Hartelijk dank voor uw uitnodiging om deel te nemen aan sessie 3 over bedrijfsspionage. Hierbij behandel ik beknopt uw onderwerpen en draag ik materiaal aan voor eventuele vervolgvragen. Wellicht ten overvloede verwijs ik u naar mijn korte gespreksnotitie voor een RTG in de Tweede Kamer eind juni 2013, over bulk surveillance en versleuteling.[1]

Thema 1: 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?

1. 'Backdoors' zijn inherent onverantwoord. Een backdoor geldt ongericht voor iedere gebruiker, die door de backdoor kwetsbaar wordt voor iedere aanvaller – inclusief cybercriminelen en cyberlegers waar dan ook ter wereld. Het is een uiterst ongerichte wijze van industriële sabotage, die de robuustheid van en het vertrouwen in IT-infrastructuur op het spel zet.
2. In het afgelopen jaar hebben robuustheid van en vertrouwen in kritieke IT-infrastructuur daadwerkelijk onherstelbare schade opgelopen, niet in de laatste plaats onder technici. Met name sinds de onthullingen rondom backdoors in operatie BULLRUN en EDGEHILL is bekend geworden dat standaardorganisaties als IETF en NIST jarenlang zijn gemanipuleerd, cruciale encryptie-algoritmes ondermijnd en zelfs bedrijven als RSA werden omgekocht.[2]
3. Niet alleen backdoors, ook het gebruikmaken – en daarmee verzwijgen – van bestaande kwetsbaarheden heeft aan de ernstige deuk in vertrouwen bijgedragen. Zo blijken de automatische beveiligingsupdates en 'crash reports' van Microsoft een aanvalsvector voor inlichtingendiensten.[3] Security expert Bruce Schneier noemt dit het digitale equivalent van het plaatsen van sniper-soldaten in Rode Kruis trucks, omdat het gezond en up-to-date houden van hard- en software nu in zichzelf een beveiligingsgevaar vormt. Zulke praktijken dienen dan ook ernstig veroordeeld te worden.

Thema 2: In welke mate verspreiden inlichtingendiensten malware, en is dat toelaatbaar?

4. Over Nederlandse inlichtingdiensten is weinig bekend, maar door Edward Snowden weten we nu dat Amerikaanse- en Britse diensten beschikken over onvoorstelbare mogelijkheden voor het inbreken in hard- en software van zowel netwerken (o.a. QUANTUM; routers bij ISPs, op knooppunten) als systemen (o.a. TAO; hacken van computers, smartphones, etc.).[4] Daarbij kan malware zijn ingezet, zowel op grote en schaal en ook individueel. Zo heeft de NSA sinds 2007 al 140.000 botnets gecoöpteerd, om voor surveillance doeleinden met cybercriminelen mee te liften.
5. Ons juridische denken schiet ernstig tekort om het vraagstuk van (on)rechtmatige overheidsmalware te adresseren. Uiteraard is er het grondrecht op privacy, maar het verzwakken van IT-infrastructuur via backdoors en met malware gaat meestal vooraf aan een privacy schending. De heer Modderkolk illustreerde in de vorige sessie treffend hoe Nederlandse diensten huidige juridische beperkingen kunnen omzeilen door complete computeromgevingen te hacken (het NRC), om daar vervolgens een mailtje uit te vissen (van NRC naar de Eerste Kamer).[5] Andere diensten infecteren 'alvast' 100.000 internetrouters wereldwijd, om later surveillance mogelijk te maken.
6. Het Duitse Federale Constitutionele Hof heeft in 2008 een nieuw grondrecht geformuleerd op de 'vertrouwelijkheid en integriteit van IT-systemen'.[6] De vragen in uw voorbereidende notitie worden in deze 'Bundestrojaner'-uitspraak geadresseerd. Het Hof keurt 'hackwetgeving' ten zeerste af, en geeft de strengste juridische criteria mee aan de wetgever mocht zij opnieuw wetgeving rondom malware willen formuleren; veel strenger dan voor huiszoekingen en telefoontaps. Het

1 Zie: http://www.ivir.nl/publicaties/arnbak/Gespreksnotitie_Tweede_Kamer_26_juni_2013.pdf
2 Zie: http://www.theguardian.com/world/interactive/2013/sep/05/nsa-project-bullrun-classification-guide
3 Zie: http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969-2.html
4 Zie: https://firstlook.org/theintercept/article/2014/03/12/nsa-plans-infect-millions-computers-malware/ en noot 3.
5 EK 2013–2014, CVIII, nr. A, 12 mrt. 2014, p. 2
6 Meer informatie: A.M. Arnbak, '9 Problems of Government Hacking: Why IT-Systems Deserve Constitutional Protection', CITP, Princeton University, 20 February 2014, zie: https://freedom-to-tinker.com/blog/axel/9-problems-of-governments-hacking-why-it-systems-deserve-constitutional-protection/

volstaan van een eigen gunstige interpretatie door de AIVD van de Wiv 2002 is in vergelijking met deze praktijk opzienbarend en een punt van zorg.

Extra thema's: noodzaak betrouwbare cijfers voor beleidsvorming bedrijfsspionage en ongerichte kabelgebonden interceptie

7. Helaas zijn de door de Minister genoemde ramingen van geleden schade door industriële spionage onbruikbaar voor beleidsvorming.[7] Toponderzoek heeft vastgesteld dat zulke ramingen, inclusief het TNO-cijfer voor Nederland ("ca. 2 miljard euro"), overdreven en in ieder geval onbetrouwbaar zijn.[8] De 'hype' verklaren de onderzoekers uit het opnemen van entertainment-downloads en het overdrijven van schadecijfers door de security-industrie die daar direct belang bij heeft. Verder gaan de cijfers vooral over cybercrime, niet over cyber intelligence door staten.

8. Een mogelijke uitbreiding van bevoegdheden voor ongerichte kabelgebonden interceptie stuit direct op de recente verwerping van de dataretentierichtlijn ('de bewaarplicht') door het Hof van Justitie van de Europese Unie.[9] Het ongerichte opslaan van metadata door telecomproviders wordt daarin ernstig veroordeeld, nog los van de daaropvolgende toegangseisen voor autoriteiten, dan wel de doelen waarvoor ongericht opgeslagen gegevens gebruikt worden. Oftewel: ongerichte interceptie, doel, toegang en analyse zijn onlosmakelijk met elkaar verbonden. De discussie in Nederland over ongerichte kabelgebonden interceptie om te beschermen tegen bedrijfsspionage kan sinds de uitspraak van het Hof niet los gezien worden van massale surveillance, en zal hoogstwaarschijnlijk stuiten op een vernietigende uitspraak.

7 EK 2013–2014, 33 169, nr. P, p. 3.
8 R. Anderson, M. van Eeten, et. al., 'Measuring the Cost of Cybercrime', WEIS 2012, zie: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.
9 Zie: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf