Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2016–2017

34 372 Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)

33 542 Wijziging van het Wetboek van Strafvordering in verband met de regeling van het vastleggen en bewaren van kentekengegevens door de politie

E HERDRUK[1]

VERSLAG VAN EEN DESKUNDIGENBIJEENKOMST

Vastgesteld 11 juli 2017

De vaste commissie voor Veiligheid en Justitie[2] heeft op 20 juni 2017 een gesprek gevoerd met deskundigen over:

– privacy – in het kader van de wetsvoorstellen Vastleggen en bewaren kentekengegevens door politie (33 542) en Computercriminaliteit III (34 372).

Van dit gesprek brengt de commissie bijgaand geredigeerd woordelijk verslag uit.

De voorzitter van de vaste commissie voor Veiligheid en Justitie,
Duthler

De griffier van de vaste commissie voor Veiligheid en Justitie,
Van Dooren

[1] Letter E heeft alleen betrekking op wetsvoorstel 34 372; herdruk in verband met enkele redactionele aanpassingen.

[2] Samenstelling:
Engels (D66), Ruers (SP), Van Bijsterveld (CDA) (*vicevoorzitter*), Duthler (VVD) *(voorzitter),* Ten Hoeve (OSF), Koffeman (PvdD), Strik (GL), Knip (VVD), Backer (D66), Barth (PvdA), Beuving (PvdA), Hoekstra (CDA), Schouwenaar (VVD), Schrijver (PvdA), Van Strien (PVV), Kok (PVV), Gerkens (SP), Bredenoord (D66), Dercksen (PVV), D.J.H. van Dijk (SGP), Van Rij (CDA), Rombouts (CDA), Van de Ven (VVD), Wezel (SP), Bikker (CU), Baay-Timmerman (50PLUS)

kst-34372-E-n1
ISSN 0921 - 7371
's-Gravenhage 2017

Voorzitter: Duthler
Griffier: Van Dooren

Aanwezig zijn negen leden der Kamer, te weten:

Beuving, Bredenoord, Dercksen, Duthler, Gerkens, Rombouts, Strik, Van de Ven en Wezel,

en de volgende deskundigen:

Thema I: Noodzaak en belang van de voorgestelde wetgeving

J.W. Soeteman, NVSA (Nederlandse Vereniging van Strafrechtadvocaten)
M. Egberts en M.J. (Melanie) Nijenhuis, Openbaar Ministerie
V.A. Böhre, Stichting Privacy First
J.J. Oerlemans, Universiteit Leiden
H.L. de Vries, NCSC (Nationaal Cyber Security Centrum)
A.M. Arnbak, Universiteit van Amsterdam en advocaat De Brauw Blackstone Westbroek N.V.

Thema II: Te respecteren privacywetgeving, databescherming en Europees kader

A. Wolfsen, Autoriteit Persoonsgegevens
N. de Vries, Amnesty International Nederland
T. Bruning, NVJ (Nederlandse Vereniging van Journalisten)
M.M.C.G. Peters – Rathenau Instituut
F.J. Zuiderveen Borgesius, Universiteit van Amsterdam
B.J. Koops, Tilburg University en NIAS (Netherlands Institute for Advanced Study in the Humanities and Social Sciences)

Thema III: Uitvoerbaarheid en handhaafbaarheid

T.G. van der Plas en R. (Rogier) Rijpkema, Nationale Politie
A.G.M. Siedsma, Bits of Freedom
J.K.A. de Groot, Microsoft Benelux
L. Postma, Google
R. Prins, Fox-IT
B.P.F. Jacobs, Radboud Universiteit Nijmegen

Aanvang 9.03 uur.

Thema I: Noodzaak en belang van de voorgestelde wetgeving

De **voorzitter**:
Ik heet iedereen hartelijk welkom. Dat geldt uiteraard ook voor alle aanwezigen en belangstellenden. Aan de orde is het eerste blok, namelijk noodzaak en belang van de voorgestelde wetgeving. Ook een hartelijk welkom aan alle sprekers. Dat zijn de heer Soeteman van de Nederlandse Vereniging van Strafrechtadvocaten, de heer Egberts en mevrouw Nijenhuis van het Openbaar Ministerie, de heer Böhre van de Stichting Privacy First, de heer Oerlemans van de Universiteit Leiden, de heer De Vries van het Nationaal Cyber Security Centrum en de heer Arnbak van de Universiteit van Amsterdam en advocaat bij De Brauw Blackstone Westbroek N.V. Fijn dat u de moeite hebt genomen om hiernaartoe te komen en dat u zelfs position papers hebt geschreven. We werken vandaag met elevator pitches. Alle sprekers krijgen maximaal vijf minuten. Ik houd dat bij middels een timer. Als de vijf minuten voorbij zijn, wordt er gepiept. Volgens mij moet dit allemaal kunnen, zeker met de position papers, die we nog kunnen nalezen.

Deze deskundigenbijeenkomst past in de goede traditie van de vaste commissie voor Veiligheid en Justitie van deze Kamer. Daar waar er wetsvoorstellen aan de orde zijn die ingrijpen op grondrechten en op mensenrechten, en meer in het bijzonder op gegevensbescherming en privacy, plegen we nogal eens deskundigenbijeenkomsten te houden. Deze is daar een van. Wij hebben, zoals gezegd, vijf minuten per spreker. Ik stel voor dat ik u allemaal de gelegenheid geef om in vijf minuten uw punt te maken. Daarna geef ik de woordvoerders de gelegenheid om vragen te stellen. Ik stel voor om dat in blokjes van twee of drie vragen te doen. Ik hoop dat wij een heel goede discussie zullen krijgen.
Mijnheer Soeteman, u bent strafrechtadvocaat en voorzitter van de Nederlandse Vereniging van Strafrechtadvocaten. Van harte welkom. Mag ik u als eerste het woord geven?

De heer **Soeteman**:
Dank u wel voor deze uitnodiging. Ik zal me vandaag uitsluitend bezighouden met kentekens: het vastleggen en bewaren van de kentekens, de Automatic NummerPlate Recognition (ANPR). De voorgestelde wetgeving die hierop toeziet, brengt een vergaande en zorgelijke schending van de privacy van de burgers met zich mee. Ik zal dat uitsluitend vanuit het strafrechtelijk perspectief benaderen. Een aantal andere organisaties zal zich meer richten op de privacy en de schending van artikel 8 EVRM, een schending waarover wij ook zorgen hebben. Vandaag dus echter alleen het strafrechtelijk perspectief, omdat de gegevens die verzameld worden via ANPR ook nu al, zeker tien jaar, in het strafrecht worden gebruikt als bewijsmiddel, soms ontlastend, maar meestal belastend. Die ANPR-gegevens vormen dan een bewijsmiddel op basis waarvan de verdachte, de burger, wordt veroordeeld. Het moge voor eenieder duidelijk zijn dat daarvoor op dit moment een wettelijke grondslag ontbreekt. Dat is de afgelopen tien jaar eigenlijk door alle rechters vastgesteld, in lagere en hogere instantie.
Ondanks het feit dat die wettelijke grondslag ontbreekt en er dus sprake is van een schending van artikel 8 van het EVRM, het recht op privacy, staat de Hoge Raad toe dat die gegevens worden gebruikt. Ik wil vandaag met u spreken over dat facet van de overheid dat noodzakelijk is voor de burger, de advocaat en de verdachte, namelijk een betrouwbare overheid. De Hoge Raad zegt dat de ANPR-gegevens weliswaar een wettelijke grondslag ontberen, maar toch als bewijs mogen worden gebruikt in strafzaken. Daarom is het, sprekende over de noodzaak van de voorgestelde wetgeving, belangrijk dat die wetgeving er komt. Er moet immers wetgeving zijn, en die ontbreekt al zo lang.
De Hoge Raad zegt dus dat het bewijs mag worden gebruikt, ondanks het ontbreken van een wettelijke grondslag. Waarom? De Hoge Raad zegt dat de privacy wordt geschonden, maar dat daarmee nog niet het recht op een eerlijk proces wordt geschonden. Dat is heel iets anders in de ogen van de Hoge Raad. Verder zegt de Hoge Raad – dat is een wat lastiger onderbouwing – dat die gegevens, die zonder wettelijke grondslag zijn verzameld, niet zijn verzameld in een specifieke strafzaak tegen een specifieke verdachte. De individuele verdachte kan dan ook geen rechten ontlenen aan het feit dat de overheid de wet heeft overtreden. Feitelijk zegt de Hoge Raad, om het strafrechtelijk te duiden: het is goed dat de overheid gegevens die zij onrechtmatig verkrijgt, gebruikt. Eigenlijk zegt men: het is goed dat de overheid gegevens witwast. Daarom is het noodzakelijk dat er wetgeving komt.
Ik wil in het bijzonder aandacht vragen voor de zorg over de vernietigingsplicht. Het voorgestelde wetsartikel kent twee termijnen. Er is er een van vier weken op basis waarvan wordt gezegd dat de verzamelde gegevens vernietigd worden. In de toelichting op het besluit dat in maart door Minister Blok is toegezonden, staat dat het geautomatiseerd wordt vernietigd. Maar zoals de Nederlandse Orde van Advocaten in een brief

van 17 maart aan de Minister opmerkt, is geautomatiseerd vernietigen niet hetzelfde als automatisch vernietigen. Daar ligt wat mij betreft een grote zorg. Ervaringen uit het verleden op het gebied van DNA en de ANPR maken duidelijk dat de overheid een onbetrouwbare partner is als het gaat om het naleven van wetgeving. DNA moet worden vernietigd als een verdachte wordt vrijgesproken of niet wordt vervolgd, maar vaak doet de overheid dat niet om vervolgens wel bewust het DNA later weer te gebruiken in andere strafzaken. ANPR-gegevens liggen bij de Belastingdienst. Op dit moment liggen ongeveer 7 miljard foto's van kentekens bij de Belastingdienst; 7 miljard foto's die voor een deel ten onrechte niet door de Belastingdienst zijn vernietigd, ondanks de wettelijke plicht daartoe, en die ook worden gebruikt in belastingzaken.
Gelukkig heeft de Hoge Raad op 24 februari van dit jaar in fiscale zaken geoordeeld dat vanwege het ontbreken van een wettelijke grondslag om de ANPR-gegevens te verzamelen, de gegevens niet mogen worden gebruikt in fiscale zaken. De Hoge Raad heeft gezegd: het moet van het bewijs worden uitgesloten. De Hoge Raad maakt dus een belangrijk verschil. Bij het strafrecht zegt men «het is akkoord» en bij het fiscale recht zegt men: het moet van het bewijs worden uitgesloten. Het gaat er om dat het noodzakelijk is dat de vernietigingsplicht die bestaat, wordt nageleefd. Immers, de overheid heeft laten zien dat het niet gebeurt. Als dat het geval is, zal de burger het vertrouwen ook in deze wetgeving verliezen.
Eenzelfde opmerking kan ik maken over de driedagentermijn in de voorgestelde wetgeving waarbinnen een officier van justitie een mondeling gegeven bevel schriftelijk moet vastleggen. Ook daarvan zegt de Hoge Raad: als u zich niet aan die dagen houdt, ondervindt de verdachte daar geen schade van; zijn belangen worden daarmee niet geschaad. Als u in de Eerste Kamer deze wetgeving toestaat, moet men weten en ook zien dat er een sanctie is verbonden aan een overschrijding van de termijn.

De **voorzitter**:
Wat keurig, exact binnen vijf minuten! Hartelijk dank. Een overheid die gegevens witwast ... Ik vind het heel bijzonder. Ik geef graag het woord aan de heer Egberts. Mijnheer Egberts, u bent landelijk cibercrime-officier van justitie. U hebt vijf minuten. Mevrouw Nijenhuis, u hebt ook vijf minuten. U krijgt dus allebei vijf minuten. Het woord is eerst aan de heer Egberts.

De heer **Egberts**:
Geachte leden van de commissie voor Veiligheid en Justitie. Hartelijk dank voor de uitnodiging om namens het Openbaar Ministerie in te gaan op het belang van het wetsvoorstel Computercriminaliteit III. De voorzitter heeft mij en mijn collega net voorgesteld, dus ga ik meteen door.
Ik begin met een toelichting op het wetsvoorstel Computercriminaliteit III. Dat is een belangrijk en noodzakelijk wetsvoorstel, want dagelijks zie ik vanuit de praktijk dat de bestaande bevoegdheden voor de opsporing steeds minder effectief worden. Zonder wettelijke grondslag mag het Openbaar Ministerie geen inbreuk maken op iemands privéleven. Dat klinkt logisch en dat is het ook. De andere kant van de medaille is echter dat met die wettelijke grondslagen, het Openbaar Ministerie in staat moet zijn om zijn taken betreffende de opsporing, vervolging en preventie van criminaliteit goed te kunnen vervullen. Als de technologie de samenleving en de wereld verandert, zullen bevoegdheden mee moeten veranderen om te voorkomen dat er een vrijplaats komt voor criminaliteit. We zien steeds vaker situaties waarin cybercriminaliteit immateriële en zelfs fysieke zin gevolgen heeft. Recentelijk kon men zien dat een wereldwijde aanval met het WannaCry ransomwarevirus ertoe leidde dat afdelingen in ziekenhuizen sloten en dat bedrijven ontwricht werden. De opsporingsmo-

gelijkheden van politie en Openbaar Ministerie worden steeds minder effectief om dergelijke aanvallen op te sporen als er geen moderne bevoegdheden beschikbaar komen.
Ik en mijn collega's binnen het OM en de politie hebben steeds vaker het gevoel te vechten met onze handen op de rug. Een van de belangrijkste redenen hiervoor is het gemak waarmee criminelen technisch hoogwaardige versleutelingstechnieken gebruiken en zich succesvol anoniem online kunnen bewegen. Dit maakt de daders namelijk onvindbaar voor opsporingsdiensten. De gevolgen hiervan zijn niet onvindbaar of onzichtbaar voor burgers. Die worden namelijk het slachtoffer van ransomware, kinderporno, liquidaties of drugshandel.
De vraag in welke opsporingsonderzoeken er doelbewuste afscherming wordt tegengekomen, moet in feite worden omgedraaid. Er is geen cybercrimeonderzoek meer waarbij dit niet het geval is. Zelfs in veel reguliere opsporingsonderzoeken en bijna alle zwacri-onderzoeken zijn afscherming en versleuteling aan de orde van de dag. Een bekend en effectief voorbeeld van afscherming begint vaak bij het gebruik van, en ik benadruk dit maar even, het volstrekt legitieme VPN-netwerk: een dienst waarmee je een versleutelde verbinding opzet met een server waar dan ook ter wereld. Je gebruikt daarbij niet je eigen IP-adres, maar dat van de VPN-aanbieder. Omdat deze aanbieders in het algemeen bewust niet registreren welke klant op welk moment van hun IP-adres gebruikmaakt, kan er ook geen koppeling plaatsvinden. In de bijlage van de position paper van het OM is de werkwijze van de VPN-dienst in versimpelde vorm opgenomen. Ook wordt uitgelegd waarom deze dienst de opsporing zo bemoeilijkt.
Deze VPN-diensten worden in onderzoeken naar terrorisme, kinderporno en cybercrime veel teruggezien. Een ander voorbeeld is uiteraard de Onion Router, de Tor Browser, waarmee het dark web toegankelijk wordt. Deze dienst is ook niet ontworpen voor crimineel gebruik, maar er wordt inmiddels wel veel misbruik van gemaakt om zo anoniem mogelijk drugs, wapens en cybercrimetools te verkopen of te kopen. Niet alleen zijn de bezoekers niet te achterhalen, ook draaien de websites waar deze spullen worden verkocht, op zogeheten torhidden services, die vrijwel niet te lokaliseren zijn. Het is gewoon een vrijplaats om je drugs, wapens of andere tools te verkopen of te kopen, zonder dat het Openbaar Ministerie daar in feite iets aan kan doen.
Alle genoemde voorbeelden van afscherming zijn uiteraard niet illegaal om te gebruiken, integendeel. Veel van die diensten en producten dragen bij aan een veilige digitale infrastructuur. Alleen, criminelen maken dankbaar gebruik van deze diensten, waardoor regelmatig de bestaande opsporingsbevoegdheden niet meer toereikend zijn om ernstige feiten zoals terreur, kinderporno, cybercrime en georganiseerde criminaliteit op te sporen, bewijs te verzamelen en te kunnen vervolgen. Om beter op te kunnen treden tegen dit soort vormen van criminaliteit, is de bevoegdheid nodig om heimelijk en op afstand geautomatiseerde werken te betreden en zeer gericht data te verzamelen die relevant zijn voor onderzoek. Dat kan slechts een IP-adres zijn, maar het kan ook meer zijn. Deze mogelijkheid zal alleen worden ingezet bij verdenking van ernstige strafbare feiten en pas na een professionele toetsing binnen het Openbaar Ministerie en uiteraard een afweging en machtiging van de rechter-commissaris.
Het wetsvoorstel beperkt zich niet tot enkel die bevoegdheid. Ook heling van digitale gegevens wordt strafbaar gesteld. Door het strafbaar stellen van dit soort gegevens, het wederrechtelijk overnemen van die gegevens, worden gedragingen strafbaar die kunnen worden beschouwd als heling. Dit voorstel voorziet in een betere strafrechtelijke bescherming van computergegevens van ons allemaal.
U zult vandaag verschillende standpunten horen. Ik hoop dat u op het moment dat u over deze wet een afweging moet maken, zich rekenschap

geeft van de noodzaak voor politie en Openbaar Ministerie om überhaupt bewijs te kunnen verzamelen om misdrijven succesvol te kunnen vervolgen, iets wat we zonder deze wet in toenemende mate niet meer kunnen.

De **voorzitter**:
Hartelijk dank voor dit duidelijke verhaal. Mevrouw Nijenhuis in aanvulling hierop.

Mevrouw **Nijenhuis**:
Voorzitter, geachte leden van de commissie voor Veiligheid en Justitie. Ook ik dank u zeer voor de uitnodiging om hier uiteen te zetten hoe het OM aankijkt tegen het wetsvoorstel Vastleggen en bewaren van kentekengegevens door de politie. Het wetsvoorstel regelt dat de politie met ANPR-camera's de kentekens van alle passerende voertuigen mag vastleggen, gedurende vier weken mag bewaren en daarna onder strikte voorwaarden in deze gegevens mag zoeken nadat zich een ernstig strafbaar feit heeft voorgedaan, om na te gaan of er een relatie is tussen dat strafbare feit en bepaalde voertuigbewegingen. Denk bijvoorbeeld aan ontvoering of een ander ernstig misdrijf. Na een melding kan de politie op basis van het voorliggende wetsvoorstel terugkijken in de ANPR-gegevens en zo zien of het kenteken of het voertuig dat door getuige is genoemd, langs de ANPR-camera's is gereden. Op basis daarvan kan in een verder onderzoek naar de verblijfplaats van verdachten of slachtoffers worden gefocust op een kleiner geografisch gebied of specifieke voertuigen. Zo kan tot een effectievere inzet of een sneller resultaat worden gekomen en wellicht ook tot een snellere vondst van daders of slachtoffers, voor het te laat is. Zonder dit wetsvoorstel is er geen mogelijkheid om ANPR-gegevens te bewaren en kan er dus ook niet worden teruggezocht in deze gegevens.
Tot nu toe was het alleen mogelijk om situaties op het spoor te komen met betrekking tot voertuigen die al voorafgaand aan het plegen van een strafbaar feit in de aandacht stonden, namelijk door middel van referentiebestanden. Dat zijn lijsten van kentekens van bijvoorbeeld een auto die gestolen is of waarvan de eigenaar een rijontzegging heeft. Als er een hit is, wordt zo'n hit opgeslagen. De hits leiden tot vervolgacties van de politie. Ook kan ANPR op grond van criteria die de Hoge Raad heeft uitgekristalliseerd, worden ingezet. Bijvoorbeeld bij een hausse aan woninginbraken kunnen in een bepaald gebied met een projectplan en een vast omschreven periode kentekengegevens in de toekomst worden opgeslagen om aan de hand daarvan daders van inbraken te kunnen identificeren. Dat is iets anders dan wat het wetsvoorstel biedt, want dat biedt een bewaarmogelijkheid om terug te kijken.
Zoals ik al zei, voorziet de huidige wetgeving niet in een direct alternatief voor hetgeen het wetsvoorstel biedt. Als nu van een voortvluchtige of een verdachte alleen een kenteken of een voertuig bekend is, kan niet worden teruggerechercheerd op het kenteken. Zonder intensief speurwerk is niet te achterhalen waar het voertuig is geweest voorafgaand aan het strafbare feit. Camerabeelden van particulieren opvragen is zoeken naar een speld in een hooiberg en elke splitsing in een weg maakt het onderzoek ingewikkelder. Die onderzoeksmethode levert bovendien vaak niets op.
Samenvattend wil ik de Kamer meegeven dat dit wetsvoorstel volgens het OM noodzakelijk is en dat die noodzaak gelegen is in een effectieve en doelmatige opsporing. Bovendien gaat het volgens het OM in dit wetsvoorstel om een afgebakende, beperkte bewaarperiode, een strikte doelbinding, een toets van een officier van justitie en raadpleging door geautoriseerde en opgeleide opsporingsambtenaren die niet met het onderzoek belast zijn.

De **voorzitter**:

Hartelijk dank voor dit duidelijke verhaal. Het standpunt is duidelijk. Ik heb voornamelijk positieve reacties gehoord op het wetsvoorstel, weliswaar met kanttekeningen. Ik ga snel naar de volgende sprekers. Ik geef graag het woord aan Vincent Böhre, directeur van de Stichting Privacy First.

