienst A, informatie aan dienst B om hun vertrouwen te winnen.

[185] ANDREW, C. & MITROHHIN, V., *The sword and the shield. The Mitrokhin archive and the secret history of the KGB*, New York, Basic Books, 1999, p.19-20
[186] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.198-200

- Deze informatie bevat zowel kernen van waarheid als onwaarheden. Dit kan best gevaarlijk zijn omdat dienst A zo ook gevoeligheden doorgeeft om het overlopen realistisch te doen lijken. Eenmaal binnen kan de officier na vele jaren informatie beginnen doorlekken van dienst B naar dienst A. Er zit dus een mol binnen de inlichtingendienst zelf.

Er is wel een enorm belangrijk aandachtspunt bij zowel dubbel - als triple spionage. Namelijk het acteerwerk van de agent in kwestie. Er wordt immers verwacht dat de inlichtingenofficier drie verschillende identiteiten 'speelt' met ieder een eigen karakter. Iets wat niet voor iedereen is weggelegd en zeker niet wanneer je dekmantel (of leven) op het spel staat. Hetzelfde geldt voor een overloper die berouw heeft gekregen van zijn eerste dubbelspionage spel. Wie is nog in staat dergelijk narcistisch en ontrouw individu om te gaan. Er is dan ook nog de vrees dat dergelijk individu een quadrupel agent kan worden. Hij is niets meer aan het doen dan '*cherry picking'*. Een triple agent is al zeldzaam laat staan een quadrupel agent maar het kan altijd. Naast dit type van agenten bestaat er ook nog volgende soort agent;[187]

- Agent-provocateur: Een agent-provocateur is zeer doeltreffend om zaken van inmenging op te sporen. Wanneer iemand met een politiek mandaat contacten heeft met een beïnvloedingsagent of buitenlandse inlichtingendienst, kan een agent provocateur hierop inspelen. Hij doet zich voor alsof hij voor deze agent of dienst werkt en dat hij in contact moest treden met de politicus. Door zich zo voor te stellen is hij in staat compromitterende handelingen of gesprekken toonbaar te maken die worden opgenomen. Daarrna wordt het bewijsmateriaal gebruikt om de politicus uit zijn mandaat te zetten. Het gebruik van dergelijke agenten vindt zijn weerslag vooral in het uitlokken van compromitterend gedrag door anderen. Dit wordt niet gedaan in België maar wel in andere landen. Zo kan een pro-democratische betoging in een dictatoriaal land geïnfiltreerd worden door agenten-provocateurs die de menigte geleidelijk opjutten tot bepaalde acties. Acties die de orde verstoren en de betogers in een slecht daglicht stellen. Dit komt dan (inter)nationaal in de media. Alle acties tegen de betoging zullen dan genieten van het goedkeuren van de eigen burgers en landen.

[187] PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, p.201-202

Naast al deze vormen van desinformatie is het ook gewoon mogelijk om, na voldoende bewijslast, een vijandige agent aan te houden. De inlichtingendienst zal dan zelf moeten beslissen of dit wel wijs is.

Tenslotte is de kans groot dat het thuisland van de spion om zijn uitlevering vraagt en de volgende dag zelf al een andere agent stuurt om de opdracht van de spion te voltooien. Door de agent te observeren en te frustreren kan men soms meer bereiken.
Zo komen zijn opdrachten en interesses in bepaalde informatie aan het licht en kan de CI dienst ervoor zorgen dat die informatie juist beter bewaakt wordt of overgeplaatst. Het frustreren van agenten doet ook hun eigen hoofdkwartier en dienst frustreren wegens het verlies van zowel kostbare tijd als financiële middelen.

Daarom is de belangrijkste methode van CI het penetreren van de inlichtingendienst van de tegenstander. Pas dan kan een vijandige inlichtingendienst bedwongen worden door zijn plannen steeds op voorhand te weten. Bij penetratie van de top van de inlichtingendienst van de tegenstander, is het mogelijk om erachter te komen of er in de eigen dienst mollen zitten.[188]
Om Bill Gertz, van" The Washington Times" te citeren; *"Counterintelligence is part art, part science, a discipline aimed at identifying and exploiting or stopping foreign spies. Law enforcement is easier: You identify the bad guys and arrest them."*

6. TOEPASSING DOOR DE BELGISCHE INLICHTINGENDIENSTEN

De vraag die nu nog moet beantwoord worden is hoe de Belgische inlichtingendiensten aan CI doen. Dit is een vraag die moeilijk te beantwoorden valt. De inlichtingendiensten zelf laten hier weinig over los alsook de wetgeving die een ruime interpretatieruimte geeft. [189] Als er gekeken wordt naar de defensieve zijde is het duidelijk dat de Belgische inlichtingen - en veiligheidsdiensten dit type van CI in grote mate beheersen. De offensieve kant is eerder giswerk. Geen enkele inlichtingen - en veiligheidsdienst zal maar al te graag informatie meedelen aan een buitenstaander. Het gevaar bestaat dat er dergelijke tactieken kunnen gelekt worden. Het staat alleszins vast dat ADIV aan offensieve detectie en neutralisatie doet op vlak van cyberaanvallen. Wat wel is geweten, is dat de CI in België voornamelijk reactief optreedt, en dit vaak na een melding van een buitenlandse bevriende inlichtingendienst.

[188] REAGAN, M.L., *Intro to U.S. Counterintelligence. CI 101 : A Primer.,* Amerika, HSDL, 2005, p.35
[189] Interview met afdelingscommissaris X, Hoofd Analyse Counter Intelligence

Er wordt te weinig proactief aan CI gedaan. Het gebrek is niet te wijten een demotivatie maar aan een tekort aan middelen en manschappen.[190] Een probleem dat vaak ook aangekaart wordt door de officieren van de gerechtelijke politie, die met identiek hetzelfde probleem kampen.

Naast een risico inschatting van mogelijke cyberdreigingen en het defensief optreden zal de dienst ook offensief kunnen optreden. ADIV kan cyberbaanvallen die gericht zijn tegen nationaal grondgebied afslaan. Deze dienst is ook bevoegd voor het neutraliseren van vijandige systemen in het buitenland in geval van een cyberaanval op de informatiesystemen van Defensie, in overeenstemming met de bepalingen van het recht bij gewapende conflicten. Hieruit volgt dat de dienst de daders van de aanval mag opsporen en identificeren, onverminderd het recht om onmiddellijk met een eigen cyberaanval te reageren. Echter laat de Belgische wetgeving dergelijke neutralisatiepraktijken niet toe als de buitenlandse aanval plaatsvindt op andere federale overheidsdiensten of nationale kritieke infrastructuur. Dan mag er slechts achteraf defensief op worden gereageerd, zonder neutralisatie van het vijandige systeem.[191]

Meer beschikbare kennis over de toepassing van specifieke CI tactieken door Belgische inlichtingen - en veiligheidsdiensten bestaat vrijwel niet. Het is echter gissen en trachten vergelijkingen te trekken met naburige (Europese) landen. Daarom is de counterintelligence in dit hoofdstuk zeer ruim en internationaal bekeken. Vele structurele waarden en methoden zullen zonder twijfel gehanteerd worden door de VSSE en ADIV. Voor andere tactieken en methoden geldt het volgende; ofwel mogen ze niet gebruikt worden door het legaliteitsbeginsel ofwel hoeven ze niet gebruikt te worden door het opportuniteitsbeginsel, ofwel kunnen ze niet gebruikt worden door gebrek aan financiële ondersteuning, wat vooral eigen is aan België.

7. BESLUIT

Het laatste gedeelte omvat counterintelligence in de standaardvorm. De counterintelligence dienst van ieder land bestaat normaal uit de elite van de inlichtingendiensten zelf. Ze zijn niet alleen in staat om aan contraspionage en contra inmenging te doen maar het ook op te sporen.

[190] Interview met afdelingscommissaris X, Hoofd Analyse Counter Intelligence
[191] FRANCEUS, F., "Cyberaanvallen en het recht van de gewapende conflicten : bemerkingen bij een juridische primeur in België en de Verenigde Staten" in *Cahiers Inlichtingenstudies-n°2*, COOLS, M., DEBRUYNE, E, FRANCEUS, F., LEROY, P., LIBERT, R., PASHLEY, V., RAPAILLE, G., SEGERS, A., STANS, D., TESTELMANS, D., WINANTS, A., (eds.), Antwerpen, Maklu, 2012, 105-138

Er wordt stilgestaan op de defensieve zijde die eerder preventief optreedt. Door gebruik te maken van risicomanagement is het mogelijk een dreiging in te schatten evenals het risico dat een dreiging inhoudt. Hierdoor is het mogelijk meer gericht bepaalde dreigingen aan te pakken waarvan het risico grotere schade tot gevolg heeft dan andere dreigingen van een kleinere aard.

