Outline bijdrage aan de expertmeeting Eerste Kamer, 6 mei

Technologische ontwikkelingen sinds de invoering van de Wiv 2002

Een wereld zonder internet en digitale technologie is ondenkbaar geworden. Iedereen wordt in hoog tempo met iedereen verbonden. Deze ontwikkeling schept nieuwe kansen en nieuwe risico's. Het digitale tijdperk heeft verstrekkende gevolgen voor iedereen. De snelle, mondiale opkomst van deze technologie tot in alle haarvaten van samenlevingen is in tal van opzichten een *gamechanger*.

Concreet:

- mobiele *devices*, zoals smartphones, en Wifi-netwerken hebben sinds 2002 overal ter wereld massaal hun intrede gedaan. De mobiliteit van gebruikers van telecommunicatiemiddelen en het aantal en de diversiteit van deze middelen is daardoor drastisch toegenomen. Er zijn momenteel meer mobiele devices dan mensen. De komende jaren vindt de groei vooral plaats in de 'gordel van instabiliteit' (VN-gegevens);
- sociale media zijn onlosmakelijk onderdeel geworden van het dagelijkse leven. Ook dit is een wereldwijde ontwikkeling. Facebook, Twitter, Whatsapp en YouTube bestonden in 2002 nog niet. Per dag worden er 140 miljoen tweets de wereld ingestuurd. In 60 dagen voegen YouTube's 490 miljoen gebruikers meer videomateriaal toe dan Amerikaanse televisienetwerken in 60 jaar;
- de hoeveelheid en diversiteit van gegevens is de afgelopen tien jaar mondiaal exponentieel gegroeid. Er is sprake van een 'dataexplosie': 90 procent van alle data wereldwijd is gecreëerd in de laatste twee jaar. Elke dag komen er, naar schatting van IBM, 2,5 triljoen (1 met achttien nullen) bytes data per dag bij. De wereldbevolking verzond vorig jaar (2013) elke dag 182 miljard e-mails. Tegelijkertijd is de versleuteling van telecommunicatie aanzienlijk geavanceerder geworden en breed beschikbaar;
- behalve 'big data' is sprake van 'fast data': gegevens die ontstaan door een gebeurtenis, activiteit of interactie via sociale en online kanalen, mobiele apparaten, sensoren, point-of-sale, het internet-van-alles. Ze zijn vluchtig, hebben een beperkte houdbaarheid en lenen zich vooral voor het ondersteunen van actuele beslissingen en acties, hier en nu, zodat bedrijven hun aanbod kunnen personaliseren, processen real-time kunnen bijsturen en tijdig maatregelen kunnen nemen;
- ongeveer 90 procent van alle telecommunicatie heeft zich sinds 2002 verplaatst van de lucht naar kabelnetwerken, die in korte tijd de 'backbone' zijn geworden van de mondiale telecommunicatie. In Nederland bevindt zich een van de meest moderne kabelinfrastructuren ter wereld met diverse belangrijke internationale dataverbindingen;
- de complexiteit en de 'dichtheid' van netwerken is snel toegenomen. Binnen het mondiale telecommunicatienetwerk wordt verkeer gerouteerd op basis van overwegend economische factoren in relatie tot transportmogelijkheden. De ene dag wordt verkeer gerouteerd via de lucht, de volgende dag via de kabel.

Gevolgen

De snelle opkomst van het internet en digitale technologie is ook een *gamechanger* vanuit het oogpunt van inlichtingen en veiligheid. In het belang van Nederland, ook van burgers en bedrijven, moeten de I&V-diensten actief kunnen inspelen op deze ontwikkelingen, binnen de grenzen van de wet en met eerbiediging van de persoonlijke levenssfeer.

Als gevolg van de genoemde technologische en maatschappelijke ontwikkelingen is het voor de Nederlandse I&V-diensten paradoxaal genoeg steeds moeilijker geworden inzicht te krijgen in de communicatie van degenen die kwaad in te zin hebben.

Ten eerste neemt in het digitale tijdperk met zijn mobiele devices en complexe netwerken de opbrengst van 'klassieke' interceptiemethodes als het gerichte aftappen van vaste telefoonverbindingen onmiskenbaar af. Ook de sterk toegenomen versleuteling van telecommunicatie zorgt ervoor dat relevant berichtenverkeer steeds moeilijker bereikbaar wordt.

