2. De voor- en nadelen van *Signals intelligence*

Over *Signals intelligence* tijdens de Koude Oorlog en na de val van de muur is weinig bekend.[12] *Signals intelligence* is namelijk nogal technisch van aard, en daardoor is vaak moeilijk uit te leggen wat het belang ervan is. Mede hierdoor hebben wetenschappers en journalisten het onderwerp veelal gemeden.

De schaarse aandacht die er wel voor was had meestal betrekking op de Tweede Wereldoorlog.[13] Toch was *Signals intelligence* door de specifieke informatie die dit opleverde de belangrijkste bron van *intelligence* bij militaire conflicten tijdens en na de Koude Oorlog. Sinds mensenheugenis hebben regeringen immers altijd willen weten wat hun vijanden, maar ook hun vrienden in hun schild voerden. De gemakkelijkste manier daarvoor is om gewoon naar hun communicatieverkeer te luisteren. Het voormalige hoofd van de *US Navy Communications Intelligence Organization* schreef bijvoorbeeld: 'The ambition of every nation has been to develop unbreakable ciphers for its own use and to solve every cipher in use by its actual or potential enemies.'[14]

Voordelen van Signals Intelligence

Door het specifieke karakter van de verkregen informatie heeft *Signals intelligence* een aantal eigen kwaliteiten, waardoor dit een zeer effectieve methode is om *intelligence* te vergaren. In oktober 1998 beschreef John Millis, wijlen *staff director* van het *House Permanent Select Committee on Intelligence*, dat *Signals intelligence* 'has been and continues to be the intelligence of choice of the policy maker and the military commander'. Hij voegde hieraan toe: 'the fact of the matter is, it's there quickly when needed. It's always there. Or it has always been there.'[15] Hierna komen een negental voordelen aan de orde.

Een eerste voordeel van deze vorm van *intelligence* is dat het hier een passieve methode betreft, in het algemeen uitgevoerd zonder dat het doelwit daar weet van heeft. Verder kan *Signals intelligence* gebruikt worden tegen een doel dat soms honderden of zelfs duizenden kilometers ver ligt; het is vaak niet nodig om onderscheppingenapparatuur dichtbij het doel te hebben. *Signals intelligence* kent daarom weinig politieke of fysieke risico's; een uitzondering hierop vormde de vergaring van deze informatie vanuit vliegtuigen langs de kust van verschillende staten.

In de tweede plaats is *Signals intelligence* objectief; de betrouwbaarheid ervan is groot, en dat kan soms een perfect *intelligence*-product opleveren. Het zal, in tegenstelling tot inlichtingen vergaard door menselijke bronnen, *Human intelligence*, altijd vrij zijn van politieke vooringenomenheid en zal niet worden beïnvloed door de politieke perceptie van de bronnen van de agent. *Human intelligence* kan soms politiek gekleurd zijn, omdat deze wordt aangeleverd door verraders, of vanwege chantage, corruptie, politiek of financieel gewin. Maar *Signals intelligence* levert in ruwe vorm precies wat er geregistreerd wordt in een onverbloemde, niet-gekleurde en onverdraaide gedaante. *Signals intelligence* verwierf hierdoor een belangrijke status bij de afnemers van *intelligence*. Zo stelde een voormalige CIA-agent: 'You know the origin and you know that this is genuine. It's not like a clandestine [*Human intelligence*] report where you don't know if this is a good agent or a weak agent or a bad agent or a double agent.' Een andere CIA-medewerker noemde hierbij meteen ook de schaduwzijde: 'Electronic intercepts are great, but you don't know if you've got two idiots talking on the phone.'[16]

Een derde voordeel is dat sommige – zeker niet alle – *intercepts* een zelfstandig *intelligence*-product kunnen zijn, zonder dat het nodig is om de informatie te verifiëren via andere bronnen. De voormalige directeur van de CIA, Stansfield Turner, schreef in 1991:

> Electronic intercepts may be even more useful [than agents] in discerning intentions. For instance, if a foreign official writes about plans in a message and the United States intercepts it, or if he discusses it and we record it with a listening device, those verbatim intercepts are likely to be more reliable than second-hand reports from an agent.[17]