De heer **Böhre**:
Dank voor uw uitnodiging voor deze bijeenkomst. Net als in onze position paper zal Privacy First tijdens deze bijeenkomst vooral ingaan op het wetsvoorstel over ANPR. Dit wetsvoorstel vormt immers de voornaamste reden waarom u ons hebt uitgenodigd. Reeds sinds de indiening van het oorspronkelijke voorstel van Minister Hirsch Ballin in 2010 om ieders kentekendata oftewel locatiedata op te slaan voor opsporing en vervolging, heeft Privacy First het standpunt ingenomen dat een dergelijk voorstel volstrekt onrechtmatig is wegens gebrek aan noodzaak en proportionaliteit. Dit standpunt wordt inmiddels bevestigd door Europese rechtspraak. Mocht het wetsvoorstel desondanks tot wet verheven worden, dan zal Privacy First het onverbindend laten verklaren wegens strijd met artikel 8 EVRM. Privacy First heeft dat de laatste jaren diverse malen kenbaar gemaakt aan zowel de Tweede Kamer als aan Minister Opstelten en Minister van der Steur persoonlijk.
Bij onze meeting met Minister Opstelten in juli 2013 waren tevens het Nederlands Juristen Comité voor de Mensenrechten en de Vereniging Privacy Recht kritisch aanwezig. Op het vooruitzicht van een rechtszaak tegen het wetsvoorstel ANPR reageerde Minister Opstelten destijds als volgt. «De rechter voert de wetgeving uit.» Alsof de rechterlijke macht slechts een verlengstuk van de uitvoerende macht zou zijn. Privacy First antwoordde daarop dat de rechter tevens nationale wetgeving toetst aan internationale verdragen. Daarna viel er een pijnlijke stilte bij Opstelten en diens topambtenaren. Bij latere meetings met deze ambtenaren heeft Privacy First zich overigens nooit aan de indruk kunnen onttrekken dat hun verdediging van het wetsvoorstel enigszins contrecoeur was. Dit was de laatste jaren ook het geval met wetten die op vergelijkbare wijze massale privacyschendingen teweeg zouden brengen, waaronder de opslag van ieders vingerafdrukken onder de Paspoortwet. Eind 2010 was er in heel Nederland geen ambtenaar meer te vinden die dat nog publiekelijk durfde te verdedigen. De maatschappelijke weerstand tegen dergelijke opslag was en is groot. Zowel de opslag van ieders vingerafdrukken als de opslag van ieders telecommunicatiedata is inmiddels door diverse hoogste rechters in Europa onrechtmatig verklaard. Privacy First hoopt dat het met dit wetsvoorstel ANPR niet zover zal hoeven komen. Hierbij verzoeken wij de Kamer dan ook om dit wetsvoorstel te verwerpen.
Dan nog kort enkele opmerkingen over het wetsvoorstel Computercriminaliteit III. Evenals bij het wetsvoorstel ANPR is bij dit wetsvoorstel nooit sprake geweest van een grondige en onafhankelijke privacy-impactassessment. Beide wetsvoorstellen lijken vooral gedreven door technologisch determinisme. Alles wat technisch kan, wordt wettelijk mogelijk gemaakt. Evenals bij het wetsvoorstel ANPR zijn de vereiste maatschappelijke noodzaak en proportionaliteit tot op heden echter nooit hard aangetoond. Van enige inperking in technologische zin is bewust geen sprake. De werking van het wetsvoorstel zal zich uitstrekken tot alles wat met het internet in verbinding staat. In de toekomst dus vrijwel de gehele maatschappij, waaronder het Internet of Things, vitale infrastructuur en medische systemen. In politiekringen wil men zelfs rijdende auto's kunnen hacken en stilzetten, met alle gevaren van dien voor de verkeersveiligheid.
Het gebruik en misbruik van onbekende ICT-kwetsbaarheden wordt bovendien nauwelijks ingedamd en de misdrijven waarbij dit wetsvoorstel kan worden ingezet, kunnen voortdurend worden uitgebreid bij algemene maatregel van bestuur. Dat is geen privacy by design, dat is function

creep by design. Privacy First verzoekt uw Kamer dan ook om dit wetsvoorstel eveneens te verwerpen.

De **voorzitter**:
Hartelijk dank, mijnheer Böhre. Keurig binnen de tijd. Ik geef snel het woord aan Jan-Jaap Oerlemans, onderzoeker aan de Universiteit van Leiden en gepromoveerd op het onderwerp cybercrime.

De heer **Oerlemans**:
Hartelijk dank voor de uitnodiging. Dit wetsvoorstel heeft zijn oorsprong in 2009. Destijds stuurde de Minister een brief aan de Tweede Kamer. Daarin legde hij uit dat anonimiteit en versleuteling cybercrime-onderzoeken bemoeilijkten. Hij schreef dat de mogelijkheden werden onderzocht om een online doorzoeking mogelijk te maken, omdat dat zou helpen om cybercrime op te sporen en te bestrijden. De voorgestelde hackbevoegdheid in het wetsvoorstel Computercriminaliteit III biedt inderdaad de mogelijkheid om deze twee problemen van anonimiteit en versleuteling tegen te gaan, in het bijzonder door het mogelijk maken van onlinedoorzoeking en het plaatsen van software om de bron, de computer en daarmee het gedrag achter de computer, te monitoren. Pas in het concept van het wetsvoorstel uit 2013 is erkend dat een expliciete grondslag noodzakelijk is. De hackbevoegdheid moest dus worden gecreëerd in het Wetboek van Strafvordering. In de toelichting op het wetsvoorstel en in de nota naar aanleiding van het verslag wordt mijns inziens goed uitgelegd waarom de hackbevoegdheid noodzakelijk is.
In het kader van mijn proefschriftonderzoek, waarmee ik me meer dan zes jaar heb beziggehouden, heb ik dossiers en literatuur onderzocht. Op basis daarvan ben ik tot de conclusie gekomen dat de hackbevoegdheid inderdaad noodzakelijk kan zijn in cybercrime-onderzoeken. Tegelijkertijd moet worden gerealiseerd dat de voorgestelde hackbevoegdheid een paraplubevoegdheid is. Dus na het op afstand binnendringen in een geautomatiseerd netwerk kunnen andere opsporingsmethoden worden ingezet, zoals het vastleggen van gegevens, het uitvoeren van observatie, het direct afluisteren en het ontoegankelijk maken van gegevens. De software die daarvoor kan worden gebruikt, biedt een breed scala aan functionaliteiten, zoals het vastleggen van toetsaanslagen, het maken van screenshots, het aanzetten van een microfoon of camera of het aanzetten van de GPS-functionaliteit. De bevoegdheid kan in sommige gevallen dus omschreven worden als een combinatie van een inkijkoperatie, een heimelijke doorzoeking en afluisteren ineen. Dat is ook de reden dat strikte waarborgen nodig zijn bij het toepassen van de bevoegdheid.
Deze waarborgen zijn ook in het wetsvoorstel geïmplementeerd. Zorgelijker vind ik de bevoegdheid om het middel ook in te zetten voor handhavingsdoeleinden. In de memorie van toelichting wordt duidelijk gemaakt dat de bevoegdheid ook kan worden ingezet voor verstoringsacties. Daarbij moet meer expliciet worden gedacht aan het onklaar maken van het botnetinfrastructuur van een nog onbekende verdachte of het ontoegankelijk maken van kinderpornografie op onlinefora. Op zichzelf kan de wetgever het wenselijk achten autoriteiten meer bevoegdheden te geven om cybercrime beter te handhaven. Waar het mijns inziens echter aan ontbreekt, is controle achteraf. Mijn inschatting is dat cybercrime-onderzoek in deze operaties in veel gevallen niet leidt tot vervolging van de dader. In dat geval is er geen zittingsrechter die oordeelt over de rechtmatigheid van het gebruik van de opsporingsmethode en is de kans gering dat de betrokkenen gebruikmaken van de bestaande klachtprocedure.
Een soortgelijke zorg heb ik bij de takedownbevoegdheid in artikel 126p uit het wetsvoorstel. De bevoegdheid kan worden ingezet bij meer ernstige misdrijven. Gelukkig moet de rechter-commissaris een machtiging geven voor de inzet van de bevoegdheid. Maar realiseren wij

ons wel dat het ontoegankelijk maken van online-informatie in de meest extreme vorm leidt tot een internetblokkade op het niveau van IP-adressen en wat dat voor ons betekent? Ik vraag mij bijvoorbeeld af of deze bevoegdheid van een takedownbevel na verloop van tijd leidt tot een zwarte lijst van websites die Nederlandse accesproviders en hostingproviders moeten blokkeren. Het is veelzeggend dat het College van procureurs-generaal in een advies over een oudere versie van het wetsvoorstel waarschuwt voor een censurerende internetpolitie. Natuurlijk moeten er in het kader van subsidiariteit eerst andere stappen worden gezet en kan pas in de laatste plaats het materiaal bij de internetaccesprovider worden geblokkeerd, maar net als bij het wetsvoorstel Computercriminaliteit III vraag ik mij af of uiteindelijk een zittingsrechter zal oordelen over de rechtmatigheid van de bevoegdheid en of er gebruikgemaakt wordt van de klachtprocedure. Ook hier is toezicht achteraf noodzakelijk.
Hierover wil ik nog zeggen dat Staatssecretaris Dijkhoff zich ervoor heeft ingespannen om de Inspectie Veiligheid en Justitie meer mogelijkheden te geven om de hackbevoegdheid te controleren. Die controle ziet echter niet op de rechtmatigheid van de inzet van die hackbevoegdheid. Juist die toets op rechtmatigheid vind ik van belang. Ik ben ook niet de enige die dit heeft gezegd. Verschillende Tweede Kamerleden hebben dat ook gesuggereerd en, niet onbelangrijk, het Kenniscentrum Cybercrime van het Gerechtshof Den Haag heeft dat ook gezegd.
Resumerend. De bevoegdheid tot hacken en takedownbevel zijn potentieel machtige instrumenten van de overheid om cybercrime en digitaliserende criminaliteit beter te bestrijden. Met de voorwaarden voor de inzet van deze bevoegdheden zit het wel goed. Het is echter onduidelijk op welke schaal en met welke gevolgen de bevoegdheden in de toekomst worden ingezet. Dat vereist ook toezicht achteraf.

De **voorzitter**:
Hartelijk dank voor dit eveneens duidelijke verhaal. Het zal ongetwijfeld wat vragen oproepen, maar daar hebben we straks ruimschoots de gelegenheid voor. Ik geef graag eerst het woord aan de heer De Vries. Hij is hoofd van het NCSC, het Nationaal Cyber Security Centrum.

De heer **De Vries**:
Goedemorgen. Uiteraard wil ik mijn dank uitspreken voor de mogelijkheid om vanuit mijn rol als hoofd van het Nationaal Cyber Security Centrum bij te dragen aan deze hoorzitting. Zoals u in mijn schriftelijke inbreng hebt kunnen zien, nemen wij als NCSC een bijzondere en centrale rol en positie in op het gebied van cyber security in Nederland. Onderdeel van deze rol is dat wij het Cybersecuritybeeld Nederland maken. Dat doen wij samen met diverse spelers in het veld, onder verantwoordelijkheid van de NCTV, de Nationaal Coördinator Terrorismebestrijding en Veiligheid. Daarmee maken wij een onafhankelijk en feitelijk dreigingsbeeld ten behoeve van besluitvorming. Wat mij betreft is het dreigingsbeeld zeer relevant als we kijken naar nut en noodzaak van de voorgestelde wet- en regelgeving. Dat is ook de reden dat het CSBN jaarlijks aan de Tweede Kamer wordt aangeboden. Dat zal later deze week ook weer gebeuren met de editie van 2017. Ik hoop dat u mij permitteert dat ik formeel verwijs naar de editie van 2016. Ik kan u echter al wel aangeven dat het nieuwe dreigingsbeeld niet substantieel veranderd is ten opzichte van het CSBN 2016 waarnaar ik verwees.
Zoals u ook al zag in mijn schriftelijke inbreng, is de dreiging in het digitale domein zeer serieus en realistisch. Wij kunnen het ons niet veroorloven om achterover te leunen. De komende jaren zullen we extra stappen moeten zetten. Ik zal u eerlijk zeggen dat ik, als ik verkeerde bedoelingen had gehad, wel cybercrimineel zou zijn geworden en geen klassieke bankrover. De potentiële opbrengsten zijn hoog en de kans om

opgepakt te worden bij een ramkraak is een stuk groter dan bij relatief veilig achter een anonieme pc zitten.
Laat me dit illustreren met feiten uit het CSBN. De afgelopen jaren viel op dat cybercriminelen bereid zijn om veel tijd te investeren in voorbereiding van digitale aanvallen. Dit was bijvoorbeeld te zien bij Carbanak, een geavanceerde aanval op Oost-Europese banken. Via malware konden de criminelen de activiteiten van bankmedewerkers lange tijd digitaal observeren, zodat de criminelen uiteindelijk grote sommen geld naar bankrekeningen konden overmaken en geldmachines konden manipuleren. Niet alleen tonen cybercriminelen meer geduld in de uitvoering van hun activiteiten en zijn ze goed georganiseerd, ook worden ze creatiever in het verzilveren van de gestolen gegevens. In de Verenigde Staten onttrokken aanvallers met een zeer gerichte malwarecampagne beursgevoelige informatie aan de farmaceutische sector. Op basis daarvan was het mogelijk om koersen te voorspellen.
U ziet het al, de businesscase van cybercriminelen werkt. Sterker nog, cybercriminelen specialiseren zich en werken uitstekend samen. Onze collega's van politie en OM kunnen u vast nog meer vertellen over hun ervaringen. Wat ik vanuit de mijne aan deze hoorzitting wil bijdragen, is dat er sprake is van een realistische dreiging en dat dit iets is waar wij als maatschappij een antwoord op dienen te vinden. Vanuit ons werk als Nationaal Cyber Security Centrum zijn we daar dag in, dag uit mee bezig. Gelukkig weten we partijen vaak tijdig te informeren, waardoor ze zich kunnen beveiligen, maar ook dan zal er sprake zijn van incidenten. Voorkomen is beter dan genezen, maar als er een incident is, dan is het van belang om als overheid over de juiste middelen te beschikken om de daders te kunnen achterhalen. Uiteraard kan het nooit alleen gaan over opsporing en moeten we er in de breedte voor zorgen dat Nederland een digitaal veilige plek is. Daarom is het dus van belang om nu en in de toekomst in te zetten op het verhogen van cybersecurity en het bestrijden van cybercrime.

De **voorzitter**:
Heel hartelijk dank, ruimschoots binnen de vijf minuten. Mijnheer Arnbak, u bent de laatste spreker in de rij. U bent zowel onderzoeker als advocaat, dus u past de wet ook toe in de praktijk. Wij zijn benieuwd naar uw visie.

De heer **Arnbak**:
Hartelijk dank. Onder het toeziend oog van Koning Willem II voel ik mij een beetje alsof ik in een aflevering van De Wereld Draait Door ben beland, met deze stopwatch. Ik zal het daarom ook kort houden. Mijn inbreng ziet u al in de klapper. Ik wilde graag een fundamenteel punt aansnijden en wat praktische adviezen geven aan de Eerste Kamer. U bent toch de chambre de réflexion, de grondrechtenwaakhond in ons constitutionele bestel. In Nederland hebben wij helaas geen Bundesverfassungsgericht zoals onze oosterburen. Daar is de Online-Durchsuchung met – ik wil dit zo graag een keertje zeggen – Bundestrojaner, wat een eng woord is dat toch, verpulverd door het constitutioneel hof aldaar. De hackbevoegdheid op zichzelf is daar niet ongrondwettig verklaard, maar er zijn al in 2008 heel interessante waarborgen ontwikkeld die hier in het parlementaire debat nog niet echt aan de orde zijn gekomen. U bent in de Senaat ons Bundesverfassungsgericht en ik zal daarom een aantal van die waarborgen even bespreken. Die waarborgen zijn overigens ook relevant in de bredere herziening van het Wetboek van Strafvordering die momenteel in behandeling is.
Door het Bundesverfassungsgericht is een nieuwe categorie ontwikkeld die ook door het Kenniscentrum ICT reeds in de Eerste Kamer is besproken, namelijk het hacken over de grens en dat dat zo ongeveer alleen bij acuut gevaar voor lijf en leden mag. Als Nederlandse opsporingsautoriteiten over de grens gaan hacken, is dat een schending van het

internationaal recht, tenzij er acuut gevaar voor lijf en leden is. Dat is eigenlijk een waarborg die we in het Wetboek van Strafvordering nog niet kennen en het is interessant om daar verder onderzoek naar te doen. Hoe zit dat internationaalrechtelijk en kan de Nederlandse wetgever iets met die waarborg?
Een ander fundamenteel punt – ik wil graag de inbreng van Jan-Jaap Oerlemans verder brengen, hij had helaas zelf maar vijf minuten – is het toezicht achteraf. Ook daar kwamen de rechters zelf mee. We zagen dat wij in Nederland goed zijn in het treffen van waarborgen die zien op het proces. Dat blijkt bijvoorbeeld uit het CIOT, de databank die is opgericht voor telecommunicatiegebruikersgegevens, maar ook uit het aftappen. Dat wij goed zijn in dat soort waarborgen – dus de toestemming van de rechter-commissaris, de procedurele waarborgen – ligt denk ik in onze cultuur besloten. Daarentegen hebben wij niet zo veel met inhoudelijke waarborgen zoals de net genoemde waarborg van het Duitse constitutionele hof van acuut gevaar voor lijf en leden. Deze proceduralisatie van surveillancewaarborgen hebben mijn collega Frederik Borgesius, die in het volgende blokje komt te spreken, en ik beschreven in een paper dat ik nog niet in de klapper zag, maar dat volgens mij wel onder uw leden wordt gedistribueerd door de griffier.
Dan de technologie. Het WannaCry-incident kwam al ter sprake. WannaCry is er nu net een uitstekend voorbeeld van hoe het niet-rapporteren van kwetsbaarheden juist heeft geleid tot een mondiale cyberaanval. Omdat dit wetsvoorstel al zo ontzettend lang in voorbereiding is, zijn er in de parlementaire behandeling al heel innovatieve stappen gezet bij het melden van kwetsbaarheden. Wij zien ook – dat zie ik in de dagelijkse praktijk als advocaat – dat het Nederlandse Team High Tech Crime uitstekende mensen heeft die zich ook in het opsporingsonderzoek zelf zeker verwittigen van dit soort belangen. Alleen gaan de stappen die de wetgeving zet op dat gebied in mijn optiek nog niet ver genoeg. Zo is bijvoorbeeld het gebruik van commerciële spyware zoals de FinFisher-spyware, aangeschaft bij organisaties als FinFisher, nog niet gereguleerd. Het is goed om zich te realiseren dat dat bij internetserviceproviders op een vrij hoog niveau in het netwerk wordt geïnstalleerd. Met dat soort spyware installeer je dus in het netwerk, op een vrij hoog niveau – dus ergens waar het veel gebruikers kan treffen – fundamentele kwetsbaarheden, waar cybercriminelen juist gebruik van kunnen maken. Dat is ook iets om verder te onderzoeken, voordat u uw goedkeuring verleent aan deze wetgeving.
Ten slotte kom ik bij een eerdere hoorzitting die we hier hebben gehad. De Snowden-onthullingen waren net geweest en we hebben hier toen gesproken over cyberintelligence en het publieke belang. Op basis van uitstekend werk van de Eerste Kamer is toen een vijftal moties aangenomen, onder andere over het subsidiëren van OpenSSL en het verbieden van backdoors. Dat was nu echt een voorbeeld van visie van de Eerste Kamer en de kans om die visie te tonen hebt u ook met dit wetsvoorstel. Dus afsluitend: u bent een hoeder van de grondrechten, vergeet dat niet, maar ook voor het vestigingsklimaat in Nederland is het van belang om dit soort zaken serieus te nemen. De hackbevoegdheid moet er misschien komen, maar gebruik dit als aanleiding om het echt goed te organiseren in Nederland.

De **voorzitter**:
Heel hartelijk dank voor deze boeiende inleiding en de vele gezichtspunten. De Senaat als Bundesverfassungsgericht, nou, we hebben er weer iets bij gekregen, leuk. Ik geef nu graag het woord aan de leden om vragen te stellen. Ik wil dat doen in blokjes van twee of drie. Kijkt u even of de vraag die u hebt, aansluit bij de spreker en als u een vraag stelt, wilt u er dan ook bij vermelden aan wie u de vraag stelt? Zijn er überhaupt vragen? Ik kan me niet voorstellen dat die er niet zijn. Ik zie mevrouw

Strik, de heer Van de Ven, mevrouw Gerkens en mevrouw Bredenoord, bijna iedereen. Ik begin met mevrouw Strik.

Mevrouw **Strik** (GroenLinks):
Hartelijk dank aan alle sprekers voor een mooi pallet aan verschillende standpunten en informatie. Ik heb een vraag over de ANPR voor de heer Böhre en mevrouw Nijenhuis. De heer Böhre zei, gelet op jurisprudentie van het hof van justitie – ik denk dat hij de Dataretentierichtlijn bedoelt – maar wellicht ook jurisprudentie van het EHRM moet dit wetsvoorstel vernietigd worden en is het ongeldig, gelet op de privacyregels van de EU en artikel 8 EVRM. Maar mevrouw Nijenhuis gaf aan dat het noodzakelijk is om terug te kunnen kijken en misdrijven op te kunnen sporen, en dat is beperkt in de tijd. Ik zou het prettig vinden als u zou willen aangeven of dit wetsvoorstel ten aanzien van de argumenten noodzaak, effectiviteit en privacy daadwerkelijk lijkt op bijvoorbeeld de bewaarplicht die we hebben gehad en die hierdoor onder vuur is komen te liggen. Van mevrouw Nijenhuis hoor ik graag een reactie op de stelling van de heer Böhre dat die in strijd is met EU-wetgeving. Ik vraag haar met name om in te gaan op het arrest over de Dataretentierichtlijn.

De **voorzitter**:
Hartelijk dank. Zijn er andere woordvoerders die een vraag hebben die hierop aansluit? Dat is niet het geval. Dan geef ik eerst het woord aan de heer Böhre en daarna aan mevrouw Nijenhuis.

De heer **Böhre**:
Ik kan er best kort over zijn. Bij de dataretentiearresten ging het ook om locatiedata, deels, en om de massale opslag van ieders locatiedata. Die werd onrechtmatig verklaard door het Europees Hof van Justitie, tweemaal, eerst in de zaak-Digital Rights in 2014 en daarna in de zaak-Tele2 eind 2016. Als je dat arrest leest, staat daar eigenlijk een heel duidelijk richtsnoer in voor de toekomst, namelijk: de massale ongerichte opslag van data van onschuldige burgers is simpelweg niet meer toegestaan. Het moet heel gericht zijn, in tijd, in locatie, maar ook gericht op strafrechtelijk relevante personen en dus niet onschuldige mensen. Dat zijn best harde voorwaarden.
Die jurisprudentie is deels geïnspireerd door eerdere jurisprudentie van het Europees Hof voor de Rechten van de Mens. Ik denk dat hier met name de zaak-S & Marper tegen het Verenigd Koninkrijk uit 2008 relevant is. De zaak M.K. tegen Frankrijk van een paar jaar later is ook relevant. Die ging over de massale opslag van ieders vingerafdrukken. Daarvan zei het Hof in Straatsburg toen: dat is disproportioneel en inadequaat. Dat is een iets minder bekende zaak, maar zeker zo relevant. Dus ja, voor ons is het eigenlijk klip-en-klaar dat de massale ongerichte opslag van ANPR-data en daarmee ieders locatiedata, van alle automobilisten in Nederland, simpelweg niet door de beugel kan. Hoe je dat dan heel gericht alsnog zou moeten willen of kunnen optuigen, is voor ons op dit moment ook een vraag.
Die vraag speelt nu ook op het gebied van dataretentie. Daar wordt ook over nagedacht op Europees niveau, door de Europese Commissie, door de EU-lidstaten, waar ook onderlinge consultaties gaande zijn. Wij hebben het idee dat men momenteel een beetje met de handen in het haar zit over hoe men in de toekomst alsnog weer massale dataretentie zou kunnen gaan optuigen. Het kan namelijk eigenlijk niet. Dat moet dan maar de conclusie zijn.

De **voorzitter**:
Goed, duidelijk. Dank u wel. Mevrouw Nijenhuis.

Mevrouw **Nijenhuis**:

Ik denk dat de heer Böhre al vrij goed heeft aangegeven om welke punten het draaide in het Europees arrest. Dit wetsvoorstel voorziet, anders dan waar het in dat arrest om ging, in een heel gerichte opslag van data, namelijk alleen data van de vervoersbewegingen van kentekens die langs de ANPR-camera's komen in Nederland. Bovendien worden die voor een beperkte periode opgeslagen. Die 28-dagentermijn is er naar aanleiding van eerdere behandelingen in de Tweede Kamer zo in gekomen. Ook gaat het – ik heb dat in mijn samenvatting al genoemd – om heel specifieke vereisten waaraan voldaan moet worden voordat specifieke, daarvoor geautoriseerde en getrainde opsporingsambtenaren daar toegang toe hebben. Het is niet zo dat je voor iedereen daarin mag gaan graven of grasduinen. Het moet gaan om iemand die verdachte is en dan kan een opsporingsambtenaar een vordering doen bij de officier van justitie en kan er gezocht gaan worden. Ik wil ook graag verwijzen naar hetgeen al eerder is gewisseld, onder andere in de memorie van toelichting over dit wetsvoorstel, ten opzichte van dat eerdere Europese arrest dat genoemd is.

