VAST COMITÉ VAN TOEZICHT
OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Toezichtonderzoek (2007.181)

Besluiten en aanbevelingen van het onderzoek naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om de informatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland

De bescherming van de informatiesystemen en hun interconnecties die worden beheerd met nieuwe informatietechnologieën, komt geregeld ter sprake in het federale parlement. De veiligheid van de elektronische communicatienetwerken is een van de essentiële elementen voor de ontwikkeling van de informatiemaatschappij. De huidige technische middelen inzake interceptie en interferentie in de informatie- en telecommunicatiesystemen brengen onbetwistbaar bedreigingen met zich mee, niet alleen voor de veiligheid en de militaire, strategische en economische belangen van het land, maar ook voor de fundamentele rechten en vrijheden van de burgers.

Het Vast Comité I heeft dit al meermaals onderstreept in zijn verslagen. De parlementaire commissies die belast zijn met de begeleiding van het Vast Comité I delen deze bezorgdheid en hebben de regering daarvan kennis gegeven. In 1994 al vestigde het Comité de aandacht van het Parlement op het belang van de veiligheid van de officiële informatiesystemen: het formuleerde toen de aanbeveling dat een officiële instantie de opdracht zou moeten krijgen een globaal veiligheidsbeleid voor de informatiesystemen te ontwikkelen en te implementeren voor het gehele openbaar ambt.

Sindsdien is de wet van 10 juni 1998 tot wijziging van de wet van 30 juni 1994 ter bescherming van de persoonlijke levenssfeer tegen het afluisteren, kennisnemen en opnemen van privé-communicatie en -telecommunicatie op 2 oktober 1998 in werking getreden.

In zijn activiteitenverslag 2006 wees het Comité er nog op dat het aangewezen was om het algemene voorzorgsprincipe te hanteren bij het ontwikkelen van dit globale veiligheidsbeleid. Het merkte ook op dat de wet van 30 november 1998 houdende

regeling van de inlichting- en veiligheidsdienst aan de Algemene Dienst Inlichting en Veiligheid (ADIV) de opdracht toevertrouwde om de militaire informatie- en communicatiesystemen te beschermen.

In dit kader had het Comité aanbevolen dat Landsverdediging aanvullende regels zou opstellen tot uitvoering van de NAVO- en EU-normen teneinde elke poging tot binnendringing in haar informatiesystemen te identificeren en te neutraliseren. Het Comité heeft dus nooit zijn aandacht laten verslappen in verband met de wijze waarop de Belgische inlichtingendiensten de bedreigingen voor de veiligheid van de telecommunicatiesystemen aanpakken, met inbegrip van de bedreigingen die konden uitgaan van bondgenoten van België.[1]

We merken bij veel buitenlandse regeringen ook de trend om de prerogatieven en actiemiddelen van de inlichtingendiensten te versterken, meer bepaald hun bevoegdheden om elektronische telecommunicatie en berichten af te luisteren en te onderscheppen, zowel binnen als buiten hun landsgrenzen.[2]
Omdat de technologieën die de interceptie van communicatie via satellieten of op internet mogelijk maken steeds performanter en toegankelijker worden, begeven ook handelsvennootschappen zich op deze interceptie- en veiligheidsmarkt, waarvoor de inlichtingendiensten een bijzondere belangstelling aan de dag leggen.[3]

België vormt geen uitzondering op de trend om de afluistermiddelen te versterken. Dat blijkt meer bepaald uit een aantal bepalingen van de nieuwe wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten.[4]

In dit verband wijst het Comité erop dat het toezicht op de manier waarop de ADIV communicaties in het buitenland onderschept, al tot zijn wettelijke opdrachten behoort. Zo waakt het Comité erover dat de interceptiecapaciteiten van deze dienst uitsluitend worden aangewend conform hun wettelijk doel, dat erin

---

1 VAST COMITÉ I, *Activiteitenverslag 2000*, 29, 'Syntheseverslag van het onderzoek over de manier waarop de Belgische inlichtingendiensten reageren op het eventueel bestaan van een Amerikaans systeem, Echelon genaamd, voor het onderscheppen van telecommunicaties in België';
VAST COMITÉ I, *Activiteitenverslag 2000,* 62 'Verslag van het onderzoek naar de manier waarop de inlichtingendiensten hebben gereageerd op mogelijke feiten van spionage of poging tot indringing in het computersysteem van een Belgisch onderzoekscentrum',;
VAST COMITÉ I, *Activiteitenverslag 2004,* 44, 'Verslag aangaande de vaststellingen die werden gedaan in het kader van het onderzoek over een eventueel afluisteren van telefoongesprekken van magistraten door de inlichtingendiensten'.