Afschrikking en detectie zijn de twee belangrijkste onderdelen van defensieve CI. Investeren in een efficiënte en wel uitgebouwde beveiliging loont uiteindelijk op vlak van spionagebestrijding. Fysieke beveiliging van gebouwen schrikt potentiële indringers af. Diegenen die toch proberen binnen te dringen moeten eerst een aantal obstakels overwinnen en kunnen steeds door menselijke en technische middelen gedetecteerd worden. Inlichtingendiensten hebben de kennis in pacht om goed te investeren in defensieve bescherming. Maar het is financieel soms moeilijk om de efficiëntie op peil te houden.

Als er verder gekeken wordt naar het offensieve gedeelte kan er gesteld worden dat dit de overgang is naar een steeds grijzere zone. Een zone die nog weinig mensen daadwerkelijk en volledig hebben betreden en onderzocht. Er is tenslotte niet zoveel waardevolle literatuur over te vinden, wat ook niet abnormaal is. Als een mogendheid kennis heeft van de feitelijke CI werking van een bepaald land, dan heeft ze ook de kennis van haar zwaktes. In deze thesis is geprobeerd een duidelijk beeld weer te geven van wat counterintelligence inhoudt en ook de CI van de Belgische inlichtingendiensten. Counterintelligence beschrijven is een heuse opdracht en zo goed als onmogelijk op nationaal vlak.

Is de opzet van dit onderzoek dan mislukt? Neen, want het moet gezien worden als een verkennend literatuuronderzoek naar een onderwerp dat in zijn pure gedetailleerde vorm vrijwel onbestaand is in de Belgische literatuur. Er bestaat genoeg internationale literatuur over de deelaspecten van CI maar nooit in zijn volledigheid of gedetailleerdheid zoals het in dit deel aan bod is gekomen. Daar ligt juist het belang van dit hoofdstuk. Het hoofdstuk zelf kan veel meer uitgebreid worden, bestudeerd en beschreven door criminologen die gespecialiseerd zijn op het gebied van inlichtingenstudies. Dit zou ook de aanpak en de efficiëntie van de huidige CI van ADIV en VSSE gedetailleerder kunne aantonen alsook de punten waar dringend nood is aan een beter uitgewerkt managementbeleid met de weinige middelen die soms voor handen zijn.

Counterintelligence is het nationale beveiligingsmiddel bij uitstek en niet alleen op het gebied van spionage en inmenging. Het omvat zo veel meer zoals terrorisme, georganiseerde misdaad en andere zware en complexe misdrijven. Het grote verschil zit hem in de directe of indirecte schade. Terrorisme en georganiseerde misdaad zijn voorbeelden die vrijwel direct schade opleveren. Het plaatsen van explosieven of sabotage in nucleaire kerncentrales kan zware gevolgen hebben met veel gewonden als ze slagen in hun doel. Laat staan de massale angstpsychose die ontstaat bij de bevolking.

Georganiseerde misdaad brengt direct schade aan de economie van een staat en bedreigt de gevestigde orde. Daartegen is spionage en inmenging veel heimelijker en hoeft dus niet direct zijn weerslag te vinden. Beiden vormen zijn niet periodegebonden en kan jaren sluimeren vooraleer het feitelijk schade zal kunnen aanrichten op een moment dat de tegenstander zelf uitkiest. Spionage en inmenging mogen niet onderschat worden en moet dezelfde aandacht genieten als andere schadelijke activiteiten.

DEEL V. EINDCONCLUSIE

Met deze eindconclusie wordt dit interessant verkennend literatuuronderzoek langzaam afgesloten. Inlichtingenstudies zijn enorm interessant maar als onderzoek nooit volledig af. De hedendaagse evoluties en conflicten doen de activiteiten van spionage en inmenging heropleven evenals de inlichtingenwereld. De studie die hier gepresenteerd wordt is nog niet volledig af. Er zullen altijd nieuwe en onbekende pistes zijn die de nodige aandacht vereisen en steeds zullen bijdragen tot een uitbreiding van kennis. In deze conclusie zal getracht worden een antwoord te formuleren op de aanvankelijk gestelde onderzoeksvragen, evenals een bondig reflectie naar de huidige stand van zaken. De centrale onderzoeksvraag is onderverdeeld in vijf deelvragen. Deze vragen zullen aan de hand van de bevindingen die voortgekomen zijn uit deze thesis systematisch beantwoord worden om zo de centrale onderzoeksvraag te beantwoorden.

De centrale onderzoeksvraag had tot doel de reactie van de Belgische inlichtingendiensten - en veiligheidsdiensten te onderzoeken en dit op vlak van spionage alsook activiteiten van inmenging gepleegd door buitenlandse inlichtingendiensten. Vooraleer hier een duidelijk antwoord op te formuleren, is het van belang eerst de deelvragen te beantwoorden. Ze vormen immers de basis van de centrale onderzoeksvraag.

De eerste deelvraag luidde; *Wat houdt spionage en inmenging in en welke soorten vormen van spionage en inmenging bestaan er*? In de eerste twee delen van deze masterproef kwam spionage en inmenging volledig aan bod. Het eerste deel ging dieper in op de term inlichtingen als het ultieme doel van spionage. Er kan gesteld worden dat inlichtingen zeer waardevol kunnen zijn voor bepaalde personen of naties. Inlichtingen geven de sterktes evenals de zwaktes van een land weer. Dit door vertrouwelijke maar ruwe informatie in te winnen en deze te verwerken tot bruikbare inlichtingen. De sterktes handelen niet specifiek over de militaire mankracht maar wel over de technologische en economische ontwikkelingen van een land. Ontwikkelingen die andere landen ook kunnen gebruiken. Inlichtingen kunnen ook een politiek karakter hebben. Dit type van inlichtingen speelt een belangrijke rol in internationale handelsrelaties en verdragen. De vijanden van uw vijanden kunnen uw vriend worden en andersom.

Ook in conflictsituaties is het interessant om de politieke standpunten en agenda van omliggende landen te weten alsook die van de NATO of de UN. Door al deze kennis in pacht te hebben is het mogelijk om altijd twee stappen vooruit te lopen op anderen. Spionage komt in vele verschillende vormen met elk hun meerwaarde en manier van informatie inwinning. Wat vooral opvalt, is de enorme toename van mogelijkheden en toepassingen op gebied van CYBINT. Het speelveld van spionageactiviteiten is hierdoor niet verlegd maar eerder verbreed in zijn geheel.

Activiteiten van inmenging werden uitvoerig in het tweede gedeelde van deze thesis besproken. Inmenging is een containerbegrip door het veelzijdige karakter ervan. Inmenging heeft als doel de democratische rechtsorde te ondermijnen evenals de integriteit van een land aan te tasten. Het werd al snel duidelijk dat inmenging niet gemakkelijk te onderscheiden is van lobbyen waardoor bewijslast verzamelen zeer lastig wordt.

De volgende deelvraag luidde*; Welke buitenlandse inlichtingen - en veiligheidsdiensten vormen de grootste bedreiging in België en wat voor specifieke informatie zoeken zij?*
Het staat vast dat iedere buitenlandse inlichtingen - en veiligheidsdienst ongewenst is als deze doet aan spionage en activiteiten van inmenging op Belgisch grondgebied. Er is wel een belangrijk onderscheid tussen enerzijds de diensten die met toestemming en medeweten van de VSSE en ADIV actief zijn in België. Deze buitenlandse diensten zijn hier actief in het kader van een onderzoek, observatie of persoonsbescherming en vragen de medewerking van de Belgische inlichtingendiensten. Anderzijds zijn er de buitenlandse inlichtingendiensten wiens agenten 'illegaal' en zonder enige toestemming opereren binnen België. De agenten van deze diensten opereren al dan niet onder een dekmantel en trachten vertrouwelijke informatie in te winnen.

De drie grootste inlichtingendiensten die actief zijn op Belgische bodem zijn ook de diensten van drie grootmachten; Rusland, China en Amerika. Rusland en China tonen beiden enorme interesses in ontwikkelingen op gebied van militaire en industriële technologie. Rusland is meer bezig met het vergaren van internationale politieke agendapunten en vertrouwelijke dossiers. China is vooral geïnteresseerd in de economische handelsrelaties. Beide grootmachten en hun diensten zoeken specifieke informatie. Ze gaan met andere woorden voor kwaliteit. Amerika is een uitzondering doordat de CIA zoveel mogelijk kwaliteitsvolle informatie probeert te vergaren op verschillende domeinen.

Dit staat in schril contrast met de NSA die kwantiteit kiest boven kwaliteit en zo ruim mogelijk informatie tracht in te winnen. Hier komt de eerste deelvraag ook deels in terug. Iedere buitenlandse inlichtingendienst gebruikt een andere methode om informatie te vergaren. Daardoor is het belangrijk om op alle vlakken aan counterintelligence te doen om spionage en inmenging terug te dijken. Ook journalist Kristof Clerix evenals medewerkers van ADIV hebben me gewezen op de noodzaak van een goede counterintelligence. Het grote probleem zijn de financiële middelen, een verouderde structuur en managementaanpak alsook het ontbreken van een wettelijk kader bij sommige CI methoden.