De **voorzitter**:
Hartelijk dank. Ik zag dat de heer Van de Ven een vraag heeft.

De heer **Van de Ven** (VVD):
Op de eerste plaats wil ik de deskundigen hartelijk danken voor hun komst naar deze Kamer. Dat geldt voor de deskundigen die ik al gehoord heb, maar ook voor degenen die ik nog zal horen. Ik wil mij beperken tot de Wet computercriminaliteit III. Bij mijn voorbereiding op deze deskundigenbijeenkomst heb ik mij afgevraagd of ik een rode draad kan vinden, een leidraad, voor het stellen van vragen. En die heb ik gevonden in het begrip schade: onrechtmatige daad, schade en schadevergoeding. Mijn vraag in de drie themablokken zal zich richten op schade. Ik zal dat even kort toelichten. Als ik iemand toesta om mijn elektronische agenda op mijn computer binnen te dringen, dan is daarbij niet sprake van iets onrechtmatigs. Ik stem daarin toe, maar toch is er sprake van binnendringen. Als er sprake is van binnendringen zonder dat ik mij dat realiseer, dan kan dat leiden tot een onrechtmatige daad en het voorstel van wet computercriminaliteit III probeert daar de nationale politie een rechtsbasis voor te geven en dat te legitimeren. Het onderwerp schade is eigenlijk vrij beperkt aan de orde gekomen. In de nota naar aanleiding van het verslag in de Tweede Kamer, op bladzijde 69, is er enkel een korte passage aan gewijd, maar ik vind het toch van belang hoe dit van invloed is op het geheel. Ik heb een vraag aan de heer Oerlemans en die vraag is tweeërlei. Welke mogelijkheden hebben derden om schade te verhalen die wordt veroorzaakt door hacks door de nationale politie? Is het aantonen van onrechtmatige overheidsdaad in dezen realistisch en haalbaar? En mijn tweede vraag is: wat zou moeten worden veranderd of toegevoegd om dit wel mogelijk te maken?

De **voorzitter**:
Ik had eerder gezegd dat ik een blokje zou doen van drie vragen. Als u uw antwoord nog even kunt inhouden, dan geef ik mevrouw Beuving het woord voor de vraag die zij heeft.

Mevrouw **Beuving** (PvdA):
Ik heb aan een andere persoon een vraag. Ik weet niet of u nu vragen aan het verzamelen bent?

De **voorzitter**:
Nee, dat is goed.

Mevrouw **Beuving** (PvdA):

Mijn vraag is primair gericht aan de heer De Vries en ik denk dat die ook heel geschikt is voor de heer Egberts, maar ik sluit aan bij een formulering van de heer De Vries, dus vandaar dat ik mij primair aan hem richt. Ik hoorde de heer De Vries zeggen: het gaat erom dat Nederland een digitaal veilige plek wordt. Ik kan mij zo voorstellen dat dat ook het streven is van het Openbaar Ministerie. Wat ik zo interessant vind, is dat met name de heer De Vries in die context en eigenlijk in zijn hele bijdrage heel weinig zei over concreet dit wetsvoorstel. Misschien ligt dat aan de aard van zijn instelling, maar ik wil daarop wel wat doorvragen, want ik heb heel goed geluisterd – ik denk dat iedereen hier het doel van Nederland als digitaal veilige plek deelt, maar wij moeten vooral het nu voorliggende wetsvoorstel beoordelen, de Wet computercriminaliteit III. Ik wil dus eigenlijk aan de heer de Vries en ook aan de heer Egberts vragen wat zij van bepaalde kanten van het wetsvoorstel vinden. Ik bedoel het feit dat, als het wetsvoorstel wordt aangenomen, Nederlandse opsporingsinstanties gebruik kunnen gaan maken van kwetsbaarheden in software en dat zij er in feite ook belang bij gaan krijgen dat die kwetsbaarheden er zijn en dat die gebruikt kunnen worden. Dan hebben we het over software die niet specifiek door Nederlandse criminelen wordt gebruikt, maar software die wij allen gebruiken, Nederlandse burgers en Nederlandse bedrijven, in plaats van dat de enige doelstelling waar de overheid voor gaat, het dichten van dergelijke kwetsbaarheden is. Dat vind ik een interessant iets, juist in het kader van het streven om Nederland een digitaal veilige plek te maken. Hoe past dit gebruik van de overheid van dergelijke kwetsbaarheden in dat streven?

De **voorzitter**:
Hartelijk dank. Ik zie dat mevrouw Bredenoord nog iets wil zeggen.

Mevrouw **Bredenoord** (D66):
Ik denk dat mijn eerste vraag aansluit bij wat mevrouw Beuving vroeg. De heer Egberts noemde inderdaad WannaCry als een voorbeeld van moderne cybercrimeaanvallen. De heer Arnbak gaf het al aan: is dit nu juist niet het voorbeeld voor het in stand houden van fundamentele kwetsbaarheden dat met deze wet mogelijk zou worden gemaakt? Ik ben benieuwd of hij daar nog op wil reageren.
Ik vraag me nog iets anders af. Door Internet of Things zijn er steeds meer apparaten die vallen onder «geautomatiseerd werk» Op een gegeven moment valt nagenoeg je hele huis onder dat geautomatiseerd werk. Als je de Europese principes van privacy of databescherming by design zou volgen, waarom zou je dan niet werken met een lijst van limitatieve opsommingen? Ik ben benieuwd of bijvoorbeeld iemand van het OM en de heer De Vries daarop zouden kunnen reageren.

De **voorzitter**:
Iemand van het OM of de heer De Vries? Aan wie stelt u de vraag?

Mevrouw **Bredenoord** (D66):
Ik zou eigenlijk het liefst zien dat ze alle twee reageren.

De **voorzitter**:
Zo veel tijd hebben we niet. U moet kiezen.

Mevrouw **Bredenoord** (D66):
Dan de heer De Vries.
De heer Oerlemans maar ook anderen hebben in hun schriftelijke inbreng aangegeven dat het toezicht met name achteraf onvoldoende is. Wat is er nodig? Ik hoor daarop graag een reactie van de heer Arnbak.

De **voorzitter**:

Wij beginnen met de vraag van de heer Van de Ven aan de heer Oerlemans.

De heer **Oerlemans**:
Hartelijk dank voor de vraag. Daarin wordt een terecht punt opgeworpen. In mijn proefschrift heb ik veertien opsporingsmethodes onderzocht en bekeken of zij voldoen aan mensenrechtelijke vereisten die voortvloeien uit artikel 8 EVRM en het jurisdictieprobleem. Er werd gevraagd naar schadevergoeding, maar juist dit aspect heb ik daar niet echt in onderzocht. Ik vind het dus wel een lastige juridische vraag om te beantwoorden. Ik denk dat een strafrechtadvocaat daar wellicht beter op kan ingaan. Mijn eerste reactie is wel dat als er bij een huiszoeking schade wordt veroorzaakt aan bijvoorbeeld een deur, de Staat de daaruit voortvloeiende kosten vergoedt. Het is ook relevant om op te merken dat er wel een mogelijk bestaat om een klacht in te dienen op het moment dat die bevoegdheid is toegepast. Misschien kan daar in dat kader iets mee gedaan worden. Dat is mijn beperkte antwoord op de vraag.

De **voorzitter**:
Ik zie de heer Van de Ven tevreden kijken. We gaan door met de beantwoording van de vraag van mevrouw Beuving aan de heren De Vries en Egberts. Die ging over het vestigingsklimaat en Nederland als veilig land. Dan vat ik het heel kort door de bocht samen.

De heer **De Vries**:
Ik wil aangeven hoe wij aankijken tegen het gebruik van kwetsbaarheden in de cybercrime III-variant. De discussie over kwetsbaarheden is niet zwart-wit. De kwetsbaarheden zijn er, ook nu. Ze zijn op dit moment al aanwezig. Het gaat uiteindelijk om de waarborgen en het wegen van de belangen. Wij kijken in die zin naar het drieluik tussen vrijheid, veiligheid en maatschappelijke groei en proberen daar een evenwicht in te vinden. Ik denk dat het goed is om de woorden van de Staatssecretaris in de Tweede Kamer over de WannaCry ransomware te herhalen. Hij zei dat zo'n kwetsbaarheid in Nederland absoluut gewoon had geleid tot openbaarmaking. Ik ga ervan uit dat dit soort kwetsbaarheden gemeld worden in de discussie over welke software nu precies gebruikt wordt, en dat ze op die manier worden opgelost. Mijn NCSC doet er alles aan om Nederland op die manier veiliger en weerbaarder te maken. Het is juist dat die afweging moet worden gemaakt. Ik heb er het volste vertrouwen in dat het Openbaar Ministerie in staat is om die afweging gewogen te maken en dat het vanuit zijn rol de juiste dingen doet.
Delen wij kwetsbaarheden met het Openbaar Ministerie en de politie? Het antwoord op die vraag is simpelweg «nee». Zodra die kwetsbaarheden bij ons bekend zijn, worden die in overleg met de leverancier en de partners zo veel mogelijk opgelost binnen het tijdframe dat je partijen daarvoor kunt geven. Dat noemen we coordinated vulnerability disclosure. Daar steken we veel tijd en energie in, omdat we vinden dat we Nederland op die manier verder helpen.
Moet ik mijn ogen sluiten voor het feit dat er zeker criminelen zijn die absoluut weten hoe het werkt en daarmee binnen hun bandbreedte de politie kunnen uitdagen om niet gepakt te worden? Ja, die zijn er. Daar kunnen het Openbaar Ministerie en de politie veel meer over vertellen. Vanuit mijn bevoegdheid kan ik dat niet. Maar ik kan me zeer goed voorstellen dat er situaties zijn waarin je iets bijzonders moet doen om die bijzondere personen daadwerkelijk te vangen. Daar wil ik het even bij laten.

De **voorzitter**:
Dank u wel. Het woord is aan de heer Egberts.

De heer **Egberts**:
Ik zal proberen niet in herhaling te vallen. Ik heb WannaCry natuurlijk niet voor niets genoemd. Ik heb WannaCry genoemd om duidelijk te maken dat een dergelijke kwetsbaarheid vrijwel onmogelijk – ik durf wel te zeggen: onmogelijk – door het Openbaar Ministerie of de politie niet gemeld zou worden. In de discussies die ik voer over onbekende kwetsbaarheden en over de vraag of er situaties denkbaar zijn waarin het Openbaar Ministerie en de politie die voor zich zouden houden om de melding daarvan uit te stellen, is het vooral moeilijk om te verzinnen welke onbekende kwetsbaarheden er überhaupt door de politie ontdekt zouden kunnen worden, die wij niet zouden melden. Het is heel moeilijk om een voorbeeld te verzinnen waarbij wij niet gewoon direct zouden melden.
Dat schetst ook een beetje de omvang van het probleem. Wij hebben te maken met een bevoegdheid waarbij we kwetsbaarheden zullen gebruiken. Uit de praktijk blijkt dat de grootste aanvallen, zoals onder andere de Carbanak-aanval die toch tot 300 miljoen euro schade heeft geleid, gewoon op basis van bekende kwetsbaarheden hebben plaatsgevonden. Men moet zich voorstellen dat er binnen de politie een groep is van een aantal mensen die het zou moeten opnemen tegen een cybersecurity-industrie die een miljardenomzet draait en tegen gewoon allerlei ethisch hackers die op zoek zijn naar onbekende kwetsbaarheden. We zouden dan ten aanzien van die industrie eerder een bepaalde onbekende kwetsbaarheid ontdekken en die vervolgens niet melden voor een toekomstig geval, omdat ons dat zou uitkomen? Ik denk dat we in de reactie op de motie van de heer Recourt duidelijk hebben kunnen maken dat het Openbaar Ministerie en de politie daar geen enkel belang bij hebben. Het gaat ons om de meest veilige digitale samenleving. Die bestaat bij het melden van kwetsbaarheden.
Er zijn alleen zeer uitzonderlijke situaties gevallen denkbaar waarbij het belang om uiteindelijk een geautomatiseerd werk binnen te komen, groter is dan het melden van een onbekende kwetsbaarheid die slechts een heel kleine groep treft. Het opzetten van een geheel afgeschermd communicatienetwerk enkel voor tien criminelen om huurmoorden voor te bereiken, is niet zo heel moeilijk. Als daar nou een kwetsbaarheid in zit, omdat er gewoon sprake is van een verkeerde configuratie, is dat dan een situatie die we direct zouden moeten melden aan de ontwikkelaar van de app, die waarschijnlijk een van de verdachten is? Dat zijn misschien situaties waarin je uitstelt.
Ik denk dat uiteindelijk uit de beantwoording van de Staatssecretaris en ook na overleg met het Openbaar Ministerie voldoende naar voren komt dat wij helemaal geen belang hebben bij onbekende kwetsbaarheden. De kans dat we die zouden ontdekken, is heel klein. En als we er één tegenkomen, melden we altijd tenzij er sprake is van een situatie waarop de kans nog veel kleiner is. Dan moeten we het onderwerp ook niet groter maken dan het is. We hebben allemaal baat bij de meest veilige digitale samenleving. En voor de politie en het OM betekent dat melden.

De **voorzitter**:
Hartelijk dank. Dan staan de vragen van mevrouw Bredenoord nog open. Die waren ook gesteld aan de heren De Vries en Egberts. Ik zie echter dat de heer Arnbak er ook iets over wil zeggen. Mijnheer De Vries, de vraag was aan u gesteld.

De heer **De Vries**:
Ik heb het gevoel dat ik de vraag al beantwoord heb.

De **voorzitter**:
Klopt dat, mevrouw Bredenoord?

De heer **De Vries**:
De vraag ging namelijk over de specifiekheid en over de manier waarop dit gebruik in de wet past.

De **voorzitter**:
Er was ook een vraag voor de heer Arnbak over het toezicht en de controle achteraf? Misschien kan de heer Arnbak die vraag beantwoorden?

De heer **Arnbak**:
Zoals Jan-Jaap Oerlemans ook al zei, je hebt natuurlijk de inzet zelf. Dat is de rechter-commissaris. Dan heb je de zittingsrechter. Die komt vaak niet aan bod. En je hebt ook een model, zoals voor de inlichtingendienst CTIVD is ingericht, waarbij je op een wat algemenere en misschien ook wat meer beleidsmatige manier kijkt naar de praktijk van de inzet van zo'n opsporingsbevoegdheid, die in feite het hele Wetboek van Strafvordering voor de analoge wereld in één digitale variant verpakt. Dat heeft Jan-Jaap Oerlemans ook al gezegd. Het gaat dus om een heel vergaande bevoegdheid. Die verdient allicht een wat integraler toezicht, ook op beleidsniveau.
Ik denk dat hier een kans voor Nederland ligt om tussen allemaal grootmachten in de digitale wereld echt een voortrekkersrol te spelen, zoals dat bij de vorige hoorzitting en daarna OpenSSL was, de backdoordiscussie. Hier ligt een kans om bijvoorbeeld te kijken naar die kwetsbaarheden. Zoals de heer Egberts ook zegt: wij zullen bijna altijd melden. Dat is natuurlijk een heel interessante stelling. We weten nu nog niet hoe dat in de praktijk zal uitwerken. Eens in de zoveel tijd kun je daar natuurlijk vanuit een wat onafhankelijkere toezichtrol naar kijken. Een manier is bijvoorbeeld om te kijken naar kwetsbaarheden die worden ontdekt bij bedrijven en die vervolgens bekend worden voor de opsporing. Hoe snel worden die gemeld en vervolgens industriebreed geïmplementeerd? Kan Nederland zich manifesteren als een soort internetdokter in de globale cyberomgeving door zo veel mogelijk te melden? Dat is de basishouding. Dan ontstaat namelijk een praktijk van best practices. Dat zie ik ook als advocaat bij De Brauw. Je ziet ook dat de Hoge Raad steeds meer stappen zet in het accepteren van conformiteit, dus aansprakelijkheid in de ICT-omgeving. Je ziet dan dat er als het ware een basisnorm ontstaat van wat je als softwareleverancier had moeten doen. Dat betekent dat als je bekende kwetsbaarheden niet binnen afzienbare tijd repareert, je dan een niet-conform product levert.
Er is op dit moment baanbrekende jurisprudentie in ontwikkeling in een proefproces dat is gestart door de Consumentenbond tegen bijvoorbeeld Samsung over hoe veilig Samsungsmartphones nu eigenlijk moeten zijn. Dat zijn van die onderwerpen die verder moeten worden onderzocht. Daar kan de Eerste Kamer een heel belangrijke rol in spelen.
Toezicht gebeurt dus individueel, vooraf en achteraf door de zittingsrechter, maar het gebeurt ook integraal, dus meer op beleidsniveau. Daarbij kun je kijken naar de kwalitatieve en kwantitatieve inzet van zo'n bevoegdheid. Ik weet nog heel goed dat de bevoegdheid van het CIOT (Centraal Informatiepunt Onderzoek Telecommunicatie) werd besproken. Dat is een databank waarin alle gebruiksgegevens van telecommunicatie in Nederland op dagelijkse basis worden geüpload, zodat de politie meteen kan zien welke naam bij een bepaald nummer hoort. Dat was in ontwikkeling en daar werd in 2008 in de Tweede en Eerste Kamer over gesproken. Toen vroeg een senator of een Kamerlid: hoe vaak zal deze bevoegdheid eigenlijk ingezet worden? Het antwoord luidde: niet heel vaak, misschien een aantal tienduizenden keren. Intussen wordt het CIOT miljoenen keren per jaar geraadpleegd.
Uit zo'n toezichtfunctie kan dus naar boven komen dat we misschien iets toch niet helemaal goed doen. Je weet ook niet altijd van tevoren wat er

allemaal in moet zitten. Maar juist bij zo'n controversiële bevoegdheid die alle analoge strafvorderlijke bepalingen in een digitale variant bij elkaar pakt, is systematisch integraal toezicht van absolute essentie voor het bewaken van de rechtsstaat.

De **voorzitter**:
Heel hartelijk dank voor dit duidelijke antwoord. Het is inmiddels vijf over tien. Zijn er nog heel dringende vragen over dit blok?

Mevrouw **Gerkens** (SP):
Ik ben een beetje verward door de inbreng van de heer Egberts, omdat ik vind dat hij een verwarrende boodschap geeft. Hij zegt aan de ene kant dat het problematisch is dat er end-to-end-encryptie is en dat er VPN bestaat voor de opsporing. Aan de andere kant zijn dat volgens mij ook weer middelen die het internet voor ons als gebruiker heel veilig houdt. Ik heb drie vragen. Ik heb een vraag naar aanleiding van zijn uitspraak dat de kwetsbaarheden natuurlijk gemeld worden. Dat lijkt tegenstrijdig. Immers, als de kwetsbaarheid gemeld wordt en als iemand dat lek gaat dichten, verliest hij daarmee de bevoegdheid om te kunnen hacken. Hij zegt voorts «we komen op dit moment echt tekort» en houdt een enorm pleidooi voor verdere bevoegdheden. Mijn ervaring is dat het Openbaar Ministerie op dit moment niet alle bevoegdheden gebruikt die er al zijn om cybercriminaliteit aan te pakken, omdat men ervan uitgaat dat het toch niet zal werken. Kan hij daar wat meer op reflecteren?
De rechtercommissaris doet een uitspraak of er wel of niet gehackt mag worden. Die vraag is al gesteld, mijnheer Arnbak, maar die leidt bij mij tot de vraag: hoe veel verzoeken verwacht u tot het kunnen hacken? Wij hebben dezelfde mogelijkheid ook bij de taps in Nederland, bij de internet- en telefoontaps, en we weten dat die explosieve cijfers kennen, terwijl we daar in beide Kamers nooit een goede verklaring voor hebben gehad. Mijn volgende vraag aan de heer Arnbak luidt als volgt. Hij zegt dat hij meer waarborgen daaromheen moet hebben. Hoe zouden wij dat nu dan nog kunnen regelen? Als ik kijk naar Europa, dan zie ik dat daar nu regelgeving wordt opgezet waarbij end-to-end-encryptie wordt verplicht in alle elektronische communicatie en men oproept tot geen backdoors. Als dat doorgaat, wat betekent dat dan voor deze wetgeving? Dan heb ik nog een laatste vraag aan de heer Arnbak. Hij zegt dat er meer waarborgen moeten zijn. Hoe zouden wij dat nu nog kunnen regelen? In Europa wordt regelgeving opgesteld waarin end-to-end encryption verplicht wordt gesteld voor alle elektronische communicatie en wordt opgeroepen om geen backdoor te gebruiken. Stel dat dit doorgaat, wat zou dat dan betekenen voor deze wetgeving?

De **voorzitter**:
Dank, mevrouw Gerkens. Dit waren drie vragen, aan de heer Egberts en de heer Arnbak. Met het oog op de tijd wil ik u vragen om kort te antwoorden.

De heer **Egberts**:
Ik ga proberen kort te antwoorden. Heeft het Openbaar Ministerie dan wel de politie belang bij het bestaan van kwetsbaarheden? Om toegang te verkrijgen zullen kwetsbaarheden worden gebruikt, maar wat wij melden zijn onbekende kwetsbaarheden. Zoals de andere spreker al zei, is het uiteindelijk de verantwoordelijkheid van de fabrikant om kwetsbaarheden te verhelpen. De praktijk is nu eenmaal dat kwetsbaarheden die allang bekend zijn, niet verholpen worden. Dat zijn de kwetsbaarheden die het Openbaar Ministerie en de politie in beginsel zullen gebruiken: kwetsbaarheden die door de fabrikanten om economische of andere redenen – soms kan het zelfs niet eens worden verholpen in een product – niet worden verholpen. Daar hebben wij belang bij. Onbekende kwetsbaarheden die

een risico voor ons allemaal betekenen en die wel verholpen zouden kunnen worden, melden we.
De tweede vraag sla ik even over. Ik ga eerst naar de derde vraag: hoe vaak? Tijdens het rondetafelgesprek in de Tweede Kamer werd tappen als voorbeeld gebruikt. Ik denk dat ik daar eenzelfde reactie op geef. Proportionaliteit hangt niet samen met aantallen. Of een inzet proportioneel is, wordt getoetst door de rechter-commissaris, ook bij tappen. Aangezien tappen veel wordt gebruikt, wordt het ook door heel veel zittingsrechters getoetst. Om een inschatting te kunnen maken of de juiste keuzes worden gemaakt door het Openbaar Ministerie of de rechter-commissaris die de machtiging geeft of dat er heel disproportioneel gebruik van wordt gemaakt, zouden we eigenlijk gewoon moeten kijken naar de uitspraken over al die zaken waarin getapt is. Ik denk dat de uitspraken in de afgelopen jaren, en dan hebben we het niet over vijf of tien jaar maar over een langere tijd, waarin is geoordeeld dat er disproportioneel is getapt in een zaak, op één hand te tellen zijn. Dat betekent eigenlijk dat het Openbaar Ministerie en vooral ook de rechter-commissaris heel goed in staat zijn om proportionaliteit in inzet en subsidiariteit te toetsen alvorens daartoe wordt overgegaan.
Ik heb nog een laatste opmerking. U moet zich realiseren dat we, als we rechtmatig op de een of andere manier inloggegevens vinden van bijvoorbeeld een server in Nederland waartoe we gewoon toegang kunnen krijgen, op dit moment met die rechtmatig verkregen gegevens geen bewijs mogen verzamelen. Die situaties doen zich heel vaak voor. Dat betekent dat je vervolgens ergens heen moet waar je over het algemeen naar binnen gaat en versleutelde data tegenkomt.