2 Zo voorziet de wet '*Protect America Act*' van 2007 de uitbreiding van de capaciteiten voor het onderscheppen van internationale communicatie die de Amerikaanse inlichtingendiensten al genoten krachtens de wet '*Foreign Intelligence Surveillance*' (FISA).

3 *Intelligence On Line* (IOL), editie nr. 572, 15 juni 2008 - dit gespecialiseerde magazine noemt een tiental Amerikaanse, Franse en Europese bedrijven die interceptie-, veiligheids- en databeschermingssoftware leveren.

4 *B.S.* 10 maart 2010.

bestaat de externe en militaire veiligheid van het land en van de Belgische onderdanen in het buitenland te verzekeren.

Sinds enkele jaren horen of lezen we in het nieuws steeds vaker berichten over het afluisteren van telefoongesprekken, het onrechtmatig onderscheppen van telecommunicatie, lekken van gevoelige informatie en kwaadwillige indringing in de computersystemen van bedrijven of overheden, zowel in België als in het buitenland. [5]

Volgens Luc Beirens, Hoofd van de *Federal Computer Crime Unit* (FCCU), de eenheid van de Federale Gerechtelijke politie die belast is met de strijd tegen cybercriminaliteit, kunnen opzettelijke bedreigingen tegen computersystemen uitgaan van verschillende bronnen: computerpiraten die individueel of in netwerk handelen, criminele organisaties, terroristische bewegingen of zelfs sommige Staten (India, China, Noord-Korea, Rusland enz.) die systemen ontwikkelen om infrastructuur aan te vallen die van essentieel belang is voor de overheden en privébedrijven van andere landen. [6]

De uitgangsvraag van dit onderzoek heeft betrekking op de houding van de Belgische inlichtingendiensten tegenover de noodzaak om de informatiesystemen te beschermen tegen intercepties uit het buitenland. Het antwoord op die vraag is duidelijk: zowel de Veiligheid van de Staat als de ADIV zijn zich bewust van de ernst van de bedreigingen die cyberaanvallen, ongeacht of ze uitgaan van andere staten, vormen tegen de vitale (civiele en militaire) informatiesystemen van het land.

De twee diensten hebben bijgevolg initiatieven genomen om hun 'klanten' te sensibiliseren voor de algemene problematiek van de cyberaanvallen, voor de kwetsbare plekken van hun informatiesystemen en voor de noodzaak om beschermende maatregelen te nemen. Het in die zin geleverde werk is opmerkelijk.

In de mate waarin de beperkte middelen waarover ze beschikken dat toelaten, voeren de Belgische inlichtingendiensten ook onderzoek naar aanvallen tegen de informatiesystemen van zowel de burgerlijke als militaire overheden. Ook in dit geval gaat het echter om een voornamelijk defensieve benadering op basis van detectie, evaluatie en reactie. We kunnen echter niet anders dan vaststellen dat het ontbreken van een globaal federaal beleid inzake informatieveiligheid (en van een echte overheid ter zake) tot gevolg heeft dat ons land zeer kwetsbaar is voor aanvallen tegen zijn vitale informatiesystemen en -netwerken.

---

5 De actualiteit op het einde van 2010, met de lekken die de zaak "*Wikileaks*" aan het licht heeft gebracht, is daarvan een treffend voorbeeld.

6 Verslag van de Commissie van Infrastructuur, van Communicaties en van Ondernemingen betreffende '*ICT-veiligheid*' (Kamer , 2007-2008, 28 februari 2008, DOC 52 0898/001).

De bedreigingen voor die informatiesystemen kunnen afbreuk doen aan de veiligheid en de fundamentele belangen van de Staat zoals die worden gedefinieerd in de artikelen 7 en 11 van de wet van 30 november 1998 houdende regeling van de inlichting- en veiligheidsdienst.

Meerdere federale instellingen houden zich vandaag bezig met de beveiliging van de informatiesystemen: de Nationale Veiligheidsoverheid (NVO), FEDICT, BELNET en het BIPT. Geen enkele van die instellingen blijkt echter een algemeen beeld te hebben van de kritieke infrastructuur van de informatiesystemen.[7] De technische middelen waarover de NVO beschikt, zijn absoluut ontoereikend.

