Notitie Cyberintelligence en publiek belang
Expertmeeting Eerste Kamer 6 mei 2014
Rathenau Instituut

Inleiding

De recente onthullingen van Snowden over de werkwijze van de NSA vormen voor de vaste commissies voor Immigratie & Asiel / JBZ-raad en Veiligheid & Justitie van de Eerste Kamer aanleiding voor het organiseren van een openbare expertmeeting over de betekenis van deze onthullingen voor de Nederlandse situatie. Centrale vragen daarbij zijn:

- Hoe ziet een goede intelligence praktijk er uit? Welke bevoegdheden en digitale opsporingsmethoden zijn nodig?
- Aan welke grenzen dient deze praktijk te zijn gebonden? Welk toezicht - inclusief parlementair toezicht - is hierop op nodig?
- Hoe verhouden de benodigde bevoegdheden en grenzen zich tot het huidige juridisch kader (Wet op inlichtingen- en veiligheidsdiensten, Wiv 2002)?
- Hoe kan de weerbaarheid van burgers worden vergroot tegen (mogelijk) disproportioneel of onwettig handelen van binnen- en buitenlandse inlichtingendiensten?

Ter voorbereiding op de expertmeeting hebben de Eerste Kamer en het Rathenau Instituut met diverse deskundigen gesproken. Alle gesprekspartners geven aan dat de NSA op veel grotere schaal gegevens verzamelt en analyseert dan de Nederlandse inlichtingen- en veiligheidsdiensten. Dat laat onverlet dat ook in Nederland vraagtekens kunnen worden gesteld bij de werkwijze van de diensten, de toereikendheid van het huidige wettelijk kader en de organisatie van het toezicht op de diensten. Deze notitie geeft de belangrijkste bevindingen van de gesprekken weer en formuleert aandachtspunten voor de bijeenkomst op 6 mei.

Relevante ontwikkelingen

- Technologische ontwikkelingen veranderen de intelligence praktijk. Basale (wettelijke) onderscheidingen in de Wiv lijken achterhaald en vragen om modernisering van de wet. Het gaat hierbij vooral om de verschillen tussen kabelgebonden en niet kabelgebonden informatie, gerichte en ongerichte dataverzameling, en metadata en data.
- Metadata (gegevens over communicatieverkeer) kunnen anno 2014 zeer privacygevoelig zijn. Metadata zijn niet alleen vergelijkbaar met de enveloppe (denk aan afzender, geadresseerde), maar ook met gerichte observatie, zoals data over tijd, plaats, bewegingspatronen of positie in sociaal netwerk. Metadata kunnen daarom ook persoonsgegevens zijn. Het kabinet lijkt dit te onderkennen in zijn reactie op het rapport van de Commissie Dessens. Het stelt dat het onderscheid tussen metadata en de inhoud van communicatie niet het enige bepalende element moet zijn bij het vaststellen van de ernst van de privacy-inbreuk en het daarbij horende model van toestemming en toezicht.
- Volgens de huidige wet (Wiv) mag alleen niet-kabelgebonden communicatieverkeer (verkeer via de satelliet) ongericht door de inlichtingendiensten worden vergaard. Maar het grootste deel van het communicatieverkeer verloopt inmiddels niet meer via de satelliet, maar via glasvezelkabels.