Een *intercept* kan dus unieke *intelligence* opleveren. Daarom krijgt de Amerikaanse president elke morgen, naast een *Top Secret intelligence summary*, een zogeheten *Black Book* met daarin de belangrijkste *intercepts* van de afgelopen 24 uur. In Den Haag wordt onder de hoogste ambtelijke beleidsmakers een soortgelijke op Nederland gerichte publicatie verspreid, de zogeheten 'Groene Editie'.[18]

In de vierde plaats is *Signals intelligence* voor de *intelligence*-afnemer meestal de snelst beschikbare vorm van *intelligence*. Vooral de *National Security Agency* kan dankzij zijn wereldwijde afluisternetwerk *Signals intelligence* sneller aanleveren dan iedere andere vorm van *intelligence*. Tijdens de Cuba-crisis in 1962 duurde het bijvoorbeeld gemiddeld meer dan een week voordat een *Human intelligence*-rapport de CIA bereikte. *Intercepts* daar-

entegen waren voor de beleidsmakers direct beschikbaar. Hierdoor ging *Signals intelligence* (en *Imagery Intelligence*, beelden vanuit de lucht) een steeds belangrijkere rol vervullen bij waarschuwingen voor een vijandelijke aanval.

In de vijfde plaats levert *Signals intelligence* veel meer *intelligence* op over een breed scala van onderwerpen dan iedere andere vorm van *intelligence*. Aan het eind van de jaren zestig van de vorige eeuw produceerde de *National Security Agency* al meer dan 400.000 *intelligence*-rapporten per jaar, dus meer dan duizend rapporten per dag.[19]

In de zesde plaats: *Signals intelligence* 'slaapt nooit'. Agenten en hun bronnen moeten immers van tijd tot tijd rusten en *Imagery intelligence* is soms niet inzendbaar vanwege duisternis, zandstormen of meteorologische omstandigheden. *Signals intelligence* kan echter dag en nacht worden ingezet: 24 uur per dag en 365 dagen per jaar.

In de zevende plaats is *Signals intelligence* flexibeler en meer gericht op de afnemer dan de meeste andere vormen van *intelligence*. Daarom stelde een rapport van het Amerikaanse Congres uit 1998: 'much of the National Security Agency's past strength has come from its localised creativity and quick-reaction capability'.[20] Vooral de grotere *Signals intelligence* organisaties zijn in staat om snel nieuwe doelen af te luisteren. Inlichtingendiensten kunnen nu eenmaal niet binnen 24 uur een heel nieuw netwerk van agenten en spionnen opbouwen. Ook *Imagery intelligence* is niet flexibel genoeg, want er zijn enorme kosten aan verbonden om een spionagesatelliet in een nieuwe baan te brengen.

Ten achtste is het potentieel van *Signals intelligence* veel groter dan iedere andere vorm van *intelligence*. Een succesvolle doorbraak bij het breken van een buitenlandse code kan waardevollere informatie opleveren dan alle andere *intelligence*-bronnen bij elkaar. Het kraken van een code is soms het 'equivalent not of one but of a thousand spies, all ideally placed, all secure, and all reporting instantaneously'.[21] Zelfs de meest fervente voorstander van *Human intelligence*, de legendarische CIA-directeur van 1953 tot 1961 Allen W. Dulles, moest toegeven dat *Signals intelligence* 'the best and "hottest" intelligence' opleverde 'that one government can gather about another'.[22]

Ten slotte zou *Signals intelligence* de effectiefste manier zijn (vergeleken met andere methoden) om *intelligence* te verzamelen: het biedt, ondanks de hoge kosten, over het algemeen 'meer waar voor zijn geld'.[23] *Signals intelligence* is inderdaad prijzig. Tijdens de Koude Oorlog besteedde de Amerikaanse overheid vier tot vijf keer zoveel geld aan *Signals intelligence* als aan *Human intelligence*. Sinds 1945 heeft de *National Security Agency* er waarschijnlijk meer dan $ 100 miljard aan uitgegeven, waarvan 75 procent aan *Signals*

intelligence, en het overige aan de beveiliging van verbindingen (*Communications Security*).[24]

Signals intelligence was en is kortom waarschijnlijk een van de meest productieve technieken om *intelligence* te vergaren.