Ten tweede maakt de 'dataexplosie' het onderkennen van dreigingen aanzienlijk complexer. De communicatie van degenen die kwaad in de zin hebben, gaat schuil in de mondiale stortvloed van communicatie van goedwillende burgers. Het is inherent aan het digitale tijdperk dat ook de Nederlandse I&V-diensten worden geconfronteerd met grote aantallen gegevens. De moeilijkheid is hoe grote hoeveelheden data te analyseren om er zinvolle inzichten uit te destilleren. De analyse van metagegevens in plaats van de inhoud van communicatie is noodzakelijk om dreigingen tijdig te kunnen onderkennen en inbreuken op de persoonlijke levenssfeer van burgers tot het minimale te beperken. Dat geldt ook voor ‘search’-activiteiten in de ether, bijvoorbeeld in het kader van militaire missies.

Het werken met grote aantallen metagegevens kan niet worden gelijkgesteld met 'mass surveillance'. Het analyseren van metagegevens is juist noodzakelijk om tijdig schaarse capaciteit te richten op communicatie die bijdraagt aan de beantwoording van een door de politiek goedgekeurde onderzoeksvraag. Het analyseren van metadata helpt ook onnodige en disproportionele inbreuken op de persoonlijke levenssfeer te voorkomen. Het alternatief -- het op grote schaal kennis nemen van de inhoud van communicatie -- is onwenselijk, zowel vanuit het oogpunt van de doeltreffendheid en de doelmatigheid van de diensten als van dat van de privacy van burgers.

Het begrip “ongerichte interceptie” uit de Wiv 2002 kan voorts niet worden gelijkgesteld met het lukraak en massaal onderscheppen van de communicatie van Nederlandse of buitenlandse burgers. Iedere verwerving van gegevens begint met een zoekvraag in relatie tot een onderzoeksopdracht. Het gaat daarom ook hoofdzakelijk om telecommunicatie in of met het buitenland. Dat geldt ook voor de verwerving van metagegevens. Er is in deze zin dus geen sprake van ongericht

onderzoek. Vooraf moet duidelijk zijn waarnaar men op zoek is (denk aan onderzoeksopdrachten met betrekking tot Syrië, Mali, Cyber, terrorisme of de Nuclear Security Summit). De Nederlandse I&V-diensten verzamelen altijd maar een zeer klein deel van de totale communicatie, namelijk dat deel dat nodig is om door de politiek goedgekeurde taken en onderzoeksopdrachten uit te voeren.

Ten derde betekent de bepaling in de Wiv 2002 dat "ongerichte" interceptie van telecommunicatie zich dient te beperken tot "niet-kabelgebonden netwerken" dat het merendeel van alle telecommunicatie zich geheel en al aan het zicht onttrekt van de Nederlandse I&V-diensten. De CTIVD heeft onlangs onderstreept dat er bij het vaststellen van de Wiv 2002 geen grondrechtelijke reden bestond waarom een bericht dat door de kabel gaat niet mag worden onderschept terwijl datzelfde bericht wel mag worden onderschept als het door de lucht gaat. Door de snelle ontwikkeling en verspreiding van kabelgebonden technologie is toegang tot de kabel onontbeerlijk geworden voor het onderkennen van ongekende dreigingen en het tijdig vinden van communicatie van gekende dreigingen. De beperking in de WIV 2002 betekent dat cyberdreigingen en digitale spionage niet tijdig worden onderkend, Nederlandse militairen-op-missie minder goed worden beschermd en ondersteund dan nodig en mogelijk is, terroristische activiteiten mogelijk niet tijdig worden onderkend, de werkelijke intenties van risicolanden verborgen blijven en de vervreemding van intellectueel eigendom, vitale economische informatie en staatsgeheimen onopgemerkt blijft.

Tegelijkertijd is juist Nederland niet alleen een doorvoerland van goederen en een internationaal verkeersknooppunt, maar ook een belangrijk doorvoerland van data -- en van 'malware' -- geworden. Het ongestoorde functioneren van deze kabelnetwerken en internetknooppunten en het voorkomen van misbruik van dit deel van 'cyberspace' is van groot economisch en maatschappelijk belang geworden. Het internationale verkeer over kabelnetwerken is onmiskenbaar tevens van belang vanuit het perspectief van inlichtingen en veiligheid. Voor Defensie is cyberspace bovendien het vijfde domein voor militair optreden. Als ons land op het gebied van inlichtingen en veiligheid geen gelijke tred houdt met technologische ontwikkelingen neemt ook de waarde af die Nederland in de internationale samenwerking als partner vertegenwoordigt. Verschillende gelijkgestemde landen in Europa, waaronder Duitsland en Zweden, staan het verwerven van inlichtingen op de kabel al enkele jaren toe. Andere landen treffen voorbereidingen.

Een gezonde balans tussen privacy en veiligheid behoort tot de kern van de democratische rechtsorde in Nederland, die de diensten door hun taakuitvoering helpen beschermen. Met een goed waarborgenstelsel kan die balans ook in het digitale tijdperk worden getroffen.

Sebastian Reyn