De **voorzitter**:
Dank. Dat is een duidelijk antwoord. Mijnheer Arnbak, aan u het laatste woord in dit blok.

De heer **Arnbak**:
Hoe nu nog toezicht te organiseren? Deze analyse van uitspraken is bijvoorbeeld erg interessant, net als het vragen aan de Minister om nader onderzoek te doen naar de integrale inzet van de toezichtbevoegdheid. Hoe zal die eruitzien? Als zulke kwesties onderdeel worden van de parlementaire geschiedenis, heeft dat een gigantische impact, niet alleen op de verticale verhoudingen tussen de Staat en de burger, maar ook op de horizontale verhoudingen. Het punt dat ik eerder noemde van de conformiteit van IT-producten en wat een en ander bijdraagt aan de bredere cybersecurity in Nederland, moet niet worden onderschat. Dat is gigantisch belangrijk. Uiteindelijk ligt de verantwoordelijkheid voor het dichten van dit soort gaten niet bij het Openbaar Ministerie. Dat zijn allemaal van die vragen die je kunt stellen, me dunkt in een motie of in ieder geval in de parlementaire behandeling. Op basis daarvan kan misschien nog verder onderzoek plaatsvinden.
Dan de vraag over backdoors en end-to-end encryption versus de hackwet. Dat is natuurlijk wel een mogelijkheid, dat we als wetgever meer cybersecurity gaan verlangen, waardoor de inzet van zo'n hackbevoegdheid in feite gecompliceerder wordt. Maar dat kan wel vaker gebeuren met wetgeving. In een ander traject ontstaat er dan iets waardoor het lastiger wordt. Als er een verplichting komt tot end-to-end encryption, zijn er nog steeds zat manieren voor de opsporing om alsnog in de telefoon zelf als het ware in te breken in plaats van in het lijntje tussen de telefoon en de gsm-mast, om het even heel simpel neer te zetten. Dus ja, integraal toezicht is zeker voor het beleidsniveau relevant en daar is meer onderzoek voor nodig. Je hebt dat niet al georganiseerd op het moment dat een wetsvoorstel al dan niet wordt aangenomen. Dat moet dus verder worden onderzocht.

De **voorzitter**:
Hartelijk dank. Het is 10.10 uur. We moeten dit blok afronden. Ik dank u allen zeer voor uw bijdrage en het debat dat is ontstaan. Ik denk dat uw input zeker aanknopingspunten geeft voor het plenaire debat over beide wetsvoorstellen dat nog zal volgen. Er zijn een paar mooie uitspraken gedaan die we allemaal zullen onthouden, zoals «de overheid die gegevens witwast». Ik moet er nog van bijkomen. Wat wij allemaal delen, is het belang van het melden van kwetsbaarheden. Ik denk dat we allemaal het doel van beide wetsvoorstellen onderstrepen. Heel hartelijk dank. U krijgt van mij nog een presentje: Veelzijdig in deeltijd. Dat is een boek over onszelf, zodat u kunt zien wat wij nog meer doen. Terwijl ik dat aan u uitdeel, verzoek ik de volgende sprekers om plaats te nemen achter deze tafel. Nogmaals heel hartelijk dank.

De vergadering wordt enkele ogenblikken geschorst.

Thema II: Te respecteren privacywet-geving, databescherming en Europees kader

De **voorzitter**:
Na deze wisseling van de wacht gaan wij snel verder met het tweede blok dat betrekking heeft op te respecteren privacywetgeving, databescherming en Europees kader. Een heel hartelijk welkom aan de heer Wolfsen, voorzitter van de Autoriteit Persoonsgegevens, fijn dat u er bent, mevrouw De Vries van Amnesty International, ook heel hartelijk welkom, de heer Bruning van de Nederlandse Vereniging van Journalisten, mevrouw Peters, directeur Rathenau Instituut, hartelijk welkom, de heer Zuiderveen Borgesius, onderzoeker en specialist op het gebied van gegevensbescherming en privacy aan de Universiteit van Amsterdam, en de heer Bert-Jaap Koops – ook bijna een oude bekende, hij heeft eerder deelgenomen aan deskundigenbijeenkomsten – hoogleraar in Tilburg aan het TILT (Tilburg Institute for Law, Technology, and Society) en lid van de KNAW.
Ik stel, net als bij het vorige blok, voor dat de sprekers ieder maximaal vijf minuten de tijd krijgen om hun punt te maken. Ik heb het eerder elevator pitches genoemd. Zij krijgen direct na elkaar het woord. Daarna krijgen de woordvoerders de gelegenheid om vragen te stellen; wij doen dat in blokjes van twee of drie. Ik houd de tijd met een digitale stopwatch in de gaten.
Mijnheer Wolfsen, mag ik aan u het woord geven om te beginnen?

De heer **Wolfsen**:
Mevrouw de voorzitter. Wat bent u streng. Gelukkig hebben wij al geadviseerd en dat advies zal ik niet herhalen. Ik zal me beperken tot de punten die nog resten.
Wij spreken vandaag over twee wetsvoorstellen. Ten eerste de ANPR, maar daarover zal ik niet zo veel zeggen. De algemene norm kun je echter niet vaak genoeg herhalen: vrije burgers in een vrij land moeten zich vooral ook vrij kunnen bewegen en massale surveillance verhoudt zich daar niet toe, althans slecht. Maar het land moet ook veilig blijven en de politie moet dus haar werk kunnen doen. Dat kan MITS – met hoofdletters geschreven – de subsidiariteits- en proportionaliteitbeginselen getoetst zijn en er voldoende waarborgen zijn, toetsbaar en controleerbaar, checks and balances. Hoe ingrijpender de bevoegdheid, hoe zwaarder de toetsing, hoe hoger de officier, de rechter – het tritsje is bekend – en hoe steviger het toezicht moeten zijn. Ik zal daar straks nog aan refereren.
Ik heb over de ANPR-wet niet veel toe te voegen aan ons advies. Met de enorme aanpassingen kan het verantwoord als de Eerste Kamer het nodig vindt; die weging is nu aan de Kamer. Er zit wat ons betreft nog een gek ding in. Het zit in een afgescheiden bak, er zijn allerlei waarborgen, het is

beperkt toegankelijk enzovoorts, maar als het er een keer uit is, is het vrij en mag het overal worden verspreid. Dat vinden wij buitengewoon merkwaardig.
Dan de tweede wet: Computercriminaliteit III. Dat is natuurlijk een nog serieuzere wet. Ik zal daarover een korte algemene opmerking maken. Ik sprak al over het toetsingskader. Het is anders dan vroeger, dat zullen de senatoren zich realiseren. Toen zat wat je dacht in je hoofd, bleven je lichamelijke ervaringen in je lichaam, zaten de deuren dicht en was je huis beschermd evenals je communicatie, brieven enzovoorts. Nu vertaalt alles zich in data. Je telefoon weet vaak meer dan je partner, je zoekmachine weet meer over je gezondheid dan je dokter, en je kunt bijna niet dichter op de huid van mensen komen dan wanneer je in hun computers kunt kijken. Mensen realiseren zich dat maar slecht, maar het is echt waar. Dus als je daarvoor toestemming geeft, wat onder bepaalde omstandigheden moet omdat je criminaliteit wilt bestrijden, moet je daarmee buitengewoon zorgvuldig omgaan.
Ook hierbij maak ik nog een paar opmerkingen over een aantal elementen dat ons bezighoudt. Ik beperk me met name tot het hacken, het heimelijk binnendringen. Daarin zitten naar onze mening nog wat gekke dingen. Er is in de Tweede Kamer ook veel discussie geweest over de melding van een kwetsbaarheid. Wij zeggen dat er een hoger belang is en gaan dus uit van altijd melden. Ik zou het mooi vinden als de Eerste Kamer zich ook daarvan zou vergewissen, want het is lang niet duidelijk of dit altijd goed gebeurt.
Het tweede punt is dat er twee typen software zijn. Het eerste is erop gericht om binnen te dringen en het tweede op, eenmaal binnen, onderzoek. Als dat nodig is, moet dat altijd zorgvuldig en integer gebeuren. Het moet natuurlijk op een wettelijke manier verlopen, maar ook de integriteit van de computers mag niet worden aangetast. Het gekke is dat dit niet goed toetsbaar wordt gemaakt, want er hoeft geen verslag te worden gemaakt van het binnendringen en je mag zelfs met technische apparatuur die niet is getest, in iemands computer zitten. Wij zetten daar grote vraagtekens bij.
Er worden hoge barrières opgeworpen. In de wet is sprake van zeer uitzonderlijke gevallen, zware misdrijven enzovoort, maar in diezelfde wet zit ook een klein achterdeurtje: als de wet is aangenomen en de Minister denkt er na vandaag anders over, is dat ook goed. Ik heb gezocht naar een soortgelijke manier van wetgeving, maar ik heb die niet kunnen vinden. Je kunt een Minister wel toestemming geven om strenger te zijn, maar niet om minder streng te zijn. Dit is heel merkwaardig. Ik licht dat straks graag nader toe als daarover vragen worden gesteld.
Een ander punt is het gebruik van niet-gekeurde software. Dat is gevaarlijk.
Daarnaast moeten rechter-commissarissen gespecialiseerd zijn, want dit is zeer ingewikkeld en bijzonder werk en zeer ingrijpend. Daarop moet je gespecialiseerde mensen zetten.
Ik sluit af met het punt van de ernstige bezwaren. Nu worden hoge drempels opgeworpen en er is een achtjaarsgrens ingebouwd, maar je bent in Nederland toch vrij snel verdachte. Het zou mooi zijn als naast die achtjaarsgrens nog wordt getoetst of er sprake is van ernstige bezwaren, zoals bij voorlopige hechtenis, dan mag je in iemands computer. Zo is er een extra serieuze drempel om die bevoegdheid te kunnen toepassen.
Als laatste een vergelijking met de verslaglegging. Een goede en integrale toetsing en controle moeten mogelijk zijn, want lang niet alle zaken komen bij een rechter, vaak minder dan meer. Ik maak een vergelijking met het huisrecht, de Algemene wet op het binnentreden. Als er wordt binnengetreden in een huis, moet er keurig verslag worden gedaan van de wijze waarop men is binnengetreden. Dat vinden wij goed, want dat maakt het ook toetsbaar. De Minister is van mening dat het niet nodig is, want het zijn geen dingen die meewegen voor het bewijs. Dat is natuurlijk

niet zo relevant. Je wilt bekijken of iemand rechtmatig en fatsoenlijk is binnengetreden. Dus ook daarvan moet keurig verslag worden gedaan zodat het ook toetsbaar is, vergelijkbaar met de Algemene wet op het binnentreden bij het schenden van het huisrecht.
En nogmaals, daarmee sluit ik af: geconstateerde kwetsbaarheden moeten altijd worden gemeld. Daarmee is echt een groter belang gediend.

De **voorzitter**:
Heel hartelijk bedankt. Dit sluit mooi aan bij het vorige blok.
Het woord is nu aan mevrouw De Vries. U krijgt ook vijf minuten om uw visie kenbaar te maken.

Mevrouw **De Vries**:
Hartelijk dank voor de uitnodiging aan Amnesty International voor deze bijeenkomst. Ik beperk mij ook tot de hackbevoegdheid die via Computercriminaliteit III aan de politie kan worden toegekend. Ik zal kort ingaan op de impact van onder andere hack- en andere surveillancebevoegdheden op mensenrechten. Ik doe dit aan de hand van een enkel voorbeeld uit het internationale onderzoek van Amnesty en wat internationale mensenrechtelijke kaders. Amnesty International heeft zich tot nu toe niet echt gemengd in de voorbereiding van beide wetsvoorstellen. Ik kan en zal me dan ook niet heel concreet uitlaten over wat daar exact in staat. Ik beperk me tot twee zorgpunten die ik met u wil delen over Computercriminaliteit III.
Wanneer hacken door de overheid, in dit geval straks mogelijk door de politie, is gericht op een specifiek individu, een legitiem doel dient, is gebaseerd op een redelijke verdenking, voorzienbaar is, geautoriseerd is door een rechter, en geen disproportionele en niet-noodzakelijke inbreuken maakt op andere rechten of belangen, dan lijkt de bevoegdheid om te mogen hacken op het eerst gezicht best gelijkgesteld te kunnen worden met gerichte interceptie zoals een telefoontap. De inmenging met mensenrechten via overheidshacken is echter indringender.
Allereerst is hacken door de overheid een zeer vergaande bevoegdheid en een ernstige inperking van het recht op privacy. Via aftappen en afluisteren worden gesprekken gevolgd die op dat moment worden gevoerd, maar via hacken kan inzicht worden verkregen in het gehele leven van een individu. Hacken geeft toegang tot bijvoorbeeld foto's, documenten, video's en allerlei andere soorten files die tot dan toe niet met anderen zijn gedeeld en alleen aan het apparaat zijn toevertrouwd. In die zin wordt ook de vrijheid van gedachten geraakt. Bovendien is er de mogelijkheid om de bezitter heimelijk op te nemen en te filmen. Dit is eveneens een vergaande inbreuk op het recht op privacy.
Naast het feit dat het recht op privacy een recht is dat op zichzelf staat, is het ook een essentieel mensenrecht voor de verwezenlijking van andere mensenrechten. Toezicht op wat wij lezen, bekijken, schrijven, bespreken, kan ons verlammen in het verkennen van nieuwe ideeën, ook minder gangbare of zelfs heel impopulaire ideeën. Privacy is cruciaal voor het beschermen van het uiten, het vormen en het bespreken van je mening, ook impopulaire standpunten. Zo moet het ook vrij zijn om samen te kunnen komen en met anderen bijvoorbeeld politieke activiteiten te ontplooien.
In een rapport over Wit-Rusland heeft Amnesty vrij uitgebreid chilling effects gedocumenteerd. De titel zegt veel, vind ik. Its enough for people to feel it exists. Onzekerheid en onduidelijkheid over de ware aard en de ware reikwijdte van communicatie, surveillance- en opsporingsbevoegdheden van de overheid voedt de angst van mensen en activisten voor dit soort bevoegdheden. Die angst zit echt heel diep. De mensen die Amnesty heeft gesproken, beperkten hun gebruik van telefonie en e-mail uit vrees dat hun communicatie wordt onderschept, hun apparatuur wordt gehackt en dat continu wordt bijgehouden waar ze zijn. Ze durven niet meer vrij

met gelijkgestemden samen te komen en zij passen wel twee keer op voordat ze een mening of geplande activiteiten delen via e-mail, smartphone of een gewone telefoon. Deze angst, die psychologisch stress, en de zelfcensuur ondermijnen het vermogen van deze activisten en journalisten om hun werk te doen. De civil society in dat land is zwakker vanwege die surveillance- en opsporingsbevoegdheden en de verlammende effecten die volgen op de angst daarvoor.
Hoewel dit voorbeeld natuurlijk niet op de Nederlandse situatie slaat, illustreert het wel degelijk de reikwijdte van een dergelijke hackbevoegdheid die net als, en naast, andere opsporings- en surveillancebevoegdheden verlammende effecten kan hebben op de verwezenlijking van meerdere mensenrechten. Daarom is het van belang dat zo'n bevoegdheid zo wordt afgebakend dat niet onnodig disproportionele inbreuk wordt gemaakt op mensenrechten.
Ik breng graag onder uw aandacht dat de memorie van toelichting daarover toch enige twijfel laat bestaan of in ieder geval niet alle vertrouwen wekt, want daarin staat immers op pagina 75: «Daarnaast kan worden verwacht dat de inzet van onderzoek in een geautomatiseerd werk mogelijk ook andere vormen van politie-inzet kan vervangen ...» Dit lijkt in onze ogen toch een beetje een wassen neus te maken van de proportionaliteits- en subsidiariteitstoets.
Een tweede punt dat ik maak, is ook in de vorige ronde aan de orde gekomen. Het heeft betrekking op het toezicht. Een dergelijke indringende bevoegdheid hoort gepaard te gaan met sterke waarborgen en een volwaardig, onafhankelijk, bindend toezicht in alle fasen van het handelen van een opsporingsdienst. Een hackbevoegdheid geeft veel discretie aan de uitvoerende partij en daarom is dergelijk toezicht onontbeerlijk om te voorkomen dat die onrechtmatig wordt ingezet. Een dergelijk toezicht en een remedie voor onrechtmatigheden zijn in Wit-Rusland niet adequaat geregeld.
Nog even de brug met Nederland: Amnesty juicht de in het wetsvoorstel voorgestelde zogenoemde dubbele toets vooraf wel toe, maar het toezicht achteraf is nu belegd bij de Inspectie voor Veiligheid en Justitie. Amnesty heeft in het verleden kritiek geuit op het gebrek aan onafhankelijkheid van de inspectie. Ook veel andere organisaties hebben hierop kritiek geleverd. Ons oordeel is dan ook dat een toezichthoudende rol achteraf beter elders kan worden belegd.
Amnesty International hoopt dat u deze twee zorgpunten bij de verdere behandeling van dit wetsvoorstel zult betrekken.

De **voorzitter**:
Heel hartelijk dank, mevrouw De Vries.
Mijnheer Bruning, het woord is nu aan u.

De heer **Bruning**:
Veel dank voor de uitnodiging. Mijn inbreng zal werkelijk kort zijn, omdat de impact van het wetsvoorstel door de vorige sprekers genoegzaam is duidelijk gemaakt. Het gaat om het hacken in Computercriminaliteit III. Wij hebben eerder met het Genootschap van Hoofredacteuren en de Stichting Persvrijheidsfonds duidelijk gemaakt dat onze zorg natuurlijk ligt bij de mogelijkheid om ook computers van journalisten binnen te dringen en daarmee toegang te krijgen tot de bronnen van journalisten die anoniem moeten kunnen blijven.
De kern van onze zorg is het feit dat al sinds 2014 een ander wetsvoorstel in de Kamer voorligt, namelijk het wetsvoorstel met betrekking tot de journalistieke bronbescherming. Dit is nog altijd niet hier beland. Dit wetsvoorstel raakt op vele fronten aan dit soort ingrijpende wetsvoorstellen. Ik denk bijvoorbeeld aan de Wet op de inlichtingen- en veiligheidsdiensten (Wiv). Ik pleit er dan ook voor dat er eerst voor wordt gezorgd dat dat wetsvoorstel wordt aangenomen en dat de zorgen van de

journalistieke gemeenschap die raken aan een belangrijk mensenrecht, namelijk het recht van vrijheid van meningsuiting, worden weggenomen, dat wil zeggen dat dit recht goed wordt geborgd. Zo kan worden voorkomen dat wij steeds in dit soort bijeenkomsten over welk wetsvoorstel dan ook, moeten wijzen op het feit dat de journalistieke bronbescherming niet goed is geregeld. Dat is ook in dit wetsvoorstel niet het geval.
Mijn pleidooi is daarom kort en goed: houd dit wetsvoorstel aan en hetzelfde geldt voor de WIV. Geef eerst voorrang aan en leg de nadruk op het wetsvoorstel journalistieke bronbescherming. Dat is niet bijzonder, want sinds 2000 ligt er een verzoek bij de Raad voor Europa. Het Europese Hof voor de Rechten van de Mens heeft meerdere uitspraken gedaan. Zij hebben alle benadrukt dat Nederland tot een goede en zorgvuldige journalistieke bronbescherming moet komen. Dit is nu al zeventien jaar nagelaten. Ik denk dat dit een heel mooie kans is, los van de bezwaren die door andere sprekers zijn ingebracht, om dit wetsvoorstel terug te sturen. Hetzelfde geldt voor de WIV, ik zeg het nog maar een keer. Eerst moet ervoor worden gezorgd dat de journalistieke bronbescherming, een essentieel punt in al dit soort ingrijpende wetsvoorstellen, goed is geregeld in Nederland. Dat Nederland daarmee achteraan in de rij sluit ten opzichte van andere Europese landen zij dan maar zo. Beter laat dan nooit.

De **voorzitter**:
Hartelijk dank. Voor de goede orde: de Eerste Kamer heeft geen terugzendrecht, maar uw boodschap is duidelijk.
Mevrouw Peters, het woord is aan u.

Mevrouw **Peters**:
Heel hartelijk dank voor de uitnodiging om hier te spreken. Het Rathenau Instituut wil vooral een bijdrage leveren aan het wetsvoorstel Computercriminaliteit III. Onze rol is om te kijken naar technologische ontwikkelingen en de manier waarop die de samenleving en ook de mensenrechten raken. Wij hebben recent een aantal rapporten uitgebracht over cybercriminaliteit, maar ook over de ontwikkelingen van het internet en de gevolgen daarvan voor mensenrechten. Uit het onderzoek blijkt duidelijk dat het internet als vrijhaven of als vrijplaats niet kan. Wij moeten dat beeld bijstellen. Op het internet gebeurt alles wat ook in de reële wereld gebeurt.
Ik wijs er vooraf op dat de rol van de politie en de inlichtingendiensten altijd een sluitstuk is. Wij hebben in ons werk ook gewezen op de verantwoordelijkheid van de overheid, bedrijven en burgers om ervoor te zorgen dat zij een veilig internet hebben. Het is net als in de reële wereld: als de keukendeur openstaat, kan de politie ook niet handhaven. De inzet van de bevoegdheden van de politie is dus altijd een sluitstuk.
Het wetsvoorstel heeft als titel Computercriminaliteit, maar het gaat allang niet meer alleen over onze computer. Nederland wil als eerste in de wereld het 5G-netwerk uitrollen. Dit betekent dat onze computer verbonden is met onze telefoon en met allerlei andere apparaten, routers, smart devices zoals slimme thermostaten, auto's en medische apparatuur. Er werd al op gewezen dat internet en de persoonlijke omgeving niet beperkt blijven tot de computer, maar zich uitbreiden tot apparaten die voortdurend allerlei dingen in je huis en van jouw gedrag meten. Dus als bij de bevoegdheid niet wordt gespecificeerd over welke apparaten het gaat, betekent dit dat die heel vergaat. Het gaat dan om heel veel apparatuur die, zoals gezegd, heel dicht bij ons komt. Dat maakt het nog belangrijker om kritisch en onafhankelijk toezicht te hebben.
Op dit moment is het voorstel dat het toezicht vooraf wordt gevormd door de Centrale Toetsingscommissie van het Openbaar Ministerie en een rechter-commissaris. Dat is dus geen onafhankelijk toezicht in die zin dat

het de eigen dienst is die daarover oordeelt, ook al is het een zware commissie.
Het toezicht achteraf door de Inspectie Veiligheid en Justitie is te licht; het moet in ieder geval verder worden onderzocht. Als wij het vergelijken met het toezicht op de inlichtingen- en veiligheidsdiensten door de CTIVD, waarover ook al vragen zijn gesteld in de Tweede Kamer, dan denken wij dat de Inspectie Veiligheid en Justitie minder onafhankelijk is, omdat zij deel uitmaakt van het Ministerie van Veiligheid en Justitie en ook over minder bevoegdheden beschikt dan de CTIVD; zij kan bijvoorbeeld niet mensen onder ede horen. Dat kritisch en onafhankelijk toezicht is dus een punt van zorg.
In het kader van de rechtpositie van de burger – op welke manieren kunnen mensen zich verweren tegen onterecht verdenkingen? – wijzen wij op de klachtenfunctie die nu is toebedeeld aan de CTIVD, dus parallel met de bevoegdheden van de inlichtingendiensten. Dat zou in dit geval de Nationale ombudsman zijn en dat lijkt ons een onvoldoende instrument voor de burger om zich te kunnen verweren.
Er is al gesproken over de onbekende kwetsbaarheden. In de Tweede Kamer is een aantal amendementen ingediend dat beoogt dat die altijd worden gemeld en dat die spaarzaam worden gebruikt. Dit is al door een aantal woordvoerders naar voren gebracht. Wij moeten echt kunnen uitgaan van veilige producten; dat is het begin van de beveiliging in Nederland.
Wij wijzen ook op de monitoring zoals die in het wetsvoorstel is beschreven; de checks and balances die zo belangrijk zijn. Daarbij is voor deze wet een evaluatietermijn van vijf jaar voorgesteld. Ons lijkt dat die evaluatie vroeger moet plaatsvinden, ook in verband met de technologische ontwikkelingen waardoor nog meer gegevens gaan behoren tot het domein waarin gehackt zou kunnen worden.
Tot slot wijs ik nog op de cumulatieve effecten. Wij hebben in het verleden gezien dat er altijd wel een reden lijkt te zijn om deze bevoegdheden uit te breiden, maar die staan natuurlijk naast andere bestaande bevoegdheden. Wij vragen aan de Tweede Kamer, maar vooral ook aan de Eerste Kamer om te blijven toetsen of met het totaal aan bevoegdheden niet een surveillancecultuur wordt ontwikkeld. Er werd al gesproken over «function creep». Dit is geen privacy by design, maar waar zijn wij mee bezig? Ik doe een oproep aan de leden van de Eerste Kamer om het geheel aan maatregelen dat is afgesproken, te blijven bekijken, omdat de wet niet alleen betrekking heeft op cybercriminaliteit maar ook op andere criminele activiteiten.