De derde deelvraag ging over; de *VSSE, de ADIV en het wettelijk kader – Wie zijn ze? Wat zijn hun opdrachten en hun bevoegdheden?* Dit wordt volledig en gestructureerd uitgelegd in het derde gedeelde. Het is opvallend hoe groot en gediversifieerd hun takenpakket wel is. Als één van de oudste instellingen in dit land treedt de VSSE op als burgerlijke defensieve inlichtingen - en veiligheidsdienst. De ADIV treedt op de voorgrond als een militaire defensieve en offensieve inlichtingen - en veiligheidsdienst

Een vraag die hierop volgt luidt; *Hoe verloopt de samenwerking tussen ADIV, VSSE en het Federaal Parket?* De samenwerking tussen de ADIV en de VSSE zijn wettelijk bepaald en zullen daarom op weinig problemen stuiten. De samenwerking tussen de diensten met het federaal parket werd onderzocht aan de hand van interviews. Na het laatste interview met een magistrate van het federaal parket werd het duidelijk dat de huidige samenwerking veel vlotter verloopt dan voordien. De samenwerking is weliswaar bepaald door een koninklijk besluit, toch heeft het een lange tijd geduurd vooraleer ze spontaner werd.

De laatste twee deelvragen handelen beiden over het vierde deel in deze masterproef. In dit deel wordt het begrip counterintelligence in zijn geheel uiteengezet. Dit bood direct een antwoord op de vijfde vraag die als volgt luidde; *Wat is counterintelligence?* Het onderdeel CI is een speciale vorm van inlichtingenactiviteiten en onderscheidt zich ook van andere onderdelen op vlak van inlichtingen. Zijn hoofddoel is het ontdekken, observeren en identificeren van vijandige buitenlandse inlichtingendiensten op eigen grondgebied. Hiernaast moet CI de activiteiten van deze buitenlandse inlichtingendiensten desinformeren en neutraliseren. Naast dit offensieve doel moet ze ook defensief optreden. CI houdt de bescherming in van haar natie, haar onderdanen en haar WEP potentieel tegen infiltratie of inmenging. Dit door een reeks van methoden om de andere dienst af te schrikken of te detecteren.

De laatste deelvraag luidde; *En wat houdt de Belgische counterintelligence in?* De Belgische counterintelligence zal vele methoden en werkwijzen gebruiken die beschreven staan in deze masterproef. Er is heel weinig geweten over de Belgische CI behalve dat ze bestaat. De CI in deze thesis is gebaseerd op internationale werken handelend over het onderwerp. In het vierde deel wordt er zo gedetailleerd mogelijk getracht om een duidelijk beeld te krijgen van de Belgische CI. Wanneer de CI van België zou uitlekken zou deze informatie gretig en met dank gebruikt worden door andere inlichtingendiensten. Zo weten ze waar de beveiliging niet optimaal is en wat de zwakke punten zijn van de VSSE en ADIV. Zodoende is het gemakkelijker voor buitenlandse inlichtingendiensten om hun agenten een bepaalde richting uit te sturen of te waarschuwen op welke wijze de VSSE en de ADIV hun tegenstanders trachten te vangen. Of waar beide diensten geen voldoende financiële middelen of technologie voor hebben om hun taken naar behoren te kunnen uitvoeren.

De verouderde apparatuur en het gebrek van politieke aandacht gekoppeld met een constante steun aan financiële middelen maken het werk van de Belgische inlichtingendiensten er niet gemakkelijker op. Iets wat spijtig genoeg de huidige realiteit is bij een groot aantal federale diensten. Er is weinig besef van hoe belangrijk CI is in een land zoals België, waar de hoofdstad ook de hoofdstad is van Europa.

Om te eindigen is het nu mogelijk om de centrale onderzoeksvraag volledig te beantwoorden aan de hand van de kennis die is voortgekomen uit deze masterproef. Immers, zowel de antwoorden op de deelvragen, als de literatuurstudie, beschrijven de mogelijkheden waarop de Belgische inlichtingen - en veiligheidsdiensten kunnen reageren op vlak van spionage en activiteiten van inmenging gepleegd door buitenlandse inlichtingendiensten. Doordat de Belgische inlichtingen- en veiligheidsdiensten aan counterintelligence doen, zijn ze in staat gepast te reageren op mogelijke spionnen en (beïnvloedings)agenten. CI geeft de VSSE en ADIV een ruime waaier aan defensieve en offensieve methoden die, met de juiste financiële ondersteuning en een uitgebreid wettelijk draagvlak, iedere aanval kunnen afweren en opsporen die gericht is op Belgisch grondgebied. Om met de woorden van onderzoeker Kenneth A. Krantz te eindigen; "*de grootste vijand van succesvolle counterintelligence is niet een tegenstander zijn spion, maar de verkeerde perceptie hebben van counterintelligence"*

BIBLIOGRAFIE

RECHTSBRONNEN:

Internationaal Verdrag inzake Burgerlijke en Politieke Rechten van 1966

Organieke wet van 30 november 1998, houdende de regeling van de inlichtingen- en veiligheidsdiensten, Belgisch Staatsblad, 18 december 1998

KB van 19 november 1998 betreffende de verloven en afwezigheden toegestaan aan de personeelsleden van de Rijksbesturen en Omzendbrief nr. 476 van 28 mei 1999 van de minister van Ambtenarenzaken

KB van 13 december 2006 houdende het statuut van de ambtenaren van de buitendiensten van de Veiligheid van de Staat en de dienstnota's van 20 februari 2007 en 7 december 2007 van de VSSE

Parl. St.: Senaat, nr. 5-8727, 16 april 2013

Parl. St., Senaat , nr. 5-1226, 8 februari 2011

Parl. St., Senaat , nr. 4-5618, 7december 2009

BOEKEN :

ALLSOP, W., *Unauthorised access. Physical penetration testing for IT security teams, United Kingdom*, WILEY, 2009, 287 p.

ANDREW, C. & MITROHHIN, V., *The sword and the shield. The Mitrokhin archive and the secret history of the KGB*, New York, Basic Books, 1999, 700 p.

BAGLEY, T., H., *Spy wars. Moles, mysteries, and deadly games,* Londen, Yale University Press, 2007, 313 p.

BAMFORD, J., *Body of secrets. Anatomy of the ultra secret national security agency*, New Yokrk, Anchor Books, 2002, 654p.

BEAVER, K., Hacking for dummies, Hoboken, Wiley Publishing, 2010, 386p.

BIDGOLI, H., *Handbook of Information Security. Key Concepts, Infrastructure, Standards, and Protocols*, Hoboken, John Wiley & Sons, 2006, 1092p.

BLOCH, J., & TODD, P., *Global Intelligence: The World's Secret Services Today,* ,Londen, Zed Books, 2003, 240p.

BURTON, B., *Top secret : A Clandestine Operator's Glossary of Terms*, Boulder, Paladin Press, 1986, 127p.

CARPENTIER, C., en MOSER, F., *De staatsveiligheid, geschiedenis van een destabilisatie*, Leuven, Kritak, 1994, 293p.

CARR, J., *Inside Cyber Warfare: Mapping the Cyber Underworld*, Sebastopol, O'Reilly Media, 2012, 294p.

CLERIX, K., S*pionage. Doelwit Brussel*, Antwerpen, Manteau, 2013, 262 p.

CLERIX, K., Vrij spel. Buitenlandse geheime diensten in België, Antwerpen, Manteau, 207p.

CLERIX, K.,*Spionage in het hart van Europa*, België, Wereldmediahuis, 2006, 21 p.

COLE, E., RING, S., *Insider threat. Protecting the enterprise from sabotage, spying, and theft*., Rockland, Syngress ,Publishing, 2006, 397 p.

COMITE I, *Vast Comité van toezichtop de inlichtingen – en veiligheidsdiensten : Rapport van het onderzoek naar de manier waarop de Belgische Inlichtingendiensten (VSSE en ADIV) hebben gehandeld in een zaak van telefoontaps in kantoren van delegaties van de raad van de Europese Unie in Brussel*, België, 2006, 24 p.

COMITE I, *Advies van het vast Comité I bij het 'voorontwerp van wet betreffende methodes voor de verzameling van gegevens door de inlichten en veiligheidsdiensten*, België, 2006,. 27p.

COOLS, M., & HOOGENBOOM, B., *Kwetsbare kennis. Over bedrijfseconomische spionage en informatiebeveiliging*, Alphen aan den Rijn-Diegem, Samsom BedrijfsInformatie, 1996, 139 p.

COOLS, M., DE RUYVER, B., PONSAERS, P., COMITE I, V., VAN LAETHEM, W., RAPAILLE, G., FRANSEN, A., VANDOREN, A., WILLS, A., WINANTS, A., COMUT, B., FIJNAUT, C., STANS, D., FRANCEUS, F., VADILLO, F., VANDEWALLE, G., BOS, H., VANHEVELE, H., CAMERON, I., LEIGH, I., REGIBAU, J.A., DELEPIERE, J.C., DEIBERT, R., MANCHADA, A., ROHOZINSKI, R., VILLENEUVE, N., WALTON, G., GOWAN, J., BRUCE, B. en TAY, J., Tracking GhostNet : Investigating a cyber espionage network*, Information warfare monitor,* 2009*,* 53p.

DAVIES, B., The spycraft manual. The insider's guide to espionage techniques., Londen, Carlton Book, 2005, 191 p.

DECORTE, T. (2011). *Methoden van onderzoek: ontwerp en dataverzameling*. *Een handleiding*. Gent, Academia Press, 2013, 265p.

DECORTE, T., ZAITCH, D. (eds.), *Kwalitatieve methoden en technieken in de criminologie*, Leuven-Den Haag, Acco, 2010, 574p.

DE CLERCK, S., en HUYGH, J., 'Een kleine geschiedenis van de wetgeving op de inlichtingendiensten' in *De Staatsveiligheid: Essays over 175 jaar Veiligheid van de Staat*, COOLS, M., DASSEN, K., LIBERT, R., en PONSAERS, P., (eds.), Brussel, Politeia, 2005, 383p.

DELMULLE, J., VANDERBORGHT, J., CLERIX, K., MARSIA, L. & ROYEN, M.C., (eds.), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten* , INSERTIA, ANTWERPEN, 2013, 596 p.

DEPARTMENT OF DEFENSE PERSONNEL, *Unit 3. Intelligence Productions*, in *Operations Intelligence Journeyman (1N051A)*, Goodfellow, 2004, 30p

DE LEEUW, K. & BERGSTRA, J., *The history of information security. A comprehensive handbook,* Amsterdam, Elsevier, 2007, 887 p

DE VALK, G., *Dutch Intelligence: Towards a quantitative framework for analysis*, Den Haag,Boom Juridische Uitgevers, 2005, 416p.

DE VOS, L., *Strategie & tactiek. Inleiding tot de moderne krijgsgeschiedenis*, Leuven, Davidsfonds NV, 2006, 276 p.

FEDERAL BUREAU OF INVESTIGATION, *Soviet Active Measures in the United States: 1986–1987,* Washington, FBI, 1987, 87p.

FRANCEUS, F., "Cyberaanvallen en het recht van de gewapende conflicten : bemerkingen bijeen juridische primeur in België en de Verenigde Staten" in *Cahiers Inlichtingenstudies-n°2*, COOLS, M., DEBRUYNE, E, FRANCEUS, F., LEROY, P., LIBERT, R., PASHLEY, V., RAPAILLE, G., SEGERS, A., STANS, D., TESTELMANS, D., WINANTS, A., (eds.), Antwerpen, Maklu, 2012, 105-138

FINK, S., Sticky fingers. M*anaging the global risk of economic espionage*., Unites States of America, Auerbach, 2003, 326 p.

FRANCQ, A., 'The Use of Counterintelligence, Security and Countermeasures' in *Managing Frontiers in Competitive Intelligence*, FLEISHER, C. & BLENKHORN, D. Westport, Greenwood, 2001,328 p

GANSER, D., *NATO's secret armies. Operation GLADIO and terrorism in Western Europe*., Oxon, Frank Cass, 2005, 302 p.

GOETHALS, J., en PAUWELS, L., Onderzoeksvragen. In: GOETHALS J., PAUWELS, L. (Eds.), *Kwantitatieve en kwalitatieve criminologische onderzoeksmethodes: een introductie,* Leuven, Acco, 2008, 205p.

GREGORY, P., *Enterprise information security. Information security for non-technical decision makers*. Groot Brittanië, Pearson Eduction Limited, 2003, 145p

GODDEERIS, I., *Spioneren voor het communisme. Belgische prominenten en Poolse geheim agenten,* LannooCampus, Tielt, 2013, 304 p.

GOULDEN, J.C., T*he dictionary of espionage. Spyspeak into English*, New York, Dover Publications, 2012, 256 p.

GRAGIDO, W. & PIRC, J., *Cyber-crime and Espionage. An Analysis of Subversive Multivector Threats*, Burlington, Elsevier, 2011, 247 p.

GRIFFITH, S.B., *Sun Tzu. De Kunst van het oorlogsvoeren,* Kerkdriel, Librero, 2010, 272 p.

HANNAS, W.C., MULVENON, J., & PUGLISI, A.B., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* ,Abingdon , Routledge, 2013, 320p.

HASTEDT, G.P., *Espionage. A reference handbook.*, Californië, ABC CLIO, 2003, 225 p.

HAYNES, J.E., KLEHR, H., *Early Cold War spies. The Espionage trials that shaped American politics*., Cambridge, Cambridge University Press, 2006, 251 p.

HEADQUARTERS : DEPARTEMENT OF THE ARMY, FM2-22.3 (34-52) *HUMAN INTELLIGENCE COLLECTOR OPERATIONS, Field manual, Washington DC*, 2006, 384 p.

HEADQUARTERS : DEPARTEMENT OF THE ARMY, FM34-60 *Counterintelligence, Field manual, Washington DC*, 1995, 241 p.

HITZ, F.P., *Why spy? Espionage in an Age of Uncertainty*, New York, Thomas Dunne Books, 2008, 212 p.

HOEKSTRA, F., *In dienst van de B.V.D.; Spionage en contraspionage in Nederland,* Boom, Nederland, 2004, 223 p.

HUBAND, M., *Trading secrets. Spies and Intelligence in an Age of Terror*, New York, I.B. Tauris, 2013, 259 p.

JANSSENS, P., *Spionage per computer. Hackers voor Moskou over inbraak en infiltratie in onze militaire en industriële databanken en geheime computersystemen*, Amsterdam, Balans, 1989, 175 p.

JOHNSON, L.K. (ed.), *Handbook of intelligence studies*, London, Routledge, 2009, 382p.

JOHNSON, W.R., T*hwarting Enemies at Home and Abroad. How to Be a Counterintelligence Office*, Whasington, Georgetown University Press, 2009, 222p.

KAHANA, E., SUWAED, M., *Historical dictionary of Middle Eastern Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, X, United Kingdom, Scarecrow Press, 358 p.

KALUGIN, O., Spy*master. My thirty-two years in intelligence and espionage against the West*., Philadelphia, Basic books, 2003, 466 p.

KIPLING, K., *Kim*, Hertfordshire, Wordsworth classics, 1993, 251p.

LAUREYS, E., *Het Bevrijde België (1944–1945). Feiten, opinies en voorstellingen*. Brussel, Soma, 1998, 81 p.

LERNER, L. en LERNER, B., *Encyclopedia of Espionage, Intelligence & Security,* II, Detroit, Gale, 2004, 463p.

LERNER, L. en LERNER, B., *Encyclopedia of Espionage, Intelligence & Security,* III, Detroit, Gale, 2004, 432p.

MACRAKIS, K., *Seduced by secrets .Inside the Stasi's spy-tech world*., Cambridge, Cambridge University Press, 2008, 370 p.

MARK, E. & MATHER, T., *The executive guide to information security. Threats, challenges and solutions*., Indianapolis, Symantec-press, 2004, 260 p

MARSHALL, C., en ROSSMAN, G.B., *Designing qualitative research, Thousand Oaks,* Sage, 1999, 219p.

MEIJER, F., *Het Romeinse leger. Handboek voor de generaal door Vegetius*, Amsterdam, Polak & Van Gennep, 2002, p. 175p.

MELE, S., *Cyberwarfare and its damaging effects on citizens*, Milan, 2010, p.10-14

MELTON,. .K.H., *Ultimate spy. Inside the secret world of espionage*, New York, DK Publishing, 2009, 224p.

MELTHON, K.H. & WALLACE, R., *The Official CIA Manual of Trickery and Deception*, New York, Hardie Grant Books, 2009, 268p.

MINISTERIE VAN DEFENSIE, *Jaarverslag : Militaire Inlichtingen – en Veiligheidsdienst*, Nederland, Bestuurstaf/Militaire Inlichtingen en Veiligheidsdienst Defensie, 2012, 64 p.

MITROKIN, V., (ed.) KGB Lexicon: The Soviet Intelligence Officer's Handbook, Groot Brittanie, Frank Cass & co, 2002, 90p.
SERVICE, R., *Comrades!: a history of world communism,* Cambridge, Harvard University Press 2007, 592p.

MORAVEJ, K. & DIAZ, G," Critical Issues in Contemporary Counter-Intelligence" in *UNISCI Discussion Papers,* UNISCI (eds.), Madrid, 2007, 53-70

NASHERI, H., *Economic espionage and industrial spying*, Cambridge, Cambridge university press, 2005, 270p.

OPENBAAR MINISTERIE, Jaarverslag federaal parket 2012, Brussel, 2012, 289p.

PELTIER, R.T., PELTIER, J. en BLACKLEY, J., *Information security fundamentals*, Boca Raton, Auerbach Publications, 2005, 280p.

