Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2001–2002

27 591 Grootschalig afluisteren van moderne telecommunicatiesystemen

Nr. 4

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 4 april 2002

Hierbij bied ik u een notitie aan inzake de bescherming van burgers, bedrijven en instellingen tegen grootschalig afluisteren. De notitie is tot stand gekomen naar aanleiding van de zogenaamde Echelon-problematiek welke zowel binnen Nederland als op Europees niveau aandacht heeft.

Op 19 januari 2001 zond de minister van Defensie, mede namens de ministers van Justitie en van Binnenlandse Zaken en Koninkrijksrelaties, een brief over de juridische en technische aspecten van grootschalig afluisteren aan uw Kamer (TK 27 591, nr. 1). Op basis van eigen onderzoek naar het bestaan van het Echelon-systeem acht de regering het aannemelijk dat een dergelijk systeem bestaat en dat ook anderen, bijvoorbeeld criminele of terroristische organisaties, dergelijke systemen zouden kunnen hebben. Dat gegeven is van belang tegen de achtergrond van de aanslagen in de Verenigde Staten van 11 september 2001. Naar aanleiding van die aanslagen is ook de discussie over Echelon in een ander licht komen te staan. Het grootschalig afluisteren kan voor landen immers een middel zijn om de nationale veiligheid te waarborgen en de criminaliteit te bestrijden. De onlangs aangenomen Wet op de inlichtingen en veiligheidsdiensten geeft de inlichtingen- en veiligheidsdiensten de bevoegdheid om het middel van interceptie onder bepaalde condities toe te passen.

In de beantwoording op vragen van de vaste commissie voor Justitie (TK 27 591, nr. 2) heeft de regering aangegeven dat nagegaan zal worden welke mogelijkheden er zijn voor burgers, bedrijven en instellingen voor een betere bescherming tegen grootschalig afluisteren. Tijdens het overleg met de vaste commissies voor Justitie, voor Defensie en voor Binnenlandse Zaken en Koninkrijksrelaties op 29 november 2001 inzake het grootschalig afluisteren van moderne telecommunicatiesystemen heb ik een notitie hierover toegezegd. Met de bijgaande notitie voldoe ik aan die toezegging.

KST61080
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2002

De beschermingsmogelijkheden tegen grootschalig afluisteren zijn gelegen op de terreinen van achtereenvolgens de internationale rechtsbescherming; verbetering van de betrouwbaarheid van de openbare telecommunicatie infrastructuur en de maatregelen die men zelf kan treffen om de communicaties te beveiligen. De notitie bevat een overzicht van activiteiten die de overheid reeds onderneemt of voornemens is te ondernemen in dit verband. Nadrukkelijk is daarbij de Europese context betrokken. Goede nota is genomen van de resolutie van het Europees Parlement van 5 september 2001 betreffende het Echelon-interceptiesysteem (als bijlage bij de notitie opgenomen) alsmede van de aankondigingen van de vervolgstappen door de Europese Raad en de Europese Commissie.

Bij het nagaan van de mogelijkheden die de Nederlandse overheid in haar bereik acht, is vastgesteld dat op de eerste twee van de genoemde terreinen al veel ondernomen wordt in EU verband. Wat de zelfbeschermingsmaatregelen betreft moet geconcludeerd worden dat op internet al voldoende praktische en relatief goedkope middelen voorhanden zijn. Het daadwerkelijk aanwenden van deze middelen is vooral een eigen verantwoordelijkheid van burgers, bedrijven en instellingen. Om het gebruik verder te stimuleren is de overheid een publiciteitscampagne gestart ten behoeve van veilig internetgebruik onder de titel «Surf op Safe», waarin onder andere voorlichting wordt gegeven over beveiliging van gegevens en datacommunicatie.

Ook de overheid zelf dient zich afdoende te beschermen tegen grootschalig afluisteren. Hierbij moet gedacht worden aan programma's om te komen tot een infrastructuur voor betrouwbare communicatie, zoals het Rijksoverheidsintranet en Public Key Infrastructure, waarover de minister voor Grote Steden en Integratiebeleid de Kamer reeds heeft geïnformeerd. Voorts gaat het om een verbeterde beveiliging van de meest gevoelige delen van de overheidstelefonie endatacommunicatie. De voorgestelde maatregelen zullen naar verwachting tevens een nuttig uitstralingseffect hebben naar de markt. Voor een deel van de in het overzicht opgenomen activiteiten heeft al besluitvorming plaatsgevonden; voor de overige zal nog nadere besluitvorming moeten plaatsvinden. Derhalve zijn geen directe financiële of materiële consequenties verbonden aan de notitie. De in de notitie genoemde lopende dossiers worden in de uitvoering onderling goed op elkaar afgestemd.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K. G. de Vries