De **voorzitter**:
Hartelijk dank. U hebt ons al veel aanknopingspunten meegegeven voor het verdere debat.
Het woord is aan de heer Zuiderveen Borgesius.

De heer **Zuiderveen Borgesius**:
Goedemorgen dames en heren. Ik zal vooral een paar opmerkingen maken over het ANPR-wetsvoorstel. Ik kom zo op de vraag hoe massaal dat nu eigenlijk is. Ik waarschuw er alvast voor dat het massaal verzamelen van gegevens over onschuldige mensen bijna niet te rijmen is met de Europese mensenrechtenjurisprudentie. Het ANPR-wetsvoorstel komt hierbij wel erg dicht in de buurt; het blijft in ieder geval onduidelijk hoe massaal het wordt.
Hierbij dient te worden opgemerkt dat ook als je checks and balances hebt over wie uiteindelijk toegang heeft tot een databank – wat heel nuttig is – het enkele verzamelen van gegevens over mensen volgens het Mensenrechtenhof in Straatsburg en het EU Hof in Luxemburg al een inbreuk is op de privacy die niet is toegestaan als die disproportioneel is, dus afgezien van de vraag hoe goed de toegang tot de databank is geregeld.

Wij weten in Europa in ieder geval zeker dat het volstrekt algemeen en ongedifferentieerd verzamelen van gegevens niet is toegestaan, want dit bleek uit het Tele2-arrest over metadata, dat wil zeggen wie je belt, wanneer en waar je bent met je telefoon et cetera. Als je dit naast het ANPR-wetsvoorstel legt, wordt het moeilijk. In het wetsvoorstel wordt niet beschreven hoeveel camera's het uiteindelijk worden en waar ze worden ingezet. Dit staat sinds heel kort in een conceptuitvoeringsbesluit. Nee, daar staat het trouwens ook niet in. Daarin staat dat ieder jaar een cameraplan zal worden opgesteld. Voor zover ik heb kunnen nagaan, bestaat daarvoor zelfs nog geen concept. Bovendien, als de leden dat nu zouden beoordelen, kan het volgend jaar weer een ander besluit zijn. In dat camerabesluit wordt opgeschreven waar camera's kúnnen worden gebruikt. Politie en de marechaussee beslissen in de praktijk waar zij die camera's echt gaan gebruiken.
Volgens het conceptuitvoeringsbesluit kunnen onder de voorwaarden van dit wetsvoorstel – dus met vier weken opslag van de gegevens van iedereen die er langs rijdt – camera's van andere instanties worden gebruikt. Er wordt echter niet goed uitgelegd, in het uitvoeringsbesluit of de toelichting daarop, welke instanties dat zijn, laat staan hoeveel camera's dat zouden zijn.
In het uitvoeringsbesluit worden suggesties gedaan voor locaties die aangewezen zouden kunnen zijn voor het gebruik van die ANPR-camera's, zoals plekken waar veel criminaliteit wordt verwacht, maar ook locaties met intensieve verkeersstromen. Dat zijn heel veel locaties in Nederland, want dit is een druk land. Dat is dus geen echte begrenzing.
Samenvattend: het is volstrekt onduidelijk, of nog onduidelijk in ieder geval, hoe massaal dit systeem wordt. Hierbij moeten wij onthouden dat de ANPR-camera's, net als alle apparatuur, steeds goedkoper zullen worden. Het is dus heel gemakkelijk om er steeds meer aan te schaffen. Misschien is over een aantal jaren iedere politieauto met zo'n camera uitgerust.
Het is dus eigenlijk heel moeilijk, op het randje van onmogelijk, om de proportionaliteit van dit wetsvoorstel nu te beoordelen, omdat alles over het aantal camera's en de massaliteit van de inzet is uitgesteld tot ten dele nog niet bestaande documenten.
Dit was mijn belangrijkste punt. Verder onderschrijf ik wat eerdere sprekers hebben gezegd over het belang van effectief en onafhankelijk toezicht op alle fasen van een opsporingsproces. Dat geldt trouwens voor gerichte opsporing en voor meer massale surveillancesystemen. Daarbij lijkt het mij ook heel belangrijk dat de toezichthouder niet alleen op de formele vereisten checkt, maar ook op de proportionaliteit van de manier waarop de wet wordt toegepast.

De **voorzitter**:
Wat fijn. Dank u wel voor de mooie blik op vooral de ANPR-wet.
Ik geef graag als laatste in de rij het woord aan Bert-Jaap Koops.

De heer **Koops**:
Eén correctie: ik ben geen lid van de KNAW, maar ik ben fellow bij het NIAS dat een onderdeel is van de KNAW. Dat ligt subtiel, maar ik zeg het toch maar even voor de notulen.
Ik sluit me aan bij alle zorgen die zijn geuit over het hackwetsvoorstel, het omgaan met kwetsbaarheden en met name ook over het belang van toezicht. Ik onderstreep dat graag, maar omdat daarover al veel is gezegd, zal ik vooral aandacht vragen voor onderbelichte onderdelen van beide wetsvoorstellen.
Ik sluit mij aan bij de vraagtekens die zijn geplaatst bij de noodzaak van ANPR. Ik heb vooral hypothetische voorbeelden gezien van gevallen waarin het nuttig kan zijn, maar nuttig is iets anders dan noodzakelijk. Incidentele gevallen waarin het nuttig kan zijn, zijn iets anders dan de

noodzaak van massasurveillance. Het is dus echt de vraag of de noodzaak hiervan wel is aangetoond.
Ik vraag vooral aandacht voor twee onderdelen hiervan. Het eerste is al eerder kort aangestipt, namelijk het kenbaarheidsvereiste. Dat is in principe een belangrijke privacywaarborg: burgers moeten weten wat de politie kan doen. Met name hier is de kenbaarheid vooraf van belang. Dit is echter vooral van belang als je iets te kiezen hebt. Als er overal camera's hangen en er zijn geen alternatieve routes om je aan cameratoezicht te onttrekken, dan heeft een bordje met de tekst: hier vindt cameratoezicht plaats, niet heel veel zin. Dat gezegd hebbende, schat ik in dat ANPR in de eerste jaren niet heel dekkend over Nederland zal worden uitgespreid, hoewel je je kunt afvragen hoe dat in de toekomst zal zijn. In principe heb je nog wel iets te kiezen, maar het kenbaarheidsvereiste wordt nu wel heel theoretisch ingevuld, namelijk door publicatie in de Staatscourant. Daarbij kun je sowieso al vraagtekens plaatsen. Ik zou eerder verwachten dat er dan bordjes bij de inrit en langs de snelweg staan met de tekst: hier vindt ANPR plaats; dat doen wij per slot van rekening ook met cameratoezicht op straat. Maar voor de burgers die al braaf de Staatscourant lezen – hoeveel zijn dat er? – kun je voor mobiel-ANPR daaruit niets afleiden, omdat alleen het aantal camera's en de soorten plaatsen worden gemeld. Op basis daarvan kun je absoluut niet weten waar je mobiel-ANPR kunt verwachten. Het kenbaarheidsvereiste lijkt mij op dit punt dus niet juist ingevuld.
Het tweede punt dat ik wil maken, is dat weliswaar terecht wordt opgemerkt dat openbare plaatsen minder privacygevoelig zijn dan besloten plaatsen, maar dat dat alleen maar het geval is als alle andere omstandigheden hetzelfde zijn. Een foto aan de openbare weg is minder privacygevoelig dan een foto in het huis, maar 5.000 foto's van een object dat naadloos met een persoon is verbonden en waaruit je dus alle bewegingen in de openbare ruimte kunt afleiden, geven veel meer informatie over je privéleven dan een paar foto's die je binnenshuis maakt. Je kunt dus ook moeilijk zeggen dat omdat dit voorstel zich beperkt tot openbare plaatsen, het daardoor meestal minder inbreuk op de privacy oplevert. Het is heel erg afhankelijk van de vraag hoe vaak, met welke frequentie en met welke intensiteit het wordt vastgesteld. In dat kader nodig ik u uit om vooral na te denken over alternatieve normatieve kaders waarbij niet meer wordt gekeken naar openbare plaatsen ten opzichte van besloten plaatsen, maar bijvoorbeeld naar de mozaïektheorie die in Amerika wordt ontwikkeld. Kijk naar het gehele plaatje van allerlei kleine losse brokjes die elk op zich weinig zeggen, maar die wel een heel indringend beeld van de persoonlijke levenssfeer geven als ze bij elkaar worden gelegd.
Uit het voorstel Computercriminaliteit III wil ik ook twee punten lichten. In de eerste plaats de definitie waar al vraagtekens bij zijn geplaatst. In eerdere discussies zijn daarover ook al vragen gesteld. Terecht, want de definitie van geautomatiseerd werk is bijzonder ruim. Ik vraag u vooral om na te denken over de vraag en aan de Minister te vragen of het niet wenselijk zou zijn om op dit punt het Wetboek van Strafrecht en het Wetboek van Strafvordering uit elkaar te trekken. Je hoeft niet precies dezelfde begrippen te hanteren, want de belangen zijn echt anders. Als je hackers strafbaar wil stellen op basis van het Wetboek van Strafrecht, is het logisch om daarbij een ruim begrip van geautomatiseerd werk te gebruiken. Dat wil echter niet zeggen dat, als je de politie de bevoegdheid wil geven om in computers binnen te dringen – wat toch vooral bedoeld is voor klassieke computers, smartphones, laptops, tablets en dat soort apparaten – je daarmee ook alle andere apparaten die toevallig ook onder die definitie vallen, zou moeten treffen.
Een tweede punt van Computercriminaliteit III – dat wil ik benadrukken, voor zover de tijd mij nog rest – is de strafbaarstelling van het onrechtmatig overnemen van gegevens. Dat is volstrekt onderbelicht in de hele

wetsgeschiedenis. Let wel, daarbij gaat het niet om de strafbaarstelling van heling van gegevens; daarvoor is een ander voorstel. Er zit ook een bepaling in de wet, 138c, waarin staat dat je, als je gegevens waar je rechtmatig toegang toe hebt, onrechtmatig voor jezelf of een ander overneemt, daarmee strafbaar wordt. Dat is een bijzonder ruime bepaling, waarvan ik echt de noodzaak niet zie. De voorbeelden die hiervan gegeven zijn, beperken zich eigenlijk tot het onrechtmatig openbaar maken van gegevens. Daar kan ik mij iets bij voorstellen – wraakporno, bijvoorbeeld – maar het onrechtmatig overnemen van gegevens, dus het enkele kopiëren, is veel ruimer dan dat. Ik zou u er vooral toe willen uitnodigen om de Minister vragen te stellen om daarvan veel meer voorbeelden te geven die niet onder huidige strafbepalingen vallen, maar wel ernstig genoeg zijn om in zo ruime mate strafbaar te stellen.

De **voorzitter**:
Hartelijk dank, mijnheer Koops. Ik heb een heel scala aan mitsen en maren langs zien komen. Ik nodig de leden uit om vragen te stellen en daarbij weer aan te geven voor wie de vraag bedoeld is. Ik begin bij de heer Dercksen.

De heer **Dercksen** (PVV):
Voorzitter. Ik heb een vraag voor de heer Wolfsen. Hij sprak over unprecedented bevoegdheden – we kennen het Nederlandse woord bijna al niet meer – van de Minister in de Wet computercriminaliteit III. Ik wil daarover graag een verduidelijkend betoog van de heer Wolfsen horen. Gaat dat over de mogelijkheden van de Minister om allerlei zaken onder die wet te brengen en later te specificeren via een AMvB, zonder toetsing van de Staten-Generaal?

De heer **Wolfsen**:
Dank u wel, mevrouw de voorzitter. De opbouw van de wet is zo, dat het in bijzondere gevallen mag. Er is een speciale toets, er zitten allemaal zorgvuldigheidsnormen in en het mag ook alleen bij zeer ernstige delicten. De achtjaarsgrens zit erin, dus dat zijn de ernstigere delicten. Dat snap je in de logica: streng, streng, streng, want het is een zeer vergaande bevoegdheid. In diezelfde wet zit echter nog een andere bepaling: het mag alleen bij zeer bijzondere delicten, maar bij AMvB mag de Minister niet alleen nog strenger zijn, maar ook eigenlijk de hele wet illusoir maken. Dat vind ik unprecedented. Dat is vrij gek. U bent hier streng, maar u zegt tegelijkertijd: Minister, als u buiten bent, mag u het bij een fietsendiefstal ook toepassen. Dat is een theoretisch geval, maar het is gewoon open. Dat is heel uitzonderlijk; laat ik het zo zeggen.

De **voorzitter**:
Dit heeft ook reeds de aandacht van zowel de Tweede Kamer als de Eerste Kamer, dus dit zal ongetwijfeld ook plenair worden meegenomen.
Voor verdere vragen ga ik gewoon het rijtje af.

De heer **Van de Ven** (VVD):
Mevrouw de voorzitter. In de eerste plaats spreek ik wederom mijn dank uit aan de deskundigen. Wat ik gehoord heb, is verruimend voor mij; zeer veel dank. Inhoudelijk vond ik het heel goed. Ik heb gezegd dat ik een leidraad heb gekozen: schade en schadevergoeding. Ik heb twee vragen voor de heer Wolfsen. Ten eerste: hoe gaat de Autoriteit Persoonsgegevens handhaven dat er geen datalekken ontstaan door hacks die zijn gedaan door de nationale politie? Ten tweede: is deze handhaving mogelijk zonder dat de politie softwaretests gebruikt en het gebruik daarvan vastlegt via een logging?

De **voorzitter**:

Mijnheer Wolfsen, wilt u hier even over nadenken? Het is een moeilijke vraag, hè? Ik vind hem ook pittig. We komen daar straks op terug.

Mevrouw **Strik** (GroenLinks):
Voorzitter. Ook ik dank iedereen hartelijk voor de relevante bijdragen. Ik heb een vraag over ANPR. De heer Zuiderveen Borgesius zegt dat die bijna niet verenigbaar is met de EU-jurisprudentie en de EHRM-jurisprudentie. Ik ben nieuwsgierig naar dat «bijna». U zegt eigenlijk: we weten nog onvoldoende over de proportionaliteit, omdat het uitvoeringsbesluit nog niet bekend is. Kunt u aangeven wanneer wat in het document zou moeten staan opdat het wel binnen het proportionaliteitsvereiste valt? Dat is misschien ook een beetje een lastige vraag, maar ik ben op zoek naar de grenzen van dat «bijna». In dat kader zou ik het ook fijn vinden als de heer Koops iets meer kan vertellen over het mozaïeksysteem, dat misschien als alternatief normatief kader zou kunnen dienen. Als het mag, wil ik ook nog een vraag stellen over het toezicht.

De **voorzitter**:
Nee, misschien is het goed om eerst even deze twee vragen te laten beantwoorden. Daarna gaan we verder. Mijnheer Zuiderveen, volgens mij kunt u de vraag over de grenzen van het «bijna» beantwoorden.

De heer **Zuiderveen Borgesius**:
Ik ga mijn best doen, maar het blijft wel een beetje vaag. We weten zeker dat een heel land onder surveillance plaatsen niet mag. Ik zou inschatten – maar ik wacht even tot de specialisten om mij heen ja knikken – dat een week in een straat mag. Ergens daartussenin zit het dus. Het beroemdste of nuttigste arrest hierover is het Tele2-arrest van het EU-hof in Luxemburg. Meteen na dat arrest kwamen er vragen op. Iedereen onder surveillance plaatsen mag niet, maar als je de surveillance richt op een geografisch ingeperkt gebied voor niet te lange tijd, op jacht naar heel zware criminelen, mag het wel. Maar ja, helaas laat dat wel dingen open. Ik zou zeggen: een halfjaar lang heel Amsterdam onder surveillance plaatsen, lijkt mij niet snel proportioneel. Waar het precieze kantelpunt zit, is niet zo duidelijk, maar ik wil wel het volgende opmerken. Hoewel het nuttig is om toegang tot de databank te reguleren, heb je daarmee niet alle gevaren afgedekt, want voor de proportionaliteitstoets geldt het enkele verzamelen al. Hier help ik u niet zo veel verder mee, hè? Er geldt: zo miniem mogelijk verzamelen.

De heer **Koops**:
Ik zal zo de aan mij gestelde vraag beantwoorden, maar ik wil eerst iets zeggen over dit punt. Er zit een inherente tegenstelling in de argumentatie. In de eerste sessie hebben we gehoord dat het vooral van belang is in situaties waarin je nu heel veel moeite moet doen. Als je achteraf van een auto wilt weten waar die geweest is, moet je nu allerlei camerabeelden gaan opvragen. Dat is heel lastig. Daarvoor zou het belangrijk zijn – dat kan ik mij voorstellen – maar dat werkt alleen als je een landelijk dekkend systeem hebt, want anders is de kans dat je die auto in het bestand kunt vinden alsnog bijzonder klein. Dat wil zeggen dat het, als je dit zou willen, vooral nuttig en misschien ook wel noodzakelijk is, als je landelijk dekkend ANPR gaat toepassen, maar dan is het, zoals we gezegd hebben, nauwelijks meer proportioneel, omdat dat echt massasurveillance is op een schaal die niet met de EHRM-jurisprudentie te verenigen valt. Als je het niet landelijk dekkend doet, kan het soms handig zijn, maar wordt de kans dat je daadwerkelijk een bepaalde zaak hiermee oplost, aanzienlijk kleiner. Dat vind ik echt wel een moeilijkheid die inherent is aan de hele argumentatie van deze wet.
Ik zal nog kort iets zeggen over de mozaïektheorie. Die is in Amerika ontwikkeld in het Maynard-arrest en vervolgens in het Jones-arrest,.

waarin de concurring opinions deze theorie min of meer omarmen. Die zaak ging over het plaatsen van een gps-transponder op een auto. Dat is dus heel vergelijkbaar, denk ik, met ANPR-toezicht, hoewel het vergaren van informatie over autobewegingen dan van verschillende kanten plaatsvindt. Die zaak ging over het volgen van een bepaalde auto gedurende 28 dagen. Hoewel er in de Amerikaanse jurisprudentie altijd van uit werd gegaan dat het een openbare weg was en dat iedereen die auto kon zien, werd in de argumentatie met name ingegaan op het volgende punt: ja, maar niemand zal die auto gedurende 28 dagen zien op de openbare weg. De kans dat iemand daadwerkelijk al die brokjes informatie krijgt, is nihil. Dat betekent dat het bij elkaar leggen van al die brokjes wel een belangrijke inbreuk op de privacy oplevert, hoewel elk brokje afzonderlijk maar een heel kleine inbreuk oplevert. In dit geval is de theorie ontwikkeld voor toepassing van een bepaalde methode.
In Nederland kun je dat erg vergelijken met de drempel van stelselmatigheid: wanneer doe je aan stelselmatige observatie? Dit is echter, denk ik, een veel breder punt, dat al eerder is gemaakt; kijk naar het totaal van opsporingsbevoegdheden en naar de samenloop van opsporingsbevoegdheden als je proportionaliteitstoetsen gaat doen. Dat is een beetje lastig, want bij alle proportionaliteitstoetsen die we op basis van de wetgeving doen – dit geldt ook voor de wijze waarop wetgeving tot stand wordt gebracht en waarop u daarnaar kijkt – wordt voor elke afzonderlijke bevoegdheid bekeken of het nodig is en of we er belang bij hebben. Ja; en dat hebben we dan met waarborgen omkleed. Vaak is er echter te weinig ruimte om de toepassing van een bevoegdheid in het hele stelsel te bekijken, terwijl het mij wel heel belangrijk lijkt om dat te doen. Ik denk dat het, juist in deze Kamer, belangrijk is om wel vaak naar het totale plaatje te kijken.

De **voorzitter**:
Dank. Dat is helder.

Mevrouw **Bredenoord** (D66):
Ik zal proberen overlap te vermijden, maar ik heb voor de heer Koops een vervolgvraag over de mozaïektheorie. De Minister schrijft in de memorie van antwoord een paar keer over a reasonable expectation of privacy, die in de publieke ruimte gewoon minder te verwachten is. Daardoor zou bijvoorbeeld ANPR gerechtvaardigd zijn. Als ik de heer Koops hoor, zegt hij eigenlijk dat dat begrip in een vermenging van publiek-privaat en het Internet of Things minder bruikbaar is. Kan hij daar nog even op reflecteren?