Gelet op deze grote versnippering van het beleid rond de veiligheid van informatiesystemen, schaart het Vast Comité I zich achter de besluiten van het '*witboek voor een nationaal beleid voor de informatieveiligheid*'. Het Vast Comité I beveelt ook aan dat er een federale strategie ter zake wordt uitgewerkt en dat er snel een agentschap wordt opgericht met de opdracht de activiteiten rond informatieveiligheid te coördineren .[8]

Het Vast Comité I is ervan overtuigd dat de Belgische inlichtingendiensten over de nodige ervaring en knowhow beschikken die kunnen worden aangewend binnen of ten voordele van een nog op te richten agentschap voor de informatieveiligheid.

Op internationaal vlak vertegenwoordigen de ADIV en de VSSE ons land soms binnen bepaalde werkgroepen, maar dit gebeurt zonder echte coördinatie met de andere betrokken overheden. Het lijkt dus noodzakelijk om duidelijk de rol te definiëren die aan de inlichtingendiensten wordt toegewezen op het vlak van de bescherming van de informatiesystemen van ons land. Het Vast Comité I beveelt aan dat het Ministerieel Comité Inlichting en Veiligheid daartoe het nodige doet.

Het is dan wel noodzakelijk dat onze inlichtingendiensten over de vereiste middelen beschikken om die taak te vervullen. Meer bepaald moeten ze de gekwalificeerde personeelsleden kunnen rekruteren en behouden. De administratieve en financiële statuten die het Openbaar Ambt vandaag aanbiedt, oefenen, in tegenstelling tot de lonen in de privésector, geen grote aantrekkingskracht uit op werknemers met hoge kwalificaties op het gebied van informatica.

Het Vast Comité I beschouwt het huidige tekort aan gekwalificeerde personeelsleden bij de inlichtingendiensten als een groot probleem. Het beveelt

---

7 In maart 2010 werd er bij FEDICT nochtans gewerkt aan een inventaris van de kritieke ICT-infrastructuur.

8 Dergelijke agentschappen bestaan in een aantal buurlanden zoals Frankrijk (*Agence Nationale de la Sécurité des Systèmes d'Information* (ANSSI), dat ressorteert onder de Eerste Minister), Duitsland (*Bundesamt für Sicherheit in der Informationstechnik* (BSI), dat ressorteert onder het ministerie van Binnenlandse Zaken) en het Verenigd Koninkrijk (*Office of Cyber Security* (OCS), dat ressorteert onder de Eerste Minister).

aan dat deze diensten eindelijk de gekwalificeerde personeelsleden kunnen aanwerven die ze nodig hebben om hun opdracht inzake informatieveiligheid uit te oefenen.

Het Vast Comité I ziet ook het tekort aan technische certificatie- en homologatiemiddelen als een ernstig probleem op het vlak van de informatieveiligheid. Het beveelt aan om in de noodzakelijke middelen te voorzien opdat de certificatie en homologatie van de systemen die in België worden gebruikt om geclassificeerde informatie te verwerken eindelijk kunnen plaatsvinden zonder dat men afhankelijk is van buitenlandse overheden en diensten.

Het Vast Comité I beveelt ook de grootste voorzichtigheid aan bij de keuze van de beveiligde technische uitrustingen voor de verwerking van gevoelige en geclassificeerde informatie, meer bepaald in verband met de toepassing van de methoden voor het verzamelen van gegevens van de inlichtingen- en veiligheidsdiensten. Het Comité neemt de aanbevelingen over van het witboek van het overlegplatform voor de informatieveiligheid en beveelt aan dat dit materieel wordt geëvalueerd, gecertificeerd en gehomologeerd – wat betreft zijn betrouwbaarheid en veiligheid – volgens criteria en een procedure die beantwoorden aan de normen van de Europese Unie.

Het Vast Comité I beveelt ook de grootste voorzichtigheid aan bij de keuze van de leveranciers van dit materieel. Het Comité beveelt aan dat bij de gunning van deze opdrachten het bezit van een veiligheidsmachtiging wordt opgelegd aan de weerhouden firma's.

Het Vast Comité I beveelt aan dat er in het kader van het veiligheidsonderzoek bijzondere aandacht wordt besteed aan de eventuele banden van die firma's met sommige buitenlandse inlichtingendiensten.

De wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten heeft aan de ADIV een middel toegekend om te reageren op cyberaanvallen tegen de informatiesystemen van Landsverdediging.

Het Vast Comité I beveelt echter aan dat er ook wordt voorzien in de mogelijkheid om systemen in het buitenland te neutraliseren in geval van aanvallen tegen de informatiesystemen van andere ministeries dan Landsverdediging (diensten van de Eerste Minister, FOD Buitenlandse Zaken, VSSE enz.) of tegen de nationale kritieke infrastructuur. De VSSE zou met die opdracht kunnen worden belast.