BESCHERMING TEGEN GROOTSCHALIG AFLUISTEREN

Aanleiding

1. Op 19 januari 2001 zond de minister van Defensie, mede namens de ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Justitie, een notitie aan de Tweede Kamer over de technische en juridische aspecten van het grootschalig afluisteren van moderne telecommunicatiesystemen[1]. In de notitie wordt onder meer gemeld dat de regering op grond van eigen onderzoek met gebruikmaking van open bronnen het bestaan van Echelon[2] aannemelijk acht; dat zij er van uitgaat dat ook andere systemen bestaan die de mogelijkheden van Echelon bezitten en dat ook anderen dan de in verband met Echelon genoemde landen zich bezig zouden kunnen houden met grootschalig afluisteren.

2. Bij de behandeling van de genoemde notitie van de minister van Defensie in de vergadering van de ministerraad op 19 januari 2001 besloot de ministerraad dat de minister van Binnenlandse Zaken en Koninkrijksrelaties, gehoord het besprokene en in overleg met de meest betrokken bewindspersonen, ten behoeve van een volgende vergadering van de Raad voor Justitie, Bestuur en Veiligheid een plan van aanpak zal voorbereiden inzake de bescherming tegen inbreuken in brede zin op het moderne telecommunicatieverkeer van burgers, bedrijven en instellingen, met inbegrip van de overheid. Deze notitie geeft invulling aan dat besluit.

3. Naar aanleiding van de genoemde notitie van de minister van Defensie en een op 22 januari 2001 gehouden rondetafelgesprek over het onderwerp Echelon heeft de vaste commissie voor Justitie vragen gesteld aan de regering, welke door de regering zijn beantwoord[3].

4. Het Europees Parlement heeft op 5 juli 2000 de Tijdelijke Commissie Echelon-interceptiesysteem ingesteld, die onder meer het bestaan van het Echelon-systeem heeft nagegaan, de verenigbaarheid met het gemeenschapsrecht heeft beoordeeld alsmede heeft nagegaan of het Europese bedrijfsleven gevaar loopt door de wereldwijde interceptie van informatie. Op 5 september 2001 heeft het Europees Parlement het verslag[4] van de Tijdelijke Commissie aanvaard en de bijbehorende resolutie[5] aangenomen. De voorliggende notitie gaat op een aantal punten in op deze resolutie.

5. In reactie op vragen van Kamerlid Van Oven naar de initiatieven van de regering naar aanleiding van het ontwerpverslag van de Tijdelijke Commissie Echelon-interceptiesysteem van het Europees Parlement alsmede naar aanleiding van het Algemeen Overleg met de vaste commissies voor Justitie, Defensie en Binnenlandse Zaken en Koninkrijksrelaties op 29 november 2001 inzake het grootschalig afluisteren van telecommunicatie, heeft de minister van Binnenlandse Zaken en Koninkrijksrelaties aangegeven dat een notitie over dit onderwerp wordt voorbereid en dat de Tweede Kamer dit stuk op korte termijn tegemoet kan zien[6].

Kader

6. In de EU-Raadsvergadering van 29 mei 2000 hebben de lidstaten van de EU verklaard dat de interceptie van telecommunicatie een belangrijk middel kan zijn bij het bestrijden van criminaliteit en het verdedigen van de nationale veiligheid, dat echter in geen geval mag worden benut voor het behalen van commercieel voordeel. De Tijde-

[1] Brief van de minister van Defensie d.d. 19 januari 2001, Tweede Kamer, 27 591, nr. 1.
[2] Onder Echelon wordt een systeem verstaan waarmee een samenwerkingsverband van de Verenigde Staten, het Verenigd Koninkrijk, Canada, Australië en Nieuw-Zeeland in staat zijn tot het grootschalig (wereldwijd) afluisteren van moderne telecommunicatiesystemen.
[3] Lijst van vragen en antwoorden vastgesteld op 14 juni 2001, Tweede Kamer, 27 591, nr. 2.
[4] Verslag over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (ECHELON-interceptiesysteem) d.d. 11 juli 2001, Europees Parlement, A5–0264/200.
[5] Resolutie van het Europees Parlement over het bestaan van een wereldwijd systeem voor de interceptie van particuliere en economische communicatie (ECHELON-interceptiesysteem).
[6] Verslag van een Algemeen Overleg op 29 november 2001, Tweede Kamer, 27 591, nr. 3.

lijke Commissie Echelon-interceptiesysteem concludeert dat grootschalig afluisteren omwille van concurrentievoordeel in strijd is met het EU-recht. De Nederlandse regering wijst grootschalig afluisteren voor het behalen van commercieel voordeel van de hand[1].