De heer **Koops**:
Het begrip «redelijke privacyverwachting» hanteren we wat minder in Europa – dat is ook een Amerikaans begrip – maar in de praktijk wordt het wel min of meer gehanteerd zoals we het bij privacybescherming gebruiken. Dat is van oudsher sterk gekoppeld aan de plaats waar je onbevangen jezelf wilt kunnen zijn, zoals we in Nederland zeggen. Van oudsher is dat in de openbare ruimte niet door de wet beschermd. Dat komt vooral doordat je in de openbare ruimte feitelijk onbevangen jezelf kunt zijn, omdat je redelijk anoniem bent. Als je in een grote stad rondloopt, is de kans dat iemand je herkent, met name dat iemand je op verschillende plaatsen herkent en zou volgen, heel klein. De politie moet ook heel veel moeite doen, wil zij één persoon fysiek achtervolgen in de openbare ruimte. Er zijn dus heel veel natuurlijke drempels die van oudsher betekenen dat je privacy in de openbare ruimte eigenlijk niet zo hoeft te beschermen omdat je feitelijk een privacyverwachting hebt. Het begrip «redelijke privacyverwachting» is vooral een normatief begrip voor situaties waarin je wel gevolgd wordt, maar eigenlijk verwacht dat je niet gevolgd zult worden. Hoewel er nu steeds meer mogelijkheden zijn om

mensen te volgen in de openbare ruimte, denk ik dat je als burger nog steeds wel een redelijke privacyverwachting hebt als je in de openbare ruimte rondloopt. Je verwacht niet dat morgen iedereen weet waar je gisteren geweest bent. Dat betekent echter wel dat je nu actiever, met name juridisch, die privacyverwachting verder moet beschermen. De mozaïektheorie kan daar een handvat voor zijn, omdat het iets verder gaat dan dat onderscheid. Ik zou vooral de term «publieke ruimte» wat los willen laten, want in feite neem je in de publieke ruimte ook, via de smartphone en de laptop die je bij je draagt, de dingen die je vroeger in je huis achterliet, met je mee. Dat onderscheid heeft dus veel aan relevantie verloren.

De **voorzitter**:
Ik hoorde mevrouw Bredenoord zeggen – dat hangt samen met het begrip «publieke ruimte» – dat de technologie steeds verder voortschrijdt; denk maar aan het Internet of Things en de zelfrijdende auto. Toen ikzelf dit debat aan het voorbereiden was, vroeg ik mij af of het, aangezien er in auto's al zo veel data voorhanden zijn, überhaupt nog wel nodig is dat we van de overheid vragen om zo'n register aan te leggen. Kun je niet gewoon met een bevel van de officier van justitie of rechtercommissaris aan autobedrijven vragen of zij gegevens van een bepaalde mijnheer of mevrouw hebben en of je die gegevens dan mag hebben? Als voorzitter permitteer ik het mij om deze vraag aan u te stellen, mijnheer Koops.

De heer **Koops**:
Ik weet niet in hoeverre autobedrijven direct toegang hebben tot die gegevens. Soms worden ze in de auto zelf opgeslagen en moet je het kastje dat in die auto zit ...

De **voorzitter**:
Ze hebben toegang.

De heer **Koops**:
In dat geval bestaat gewoon de bevoegdheid tot het vorderen van gegevens. Daar zijn uitgebreide regelingen voor binnen de strafvordering. Deze gegevens zijn daarvan niet uitgesloten. Ik denk dat dit vergelijkbaar is met de discussie die we gevoerd hebben over het bevriezingsbevel en dataretentie. Er zijn allerlei bevoegdheden om gegevens die eenmaal bestaan, tot je te nemen, maar soms ben je te laat omdat die gegevens niet bewaard worden en weg zijn, terwijl ze wel heel handig zouden zijn geweest. We kennen daarvoor in het strafrecht een bevriezingsbevel, waarmee je heel laagdrempelig kunt vorderen dat specifiek aangewezen gegevens even worden bewaard. Stel dat er een moord plaatsvindt langs de snelweg; dan kun je bij wijze van spreken alle autobedrijven vragen om alle gegevens die ze hebben voor 90 dagen te bevriezen. Dat is, omdat het gericht is en per incident afhankelijk is van de wijze waarop je het middel inzet, een veel minder ingrijpende inbreuk dan op voorhand willen dat alle mogelijke gegevens worden bewaard. Daar hebt u, voorzitter, zeker een punt, dat samenhangt met de discussie die wij voerden over de noodzaak van massale opslag.

De **voorzitter**:
Dank. We hebben nog een paar minuten voor nog meer vragen. Ik weet niet of er nog vragen zijn? Pardon, ik zou bijna vergeten dat de heer Van der Ven een vraag gesteld had aan de heer Wolfsen.

De heer **Wolfsen**:
Ik zou niet willen vertrekken zonder de vraag van de heer Van der Ven te hebben beantwoord. Het was wel ingewikkeld, dus dank dat u mij even de gelegenheid gaf om daarover na te denken. Dit is een van de complexe

dingen. Wij gaan in algemene zin om met datalekken zoals wij ermee omgaan. Daarin verschilt de overheid niet van private bedrijven. Volgend jaar treedt, geloof ik, de nieuwe Europese verordening over algemene gegevens in werking, maar er komt ook een speciale richtlijn over rechtshandhavingsgegevens. Daar zit een klachtrecht in voor burgers. Zij kunnen bij ons klagen en wij kunnen dan ook altijd gaan kijken. Wij kunnen bij alles en hebben tot alles toegang. Wij kunnen dus ook alles controleren en in algemene zin toezicht houden op de omgang met lekken: meld je dat en heb je het adequaat beveiligd enzovoort? Wij kunnen dus ook bekijken of het allemaal goed beveiligd is.
Uw vraag, mijnheer Van de Ven, is nog iets preciezer: als het OM gebruikmaakt van de bevoegdheid om binnen te gaan, kan dat dan lekken veroorzaken? Daar zit precies een mankement. Alhoewel, mankement, ik moet voorzichtig zijn. Er lijkt een onevenwichtigheid in de wet te zitten op twee vlakken. Ik zei al in antwoord op eerdere vragen over het besluit en de wet dat je, als je binnentreedt, twee softwarepakketjes nodig hebt. Een. Je hebt een softwarepakket nodig om binnen te treden. Twee. Je hebt software nodig om in de computer te kunnen zoeken of iets ongedaan te maken. Van het tweede moet verslag worden gelegd. Dat moet gelogd worden enzovoort. Maar dat heeft niets met het lek te maken, want dan ben je al binnen. Dat is ook in het besluit geregeld. Dat is gek, want de bevoegdheid creëer je in de wet. Dan moet je de toets, de zorgvuldigheid en de toetsing ook in diezelfde wet regelen. Op die manier houd je de zaak in balans. Anders kan de Minister het later lastiger toetsbaar maken. Het belangrijkste – dat is eigenlijk de kern van uw vraag – is het verslagleggen gelijk vanaf het binnentreden in een woning. Hoe ben je binnengetreden? Hoe zag het lek er uit? Hoe ben je daar binnen gekomen? Daar hoeft echter geen verslag van te worden gemaakt, zo lijkt het. Dat gaat precies om de kwetsbaarheid van de software. Dat maakt het voor ons 100% onmogelijk om dat achteraf te controleren. Dat is op zijn zachtst gezegd merkwaardig. Als je vergaande bevoegdheden creëert, moet je die ook achteraf maximaal toetsbaar maken. Wij kunnen niet bij zaken die onder de rechter komen. Alles wat niet naar de rechter gaat, is heel veel. Daar kunnen wij goed bij, maar als er geen verslag wordt gemaakt, kunnen wij het niet controleren. Dat zou geregeld moeten worden, zo adviseer ik u.

De **voorzitter**:
Hartelijk dank. Ik zie non-verbale communicatie van de heer Egberts en ik ben zo nieuwsgierig wat hij ervan vindt, dat ik hem heel kort de gelegenheid geef om via de interruptiemicrofoon een reactie te geven. Mijnheer Egberts, u krijgt echt niet meer dan één minuut.

De heer **Egberts**:
Ik denk dat heer Wolfsen en ik het eens zijn. Je moet transparant zijn. Je moet als onafhankelijk overheidsapparaat ook heel goed kunnen toetsen of het binnendringen wel goed gebeurt. De bedoeling is ook – dat zal de politie ook nog wel verder kunnen toelichten – om dat allemaal te loggen en om toetsing door een onafhankelijke derde, bijvoorbeeld de inspectie, mogelijk te maken op het binnendringen zelf. Dat is alleen iets anders dan informatie over hoe je binnendringt, de logging en het feit dat je je hebt gehouden aan bevelen, ook te delen met verdediging. Dus ja, er moet absoluut toetsing zijn. Er moet onafhankelijk toezicht zijn door bijvoorbeeld een overheidsapparaat. Maar dat is wat anders dan dat ook delen met de verdediging in een openbaar strafproces.

De **voorzitter**:
Nu zie ik dat de heer Wolfsen nog iets wil zeggen. Mijnheer Wolfsen, u krijgt van mij nog de gelegenheid om daarop te reageren. En dan denk ik dat wij voldoende munitie hebben voor het debat. Dat voeren wij straks verder met de Minister.

De heer **Wolfsen**:
Ik zal het vragenderwijs doen. Wat fijn dat wij het eens zijn over de toetsbaarheid. Ik ben het er ook mee eens dat je het goed moet loggen, als je binnen bent geweest met een technisch gekeurd of niet-gekeurd middel; dat laatste lijkt ons onverstandig. Maar dat is niet de kern van de vraag van de heer Van de Ven. Want je slecht het lek. Er zit een kwetsbaarheid in de software. Je gaat met aparte software naar binnen. Er lijkt geen verplichting te zijn om daar verslag van te maken. Als je dat niet doet, ben je voor de volle 100% niet toetsbaar daarop. Dat lijkt me onwenselijk. Dat lijkt u, zoals ik begrijp, ook onwenselijk. Daar zal een oplossing voor bedacht moeten worden.

De **voorzitter**:
Dank. Wij nemen dit ongetwijfeld mee bij de verdere vragen aan de Minister. Heel hartelijk dank. Het is inmiddels bijna 11.05 uur. Het is tijd voor een korte pauze, maar niet nadat ik de heer Koops, de heer Zuiderveen Borgesius, mevrouw Peters, de heer Bruning, mevrouw De Vries en de heer Wolfsen heel hartelijk heb bedankt voor hun komst naar de Eerste Kamer en hun bijdrage en input voor het plenaire debat. Ik nodig u allen graag uit voor een kopje koffie en ook om het derde blok straks te volgen. Ik ga weer mijn presentjes pakken en aan u overhandigen, maar voelt u zich vrij om alvast naar de koffie te gaan, want ik wil u graag allen weer over maximaal een kwartier terug zien in de Kamer.

De vergadering wordt van 11.06 uur tot 11.22 uur geschorst.

Thema III: Uitvoerbaarheid en handhaafbaarheid

De **voorzitter**:
Wij zijn toe aan het derde blok: uitvoerbaarheid en handhaafbaarheid. Welkom aan onze gasten, de heer Van der Plas en de heer Rijpkema, allebei van de nationale politie, de heer Siedsma van Bits of Freedom, de heer De Groot van Microsoft Benelux, mevrouw Postma van Google, de heer Prins van Fox-IT en de heer Jacobs van de Radboud Universiteit Nijmegen. Heel hartelijk welkom! Heel fijn dat u de moeite hebt genomen om hier naartoe te komen om met ons uw visie op de wetsvoorstel te delen. De spelregels zijn inmiddels genoegzaam bekend: vijf minuten spreektijd. Ik heb een timer. De heren van de nationale politie hebben mij verzocht om hun spreektijd samen te voegen tot tien minuten, want de heer Van der Plas doet het woord namens de heer Rijpkema. De heer Rijpkema is voor de moeilijke vragen. Dus dat weten we dan even. Ik heb die tien minuten toegestaan met daarbij de opmerking: als het sneller kan, zou dat erg plezierig zijn. Want ik wil zo veel mogelijk ruimte laten voor de discussie.
Aan u het woord, mijnheer Van der Plas. U bent binnen de nationale politie programmadirecteur, zo heb ik begrepen, en behept met dit dossier.

De heer **Van der Plas**:
Geachte voorzitter, geachte leden van de vaste commissie voor Veiligheid en Justitie, geachte deelnemers aan deze discussie. Allereerst wil ik u danken dat ik hier namens de politie een visie mag geven op de twee voorliggende wetsvoorstellen. Ik zal hier voor zowel de ANPR als de Wet computercriminaliteit III het woord voeren. In mijn functie van programmadirecteur digitalisering cybercrime ben ik namelijk verantwoordelijk voor de implementatie van zowel de Wet computercriminaliteit III als de ANPR-wetgeving. Vanuit mijn jarenlange ervaring in opsporing en intelligence in verband met allerlei vormen van ernstige criminaliteit, wil ik beginnen met twee praktijkvoorbeelden die het belang van beide wetsvoorstellen illustreren.

Onlangs deden wij een inval bij een verdachte van kinderporno. Tijdens de inval bleek dat de verdachte, zoals we vaak zien, een kill switch had, waarmee hij met één handeling alle bewijzen voor ons als politie ontoegankelijk kon maken door versleuteling. Het materiaal zal echter hoogstwaarschijnlijk nog steeds beschikbaar zijn voor andere kinderpornoafnemers. Doortastend optreden wist dit deze keer maar net te voorkomen. Helaas hebben wij niet altijd dit succes. In dit soort gevallen kan de bevoegdheid tot binnendringen de zekerstelling van het bewijs en de verstoring van het kinderpornonetwerk mogelijk maken met een grotere kans op succes.
Ik geef een ander voorbeeld, nu met betrekking tot de bevoegdheid van de bewaarplicht ANPR. Criminelen die met explosieven geldautomaten opblazen met geen enkel gevoel voor de eventuele slachtoffers onder bewoners, zijn moeilijk te pakken. Tegelijkertijd weten we dat zij niet alleen in de nacht van de ramkraak bij de geldautomaat komen, maar al eerder aan voorverkenning doen. Het wetsvoorstel ANPR maakt het mogelijk om nieuwe verbanden te leggen met eerdere voertuigbewegingen. Daardoor kunnen wij daders opsporen en ramkraken stoppen. Dat geldt ook voor terrorisme. Was een Duitse of Belgische aanslagpleger net voor de aanslag ook in ons land? Alleen door de tijdelijke opslag van passagegegevens is dit voor zijn auto vast te stellen.
In de context van dit politiewerk zie ik vier samenhangende ontwikkelingen: digitalisering, mobilisering, versleuteling en anonimisering. Onze samenleving verandert ingrijpend en steeds sneller onder invloed hiervan. De grenzen van gemeenten in dit land en van digitaal en fysiek bestaan niet meer. Traditionele methoden als interceptie zullen door toenemend gebruik van versleuteling steeds minder als bewijs kunnen dienen. Zo dreigen wij als politie met lege handen te komen staan en komen opsporing en rechtshandhaving steeds meer onder druk te staan. Voor het bestrijden van zware en georganiseerde criminaliteit is het dan ook noodzakelijk om zicht te blijven houden op de communicatie van criminelen die ernstige feiten plegen. Daarvoor is de bevoegdheid tot binnendringen uit de Wet computercriminaliteit III nodig. Op die manier kan kennis worden genomen van de inhoud van berichten voordat deze worden versleuteld.
Deze bijeenkomst staat ook in het teken van privacy. Ik wil daar nader op ingaan. Wij zijn er als politie om de grondrechten te beschermen en voor de veiligheid van onze samenleving. Als bewaker van de rechtsstaat hecht de politie grote waarde aan het recht op privacy, maar soms kan en moet de politie inbreuk maken op individuele grondrechten, omdat andere, zwaarder wegende belangen van de samenleving als geheel dat eisen. Het Wetboek van Strafvordering kent de politie en het OM daartoe gelimiteerde en afgewogen bevoegdheden toe. Dames en heren, ik ken geen enkele andere bevoegdheid die met zo veel waarborgen is omgeven als de nieuwe bevoegdheid van heimelijk binnendringen in een geautomatiseerd werk. Die beperkt zich tot zeer ernstige strafbare feiten in een geautomatiseerd werk in gebruik bij een verdachte, onder bevel van de officier, met een CTC en een rechter-commissaris, met gekeurde technische hulpmiddelen, met geautoriseerd en opgeleid personeel en onafhankelijk toezicht achteraf door de Inspectie Veiligheid en Justitie. Deze buitengewoon hoge eisen zijn naar mijn mening terecht, omdat het om een ingrijpende bevoegdheid gaat. Ten slotte is het in internationaal opzicht belangrijk om de verhouding tot de ons omringende landen te benoemen. In Europa is al een wet vergelijkbaar met de Wet computercriminaliteit III in werking in landen als Groot-Brittannië, Duitsland, België, Frankrijk, Denemarken en Noorwegen.
Vandaag spreken wij ook over het wetsvoorstel ANPR. In de context van de veranderende wereld is de aanpassing van onze wettelijke mogelijkheden ook op dit gebied een must. Ook hier spelen maatschappelijke belangen, de noodzaak van het gebruik en de privacyaspecten. Dit

voorstel geeft de politie de mogelijkheid om achteraf beter te onderzoeken wat er in de aanloop naar een delict heeft plaatsgevonden. Het wetsvoorstel biedt de mogelijkheid om na een delict zicht te krijgen op daders, routes en eventuele mededaders. Ik noemde al de ram- en plofkraken, maar dit geldt ook voor de mobiele bendes die in heel Nederland en Europa inbreken, soms op zeer gewelddadige wijze. Na de inbraak kunnen wij met deze wet zien waar het voertuig recentelijk is geweest en daarmee in welke omgeving de verdachte tijdelijk verblijft of wat zijn vluchtplaats of vluchtrichting geweest is. Bij gijzelingen en ontvoeringen is het mogelijk om op basis van opgeslagen kentekenpassages het juiste kenteken te herkennen en ter beschikking van de politie te stellen, direct in referentiereizen te plaatsen en daarmee realtime de bewegingen van het voertuig te onderkennen. Deze directe opvolgacties waarbij de daders kort na het delict gelokaliseerd kunnen worden, zijn van groot belang voor de heterdaadkracht van de politie in haar strijd tegen criminaliteitsvormen met een mobiel karakter. De politie is zich zeer bewust van de zorgvuldigheidseisen die daaraan gesteld worden.
De invoering van beide wetten vereist – ik zeg het nogmaals – zorgvuldigheid. De politie bereidt zich hierop voor. Hiertoe heb ik een CC3-programmaorganisatie (Computercriminaliteit III) ingericht, waarin eigen specifieke deskundigheid en externe expertise bij elkaar worden gebracht. Er komt een strikte scheiding tussen het technische team, dat geautomatiseerde werken binnendringt en doorzoekt, en de tactische opsporingsteams die ondersteuning vragen. Digitaal rechercheren is vakwerk. Daarom worden alleen goed opgeleide deskundigen en gecertificeerde medewerkers aangewezen en ingezet. Hetzelfde geldt voor de invoering van de ANPR-wetgeving.
Dames en heren, ik kom tot een afronding. Criminelen maken gebruik van alle voor hen beschikbare methodes. Op dit moment staat de politie naar mijn mening op forse achterstand. U staat voor de belangrijke afweging of u een politie wilt die, als het echt moet, kan doordringen tot de diepste lagen van ernstige criminaliteit. Zonder de bevoegdheid en het vermogen om op afstand binnen te dringen en, waar nodig, gegevens ontoegankelijk te maken, halen we die achterstand nooit meer in. Zonder passagegegevens is onze kracht in de aanpak van ernstige vormen van criminaliteit beperkt. De huidige bevoegdheden schieten simpelweg tekort.
De wetsvoorstellen computercriminaliteit III en ANPR zijn voor ons een nieuw en noodzakelijk instrument om onze missie waakzaam en dienstbaar voor de veiligheid van onze samenleving invulling te kunnen blijven geven. Ik dank u voor uw aandacht.

De **voorzitter**:
U hebt het zelfs in zeven minuten gered. Dat is echt fantastisch. Dank u voor uw heldere verhaal. Ik geef graag het woord aan de heer Siedsma van Bits of Freedom.

De heer **Siedsma**:
Geachte senatoren, heel veel dank voor de mogelijkheid om vandaag met u van gedachten te wisselen over dit belangrijke onderwerp. Ik denk dat de voorgestelde hackbevoegdheid eigenlijk aantoont dat op diverse punten onvoldoende is nagedacht over de consequenties van de uitvoering van die bevoegdheid. Zonder reparatie van die aspecten staan de rechten van onschuldige burgers op het spel.
Er is in eerdere rondes heel veel gezegd over de noodzaak en over de privacybelangen. Ik zal daar niet te veel over zeggen, behalve dan dat Bits of Freedom die kritiekpunten hartgrondig deelt. Ik zal het in mijn bijdrage vooral hebben over de problematiek rond het gebruik van kwetsbaarheden. Ik zal eerst uitleggen waarom dat problematisch is en daarna zal ik kort ingaan op het gebruik van hacksoftware die op dit moment onterecht buiten de boot valt. Ik zal afsluiten met het gebrek aan technische

waarborgen bij dit voorstel. Ik zal bij elk punt ook enkele suggesties geven voor een eventuele verbetering en de vraag of dat eventueel mogelijk is.
Er is vandaag al veel gezegd over kwetsbaarheden. Ik gok dat ook de sprekers na mij daar nog het een en ander over zullen gaan zeggen. Laat mij dan volstaan met te zeggen dat Bits of Freedom tegen het gebruik van onbekende kwetsbaarheden is, vanwege het grote risico voor de onschuldige burger. Het belang dat de Nederlandse Staat heeft bij het bestaan van onbekende kwetsbaarheden, vinden wij een averechts belang. Dat staat haaks op het verbeteren van onze cybersecurity. De risico's die kunnen ontstaan – zo hebben wij vandaag al gehoord – zijn absoluut niet denkbeeldig. Nederland is natuurlijk niet het enige land dat dit doet. De Staatssecretaris hint daar ook op in de beantwoording van de vragen die uw Kamer heeft gesteld. Hij zegt: andere landen doen dit ook en de rol van Nederland is daarom eigenlijk maar klein. Dat argument laat zich eigenlijk vertalen als: ja maar, hullie doen dat ook, dus ja. Ik heb zelf in groep 7 al de harde en wijze les geleerd, dat dat een argument is waar je niet mee weg kunt komen. Ik wens dezelfde louterende werking ook toe aan het Ministerie van Veiligheid en Justitie. Ik vind vooral dat de Nederlandse overheid het gewoon beter moet doen. Nederland kan op dit punt ambitieuzer zijn. Doe dat dan ook!
Dat gezegd hebbende; stel dat u zegt – dat is uiteindelijk een politieke afweging – dat die onbekende kwetsbaarheden toch moeten worden ingezet. Nogmaals, wij vinden dat geen verstandig plan, maar mocht u dat toch willen doen, dan moet er een helder beleid zijn voor de inzet en het achterhouden van die kwetsbaarheden. Wij hebben net het Openbaar Ministerie gehoord. Dat zegt: in het geval van WannaCry zouden wij 100% zeker gemeld hebben, daar is geen twijfel over mogelijk. Ik ben er ontzettend blij mee dat het Openbaar Ministerie dat zegt, maar dat is een anekdote, dat is nog geen beleid. Dat beleid is er op dit moment niet. Dat beleid moet een helder toetsingskader neerzetten voor de afweging tussen enerzijds het achterhouden van een kwetsbaarheid uit opsporingsbelang en anderzijds het algemene belang dat gediend is bij zo snel mogelijk melden. Aanvullend moeten er onafhankelijke externe experts bij die afweging betrokken worden die, waar nodig, tegenspraak en tegenwicht kunnen bieden aan de opsporingsbelangen waar het Openbaar Ministerie mee te maken heeft. Want ik heb heel veel vertrouwen in het Openbaar Ministerie, maar natuurlijk is het Openbaar Ministerie belast met de opsporing. Het is heel fijn als er dan aanvullende experts zijn die kunnen zeggen: heb je hieraan gedacht, is dit en dit niet belangrijk? Dan kan er een evenwichtig oordeel tot stand komen. Zolang dit beleid ontbreekt, kan er wat Bits of Freedom betreft echt geen sprake zijn van het gebruik van onbekende kwetsbaarheden. Zolang je de basisvoorwaarden niet geregeld hebt, moet je het gewoon simpelweg niet doen. Dat zou ik als advies willen meegeven.
Dan kom ik op het gebruik van hacksoftware. Het beoogde gebruik van de hacksoftware illustreert eigenlijk het hele kwetsbaarhedenbeleid en het feit dat dat onvoldoende doordacht is. De politie zal off the shelf hacksoftware gaan inkopen om verdachten te kunnen gaan hacken en wel bij bedrijven die ontzettend goed zijn in het maken van dat soort software. Die bedrijven zijn natuurlijk genoegzaam bekend. Ik kan Gamma International noemen en HackingTeam. Ik weet niet of dat bedrijf nog actief is, maar ook dat heeft behoorlijk wat software geleverd. Er zijn tal van bedrijven die hier ontzettend goed in zijn.
Over de hacksoftware zijn bij de parlementaire behandeling in de Tweede Kamer en tot nu toe in de Eerste Kamer eigenlijk twee dingen duidelijk geworden. Ten eerste hoeven onbekende kwetsbaarheden die met hacksoftware worden gebruikt, niet te worden gemeld, omdat de Nederlandse politie niet weet of niet mag weten of die producten gebruikmaken van kwetsbaarheden. Ten tweede zal juist dit soort software in de praktijk veelvuldig ingezet worden. Wat betekent dit? In theorie is er

