Rondetafelgesprek Wet op de inlichtingen- en veiligheidsdiensten (Wiv 20..)

Vaste commissie Binnenlandse Zaken, 15 december 2016

Gespreksnotitie mr. P.J.F. Koop, Electrospaces.net

Bij de Wet op de inlichtingen- en veiligheidsdiensten zijn helderheid en begrijpelijkheid van groot belang voor de legitimiteit van het werk van de betreffende diensten. Vanuit die gedachte volgen hier enkele voorstellen en vragen om met name drie van de belangrijkste bevoegdheden evenwichtiger en inzichtelijker te maken.

Ongerichte kabeltoegang

Keer terug naar de oorspronkelijk term "ongerichte kabeltoegang"
De nu gebruikte term "onderzoeksopdrachtgerichte interceptie" is strikt genomen correct, maar komt geforceerd en daarmee eerder verhullend in plaats van transparant over.

Breng de drie fases voor ongerichte kabeltoegang terug tot twee
De voorgestelde drie fases zijn te complex, met name doordat fase 2 (art. 49) zowel onderzoek ten behoeve van fase 1, als onderzoek ten behoeve van fase 3 omvat. Art. 49 lid 1 kan daarom beter bij art. 48, en art. 49 lid 2 bij art. 50 worden gevoegd.
Ook het feit dat toestemmingen slechts eenmaal per kwartaal aan de minister en vervolgens de TIB worden voorgelegd zal ertoe bijdragen dat (de facto) combi-lasten de regel worden. Toestemming in meerdere fases dreigt dan een schijnwaarborg te worden.

Op welk punt in het netwerk gaat ongerichte kabeltoegang plaatsvinden?
De Memorie van Toelichting (MvT) lijkt te suggereren dat de diensten (d.m.v. *cable splitting*) een kopie van een gehele glasvezelkabel krijgen, waaruit zij dan zelf de meest interessante kanalen selecteren. Zou het niet efficiënter (en geruststellender) zijn om de providers deze selectie te laten doen en dan alleen verkeer uit de gewenste kanalen aan te laten leveren?

Zal afluisteren via ongerichte kabeltoegang ook real-time kunnen plaatsvinden?
De voorlopige wetstekst is hier niet duidelijk over, maar in de MvT wordt gezegd dat er alleen ten behoeve van cybersecurity online en real-time filtering van kabelverkeer zal plaatsvinden. Voor interceptie van telecommunicatie zullen de data alleen *opgeslagen* worden, wat opnieuw een techniek-afhankelijkheid zou zijn. Indien of zodra het mogelijk is, verdient echter ook voor telecommunicatie real-time filteren de voorkeur omdat daarmee "*select while you collect*" dan geautomatiseerd gaat en de minste inbreuk oplevert.

Bewaartermijn bulkdata
Wat betreft de bewaartermijn van 3 jaar voor ongericht verzamelde data valt nog op te merken dat er in Duitsland en het Verenigd Koninkrijk weliswaar geen wettelijke bewaartermijnen zijn (zie MvT, bijlage 5), maar dat in de praktijk het Britse GCHQ grote verzamelingen metadata ongeveer 6 maanden kan bewaren en het metadatasysteem van de Duitse BND deze gegevens slechts 90 dagen opslaat.

Cybersecurity

Breng ongerichte kabeltoegang voor cybersecurity in een eigen wetsartikel onder
Cybersecurity of *cyber defense* wordt steeds belangrijker, maar wordt nu alleen in de MvT op de artt. 48 en 49 gebaseerd. Bij cybersecurity gaat het echter niet om persoonlijke communicatie, dus zijn de getrapte toestemmingen hier niet nodig. Wel nodig is een aparte en betere beschrijving van deze functie en een beperking ervan tot defensieve detectie.

Op welke schaal zal netwerkmonitoring en malwaredetectie worden toegepast?
De MvT maakt niet duidelijk of deze methodes op een net zulk beperkt aantal glasvezelkanalen zal worden toegepast als interceptie van telecommunicatie. Cybersecurity lijkt namelijk gebaat bij het monitoren van veel grotere stromen internetverkeer. Is dat inderdaad de bedoeling en hoe verhoudt zich dat tot het Nationaal Detectienetwerk (NDN)?

Hacken

Voorzie de hackbevoegdheid van toestemming in twee fases
Mede door toenemende versleuteling van communicatieverkeer zal de hackbevoegdheid in belang en omvang toenemen en hoewel hacken doorgaans heel gericht zal zijn, kan het ook toegang geven tot een grotere bulk aan data, bijv. wanneer internetfora gehackt worden. Analoog aan de waarborgen voor ongerichte kabeltoegang, zou bijvoorbeeld een eerste toestemming vereist kunnen worden voor het verkennen en toegang verkrijgen tot een netwerk, computer of smartphone, gevolgd door een tweede toestemming om over te gaan tot het daadwerkelijk inzien c.q. downloaden van data.

Toestemming

Voer ook voor kamerleden toestemming door de rechtbank in
Het wetsontwerp voorziet dit nu alleen voor advocaten en journalisten, maar toestemming door de rechtbank Den Haag zou ook voor kamerleden gepast zijn, gezien hun bijzondere staatsrechtelijke positie en de daarmee gepaard gaande terughoudendheid om bijzondere bevoegdheden jegens hen toe te passen.

Peter Koop

www.electrospaces.net
peter.koop@electrospaces.net