7. Het opvangen van signalen uit de ether is in principe strafbaar, indien een bijzondere inspanning wordt verricht of indien de opgevangen signalen worden doorgegeven[2]. Het voorstel voor de Wet op de inlichtingen en veiligheidsdiensten (Wiv), inmiddels aangenomen door de Eerste Kamer, geeft de inlichtingen- en veiligheidsdiensten onder bepaalde condities de bevoegdheid om het middel van interceptie toe te passen. Het wetsvoorstel Wiv regelt onder meer de toestemming vooraf; de toetsing op proportionaliteit en subsidiariteit en een onafhankelijke commissie van toezicht, die toeziet op de rechtmatigheid van de taakuitoefening van de inlichtingen- en veiligheidsdiensten en de coördinator.

8. Het kabinet heeft voorgesteld het recht op vertrouwelijke communicatie op te nemen in de Grondwet ter vervanging van het huidige artikel 13 betreffende de onschendbaarheid van het briefgeheim, respectievelijk het telefoon- en telegraafgeheim[3]. Dit recht op vertrouwelijke communicatie veronderstelt dat een wijze van communiceren wordt gekozen, die een redelijke verwachting van vertrouwelijkheid biedt. Daarbij moet vooral gedacht moet worden aan de aard van het gekozen kanaal en de adressering. In het voorstel is onder meer opgenomen dat het grondrecht op vertrouwelijke communicatie in bepaalde gevallen bij wet kan worden beperkt.

9. De Telecommunicatiewet[4] kent, overeenkomstig hetgeen in de Europese privacyrichtlijn telecommunicatie is bepaald, in artikel 11.3, een zorgplicht voor de aanbieders van openbare telecommunicatienetwerken en -diensten om in het belang van de bescherming van persoonsgegevens en de bescherming van de persoonlijke levenssfeer passende technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en de beveiliging van de door hen aangeboden netwerken en diensten. De maatregelen garanderen, rekening houdend met de stand der techniek en de kosten van de uitvoering, een passend beveiligingsniveau dat in verhouding staat tot het desbetreffende risico. De aanbieders hebben voorts onder meer een plicht om de abonnees te informeren over de bijzondere risico's voor de doorbreking van de veiligheid of de beveiliging van hun diensten en netwerken.

10. Het gebruik van cryptografie in Nederland is vrij[5]. Mede in reactie op de voortschrijdende versoepeling van Amerikaanse exportbepalingen zijn de exportbeperkingen op cryptografie binnen de Europese Unie nagenoeg opgeheven[6]. De Nederlandse regering heeft zich daarvoor actief ingezet.

11. Deze notitie gaat over het op grote schaal intercepteren, eventueel gevolgd door selecteren en analyseren, van telecommunicatie door bijvoorbeeld (buitenlandse) overheden of criminele of terroristische organisaties. Deze notitie handelt derhalve over de bescherming van de vertrouwelijkheid van communicatie, in de wetenschap dat de maatschappelijke kwetsbaarheid van de informatie- en communicatietechnologie als geheel een breder probleemveld is dat elders in het (internationale) beleid aandacht krijgt[7].

12. Deze notitie gaat eerst in op de mogelijke juridische vervolgstappen van de regering ten aanzien van grootschalig afluisteren. Vervolgens

[1] Dit standpunt is reeds medegedeeld bij de beantwoording op de Kamervragen 6, 7 en 21 (zie voetnoot 3).
[2] Artikelen 139c en 441 Wetboek van strafrecht en het Zwolsman-arrest.
[3] Kabinetsstandpunt op het advies van de Commissie «Grondrechten in het digitale tijdperk», brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties van 16 oktober 2000, Tweede Kamer, 27 460, nr. 1.
[4] Hoofdstuk 11 Wet op de telecommunicatie.
[5] Brief van de minister van Justitie van 12 februari 1998 en nota Wetgeving voor de elektronische snelweg, Tweede Kamer, 25 880, nrs. 1 en 2.
[6] In- en uitvoerbesluit strategische goederen en het Wassenaar arrangement.
[7] Verwezen wordt naar bijvoorbeeld de nota's De Digitale Delta en Kwetsbaarheid Internet, het Infodrome programma, de motie Wijn en het EU-initiatief eEurope2002.

komen de technische aspecten aan bod ten aanzien van de telecommunicatie-infrastructuur respectievelijk de middelen die burgers, bedrijven en instellingen kunnen hanteren om hun eigen beveiliging te verbeteren en de vertrouwelijke communicatie te beschermen. Daarbij wordt tevens ingegaan op de maatregelen die de regering treft om de beveiliging van communicatie in de publieke sector te versterken. Tot slot wordt nader ingegaan op ontwikkelingen in Europees verband in relatie tot de Nederlandse situatie.