PERMAN, S., *Spies, Inc. Bussiness Innovation from Israel's Master of Espionage*, Upper Sadle River, Pearson Education, 2005, 241p.

PRUNCKUN, H., *Counterintelligence. Theory and practice,* Maryland, Rowman & Littlefield Publishers, 2012, 229 p.

ROBERTS, P., *Cuban missiles crisis. The essential reference guide*. California, ABC-Clio, 2012, p.278

ROMERSTEIN, H., *Soviet Active Measures and Propaganda: "New Thinking" & Influence Activities in the Gorbachev Era* , Toronto, Mackenzie Institute for the Study of Terrorism, Revolution,and Propaganda, 1989, 54p.

RUSSEL, R.L., *Sharpening Strategic Intelligence. Why the CIA gets it wrong, and what needs to be done to get it right*, Cambridge, Cambrigde University Press, 2007, 214 p.

SHAKARIAN, P., SHAKARIAN, J. & RUEF, A., *Introduction to cyber-warfare. A Multidisciplinary approach*, Waltham, Elseviers, 2013, 336p.

SCHOEN, F., en LAMB, C.J., *Deception, disinformation, and strategic communications. How one interagency group made a major difference,* Washington, National Defense University Press, 2012,155p.

SHULSKY, A. & SCHMITT, G., *Silent Warfare. Understanding the world of intelligence*., Virginia, Potomac Books, 2002, 262p.

SMITH JR, W.T., Enc*yclopedia of the Central Intelligence Agency*, New York, Facts On File, 2003, 282p.

SHULTZ, R.H. en GODSON, R., *Dezinformatsia: Active Measures in Soviet Strategy,* New York, Pergamon Brassey's, 1984, 210p.

STEVENS, D., 'De Algemene Dienst Inlichtingen en Veiligheid van de Krijgsmacht: actuele analyse' in *Geheime diensten in Benelux,Israël, en de Verenigde Staten*, MATTHIJS, H., (ed.), Brugge, die Keure, 2005, 27-47

SUIB, S., *Inside Russia's SVR. The Foreign Intelligence Service* , The Rosen Publishing Group, New York, 2003, 65p.

TILLER, J.S., *The ethical hack. A framework for business value penetration testing, Boca Raton,* Auerbach, 2005, 352 p.

TURNER, M.A., *Historical dictionary of United States Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, II, United Kingdom, Scarecrow Press, 2009, 291 p.

UNITED STATES MARINE CORPS COMMAND STAFF COLLEGE, *Projecting Organic Intelligence, Surveillance, and Reconnaissance: A critical requirement of the Stryker Brigade Combat Team,* Quantico, 2003, 46p.

VANDERHALLEN, M., VERVAKE, G., OPDEBEECK, A., GOETHALS, J. (2002). Het ontwerp van een gevalsstudie. In: *Criminologie in actie*. Brussel: Politeia, 419-444.

VAST COMITE VAN TOEZICHT OP DE INLICHTINGENDIENSTEN, *Codex inlichtingendiensten: werking,bevoegdheden en controle*, Brugge, Die Keure,1996

VAN DAELE, D. & VANGEEBERGEN, B., "De BIM-wet in vogelvlucht" in VAN DAELE, D., VANGEEBERGEN, B., & VAN LAETHEM, W. (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, p. 29-64

VAN DAELE, D., & VANGEEBERGEN, B.n "De verhouding tussen de inlichtingen- en veiligheidsdiensten en de gerechtelijke overheden" in VAN DAELE, D., VANGEEBERGEN, B., en VAN LAETHEM, W. (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, p. 207-233

VAN DAELE. D. & VANGEEBERGEN, B., *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* Intersentia, Antwerpen, 2006, 166 p.

VAN OUTRIVE, L., CARTUYVELS, Y., en PONSAERS, P., *Sire, ik ben ongerust. Geschiedenis van de Belgische politie 1794-1991*, Leuven, Kritak, 1992, 367p.

VOLKMAN, E., Spies. *The Secret agents who changed the course of history*, Amerika, Wiley 1996, 288p.

VON CLAUSEWITZ, C., *Vom Krieg*, Berlijn, Ferdinand Dümmler, 1832, 608p.

VSSE, *Jaarverslag 2011*, Brussel, Federale Overheidsdienst Justitie, 2011, 116 p.

WALLACE, R., MELTON, H.K. & SCHLESINGER, H.R., *Spycraft. The secret history of the CIA's spytech from communism to Al-Qaeda*, New York, Dutton, 2008, 548 p.

WEST, N., *Historical dictionary of international Intelligence in Historical Dictionaries of Intelligence and CounterIntelligence*, IV, United Kingdom, Scarecrow Press, 2009, 330 p.

WINANTS, A., *Veiligheid van de Staat. Jaarverslag 2010*, Brussel, Winants A., 2010, 110 p.

WYLDER, J., Strategic information security, Washington, Auerbach, 2003, 240 p.

X, *Brochure : De Veiligheid van de Staat*, Uitgeverij Politeia, Brussel, 2010, p.35

X., *B-GL-352-001/FP-001 : Intelligence, surveillance, target acquisition and reconnaissance (ISTAR)*, Canada, Land force Canada, 2004, 99p.

ARTIKELEN :

BENNET, G., The SVR. Russia's Intelligence Service in *Conflict Studio's Research Center*, Royal Military Academy Sandhurst, Camberley, 2000, 26p.

BAETS, P., De geheime deur op een kier : inlichtingendiensten: een noodzakelijk kwaad? , *Orde van de dag*. *Criminaliteit en samenleving*., Kluwer, 2008, 68

CAROLL, T.P., Syllabus section 1. *Human intelligence: From sleepers to walk-ins*, 2006, 1-29

DE JONG, B. & KELLER, P., Contra-inlichtingen en contraspionage, *Inlichtingen - en veiligheidsdiensten*, Alphen aan de Rijn, Kluwer, 2010, 275-294

EHRMAN, J.," Toward a Theory of CI**:** What are We Talking About When We Talk about Counterintelligence?", in *Studies in Intelligence,* Washington, Government printing office, 5-23

FAST, B., JOHNSON, M., SCHAEFFER, D., Cyber Intelligence : Setting the landscape for an emerging discipline. *Intelligence and national security alliance*, 2011, 1-20

GODLEWSKI, R.J, *"*Human Intelligence: Perceiving an Enemy's Thoughts*"* in *American Intelligence Journal,* COL.SPRACHER, W.C., 2009, p.29.

HAQUIN, R. & MATHIL, P., Colonel espion arrêté, Le Soir, 6 maart 1988, p.1 & 6

HURLEY, M.M., For and from Cyberspace. Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance., *Air & Space Power Journal (ASPJ*), 2012, 12-33

Interview met de directeur van de Dienst Buitenlandse veiligheid van Rusland 'Vyacheslav Trubnikov' door Andrey Poleshchuk verschenen in NEZAVISIMAYA GAZETA (1996/12/18), p. 1- 2

KERR, I., Digital Locks and the Automation of Virtue. in *Radical Extremism" to "Balanced Copyright": Canadian Copyright and the Digital Agenda,* GHEIST, M., (eds.), Ottowa, University of Ottawa, 2010, 247-303

MELE, S., '*Cyber weapons : legal and strategic aspects'*, Edizioni Machiavelli, 2013, 8-15

NICOLS, A., *A Perspective on Threats in the Risk Analysis Process,* SANS Institute, SANS Institute Reading Room, 2002, 8p.

PAGANINI, P., 'Cyber weapon', *The Hacker News*, 2012, 3-8

REAGAN, M.L., *Intro to U.S. Counterintelligence. CI 101 : A Primer.,* Amerika, HSDL, 2005, 41p.

VANGEEBERGEN, B., VANDERBORGHT, J,. EASTON, M. & GUNST, J.C., 'Een publiek debat over geheime methoden', *Orde van de dag. Criminaliteit en samenleving.*, Kluwer, 2011, 124

VAN DAELE, D. & VAN GEEBERGEN, B., 'Geheime (?) diensten. Over de noodzaak van een ernstig debat over de bijzondere inlichtingenmethoden en de rol van de inlichtingen- en veiligheidsdiensten in de opsporing" in *Orde van de dag* 2008, afl. 42, 33.