Sinds de val van de Muur is het relatieve belang van *Signals intelligence* alleen maar toegenomen. Dit geldt niet alleen voor de Verenigde Staten, maar ook voor hun Europese bondgenoten. Die werden waarschijnlijk door het ontbreken van goede capaciteiten voor *Imagery intelligence* (beelden vanuit de lucht) zelfs nog afhankelijker van *Signals intelligence*.

Een voorbeeld hiervan zijn de banden tussen de Verenigde Staten en het Verenigd Koninkrijk: al gedurende de jaren tachtig was het grootste deel (tachtig à negentig procent) van de ruwe *intelligence* die elke dag naar het Britse *Joint Intelligence Committee* toevloeide afkomstig uit *Signals intelligence*, en in mei 1999 verklaarde de Britse minister van Buitenlandse Zaken, Robin Cook, over de Britse afluisterdienst dat 'the Government Communications Headquarters work is vital in supporting our foreign and defence policies'.[25] Ook het jaarverslag over 2000 van de *Intelligence and Security Committee* van het Britse Parlement gaf het belang van *Signals intelligence* aan: 'The quality of the [Government Communications Headquarters-]intelligence gathered clearly reflects the value of the close co-ordination under the UK-USA agreement.'[26] Hiermee werd verwezen naar een verdrag dat in juni 1948 werd ondertekend door Londen en Washington, genaamd het *UK-USA Communications Intelligence Agreement*. Dit legde de verdeling vast van de *Communications intelligence*-inspanning die toen gericht was tegen Moskou en zijn bondgenoten. Later gingen ook Canada, Australië en Nieuw-Zeeland van deze UK-USA-overeenkomst deel uitmaken.[27]

Ook voor andere landen was *Signals Intelligence* van groot belang, zoals voor Canada, een belangrijke troepenleverend land van UNPROFOR. De nationale *Signals intelligence*-organisatie, de *Communications Security Establishment*, was de belangrijkste leverancier van *intelligence* in de Canadese hoofdstad Ottawa.[28] En ook in Nederland speelden verbindingsinlichtingen in het verleden een belangrijke rol, zoals tijdens de oliecrisis. Ook in latere jaren heeft de, thans genoemde *Afdeling Verbindingsinlichtingen* (AVI) van de MID belangrijke *intelligence* aangeleverd.[29]

Nadelen van Signals Intelligence

Tegenover de voordelen van *Signals intelligence* staat ook een aantal nadelen. Die zwakke kanten en beperkingen zijn overigens soms ook van toepassing op andere *intelligence*-disciplines.

Allereerst gaan *intercepts* altijd gepaard met de grootste geheimhouding. De distributie van het *Signals intelligence*-product is daarom altijd zeer beperkt. Slechts een zeer kleine kring van de allerhoogste politieke en militaire beleidsmakers heeft toegang tot ruwe *Signals intelligence*. Deze geheimhouding is ook belangrijk in de context van de *intelligence-sharing* tussen de Verenigde Staten en hun westerse bondgenoten: vaak wordt *Signals intelligence* wel verwerkt in *intelligence*-rapportages, maar de ruwe *Signals intelligence* is aan weinigen voorbehouden, en dan meestal nog alleen op een '*need to know*'-basis. De belangrijkste reden daarvoor is dat uitgelekte *Signals intelligence* grote schade kan veroorzaken. Als degene die afgeluisterd is, de 'target' in *intelligence*-jargon, dat ontdekt, kan deze namelijk snel codes of sleutels veranderen, waardoor de inspanning die geleverd is in de voorafgaande periode om die code of sleutel te breken in één klap waardeloos wordt.