- De Commissie Dessens beveelt daarom aan dat ”ongerichte kabelgebonden interceptie van communicatie moet worden toegestaan onder gelijktijdige herziening en versteviging van de wettelijke waarborgen van toestemming en toezicht”. Toegang tot de kabel betekent een verruiming van de bevoegdheden en een toename van de hoeveelheid gegevens die inlichtingendiensten over burgers kunnen vergaren. Daarom koppelt de Commissie aan deze verruiming een verstevigd toezicht.
- In de praktijk stuit ongerichte interceptie op grenzen. Het enorme volume van het communicatieverkeer betekent dat er teveel data is om te intercepteren en te analyseren. Een combinatie van gericht en ongericht zoeken lijkt daarom noodzakelijk.
- Het is onduidelijk wat de opbrengst is van sleepnettechnieken (ongerichte interceptie) en of de inzet proportioneel is met het oog op de privacy-inbreuk voor burgers.
- Ook gerichte interceptie wordt moeilijker. Het klassieke idee van het tappen van een communicatielijn, is in veel gevallen achterhaald. Mensen maken thuis, onderweg en op het werk gebruik van het internet, zonder vast IP-adres. Communicatie vindt ook plaats via steeds meer kanalen: sociale media, games, mobiele applicaties e.d.
- Als reactie daarop maken inlichtingendiensten gebruik van nieuwe digitale opsporingsmethoden, zoals het hacken van (bijvoorbeeld Jihadistische) webfora, via zogeheten *endpoint operations*. Het ene *endpoint* zijn grote internetbedrijven. Inlichtingendiensten halen daar de informatie op. Het andere *endpoint* is de gebruiker. De informatie wordt onderschept voordat het versleuteld het internet opgaat.
- Het is de vraag of het hacken van webfora en het gebruik van *endpoint operations* onder de Wiv valt. Hierbij moet worden opgemerkt dat bij het opstellen van de Wiv in 2002 sociale media net in opkomst kwamen. Hoe gericht of ongericht zijn deze methoden? Hoeveel burgers worden onderdeel van onderzoek? Welke nevenschade mag worden aangericht? Denk wat dit laatste betreft aan een mogelijke verzwakking van de IT-infrastructuur door het plaatsen van malware om toegang te krijgen tot het endpoint.
- De veranderingen in de intelligence praktijk lijken om aanscherping van het toezicht en de toestemmingsvereisten te vragen. In dit verband is het ook de vraag of het CTIVD, dat structureel toetst op rechtmatigheid, niet ook structureel op doelmatigheid moet toetsen: hoe effectief zijn gebruikte opsporingsmethoden?
- Bedrijven kunnen zich in de praktijk niet of nauwelijks beschermen tegen de geavanceerde middelen die grote inlichtingendiensten tot hun beschikking hebben. Indien bescherming al mogelijk zou zijn, zou die beveiliging dusdanig veel beperkingen opleggen dat het niet meer werkbaar is (denk aan geen internettoegang).
- Ook voor burgers is het moeilijk zich te verweren tegen de inlichtingendiensten als zij onterecht als target worden beschouwd door inlichtingendiensten. Hoe lang blijven gegevens bewaard? Kunnen ze foutieve informatie (laten) corrigeren? Is er zicht op de uitwisseling van gegevens over burgers tussen landen? Hoe kunnen burgers zich verdedigen als kwaadwillenden *malware* op hun computer plaatsen en zij daardoor als verdachte worden beschouwd?

Opzet expertsessie 6 mei

Sessie 1 Technologische ontwikkelingen
Inleider: Hoofd JSCU
Co-referent 1: Bart Jacobs
Co-referent 2: Bert-Jaap Koops

Onderwerpen:
- Wat voor soort digitale opsporingsmethoden passen inlichtingendiensten in de praktijk vooral toe (endpoint operations, verspreiding malware, combinaties van gericht/ongericht zoeken)? Wat zijn de belangrijkste doeleinden?
- Welke methoden leveren het meeste op?
- Wat betekent het toepassen van endpoint operations voor het onderscheid tussen gericht en ongericht zoeken en het daarbij horende model van toestemming?
- Is de Wiv (met betrekking tot de bevoegdheden van inlichtingendiensten) nog voldoende toegerust op de praktijk van datavergaring door inlichtingendiensten? Zijn er aanpassingen nodig en zo ja, welke dan?

Sessie 2 Toezicht
Inleider: Harm Brouwer
Co-referent: Cees Wiebes

Onderwerpen:
- Is het huidige systeem van toezicht en toestemmingsvereisten uit 2002 voldoende toegesneden op de intelligence praktijk anno 2014? Het gaat dan om zaken als het verlenen van toestemming voor *searches* door de minister, het toezicht op rechtmatigheid (CTIVD), het parlementair toezicht (CIVD) en het toezicht op doelmatigheid. Op welke punten is aanscherping nodig?
- De Commissie Dessens stelt technologie-onafhankelijke wetgeving voor (waarbij de diensten toegang krijgen tot de kabel), met gelijktijdige aanscherping van het stelsel van toezicht. Wat kunnen inlichtingendiensten met deze uitbreiding van hun bevoegdheden meer of anders dan zij nu kunnen?
- Hoe is het parlementair toezicht in de ons omringende landen geregeld? Wat kan Nederland daarvan leren?

Sessie 3 Bedrijfsspionage
Inleider: Ronald Prins
Co-referent: Axel Arnbak

Onderwerpen:
- Is het toelaatbaar dat onder druk van inlichtingendiensten bij bedrijfsnetwerken en providers/softwareleveranciers achterdeurtjes worden gecreëerd? Leidt dit tot een onverantwoorde verzwakking van de IT-infrastructuur?

- In welke mate verspreiden inlichtingendiensten malware, en is dat toelaatbaar?

Sessie 4 Rechtspositie burger
Inleider: Hoofd AIVD
Co-referent: Wilhelmina Thomassen

Onderwerpen:
- Welke mogelijkheden hebben burgers om zich te verweren indien zij onterecht als target worden beschouwd door inlichtingendiensten? Zijn die mogelijkheden afdoende?
- Functioneert de informatieplicht van de AIVD aan mensen waarover door de AIVD gegevens zijn verzameld?
- Kan persoonsgebonden informatie van burgers die vergaard is door inlichtingendiensten en bedrijven, binnen Nederland of Europa worden gehouden en zo ja, hoe? Welke afspraken heeft Nederland met andere Europese landen over informatie-uitwisseling tussen landen? Volstaan deze afspraken?