VAN DAMME, G., Cour militaire., Le Soir, 10 juni 1989 , p.7

WALSH, J.I., Intelligence-Sharing in the European Union: Institutions Are Not Enough, *Journal of Common Market Studies*, Oxford, BlackWell Publishing, 625-643

ZEGART, A.B, "Spytainment": The Real Influence of Fake Spies, *International Journal of Intelligence and CounterIntelligence*, California, Taylor & Francis Group, 2010, 599-622

X, ISO 31000 : Risk management. Risk assessment techniques., Genève, ISO, 92p

WEBSITES

AMKREUTZ, R., (12//04/18) Als studenten maar geen spionnen zijn [WWW]. De Morgen : http://www.demorgen.be/dm/nl/1344/Onderwijs/article/detail/1425069/2012/04/18/Als-studenten-maar-geen-spionnen-zijn.dhtml [03/07/2014]

BOVE, L., (2010/08/10) *De staatsveiligheid op de rooster* [WWW.] De Tijd :http://blogs.tijd.be/zaakjustitie/2010/08/de-staatsveiligheid-op-de-rooster.html [21/04/2014]

CIA (z.d.), The Intelligence Cycle, [WWW] Office of Public Affairs Central Intelligence Agency: https://www.cia.gov/kids-page/6-12th-grade/who-we-are-what-we-do/the-intelligence-cycle.html [25/12/2013]

CLERIX, K., (2014/03/14) Militaire Inlichtingendienst treedi uit de schaduw [WWW]. MO : http://www.mo.be/interview/militaire-inlichtingendienst-treedt-uit-de-schaduw [23/06/2014]

CLERIX, K., (2012/11/05) Belgische diplomaat verdacht van spionage [WWW]. MO: http://www.mo.be/artikel/belgische-diplomaat-verdacht-van-spionage [01/08/2014]

MTM (2013/10/29), Rusland probeerde Herman Van Rompuy te bespioneren met USB-stick, [WWW] DeStandaard: http://www.standaard.be/cnt/dmf20131029_00815482 [02/11/2013]

NSA (2004/05/17), NSA scientific advisory board. Panel on digital network intelligence (DNI), [WWW] The national security archive: http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa22.pdf [02/11/2013]

REED, J., (2011/01/03) Cyber Intelligence, [WWW]. DefenseTech : http://defensetech.org/2011/01/03/cyber-intelligence/ [05/02/2014]

X, (2014/05/16)Russisch Spionagevirus op computers overheid [WWW]. Gelderlander: http://www.gelderlander.nl/algemeen/buitenland/russisch-spionagevirus-op-computers-overheid-belgi%C3%AB-1.4362573 [28/05/2014]

X, *(2009/01/01)* Службы внешней разведки Российской Федерации [WWW] СВР: http://svr.gov.ru/ [03/07/2014]

X, (2011/08/21), De KGB in België (5): De rode kolonel[WWW.] Apache : /http://www.apache.be/2011/08/21/de-kgb-in-belgie-5-de-rode-kolonel/ [18/03/2014]

X, (2011) Federal agency of governmental communication and information by RF President (FAPSI) [WWW]. Agentura : http://www.agentura.ru/english/dosie/fapsi/ [28/05/2014]

X, (z.d.)Snowden en België [WWW]. Datapanik : http://www.datapanik.org/dossiers/snowden-files/snowden-en-belgie/[03/07/2014]

X, (2010/11/01) Economic and Social Research Council. [WWW]. CBPR Ethics Guide: Framework for Research Ethics 2010 Updated September 2012, http://www.esrc.ac.uk/_images/Framework-for-Research-Ethics_tcm8-4586.pdf.[05/11/2013]

X, (2012/08/29) Kaspersky looks at the wreckage of Wiper malware, [WWW]. Inforsecurity :http://www.infosecurity-magazine.com/view/27869/kaspersky-looks-at-the-wreckage-of-wiper-malware[06/02/2014]

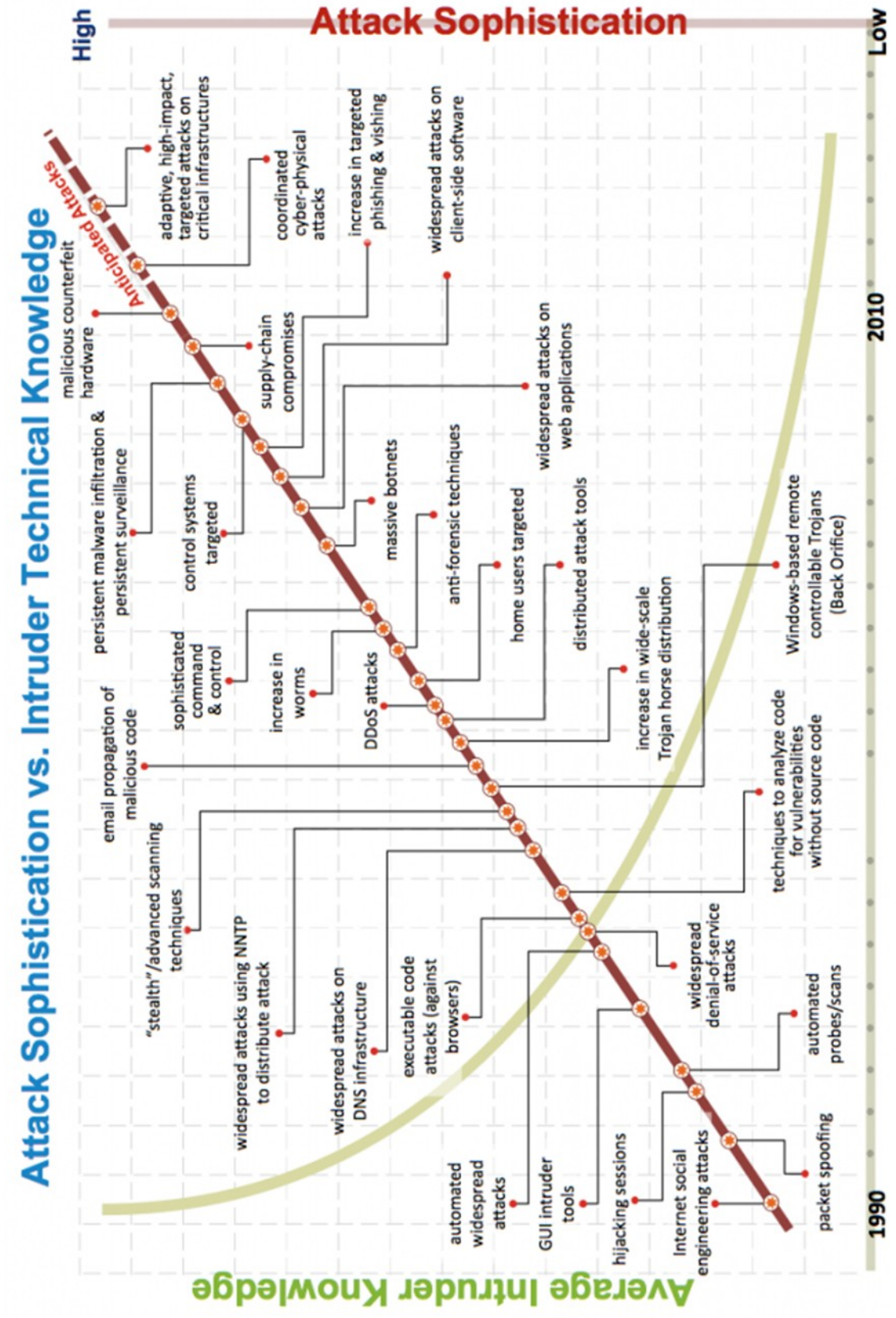
X, (2011/08/21), De KGB in België (5): De rode kolonel[WWW.] Apache :/http://www.apache.be/2011/08/21/de-kgb-in-belgie-5-de-rode-kolonel/ [18/03/2014]

X,(z.d.), Assessment spionage-weerbaarheid. Hoe weerbaar bent u tegen spionage?, [WWW]. Fox-It: https://www.fox-it.com/nl/wp-content/uploads/2012/02/Assessment-Spionageweerbaarheid-v3.pdf [02/11/2013]

X,(2013/07/05) SigInt: Types of electronic eavesdropping devices, [WWW]. StratRisks : http://stratrisks.com/geostrat/13756 [05/11/2013]