Het nadeel van deze extreme geheimhouding is dat *Signals intelligence* vaak de juiste personen op de lagere niveaus niet bereikt. Soms bereikt *Signals intelligence* de commandanten op de grond niet, omdat besloten werd dat deze een *need-to-know*-classificatie had, waardoor het *intelligence*-product geen verdere verspreiding kreeg. Dit was bijvoorbeeld het geval tijdens de oorlog in Korea: de *Communications intelligence* bereikte niet alleen de Amerikaanse troepen op de grond niet, maar evenmin de Amerikaanse marine en luchtmacht. Hierdoor bleef zeer waardevolle tactische en strategische *intelligence* ongebruikt.

De Amerikanen leerden niet veel van de Korea-oorlog, want tijdens de Vietnam-oorlog gebeurde nagenoeg hetzelfde. Belangrijke *Signals intelligence* over locaties van Noord-Vietnamese afweersystemen en MIG-gevechtsvliegtuigen, bleef bij de *National Security Agency* 'hangen', en bereikte de Amerikaanse luchtmacht en marine nooit. De gevolgen daarvan waren verstrekkend: er werden meer Amerikaanse vliegtuigen neergeschoten en er kwamen meer piloten om dan nodig was.

In het midden van de jaren tachtig, onder de regering-Reagan, weigerde de *National Security Agency* aanvankelijk zelfs om *intercepts* over steun uit Cuba en Nicaragua aan het gewapende verzet in El Salvador door te geven aan de CIA.

Ook in andere landen dan de Verenigde Staten gelden dergelijke beperkingen: in Moskou gaven KGB en de militaire inlichtingendienst GRU hun *Signals intelligence* slechts door aan een kleine groep binnen het Politbureau. Het delen van deze inlichtingen met leden van het Warschaupact was zelfs officieel verboden. En ook in Europese landen, als het Verenigd Koninkrijk, Duitsland, Frankrijk en Nederland, is de toegang tot *Signals intelligence* beperkt tot een selecte groep van beleidsmakers en militairen.[30]

Naast de extreme geheimhouding en daardoor beperkte distributie is een tweede nadeel van *Signals intelligence* de rem op het gebruik ervan. Gedurende de jaren vijftig en zestig had elk Amerikaans Communications *intelligence*-rapport de volgende vaste beginregel: '*No action is to be taken on information herein reported, regardless of temporary advantage, if such action might have the effect of revealing the existence and nature of the source.*' Waarschijnlijk wordt die beginregel nog steeds genoemd.

Deze beperking heeft tot zeer bizarre situaties geleid. Zo onderschepte de Australische *Signals intelligence*-organisatie (*Defence Signals Directorate*) in oktober 1995 Indonesische militaire berichten, waaruit bleek dat er plannen waren om vijf gearresteerde Australische journalisten op Oost-Timor te executeren. De dienst besloot om deze inlichtingen niet door te geven aan de Australische premier Gough Whitlam, omdat men vreesde dat deze vervolgens zou handelen op basis van deze onderschepte berichten, of zelfs zou openbaren. Dit zou de capaciteit van de *Defence Signals Directorate* om het Indonesische militaire verkeer mee te lezen, kunnen verraden, zo was de redenering. Vervolgens werden alle vijf journalisten vermoord door Indonesische *Special Forces*.[31]

Een derde nadeel is dat *Signals intelligence* vaak niet op waarde wordt geschat of zelfs soms niet wordt geloofd. *Signals intelligence* als bron werd bijvoorbeeld tijdens de Koude Oorlog niet betrouwbaar genoeg geacht. Ook al tijdens de oorlog in Korea hechtte de top van de Amerikaanse krijgsmacht geen waarde aan *Communications intelligence* over de werkelijke sterkte van Mao's Rode Leger. En tijdens de oorlog in Indochina weigerden Franse commandanten aandacht te schenken aan *intercepts* van vijandelijk verkeer, omdat deze niet pasten in hun eigen analyse van de militaire situatie.[32]