een meldingsplicht en op papier is melden dus het uitgangspunt, maar in werkelijkheid zal het achterhouden van die kwetsbaarheden dus de praktijk zijn. We denken nu dat wij de waarborgen ontzettend goed geregeld hebben en dat de meldingsplicht voldoet, maar we zien dat de praktijk door het gebruik van de hacksoftware totaal anders is. Dat betekent dat er een soort dode letter in de wet is en dat is voor ons onverteerbaar. Als het uitgangspunt is dat onbekende kwetsbaarheden gemeld moeten worden, dan moet dat gelden ongeacht de manier waarop die kwetsbaarheden gevonden zijn of worden gebruikt. Of dat nou via een vaardige politieagent is of omdat de kwetsbaarheden deze hacksoftwarepakketten worden ingekocht of gebruikt: onbekende kwetsbaarheden moet je melden. De Nederlandse regering mag zich dan ook niet verschuilen achter geheimzinnigheid of achter het feit dat een bedrijf geen openbaarheid wil geven. Van Nederland mag op dit gebied ook echt wel iets meer ambitie verwacht worden. Axel Arnbak zei het al: hier ligt een voortrekkersrol voor Nederland, pak die rol dan ook!
Tot slot kom ik op de technische waarborgen. Het is cruciaal dat naast de juridische waarborgen ook de technische waarborgen op orde zijn. Die bepalen namelijk voor een groot deel hoe groot het risico op ongewenste inbreuken daadwerkelijk is. Het voorgestelde besluit Onderzoek in geautomatiseerd werk biedt die waarborg helaas op een aantal essentiële punten niet. De Autoriteit Persoonsgegevens is daar ook al op ingegaan. Die heeft terecht gezegd dat de waarborgen eigenlijk pas gelden vanaf het moment dat de bevoegdheid wordt ingezet. Als je bijvoorbeeld kijkt naar huiszoeking, ontstaat inbreuk op het moment dat een deur wordt open gebeukt en niet op het moment dat een politieagent in de kamer staat. Bij het hackvoorstel betekent dit dat de waarborgen, de logging en het besluit technische hulpmiddelen dus moeten gaan gelden op het moment dat er wordt gestart met hacken en niet op het moment dat er al gehackt is en er een bevoegdheid wordt uitgeoefend. Dat is wat ons betreft echt het grootste pijnpunt.
Ik rond af. Ik ben heel blij dat het OM zelf ook al heeft gezegd dat dit aangepast moet worden. Ik kijk uit naar die aanpassingen. Er zijn heel veel problemen met deze wet. Wij raden het gebruik van onbekende kwetsbaarheden af, maar als het dan toch moet, dán op een goede manier. Nu is het gewoon niet goed genoeg. Er moet een beter beleid komen voor het gebruiken van kwetsbaarheden en dat moet ook gelden voor de aangekochte hacksoftware. Ook de technische waarborgen moeten echt nog verbeterd worden voordat we kunnen zeggen: hier is een raamwerk waar de politie mee mag optreden en waar de Staten-Generaal tevreden over mag zijn.

De **voorzitter**:
Hartelijk dank, mijnheer Siedsma. Uw visie is helder. Ik geef het woord nu aan de heer De Groot, directeur Corporate Affairs van Microsoft Benelux. Ook u hebt vijf minuten.

De heer **De Groot**:
Dank u wel. Ik heb de luxe of misschien de pech dat ik naast mij precies kan zien hoeveel seconden ik nog heb, dus ik ga gauw beginnen.
Namens Microsoft dank ik de Eerste Kamer voor haar uitnodiging om vandaag onze visie te geven op het wetsvoorstel Computercriminaliteit III. Microsoft is een wereldwijd opererend technologiebedrijf en aanbieder van onlinediensten aan miljarden mensen. We hebben in Nederland bijna 1.000 medewerkers en meer dan 7.000 partners. We hebben geïnvesteerd in grote datacenters in dit land. We zijn hier zo actief omdat Nederland beschikt over een digitale infrastructuur van wereldklasse, een hoogopgeleide beroepsbevolking, een innovatief bedrijfsleven en een overheid met ambities om Nederland digitaal te transformeren. Microsoft werkt dan ook graag samen met de Nederlandse overheid, het bedrijfsleven en de

burgers hier, zodat we samen een slimme toepassing van technologie kunnen inzetten voor economie en maatschappij.
Vandaag zit ik hier echter omdat wij ons zorgen maken. Wij vrezen dat de invulling van deze ambities door diezelfde overheid met dit wetsvoorstel zullen worden geremd. Natuurlijk begrijpt Microsoft de cruciale rol die de wetshandhaving speelt in het waarborgen van veiligheid in onze samenleving. Daarbij is het echter wel van groot belang dat wetgeving waarmee de Nederlandse politie en justitie een mandaat krijgen om criminele activiteiten te onderzoeken, in stevige waarborgen voorziet om fundamentele rechten van mensen te beschermen, zoals het recht van de gebruikers van onze technologie op privacy en op de bescherming van gegevens tegen zowel criminelen als overheden. Dat zijn kernwaarden van onze rechtsstaat, waar bij uitstek uw senaat nieuwe wetgeving aan toetst.
Het zal geen verrassing zijn, maar Microsoft maakt zich met name zorgen over de mogelijkheid die het wetsvoorstel aan de overheid laat om gebruik te maken van kwetsbaarheden in software. Op vrijdagavond 12 mei werden duizenden gebruikers van Windows in tientallen landen overal ter wereld slachtoffer van WannaCry. WannaCry was zogenaamde ransomware, waarmee bestanden op computers werden gegijzeld. Het WannaCry-virus was grotendeels gebaseerd op een virus dat door een hackerscollectief was gestolen van de Amerikaanse inlichtingendienst NSA. De NSA maakte met dat virus lange tijd gebruik van een kwetsbaarheid in Windows waarvan zij al op de hoogte was, terwijl Microsoft nog niet van het bestaan van die kwetsbaarheid wist. Zodra we leerden over die kwetsbaarheid, heeft Microsoft direct een patch ontwikkeld en Windowsgebruikers wereldwijd al twee maanden voor de daadwerkelijke uitbraak van WannaCry een update gestuurd. Gebruikers met geüpdatete versies van Windows waren daarmee beschermd op die 12de mei, maar gebruikers die geen update hadden geïnstalleerd, waaronder ziekenhuizen, bedrijven, overheden en consumenten, werden helaas door het virus getroffen.
Hoewel de schade in Nederland gelukkig beperkt bleef, moet WannaCry ook voor de Nederlandse overheid behalve een herinnering aan het grote belang van updates ook een wake-upcall zijn. Het gebruik en de opslag van zulke kwetsbaarheden en het achterhouden daarvan voor softwarebedrijven zoals Microsoft kan burgers, organisaties en de maatschappij grote schade berokkenen. In het onwenselijke geval dat de Nederlandse overheid door middel van het voorliggende wetsvoorstel toch de mogelijkheid krijgt om kwetsbaarheden te gebruiken, is het wat Microsoft betreft in ieder geval cruciaal om in sterkere waarborgen voor dat gebruik te voorzien.
WannaCry heeft laten zien dat het niet alleen van belang is dat overheden voorzichtig omspringen met kwetsbaarheden, maar dat ook het inwinnen van kennis vanuit de private sector essentieel is voor het maken van zorgvuldige afwegingen door die overheid over hoe, wanneer en met wie kwetsbaarheden worden gedeeld. Onder de regering-Obama is in de Verenigde Staten het zogeheten Vulnerability Equities Process gestart, waarmee de onthulling van niet publiekelijk bekende kwetsbaarheden binnen de Amerikaanse overheid wordt georganiseerd. In het Amerikaanse Congres is daarnaast recent een wetsvoorstel ingediend, de toepasselijk geheten PATCH Act, die dit proces verder zou verdiepen met het inrichten van een review board. Die review board zal beleid gaan opstellen om te bepalen of, wanneer en hoe de overheid informatie over niet publiekelijk bekende kwetsbaarheden met andere actoren zou moeten delen.
Wij roepen de Eerste Kamer, bij de behandeling van dit wetsvoorstel – en ook de overheid, bij de implementatie daarvan op termijn – op om bij het gebruik van kwetsbaarheden, hoe ongewenst wij dat ook vinden, naar

voorbeeld van het Vulnerability Equities Process en de PATCH Act in een veel sterker toetsingskader te voorzien.
Daar laat ik het voor nu even bij. Het spreekt voor zich dat ik deze en andere zorgen in de discussie graag nader toelicht.

De **voorzitter**:
Heel hartelijk dank. Dat was ruim binnen de vijf minuten, maar zeer helder. Dank daarvoor.
Mevrouw Postma, u bent Public Policy and Government Relations Manager bij Google. Ook aan u vijf minuten om uw visie met ons te delen.

Mevrouw **Postma**:
Heel veel dank. Allereerst dank ik u voor de uitnodiging om hieraan bij te dragen. Ik vind het goed om te zien dat veel bedrijven en organisaties die wij regelmatig spreken, hier ook aanwezig zijn.
De belangrijkste vraag die hier centraal zou moeten staan, is wat mij betreft of deze wet het internet nu veiliger of onveiliger maakt. Alle experts en bedrijven die ik spreek, trekken de conclusie dat het internet hiervan onveiliger wordt. Dat is een analyse die wij delen, en dat punt wil ik allereerst duidelijk maken.
Het wetsvoorstel an sich geeft opsporingsdiensten, waaronder de politie, een zeer ruime bevoegdheid om in te breken, te betreden of te hacken, zo u wilt. Dat mag op allerlei geautomatiseerde werken. Zoals eerder al is gezegd, is dat een ruim begrip. Het kan netwerken, systemen of allerlei apparaten betreffen. Het gaat over geautomatiseerde werken die bij een verdachte in gebruik zijn. De meest logische manier om dat te doen is door gebruik te maken van kwetsbaarheden in systemen. Dergelijke zwakke plekken worden regelmatig ontdekt. Zodra ze ontdekt worden, kunnen bedrijven ze repareren en de lekken dichten. Denk bijvoorbeeld aan de telefoon, die regelmatig updates krijgt. Dat zijn vaak oplossingen voor deze kwetsbaarheden.
Ten eerste geeft het wetsvoorstel een prikkel om de gangbare, zorgvuldige weg, namelijk informatie bij bedrijven opvragen aan de voordeur, te omzeilen. In het Wetboek van Strafvordering staat een procedure die veel juridische waarborgen bevat en ertoe noopt om hierin proportioneel te werk te gaan. Daarnaast geeft dit wetsvoorstel de opsporingsdiensten een prikkel om onbekende kwetsbaarheden te kopen en vervolgens te gebruiken om in te breken. Het is al veel gezegd, maar het vervelende als je dat doet en de informatie niet deelt, is dat bedrijven de kwetsbaarheden niet of veel kunnen repareren, waardoor iedereen een risico loopt. Bovendien gaat het hier om black boxes, zoals ook al eerder is gezegd. Je koopt eigenlijk een gereedschapskist waarvan je niet precies weet wat erin zit, maar de politie mag deze zonder te testen gebruiken.
Volgens de vele bedrijven en experts die ik spreek, wordt het internet met dit wetsvoorstel dan ook onveiliger voor de vele gebruikers. Het is slecht voor het vertrouwen in Nederland. Nederland is een leidend internetland. Het lijkt mij van het grootste belang dat we dat blijven. Omdat de toekomst van het internet in Nederland zo belangrijk is, lijkt me de inwerkingtreding van dit wetsvoorstel an sich een ongelukkige ontwikkeling.
Verregaande nieuwe bevoegdheden vragen om goede juridische waarborgen. Dat is altijd zo als er nieuwe wetgeving in de plek van oude komt. Maar gezien de kwaliteit van het wetsvoorstel ligt daar nog een ruime taak, lijkt mij. Het is al eerder genoemd, dus ik zal hier kort over zijn. Het gaat om het toezicht en om goede waarborgen voor het gebruik van onbekende kwetsbaarheden, die we ook weleens zero-days noemen. In de motie-Verhoeven van 6 juni, die is verworpen, wordt heel duidelijk aangegeven dat het op dit punt ontbreekt aan kwaliteit van beleid, terwijl het gebruik wel zou moeten worden ingeperkt. Ik vraag u om daar serieus naar te kijken. Ik wil mij verder kort aansluiten bij mijn collega De Groot

van Microsoft, die aangaf dat er in Amerika wordt gewerkt aan goede criteria en waarborgen middels de zogenoemde PATCH Act. Dat is heel belangrijk, want dat ontbreekt in Nederland nog bij het gebruik van kwetsbaarheden.
Ik kom tot een afronding. Het zou wat mij betreft te prijzen zijn als de senaat kritisch naar het wetsvoorstel keek. Nogmaals, laat er geen misverstand over bestaan: wij zijn an sich sterk voorstander van het aanpakken van misstanden op het internet. Daar werken we samen aan en daarvoor doen we allemaal ons best, of het nu gaat om criminele activiteiten of andere zaken. Het wetsvoorstel draagt daar echter niet aan bij. Het vergroot de onzekerheid en mist de noodzakelijke waarborgen.

De **voorzitter**:
Heel hartelijk dank. Ook u was helder. Kritisch naar wetsvoorstellen kijken doen we trouwens altijd; daar mag u op rekenen! Het is goed dat u ons daarvoor nog wat input hebt gegeven.
Mijnheer Prins, u bent oprichter en directeur van Fox-IT. Ook u krijgt vijf minuten het woord om uw visie met ons te delen.

De heer **Prins**:
Dat zal ik dan ook doen, waarbij ik heel kritisch ben op de mensen aan mijn rechterzijde. Ik ga het vooral hebben over de Wet computercriminaliteit III. Mijn invalshoek is dat ik positief tegenover deze wet sta. Ik denk dat die heel hard nodig is in de strijd tegen cybercrime. Fox-IT, het bedrijf waarvoor ik werk, heeft dagelijks te maken met slachtoffers van cybercrime. We zien allemaal dat het fenomeen groter wordt zonder dat de relevante daders worden aangehouden. Dat leidt ertoe dat bedrijven geen zin meer hebben om nog aangifte te doen. Ze zien toch dat de politie uiteindelijk niet in staat is om de hackzaken voor hen op te lossen. Zonder enige vorm van pakkans zal cybercriminaliteit in de toekomst voor nog veel grotere schade zorgen.
Het is alweer zeven jaar geleden dat wij de politie mochten helpen bij het ontmantelen van het botnet Bredolab. Dit is heel relevant in de discussie rondom privacy en de zorgen over het feit dat de overheid de privacy van burgers gaat schenden: de realiteit is dat er nu continu botnets zijn waarmee de privacy van gebruikers geschonden wordt. Bredolab had al 30 miljoen slachtoffers gemaakt. Er was niks tegen te doen, behalve ook toen al hacken. Dit speelde in 2009 of 2010. Er was toen nog geen wetgeving voor, maar de politie had het lef om dit toch te doen. Uiteindelijk is dat succesvol gebleken. De slachtoffers zijn gewaarschuwd en de dader is aangehouden en veroordeeld. Ik kan me niet herinneren dat de Nederlandse politie verder ooit zo'n grote zaak met zo veel impact zelfstandig heeft kunnen oplossen. De politie heeft daarna ook niet meer kunnen hacken.
Over het algemeen lopen dit soort zaken vast op het achterhalen van een spoor van de daders in het fysieke domein. Meestal loopt het spoor dood bij een IP-adres van een computer in het buitenland die speciaal voor dit doel gehuurd is. Alleen door dit soort computers te hacken, kun je sporen vinden die een relevante aanwijzing kunnen geven in het fysieke domein, zodat de politie met haar andere bevoegdheden verder kan gaan en uiteindelijk bij een dader kan uitkomen. In de praktijk blijkt dat nu ook. Als er uit een onderzoek echt een naam naar boven komt, vaak omdat private bedrijven wel de ruimte nemen om wat te hacken, kan de politie op rechtsverzoek daadwerkelijk bij de daders uitkomen.
Een ander belangrijk fenomeen dat we nu steeds meer zien is end-to-end-encryptie. Daarvan ben ik groot voorstander, maar daardoor wordt het middel van de taps, waar de politie nu zwaar op leunt, steeds minder waardevol. Daarvoor moet in de balans iets anders gevonden worden. Dat zou heel goed hacken kunnen zijn.

Veel van de negatieve reacties komen volgens mij voort uit onterechte angsten. Ik denk dat de wet voldoende waarborgen biedt om te voorkomen dat willekeurige politiemensen bij te veel mensen in hun iPhone mee gaan kijken. Maar los van de juridische beperkingen brengt de techniek ook een natuurlijke hindernis met zich mee. Hacken is een complexe operatie om uit te voeren. Elke computer is anders geconfigureerd. Zeker als je als hacker, in dit geval dus als politie, niet gezien wilt worden, moet je echt heel omzichtig te werk gaan. Het massaal hacken van veel computers zal dus niet mogelijk zijn.
Bovendien moet u zich het hacken door de politie niet te complex voorstellen. Soms komt uit een tap of uit een gesprek bijvoorbeeld een wachtwoord naar voren dat toegang biedt tot een cruciale server; volgens mij heb ik dat voorbeeld net ook al gehoord. De politie mag dat wachtwoord op dit moment niet gebruiken. Het lijkt me heel duidelijk dat dit snel opgelost moet worden.
Voor de uitvoerbaarheid van de wet is het van belang om te weten wat de politiemensen daadwerkelijk kunnen. Ik heb een heel hoge dunk van de mensen die bij de politie aan cybercrime werken. Zij kunnen technisch goed hacken, maar weten daarbij verdomd goed wat ze moeten doen om te voorkomen dat elke hack die ze uitvoeren leidt tot te veel nevenschade. Daarmee heb ik alvast een vraag van de heer Van de Ven beantwoord. Collateral damage is best een risico bij hacken. Dat houdt in dat je moet weten wat je doet. Ik acht de Nederlandse politie daartoe goed in staat.
Daarnaast vind ik de regeling rondom onbekende kwetsbaarheden onbegrijpelijk; volgens mij ben ik daarin de enige vandaag. De politie is al geholpen als zij alleen gebruik kan maken van bekende kwetsbaarheden, maar ik voorzie zeer relevante incidenten waarbij de politie zal moeten terugvallen op paardenmiddelen zoals zero-days. Juist in onderzoeken waarbij er weinig tijd is en waarbij het afbreukrisico hoog is, zijn deze onbekende kwetsbaarheden essentieel. Mijn indruk is dat het gebruik hiervan de politie met de aankomende wetgeving in de praktijk ontnomen wordt.
Desondanks denk ik dat we echt niet langer kunnen wachten met nieuwe wetgeving. De politie zal het moeten doen met de bekende kwetsbaarheden. Voor een deel van de zaken zal dat wel degelijk helpen. Ik hoorde net dat er na vijf jaar een evaluatie komt. Mijn voorstel is: doe dat nou na drie jaar. Dan zal blijken dat we misschien toch eens opnieuw moeten kijken naar de inzet van onbekende kwetsbaarheden. Misschien is er in het vragenrondje nog meer tijd voor, maar ik heb zojuist heel veel onzin gehoord over het gebruik van die kwetsbaarheden, bijvoorbeeld de conclusie dat het gebruik van kwetsbaarheden door de politie Nederland onveiliger maakt. Volgens mij is de realiteit dat die computers nu al onveilig zijn. Die kwetsbaarheden zitten erin. Het enkele feit dat de politie een van die kwetsbaarheden ontdekt, maakt Nederland echt niet onveiliger. Eerder zal de politie in staat zijn om die kwetsbaarheid in te zetten om criminelen te kunnen aanhouden en Nederland daarmee netto wel veiliger te maken.

De **voorzitter**:
Geweldig, dank u wel.
Mijnheer Jacobs, aan u om de rij te sluiten.