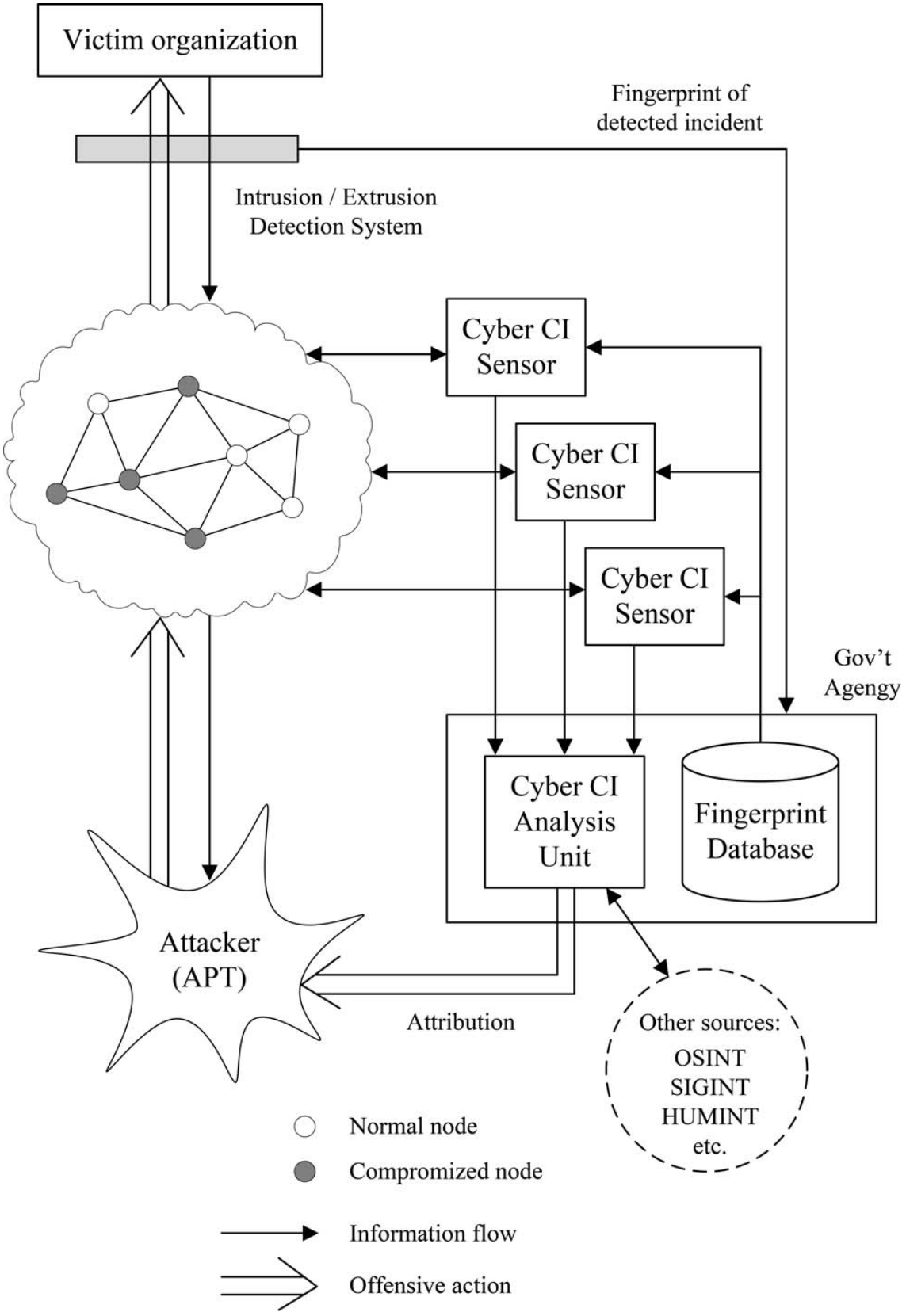
BIJLAGE 1

De evolutie van CYBINT aanvalstechnieken en ontwikkelingen



BIJLAGE 2

Een lay-out van het offensief CCI attributie proces



BIJLAGE 3

Enkele pagina's uit de gelekte NSA catalogus waarin gesofisticeerd spionage materiaal staat beschreven.

TOP SECRET//COMINT//REL TO USA, FVEY

CTX4000

ANT Product Data

(TS//SI//REL TO USA,FVEY) The CTX4000 is a portable continuous wave (CW) radar unit. It can be used to illuminate a target system to recover different off net information. Primary uses include VAGRANT and DROPMIRE collection.

8 Jul 2008

(TS//SI//REL TO USA,FVEY) The CTX4000 provides the means to collect signals that otherwise would not be collectable, or would be extremely difficult to collect and process. It provides the following features:

- Frequency Range: 1 - 2 GHz.
- Bandwidth: Up to 45 MHz
- Output Power: User adjustable up to 2 W using the internal amplifier; external amplifiers make it possible to go up to 1 kW.
- Phase adjustment with front panel knob
- User-selectable high- and low-pass filters.
- Remote controllable
- Outputs:
- Transmit antenna
- I & Q video outputs
- DC bias for an external pre-amp on the Receive input connector
- Inputs:
    - External oscillator
    - Receive antenna

Unit Cost: N/A

Status: unit is operational. However, it is reaching the end of its service life. It is scheduled to be replaced by PHOTOANGLO starting in September 2008.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOP SECRET//COMINT//REL TO USA, FVEY

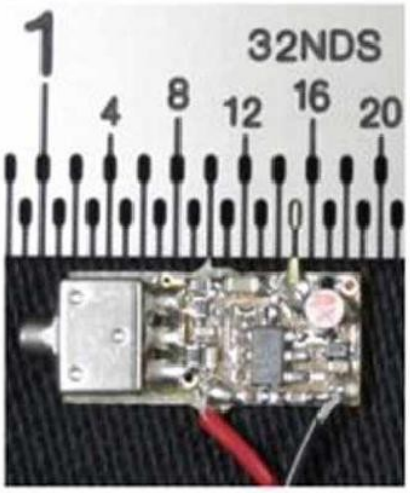
LOUDAUTO

ANT Product Data

07 Apr 2009

(TS//SI//REL TO USA,FVEY) Audio-based RF retro-reflector. Provides room audio from targeted space using radar and basic post-processing.

(U) Capabilities



(TS//SI//REL TO USA,FVEY) LOUDAUTO's current design maximizes the gain of the microphone. This makes it extremely useful for picking up room audio. It can pick up speech at a standard, office volume from over 20' away. (NOTE: Concealments may reduce this distance.) It uses very little power (~15 uA at 3.0 VDC), so little, in fact, that battery self-discharge is more of an issue for serviceable lifetime than the power draw from this unit. The simplicity of the design allows the form factor to be tailored for specific operational requirements. All components at COTS and so are non-attributable to NSA.

(U) Concept of Operation

TS//SI//REL TO USA,FVEY) Room audio is picked up by the microphone and converted into an analog electrical signal. This signal is used to pulse position modulate (PPM) a square wave signal running at a pre-set frequency. This square wave is used to turn a FET (field effect transistor) on and off. When the unit is illuminated with a CW signal from a nearby radar unit, the illuminating signal is amplitude-modulated with the PPM square wave. This signal is re-radiated, where it is picked up by the radar, then processed to recover the room audio. Processing is currently performed by COTS equipment with FM demodulation capability (Rohde & Schwarz FSH-series portable spectrum analyzers, etc.) LOUDAUTO is part of the ANGRYNEIGHBOR family of radar retro-reflectors.

Unit Cost: $30

Status: End processing still in development

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

NIGHTSTAND

Wireless Exploitation / Injection Tool

(TS//SI//REL) An active 802.11 wireless exploitation and injection tool for payload/exploit delivery into otherwise denied target space. NIGHTSTAND is typically used in operations where wired access to the target is not possible.

07/25/08

(TS//SI//REL) **NIGHTSTAND** - Close Access Operations • Battlefield Tested • Windows Exploitation • Standalone System

System Details

- (U//FOUO) Standalone tool currently running on an x86 laptop loaded with Linux Fedora Core 3.
- (TS//SI//REL) Exploitable Targets include Win2k, WinXP, WinXPSP1, WINXPSP2 running internet Explorer versions 5.0-6.0.
- (TS//SI//REL) NS packet injection can target one client or multiple targets on a wireless network.
- (TS//SI//REL) Attack is undetectable by the user.

NIGHTSTAND Hardware

(TS//SI//REL) Use of external amplifiers and antennas in both experimental and operational scenarios have resulted in successful NIGHTSTAND attacks from as far away as eight miles under ideal environmental conditions.

Unit Cost: Varies from platform to platform

Status: Product has been deployed in the field. Upgrades to the system continue to be developed.

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

NIGHTWATCH

ANT Product Data

(TS//SI//REL TO USA,FVEY) NIGHTWATCH is a portable computer with specialized, internal hardware designed to process progressive-scan (non-interlaced) VAGRANT signals.

24 Jul 2008

(U) Capability Summary

(TS//SI//REL TO USA,FVEY) The current implementation of NIGHTWATCH consists of a general-purpose PC inside of a shielded case. The PC has PCI digitizing and clock cards to provide the needed interface and accurate clocking required for video reconstruction. It also has:

- horizontal sync, vertical sync and video outputs to drive an external, multi-sync monitor.
- video input
- spectral analysis up to 150 kHz to provide for indications of horizontal and vertical sync frequencies
- frame capture and forwarding
- PCMCIA cards for program and data storage
- horizontal sync locking to keep the display set on the NIGHTWATCH display.
- frame averaging up to 2^16 (65536) frames.

(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The video output from an appropriate collection system, such as a CTX4000, PHOTOANGLO, or general-purpose receiver, is connected to the video input on the NIGHTWATCH system. The user, using the appropriate tools either within NIGHTWATCH or externally, determines the horizontal and vertical sync frequencies of the targeted monitor. Once the user matches the proper frequencies, he activates "Sync Lock" and frame averaging to reduce noise and improve readability of the targeted monitor. If warranted, the user then forwards the displayed frames over a network to NSAW, where analysts can look at them for intelligence purposes.

Unit Cost: N/A

Status: This system has reached the end of its service life. All work concerning the NIGHTWATCH system is strictly for maintenance purposes. This system is slated to be replaced by the VIEWPLATE system.