Een volgend nadeel bestaat er omgekeerd juist uit dat veel landen tijdens de Koude Oorlog te afhankelijk waren van *Signals intelligence*. In 1978 was de Amerikaanse *intelligence*-gemeenschap daarvan zo afhankelijk geworden dat president Carter een duidelijke waarschuwing afgaf: 'Recently (...) I have been concerned that the trend that was established about 15 years ago to get intelligence from electronic means might have been overemphasized.'[33] Ook de militaire leiding van de Sovjet-Unie bleek volstrekt van *Signals intelligence* afhankelijk te zijn geworden waar het ging om een tijdige waarschuwing voor een nucleaire of conventionele aanval. Dat had zeer onaangename gevolgen, zoals bleek in de herfst van 1983. Er dreigde toen een serieuze nucleaire crisis, als gevolg van misverstanden: Sovjet- en Warschaupact-grondstations interpreteerden een NAVO-oefening volstrekt foutief, op grond van *Signals intelligence*: ze dachten dat er een verrassingsaanval met Pershing-raketten ging komen.[34] En in mei 1998 leidde een verkeerde interpretatie van *intercepts* bij de *Signals intelligence*-organisatie van het leger van India bijna tot een nucleaire confrontatie tussen India en Pakistan.[35]

Hiermee hangt het vijfde nadeel samen: blind vertrouwen in verbindingsinlichtingen kan leiden tot een soort *Signals intelligence snobbery*. Zo werd tijdens de Koude Oorlog en daarna het belang dat men aan *Signals intelligence* hechtte steeds groter. Vooral de introductie van spionagesatellieten en het spionagevliegtuig U-2 leidde tot een verwaarlozing van *Human intelligence*. Er ontstond een soort *intelligence*-elitisme, ook wel bekend als het 'Groene-Deur-syndroom': het idee dat alleen *Signals intelligence* (en in zekere mate ook *Imagery intelligence*) nog betrouwbaar zou zijn. *Human intelligence* werd dan veelal afgedaan als onbetrouwbaar. De zogeheten *BrixMis*-spionagemissies in de DDR hadden hieronder te lijden; hun missierapporten weken namelijk soms af van de *Signals intelligence*-rapportage over hetzelfde onderwerp. Dan werd meestal de *Signals intelligence* geloofd,

omdat rapportages van het *Government Communications Headquarters* nu eenmaal veel hoger geclassificeerd waren ('Secret' of 'Top Secret'), terwijl dezelfde *intelligence* in het *BrixMis*-rapport slechts 'UK Confidential' als classificatie meekreeg.[36]

In een te groot vertrouwen in *Signals intelligence* schuilt nog een extra risico, dat als het zesde nadeel geldt: dit *intelligence*-product moet namelijk vaak bekeken worden in samenhang met *Human intelligence* en *Imagery intelligence*. Op *Signals intelligence* als exclusief *intelligence*-product valt slechts in speciale gevallen te bouwen: *Signals intelligence* geeft veelal alleen een stukje van de puzzel, en zelden de gehele puzzel. Veel verbindingsinlichtingen zijn namelijk fragmentarisch en indirect. Dat betekent ook dat op *intelligence* van de *National Security Agency* niet valt te bouwen, omdat deze alleen ruwe verbindingsinlichtingen produceert en geen *finished intelligence*. De verantwoordelijkheid om tot een afgerond *intelligence*-product te komen, ligt bij de afnemers (de consumenten) van het ruwe materiaal van de *National Security Agency*. Analisten binnen die Amerikaanse *intelligence*-gemeenschap moeten dan ook vaak honderden of zelfs duizenden verbindingsinlichtingen analyseren, wil het 'plaatje' duidelijk worden. Een medewerker van een Amerikaanse inlichtingendienst verklaarde in dit verband: 'You rarely get a Signals intelligence smoking gun. It's usually very fragmentary (...) Very often you don't even know who you're listening to.'[37] Dat is een bevestiging dat ook *Signals intelligence* niet alle antwoorden geeft; toepassing daarvan is zeker niet voldoende om de politieke voornemens of de interne politieke machinaties binnen een buitenlandse overheidsadministratie bloot te leggen. Overigens zijn ook *Imagery intelligence* en *Human intelligence* daar zelden toe in staat.