De heer **Jacobs**:
Dank u wel, mevrouw de voorzitter. Ik wil om te beginnen kort iets zeggen over de ANPR. Wat ik opmerkelijk vind aan deze wetgeving, is dat ze zo techniekafhankelijk geformuleerd is. Het gaat over visuele waarneming van auto's en het registreren van kentekens. Je kunt al voorspellen dat dit snel wordt achterhaald door de ontwikkelingen rond connected cars, die op allerlei manieren met hun omgeving communiceren. Zoals ik de wetgeving begrijp en lees, worden die mogelijkheden niet gedekt door de

huidige formuleringen. We hebben op andere gebieden gezien dat techniekafhankelijke formulering van wetgeving vrij snel tot problemen gaat leiden. Ik voorspel dat dit ook op dit gebied gaat gebeuren.
Ik ben helemaal voor het gebruik van nieuwe technieken in de opsporing. Mijn achtergrond is ook technisch van aard. Ik vind het uitstekend dat de opsporing daarmee experimenteert. Maar ik ben altijd wel heel erg voor horizonbepalingen daarbij. Ik vind het altijd zo jammer dat dat nooit opgepakt wordt, zodat je tegen de politie kunt zeggen: jullie hebben nu deze nieuwe technieken, probeer ze twee jaar uit, maar laat dan zien dat het daadwerkelijk iets oplevert. In het geval van ANPR lijkt mij dat heel simpel. Laten ze maar aantonen dat het binnen twee of drie jaar iets oplevert en anders wordt de bevoegdheid gewoon weer teruggenomen. Dit lijkt me heel goed om adequater op technische ontwikkelingen te reageren en ook om het publiek meer vertrouwen te geven. De reactie van de Minister is dan vaak: ja, ja, maar we doen na zoveel jaar een evaluatie van de wet. Maar een evaluatie leidt in de praktijk nooit tot afschaffing van bevoegdheden, terwijl een horizonbepaling toch een andere formulering heeft.
Over de juridische status van deze wet hebben mijn academische collegae hiervoor volgens mij heel verstandige dingen gezegd. Ik vermoed dat deze wet snel aangevochten gaat worden bij het Europese Hof in Luxemburg. Je kunt je afvragen of je er als overheid verstandig aan doet, als je dit soort trajecten kunt voorzien.
Dan kom ik tot het hacken. Hacken vind ik een heel lastig onderwerp. Als samenleving hebben wij te maken, als ik het even versimpel, met de discussie: wil je end-to-end encryption of hacken? Als u mij het mes op de keel zet, kies ik hierbij voor de hackbevoegdheid. Ik vind end-to-end encryption een belangrijker gegeven voor het beschermen van onze infrastructuur.
Ik ben lid van de kenniskring van de CTIVD, de Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten. Het is hierbij interessant op te merken dat de hackbevoegdheid allang bestaat voor de diensten. Wat mij enigszins zorgen baart, is dat voor deze wetgeving niet of nauwelijks gekeken is naar de ervaringen op dat gebied. Bijvoorbeeld in de context van de update van de Wet op de inlichtingen- en veiligheidsdiensten, die binnenkort hier in deze senaat behandeld gaat worden, is uitdrukkelijk aandacht besteed aan het hacken via derden, wat vaak in de praktijk voorkomt. Ik heb niets in het voorliggende wetsvoorstel gezien over de zorgvuldigheid die daarvoor nodig is, de extra proportionaliteitstoets die daarbij nodig is en hoe om te gaan met eventuele nevenschade.
Voor mij is het onafhankelijke toezicht het belangrijkste punt. Ook daarin zie je dat de ervaringen van inlichtingendiensten niet of nauwelijks meegenomen zijn. In die context wordt een nadrukkelijke druk ervaren vanuit het Europese Hof in Luxemburg om de onafhankelijkheid van het toezicht beter in te richten. De nieuwe Wiv heeft ook een TIB, een Toetsingscommissie Inzet Bevoegdheden. Ik zou willen pleiten voor echt onafhankelijk toezicht. Dat heb ik eerder in de Tweede Kamer ook gedaan. Dat is om verschillende redenen. Niet zozeer uit wantrouwen tegenover de politie; onafhankelijk toezicht leidt ook tot professionalisering. Ik denk dat dat heel belangrijk is op een relatief onbekend terrein. Daar moet je ook eerlijk bij zeggen: de politie is een organisatie van doeners en niet een organisatie waarin het reflectieniveau tot het hoogste niveau ontwikkeld is. Dit is nou net een gebied waar we toch een aantal dingen nog moeten verkennen. Ik zie enige reactie. Ik probeer beleefd te formuleren. Even tussendoor: ik geef wel eens een voordracht in politiekringen. Dan zeg ik wel eens plagerig: de politie is een mbo-organisatie. Dan zit iedereen te balen, maar uiteindelijk zeggen ze wel: eigenlijk is dat wel zo. Het is wel goed om dat hierbij enigszins in perspectief te zetten. Het zijn allemaal technisch inhoudelijke specialisten die hieraan gaan werken, maar het reflectieniveau is een groot issue hierbij.

De **voorzitter**:
Mijnheer Jacobs, de timer heeft gepiept, al een tijdje geleden. Wilt u tot een afronding komen?

De heer **Jacobs**:
Ja. Ik wilde nog belangrijke dingen zeggen over de zero days. Hopelijk komt er dan een vraag over.

De **voorzitter**:
We gaan er ongetwijfeld vragen over stellen. Dank u wel. Voordat ik de woordvoerders de gelegenheid geef, had ik de indruk dat de heer Van der Plas van de nationale politie iets wilde zeggen. In het kader van hoor en wederhoor is dat misschien ook wel nuttig.

De heer **Van der Plas**:
De uitspraak dat er geen reflectief vermogen in de politieorganisatie is, deel ik uiteraard niet met de heer Jacobs. Natuurlijk hebben we een aantal mbo-mensen, maar er zijn ook wetenschappelijk opgeleide mensen bij ons in dienst. Ik wijs er ook op dat we nogal wat zijinstromers hebben op hbo- en wo-niveau die zeker ook met allerlei technische expertise bij ons binnen komen. Dus ik denk dat dat redelijk gewaarborgd is.

De **voorzitter**:
Hartelijk dank. Ik ga de woordvoerders de gelegenheid geven. Ik zie bijna overal vingers. Mevrouw Gerkens, u was dit keer als eerste. U krijgt ook als eerste de gelegenheid om uw vraag te stellen. Graag aangeven aan wie u de vraag stelt.

Mevrouw **Gerkens** (SP):
Voorzitter. Als eerste wil ik voortborduren op de inbreng van de heer Jacobs en stel ik een vraag aan de heer Van der Plas. Het gaat niet om het mbo-niveau, maar wat we wel vaak horen en ook zien is dat het kennisniveau van de politie bij cybercrime nogal divers in kwaliteit is. Bij de cyberteams zit natuurlijk heel veel kennis. Bij de gewone agenten bij wie je op het bureau aangifte doet, worden mensen nogal eens naar huis gestuurd met opmerkingen als: oplichting op het internet bestaat niet; je had je naaktfoto maar niet moeten rondsturen; daar kunnen we toch verder niets tegen doen. Hoe oordeelt u daarover? Als u zegt dat we de strijd gaan verliezen, is het dan niet belangrijk om daar eerst op in te zetten?
Ik heb een tweede vraag. Ik hoor u en de heer Prins veel zeggen over end-to-end encryptie. Bij end-to-end encryptie werkt het binnendringen natuurlijk niet, want het staat nog steeds encrypted op het toestel. Je moet dus meekijken, zeg maar. Is dat ook de bedoeling die u hebt? Als het anders is, hoor ik het graag.
Ik zou nog graag de mening van de heer Jacobs over zero days willen weten.

De **voorzitter**:
U stelt drie vragen aan drie verschillende mensen. De heer Van der Plas was de eerste in het rijtje. Ga uw gang.

De heer **Van der Plas**:
Mevrouw Gerkens vraagt over de brede kwaliteit op het gebied van cybercrimebestrijding. In 2007 waren wij de eersten die met het Team High Tech Crime het specialisme cybercrime aanpakten. Ondertussen zijn we tien jaar verder. Ik ben het zeer met mevrouw Gerkens eens dat het inmiddels op een veel breder gebied noodzakelijk is dat de politieorganisatie daarvoor geëquipeerd is. Dat geldt voor de mensen die in de dienstverlening aan de balie werken tot en met de korpschef. Wij werken

op alle fronten. Zowel in de dienstverlening, die een tandje bij moet zetten om te ontdekken waarvan iemand aangifte komt doen, als in de cybercrimeteams die in de eenheden komen. Er komen tien teams bij de regionale eenheden. Die gaan de cybercrimezaken oppakken, maar ook voor een deel bekijken hoe het zit met de kennis in de eenheid. Daarnaast hebben wij in de eenheden zelf al de digitale opsporingsspecialisten. Dat zijn er bijna 300. Zij helpen ook om de cybercrime te ontdekken en te zien hoe het in elkaar steekt. Ik ben het zeer met mevrouw Gerkens eens dat de ontwikkelingen snel gaan en dat het kennisniveau nog niet op peil is. We werken er hard aan om dat in de komende jaren voor elkaar te krijgen.

De **voorzitter**:
Dank u wel. Er waren ook vragen aan de heer Prins gesteld?

Mevrouw **Gerkens** (SP):
Aan mijnheer Van der Plas.

De **voorzitter**:
Wel nog aan mijnheer Jacobs.

De heer **Jacobs**:
Over de zero days inderdaad. Ik vind het eigenlijk een non-issue, die hele discussie. Ik verbaas me erover dat het zo veel aandacht krijgt. Dat geldt ook voor de enorme aandacht voor de hacksoftware en hoe dat allemaal gekeurd moet gaan worden. In de praktijk is het hacken van systemen van verdachten iedere keer maatwerk. Er wordt niet op een knop gedrukt van software die je ergens gekocht hebt. Je verkent het systeem van de verdachte om te kijken wat er in dat geval precies voor kwetsbaarheden in zitten. Wat ik begrijp van de politiemensen van Team High Tech Crime en die kringen, is dat ze in de praktijk meer dan voldoende hebben aan de enorme lijsten van bekenden kwetsbaarheden en alle configuratiefouten die mensen maken bij het installeren van die software. Daarmee kom je in heel veel gevallen binnen. De aandacht voor zero days is dus volstrekt overtrokken. Na WannaCry zijn ze natuurlijk internationaal nog omstredener geworden. Ik zou ervoor willen pleiten dat Nederland een nadrukkelijk internationaal signaal zou geven en zegt: wij gebruiken geen zero days en wij melden ze direct. Je moet ook niet denken dat ze kapot zijn als je ze direct meldt. Na de melding hebben de bedrijven nog enige tijd nodig om een patch uit te brengen. Dat duurt misschien een paar weken. Die patchen een keer in de maand. Vervolgens is er in de praktijk ook nog een heel lange periode voordat iedereen dat uitgerold heeft. Dat zag je bij WannaCry. Het is dus helemaal niet zo dat het weg is nadat je het gemeld hebt. Ik vind dus dat we als Nederland een signaal moeten geven: wij gebruiken geen zero days voor dit soort dingen. In de praktijk zijn ze toch beperkt nuttig. Mijn collega naast me verschilt enigszins van mening hierover. Maar dan nog denk ik dat de in de praktijk bestaande dingen voorlopig genoeg zijn.

De **voorzitter**:
Hartelijk dank. Ik zag meer vingers, onder anderen van mevrouw Beuving.

Mevrouw **Beuving** (PvdA):
Ik denk dat mijn vraag goed aansluit bij de opmerking van de heer Jacobs. Mijn vraag is aan zijn buurman gericht, de heer Prins. Ik had gesignaleerd dat de heer Prins een wat ander geluid laat horen dan verschillende andere sprekers. Dat vind ik heel interessant. Ik heb een aantal van die opmerkingen ook al erg ter harte genomen. Ik zal het verslag na afloop goed nalezen. Ik hoorde de heer Prins zeggen dat het belang van het gebruik van de kwetsbaarheden wel groot is. Ik meen ook te hebben gehoord dat hij concludeert dat dit wetsvoorstel het gebruik van

onbekende kwetsbaarheden in feite onmogelijk maakt. Dan denk ik: heb ik een ander wetsvoorstel gelezen? Want ik zie nog heel veel mogelijkheden, maar dan wel binnen een systeem van: in principe melden, maar met toestemming van de rechter-commissaris kan het, als het onderzoeksbelang groot genoeg is, worden uitgesteld.

De **voorzitter**:
Uw vraag is aan de heer Prins, neem ik aan. Mijnheer Prins, wilt u hierop reageren?

De heer **Prins**:
Heel graag zelfs. Laat ik het toespitsen op het in de praktijk onmogelijk maken van het gebruik van onbekende kwetsbaarheden, de zero days. In het algemeen kom je heel ver met de bekende kwetsbaarheden, maar ik kan me situaties voorstellen waarbij je acuut, op dat moment ergens bij een computer wil inbreken. Dan heb je dus geen voorbereidingstijd, geen tijd om te gaan scannen van tevoren en ook geen tijd om te zoeken welke kwetsbaarheid in het apparaat zit. Dan wil je gegarandeerd naar binnen in een toestel van iemand die een ontvoering aan het plegen is of je wilt de locatie van het toestel weten, omdat het misschien wel in de buurt van een ontvoerd kind is of zo. Dan wil je iets op de plank hebben liggen om op dat moment in een gebruikte iPhone 7 onmiddellijk te kunnen inbreken. Dan kun je niet eerst nog gaan shoppen of bij de buren gaan vragen. Ik denk, en dat zie je bij inlichtingendiensten ook, dat het dan essentieel is dat je die dingen op de plank hebt liggen en kunt gebruiken. Maar het hele debat in de Tweede Kamer heeft ertoe geleid dat zodra de politie iets weet van een onbekende kwetsbaarheid, zij die vooral niet op de plank mag leggen, maar moet melden. Het idee achter dat melden is dat wij dan met zijn allen veiliger worden. Dat bestrijd ik heel erg. In elk product zitten nu al honderden onbekende kwetsbaarheden. Dat kun je de leveranciers niet kwalijk nemen. Dat de politie erin investeert om er eentje te vinden in een iPhone en die op de plank legt, maakt dat toestel niet onveiliger. Het maakt het toestel ook niet veiliger als de politie het wel meldt. Er zitten nog 499 kwetsbaarheden in die andere hackers die op zoek gaan ernaar, ook kunnen vinden. In onze dagelijkse praktijk, waarbij wij gevraagd worden om in te breken in allerlei systemen, lukt het inderdaad heel vaak met bekende kwetsbaarheden. Maar in die gevallen waarbij het niet lukt, lukt het ons bijna ook altijd om wel een nieuwe onbekende kwetsbaarheid te vinden. Het kost wel drie, vier weken voordat je naar binnen kunt. Als ik het verslag bij het wetsvoorstel lees, zie ik niet dat de politie in staat zal zijn om onbekende kwetsbaarheden op de plank te hebben liggen en die te kunnen gebruiken op het moment dat dat nodig is.

De **voorzitter**:
Ik zie de heren van de nationale politie knikken.

Mevrouw **Wezel** (SP):
Ik dank de deskundigen voor hun goede inhoudelijke inbreng, waar wij als Kamerleden heel veel aan hebben voor de debatten. Ik heb nog een vraag voor de politie. Iedereen draagt een mobieltje bij zich. Je kunt nu al met gsm-palen precies zien wie er in een bepaald gebied aanwezig is en aanwezig is geweest. Dat kun je terugkijken. Wat is dan nog de toegevoegde waarde om alle kentekens bij te houden? Bij een kenteken heb je nog niet de bestuurder en weet je niet wie de bestuurder was en wie er verder nog in de auto zaten. Als er vier mensen in een auto zitten, heb je ze alle vier met de mobiele nummers. Wat voegt deze wet toe aan wat er nu al kan?

De **voorzitter**:

De heer Rijpkema zou de moeilijke vragen beantwoorden ...

De heer **Rijpkema**:
Hetzelfde probleem doet zich voor bij telefoons, namelijk de anonimisering. Een telefoon staat niet altijd op naam. Een telefoon kan ook een anonieme simkaart bevatten. Het is voor ons een eerste proeve van bekwaamheid om in het opsporingsonderzoek te ontdekken wie van welke telefoon gebruikmaakt. Natuurlijk proberen we dat. Natuurlijk kunnen we achteraf zien op welke locatie de telefoon geweest is. Maar om dat te koppelen aan de persoon is een hele tour de force. Je kunt niet zeggen: dit hebben we niet meer nodig, omdat we van de kentekenregistratie gebruik kunnen maken, of andersom. Het is vaak de combinatie die maakt dat we elke keer een stukje van de puzzel bij elkaar krijgen om het opsporingsonderzoek te volvoeren.

De **voorzitter**:
Dank u voor dit duidelijke antwoord.

Mevrouw **Strik** (GroenLinks):
Ook ik dank de sprekers hartelijk voor hun relevante bijdrage. Mijn vraag heeft betrekking op het onafhankelijk toezicht. Tijdens vorige sessies kwam steeds naar voren hoe belangrijk dat is. We hebben natuurlijk de inspectie. Er is gevraagd of het onafhankelijk toezicht op deze manier voldoende geborgd is. De heer Jacobs sprak daar al over. Wat kunnen we leren van de Wiv? Hoe zou dat eruit moeten komen te zien? Moeten er klachtenprocedures voor burgers komen? Misschien kan de heer Siedsma daar ook nog wat over zeggen. Ik zou het fijn vinden als hij ook kan zeggen of dit niet ook voor ANPR moet gelden. Op welke wijze moet dat belegd worden? De Kamer kan niet achteraf blijven toetsen op welke wijze dat gebeurt.
Ik heb een vraag over de politie, in het bijzonder het opvragen van gegevens bij computercriminaliteit. Mevrouw Postma zei dat die hackbevoegdheid het mogelijk of te makkelijk kan maken om de normale waarborgen bij het opvragen van gegevens te omzeilen. Hoe kunnen wij er zeker van zijn dat, als er volstaan kan worden met het opvragen van gegevens, dat dan ook gebeurt? Vindt die toetsing voldoende plaats?

De **voorzitter**:
Als ik het goed begrepen heb, zijn uw vragen gericht aan mijnheer Jacobs, mijnheer Van der Plas en mijnheer Siedsma.

De heer **Jacobs**:
Ik vind dit een heel belangrijk onderwerp. In de toelichting heb ik gelezen hoe de Inspectie Veiligheid en Justitie dat toezicht zou moeten gaan doen. Dat klinkt in mijn oren heel erg ambtelijk en box ticking, waarbij de zaak per geval bekeken wordt. Wat ik graag zou zien, is een breder toezicht op alle gevallen waarin dit gebruikt wordt, en ook een rapportage daarover. Ik verwijs naar de CTIVD-context. Van mensen uit de inlichtingendienstenwereld hoor ik weleens dat zij vinden dat zij onder scherper toezicht staan dan de politie. De politie functioneert in een opsporingskader waarin je met allerlei daarmee samenhangende eisen te maken hebt. De inrichting van onafhankelijk toezicht is daardoor wat subtieler en misschien moeilijker.
Stel dat er een soort CTIVD komt voor de politie en dat die een uitspraak doet over een bepaalde zaak. Hoe moet je dat strafrechtelijk dan begrijpen? Kan het leiden tot een herziening van zo'n zaak? Je moet dus goed kijken naar de plaatsing van zo'n commissie.
Ik spreek ook mensen bij het Team High Tech Crime. Zij zeggen dat zij zelf ook wel behoefte hebben aan zo'n klankbordfunctie van onafhankelijke experts die meedenken en af en toe in concrete zaken grenzen stellen. Het

zijn onderwerpen die zeer in beweging zijn en die maar af en toe bij de wetgever voorliggen. In de dagelijkse praktijk met zich snel ontwikkelende techniek zijn er elke keer nieuwe gevallen waar een onafhankelijke toezichthouder dichter bovenop kan zitten. Hij kan rapporteren. De CTIVD-rapporten zijn erg nuttig om inzicht te krijgen in wat er in grote lijnen gebeurt. Een goede klachtenregeling is belangrijk. Als de politie deze hackbevoegdheid krijgt, kun je voorspellen dat Jan en alleman iedere keer dat er iets mis is met een computer gaan roepen: daar heeft de politie in gezeten. Je moet bij een instantie terechtkunnen die met gezag onafhankelijk kan zeggen: nee, de politie was daar niet bezig. Dat soort issues zullen ongetwijfeld naar voren komen. De onafhankelijkheid is ook vanuit Europees perspectief belangrijk.

De **voorzitter**:
Mijnheer Siedsma, aan u was ook een vraag gesteld.

De heer **Siedsma**:
Ik sluit me aan bij eerdere sprekers dat het toezicht ontzettend belangrijk is en dat dat eigenlijk een systematisch toezicht moet zijn. Er moet niet alleen naar individuele gevallen worden gekeken, maar ook naar de procedures, de systemen, de brede werking. Er moet ook kunnen worden gekeken naar de rechtmatigheid in gevallen waarin een zaak niet voor de rechter komt. Heel vaak komt een zaak niet voor de rechter. De ex-verdachte weet dan van niks en wordt, als het systeem goed werkt, misschien genotificeerd.
Na de IRT-affaire hebben we gezegd: we moeten een notificatiesysteem hebben. Dat is een heel belangrijke waarborg. Iemand die niet meer verdacht is, moet weten dat hij onderwerp van onderzoek is geweest. Het blijkt dat die notificatieplicht heel vaak niet wordt nageleefd. Daar zit dus een soort lacune.
Je kunt dan twee dingen doen: je kunt verplichten dat die notificatie wordt nageleefd of je kunt aanvullend toezicht optuigen. Ik pleit voor beide. Ook als notificatie plaatsvindt, weet een ex-verdachte heel vaak niet wat er precies is gebeurd. Misschien krijgt hij een brief: de politie heeft onderzoek naar u gedaan, met vriendelijke groet, de politie. Er staat niet bij: u bent op dat en dat apparaat toen en toen gehackt. Het is dus heel erg de vraag wat de ex-verdachte dan weet en hoe hij kan opkomen tegen de inbreuk die bij hem is gemaakt.
Het zou dus best goed zijn om ook te kijken naar de rechtmatigheid, zeker in gevallen waarin het niet voor de rechter komt. Er zijn procedurele dingen waarbij een verdachte uiteindelijk niet kan zeggen ... Ik geef een voorbeeld. Stelt u zich een technisch hulpmiddel voor dat wel gekeurd is, maar niet helemaal goed. Dan wordt er vaak gezegd: het klopt dat het niet helemaal goed is gegaan, maar deze bepaling is niet in uw belang geschreven. De verdachte heeft daar niks aan en het OM of de politie krijgen geen corrigerende tik op de vingers. Het blijft gewoon in stand. Dan is het heel goed als je daar een onafhankelijk toezichtssysteem of -orgaan voor hebt. Dat kan in zulke gevallen zeggen: hier en hier en hier gaan dingen echt systematisch niet goed; hier moeten we iets mee doen.
Dan nog even over ANPR. Ik stel voor om het veel breder te trekken. Er komt een modernisering van het Wetboek van Strafvordering aan. Ik zou zeggen: neem dat systematische toezicht daarin op, niet alleen voor ANPR, maar ook voor online surveillance, peilbakens en andere technische hulpmiddelen die de politie inzet.

De **voorzitter**:
De heer Rijpkema beantwoordt de moeilijke vraag van mevrouw Strik.

De heer **Rijpkema**:

Het schijnt een heel lastige vraag te zijn. Het gaat over waarborgen tijdens een onderzoek. Als een onderzoek plaatsvindt, is het aan de officier van justitie in samenwerking met de rechter-commissaris om in een bevel op te schrijven waarvoor de inzet nodig is. Daar worden een proportionaliteitstoets en een subsidiariteitstoets op uitgevoerd. En pas nadat duidelijk is dat alles binnen de wettelijke kaders valt, zal de inzet tot het binnendringen beginnen. Daarmee denken wij voldoende waarborgen aan de voorkant in te bouwen om het onderzoek op een juiste manier te laten uitvoeren.

Mevrouw **Strik** (GroenLinks):
Wordt daarbij ook getoetst of kan worden volstaan met minder ingrijpende of minder riskante ...

De heer **Rijpkema**:
Ja, die toets wordt ook uitgevoerd.

De **voorzitter**:
Heel hartelijk dank. Wij hebben deze ochtend uitvoerig gesproken over alle voors en tegens, mitsen en maren van beide wetsvoorstellen. Wij hebben het gehad over het belang van technische en juridische waarborgen. Wij hebben over het belang van onafhankelijk toezicht gesproken. Ook de mogelijkheid van een evaluatie en een horizonbepaling zijn aan de orde geweest. Wij hebben meer dan voldoende aanknopingspunten gekregen om het debat te verder te kunnen verdiepen. Heel veel dank daarvoor. Binnen acht dagen is een woordelijk verslag van deze bijeenkomst beschikbaar. De bijeenkomst is ook terug te kijken via de website van de Eerste Kamer. Wij kunnen er dus rustig op terugkijken en over nadenken. Dank voor uw komst naar de Eerste Kamer, voor al uw input en voor de deelname aan de gedachtewisseling.

Sluiting 12.20 uur.