POC: [redacted] S32243, [redacted] [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

PICASSO

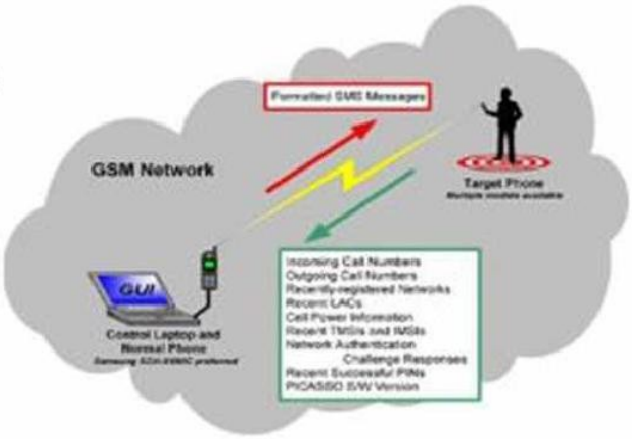
GSM HANDSET

(S//SI//REL) Modified GSM (target) handset that collects user data, location information and room audio. Command and data exfil is done from a laptop and regular phone via SMS – (Short Messaging Service), without alerting the target.

06/20/08

(S//SI) Target Data via SMS:

- Incoming call numbers
- Outgoing call numbers
- Recently registered networks
- Recent Location Area Codes (LAC)
- Cell power and Timing Advance information (GEO)
- Recently Assigned TMSI, IMSI
- Recent network authentication challenge responses
- Recent successful PINs entered into the phone during the power-on cycle
- SW version of PICASSO implant
- ' Hot-mic' to collect Room Audio
- Panic Button sequence (sends location information to an LP Operator)
- Send Targeting Information (i.e. current IMSI and phone number when it is turned on - in case the SIM has just been switched).
- Block call to deny target service.



(S//SI) PICASSO Operational Concept

(S//SI//REL) Uses include asset validation and tracking and target templating. Phone can be hot mic'd and has a "Panic Button" key sequence for the witting user.

Status: 2 weeks ARO (10 or less)

Unit Cost: approx $2000

(S//SI//REL) Handset Options

- Eastcom 760c+
- Samsung E600, X450
- Samsung C140
- (with Arabic keypad/language option)

POC: [redacted] S32242, [redacted] [redacted]@nsa.ic.gov

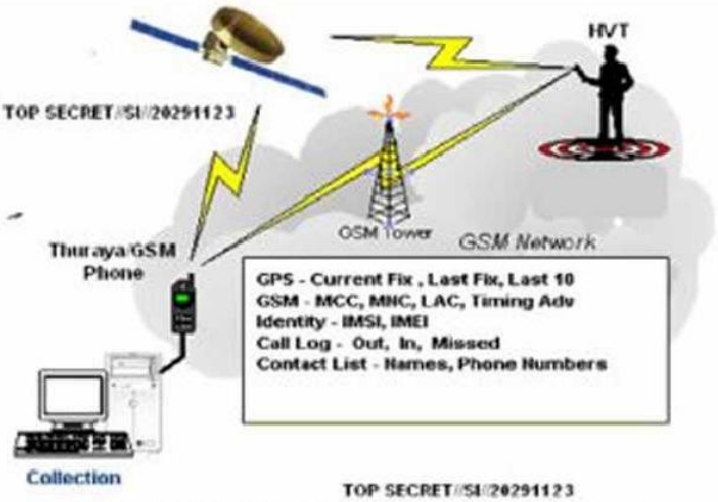
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOTECHASER

ANT Product Data

10/01/08

(TS//SI//REL) TOTECHASER is a Windows CE implant targeting the Thuraya 2520 handset. The Thuraya 2520 is a dual mode phone that can operate either in SAT or GSM modes. The phone also supports a GPRS data connection for Web browsing, e-mail, and MMS messages. The initial software implant capabilities include providing GPS and GSM geo-location information. Call log, contact list, and other user information can also be retrieved from the phone. Additional capabilities are being investigated.



(U//FOUO) TOTECHASER – Operational Schematic

(TS//SI//REL) TOTECHASER will use SMS messaging for the command, control, and data exfiltration path. The initial capability will use covert SMS messages to communicate with the handset. These covert messages can be transmitted in either Thuraya Satellite mode or GSM mode and will not alert the user of this activity. An alternate command and control channel using the GPRS data connection based on the TOTEGHOSTLY implant is intended for a future version.

(TS//SI//REL) Prior to deployment, the TOTECHASER handsets must be modified. Details of how the phone is modified are being developed. A remotely deployable TOTECHASER implant is being investigated. The TOTECHASER system consists of the modified target handsets and a collection system.

(TS//SI//REL) TOTECHASER will accept configuration parameters to determine how the implant operates. Configuration parameters will determine what information is recorded, when to collect that information, and when the information is exfiltrated. The configuration parameters can be set upon initial deployment and updated remotely.

Unit Cost: $

Status:

POC: U//FOUO [redacted], S32222, [redacted]@nsa.gov

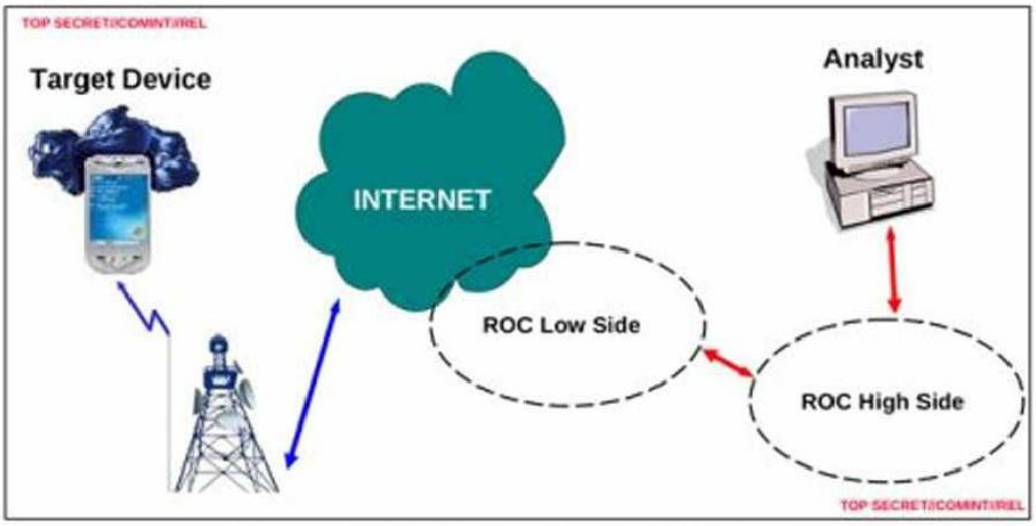
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

TOTEGHOSTLY 2.0

ANT Product Data

(TS//SI//REL) TOTEGHOSTLY 2.0 is a STRAITBIZARRE based implant for the Windows Mobile embedded operating system and uses the CHIMNEYPOOL framework. TOTEGHOSTLY 2.0 is compliant with the FREEFLOW project, therefore it is supported in the TURBULENCE architecture.

10/01/08



(U//FOUO) TOTEGHOSTLY – Data Flow Schematic

(TS//SI//REL) TOTEGHOSTLY 2.0 is a software implant for the Windows Mobile operating system that utilizes modular mission applications to provide specific SIGINT functionality. This functionality includes the ability to remotely push/pull files from the device, SMS retrieval, contact list retrieval, voicemail, geolocation, hot mic, camera capture, cell tower location, etc. Command, control, and data exfiltration can occur over SMS messaging or a GPRS data connection. A FRIEZERAMP interface using HTTPSlink2 transport module handles encrypted communications.

(TS//SI//REL) The initial release of TOTEGHOSTLY 2.0 will focus on installing the implant via close access methods. A remote installation capability will be pursued for a future release.

(TS//SI//REL) TOTEGHOSTLY 2.0 will be controlled using an interface tasked through the NCC (Network Control Center) utilizing the XML based tasking and data forward scheme under the TURBULENCE architecture following the TAO GENIE Initiative.

Unit Cost: $0

Status: (U) In development

POC: U//FOUO [redacted], S32222, [redacted] [redacted]@nsa.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

GENESIS

Covert SIGINT Transceiver

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

01/27/09

(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

➢ **(S//SI//REL) Features:**

- Concealed SDR with Handset Menu Interface
- Spectrum Analyzer Capability
- Find/Fix/Finish Capability
- Integrated Ethernet
- External Antenna Port
- Internal 16 GB of storage
- Multiple Integrated Antennas

➢ **(S//SI//REL) Future Enhancements:**

- 3G Handset Host Platform
- Additional Host Platforms
- Increased Memory Capacity
- Additional Find/Fix/Finish Capabilities
- Active Interrogation Capabilities

Status: Current GENESIS platform available. Future platforms available when developments are completed.

Unit Cost: $15K

POC: [redacted], S32242, [redacted] [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108