Een zevende nadeel bestaat erin dat *Signals intelligence* weliswaar snel is, maar desondanks soms toch te laat arriveert. Tijdens de Suez-crisis in 1956 en de invasie van Tsjechoslowakije in 1968 was er bijvoorbeeld voldoende *Signals intelligence* beschikbaar, maar de verwerking, analyse en rapportage bleek te tijdrovend. Pas dagen na beide invasies was de *Signals intelligence* beschikbaar.

Dit hangt weer samen met het achtste nadeel, dat waarschijnlijk het belangrijkste is: de stroom informatie is enorm, maar de analysecapaciteit is onvoldoende. Krachtige computers kunnen een snelle voorselectie uitvoeren en het kaf van het koren scheiden, maar de analist moet uiteindelijk toch bepalen of een bericht waardevol is. *Signals intelligence*-organisaties worden tijdens een crisis overspoeld met massa's *intercepts*. CIA-analisten waren niet in staat om de oorlog in het Midden-Oosten in 1973 te voorspellen, omdat er honderden *Communications intelligence*-rapporten van de *National Security Agency* op hun bureau landden: daardoor werd het overzicht verloren.

De directeur van *National Security Agency* in 1995, admiraal McConnell, verklaarde bijvoorbeeld dat de 'National Security Agency's capability to intercept far exceeds its capability to decode, analyze and report. The goods news is the agency can decode and analyze a million messages a day; the bad news is the agency must decide which million, of the billions of messages sent globally, to decode.'[38] Omstreeks 1995 verwerkte de *National Security Agency* inderdaad slechts ongeveer één procent van alle *intercepts* die het hoofkwartier in Fort Meade bereikten; in de jaren tachtig was dat nog twintig procent. Tekenend voor de verhouding tussen binnenkomende *intercepts* en uitgaande *intelligence* bij de *National*

Security Agency is daarbij dat de huidige directeur van de *National Security Agency*, generaal Hayden, moest toegeven dat de *National Security Agency* inmiddels wel *minder* produceerde aan *intelligence* dan tien jaar geleden. Bij de *intelligence*-productie van de *National Security Agency* hielp ook niet – zoals een interne studie in het voorjaar van 1995 onthulde – dat er voortdurend bureaucratische gevechten binnen de *National Security Agency* plaatsvonden, tussen de militaire en de civiele delen van de Divisie Operaties van deze organisatie. Dat vertraagde de stroom van *intelligence* naar andere diensten aanzienlijk; veel afnemers van het *intelligence*-product van de *National Security Agency* klaagden midden 1995 dat de *National Security Agency* niet in staat bleek te zijn om aan hun behoefte te voldoen.[39]

Een negende nadeel is de inherente kwetsbaarheid van verbindingsinlichtingen. Verbindingen worden beveiligd, codes kunnen plotseling veranderd worden, er kan *frequency hopping* plaatsvinden bij de zenders; daarbij springt de zender volgens een, alleen bij de legitieme ontvanger bekend, patroon tussen verschillende frequenties. Ook kunnen er zogeheten *bursttransmissies* optreden, waarbij in enkele seconden enorme hoeveelheden informatie wordt verzonden. En er kan sprake zijn van *spread spectrum*, waarbij de te verzenden informatie verdeeld over simultaan uitgezonden frequenties wordt uitgezonden. Een andere voor de hand liggende manier om de verbindingsinlichtingen te storen door degene wiens berichtenverkeer wordt onderschept, is om opzettelijk valse berichten te verspreiden, in de hoop dat die opgevangen worden. Ook cryptografie is een uitstekend middel om het berichtenverkeer te beschermen. Millis noemde dit een van de grotere bedreigingen voor de inspanningen van de *National Security Agency*: *Signals intelligence* verkeerde volgens hem door deze factoren in een crisis, en de wereld van het communicatieverkeer was niet langer *Signals intelligence*-vriendelijk te noemen.[40]

Alle inspanningen kunnen natuurlijk ook tenietgedaan worden door spionage of verraad. Sovjet-spionnen als William Weisband, William H. Martin en Bernon F. Mitchell hebben enorme schade toegebracht aan de Amerikaanse pogingen om verbindingsinlichtingen te verwerven. Versprekingen van de Amerikaanse president kunnen hetzelfde resultaat opleveren. Zo onthulde president Richard M. Nixon in 1969 tijdens een persconferentie dat de *National Security Agency* in staat was om het communicatieverkeer van de Sovjet-Unie en Noord-Korea te lezen. Na die verklaring veranderden Moskou en Pyongyang hun cryptografische systemen, en was de *National Security Agency* direct 'doof'. De *National Security Agency* had maanden nodig om de schade die veroorzaakt was door Nixons verspreking te herstellen.

Een tiende nadeel is dat *Signals intelligence* vanwege de beperkte verspreiding ook voor eigen politieke doeleinden aangewend kan worden. Dat deed Henry Kissinger als *National Security Advisor* van Nixon; bepaalde gevoelige *intercepts* werden niet met de ministers van Defensie en Buitenlandse Zaken gedeeld.[41] En in 1986 weigerde de *National Security Agency* zelfs *Signals intelligence* over de Iran-Contra-affaire te delen met de minister van Defensie, Weinberger: de redenering was dat het Pentagon geen 'need-to-know' had.[42]

Als elfde nadeel geldt soms het ontbreken van gecoördineerde *Signals intelligence*-verzamelactiviteiten. Tijdens de Koude Oorlog waren de verschillende *Signals intelligence*-organisaties van de drie Amerikaanse krijgsmachtonderdelen en van de diverse inlichtingendiensten vaak bezig met hetzelfde doel. Er ontstond zo een enorme verdubbeling van verbindingsinlichtingen. Ook na de Koude Oorlog kwam dat voor, bijvoorbeeld bij de jacht op drugskoning Pablo Escobar in 1992-1993: de *National Security Agency,* de *Signals intelligence*-eenheden van de CIA en de Amerikaanse krijgsmacht opereerden toen volstrekt onafhankelijk van elkaar, om aan te tonen dat hun personeel en materieel 'beter' waren dan die van de andere organisatie. Ook in de Sovjet-Unie werkten de KGB en de militaire inlichtingendienst GRU vaak langs elkaar heen, en dit fenomeen deed zich niet alleen voor bij deze twee grote mogendheden: in Duitsland vochten de *Bundesnachrichtendienst* en de Duitse militaire inlichtingendienst meer dan twintig jaar over de vraag wie er zeggenschap over *Signals intelligence* zou krijgen.[43] In hoofdstuk 3 kwam al aan de orde dat er ook in Nederland drie afzonderlijke militaire organisaties bestonden voor verbindingsinlichtingen; van samenwerking of serieuze pogingen tot integratie was amper sprake. Pas in 1996 werden deze drie diensten geïntegreerd tot de Afdeling Verbindingsinlichtingen.

Tot slot zijn ook technische obstakels een zekere belemmering bij *Signals intelligence.* Atmosferische storingen, ruis, zwakke ontvangst en het af en toe wegvallen van verbindingen kunnen een goede onderschepping in de weg staan. De gesteldheid van het terrein kan eveneens een belemmerende factor zijn. Dichtbewoonde gebieden, maar ook bergen en valleien, maken een goede *interceptie* van veraf vaak onmogelijk. Ten slotte kunnen storingen worden veroorzaakt door industriële activiteiten die de *interceptie* onmogelijk maken.[44]

Samengevat: *Signals intelligence* is een belangrijke, veilige, snelle, permanent inzetbare, kostbare, productieve en zeer betrouwbare methode om *intelligence* in de vorm van verbindingsinlichtingen te vergaren. Er kleven evenwel ook nadelen aan waarvan de belangrijkste zijn: de stortvloed aan onderschepte gegevens, het ontbreken van voldoende analysecapaciteit, de beperkte mogelijkheden van *interceptie* vanwege cryptografie, beveiligde verbindingen via landlijnen, de terreingesteldheid en atmosferische omstandigheden.

Voordat de vraag wordt beantwoord welke factoren hiervan belangrijk zijn geweest tijdens de oorlog in Bosnië, wordt eerst kort stilgestaan bij de geschiedenis van de belangrijkste afluisterdiensten.