Uitgangspunten

13. Grootschalig afluisteren kan voor landen een middel zijn om de nationale veiligheid te waarborgen en de criminaliteit te bestrijden. In de Nederlandse situatie wordt de inzet van een dergelijk middel, dat inbreuk maakt op de privacy en het recht op vertrouwelijke communicatie, slechts toegestaan indien is voldaan aan de eisen die de nationale wetgeving alsmede de internationale verdragen hieraan stellen. Zo dient bij de inzet van een dergelijk middel onder meer te worden voldaan aan de eisen van proportionaliteit en subsidiariteit.

14. De regering beschikt niet over bewijsmateriaal waaruit blijkt dat burgers, bedrijven of instellingen in Nederland subject zouden zijn of zouden zijn geweest van grootschalig afluisteren door andere landen -ook niet als het gaat om economische spionage- of waaruit blijkt dat landen daartoe strafbare voorbereidingshandelingen hebben verricht, zoals zich op Nederlands grondgebied begeven om dataverkeer te onderscheppen. Om die reden zijn diplomatieke en internationaal juridische stappen, zie bijlage 1[1], niet aan de orde. Dergelijke stappen zouden bovendien weinig effectief zijn bij gebrek aan bevestiging door de landen zelf, omdat in de regel geen mededelingen worden gedaan over dergelijke activiteiten[2]. De regering zal in internationaal verband benadrukken dat zij interceptie ten behoeve van commerciële doeleinden afwijst.

15. De Nederlandse wetgeving regelt dat (grootschalig) afluisteren door de bevoegde Nederlandse instanties van burgers, bedrijven en instellingen alleen onder bepaalde bij de wet gestelde voorwaarden is toegestaan.

16. Indien burgers, bedrijven of instellingen vermoeden, dat zij door een buitenlandse overheid zijn afgeluisterd bestaan er vrijwel geen mogelijkheden om dat vermoeden bevestigd te krijgen. Ook de mogelijkheden om er achteraf iets aan te doen, bijvoorbeeld door het desbetreffende land voor de rechter te dagen, zullen in de praktijk niet veel opleveren.

17. Het internationale recht is nog niet uitgekristalliseerd op het punt van de rechtsbescherming van (Nederlandse) burgers, bedrijven en instellingen tegen inbreuken op hun rechten vanuit het buitenland. De rechtspositie van burgers, bedrijven en instellingen in Nederland, die vanuit een ander land worden afgeluisterd, dient in internationale afspraken en verdragen te worden verhelderd. Een aanzet hiervoor is gegeven, mede op initiatief van de Nederlandse regering, in het Europese Rechtshulpverdrag. De Tijdelijke Commissie van het Europees Parlement roept op tot harmonisering van de rechtsbescherming op het hoogste beschermingsniveau dat bij de lidstaten binnen de Europese Unie wordt aangetroffen. Landen blijken tot dusver echter weinig responsief te zijn op het onderwerp internationale rechtsbescherming. Het zal dan ook naar verwachting enige tijd duren voordat de resultaten van een dergelijke aanpak zichtbaar zullen zijn.

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[2] Dit standpunt is reeds medegedeeld bij de beantwoording op de Kamervragen 11, 25 en 88 (zie voetnoot 3).

18. Het is praktisch onmogelijk om ex post vast te stellen of interceptie van telecommunicatie heeft plaatsgevonden. Daarom zal, om inbreuken tegen te gaan, vooral gezocht moeten worden naar mogelijkheden om het afluisteren preventief tegen te gaan door – waar nodig – een adequate beveiliging aan te brengen, in het bijzonder door het toepassen van cryptografie. Deels zou dat kunnen door de technische infrastructuur te voorzien van betere beveiliging op dit punt, maar in aanzienlijke mate zal het nodig zijn dat beveiliging wordt aangebracht in eindgebruiker apparatuur, zoals een telefoon of een personal computer. Ook een veilig gedrag door diegenen die deelnemen aan de communicatie is van belang. Dezen dienen zich bewust te zijn van het risico op afluisteren.

19. De mogelijkheden om telecommunicatieverkeer in algemene zin meer te beveiligen dan thans gebeurt, zijn zeer beperkt. Extra beveiliging van het internationale bulkverkeer, bijvoorbeeld door encryptie, wordt niet zinvol geacht, omdat dit bulkverkeer altijd ergens weer onvercijferd aan de oppervlakte komt[1]. Dit betekent dat de aanzienlijke inspanningen die de aanbieders van telecommunicatie zich zouden moeten getroosten om de communicatie te vercijferen, slechts van weinig waarde zullen zijn. Een dergelijke maatregel moet derhalve disproportioneel en ongewenst worden geacht. Bovendien is in de telecommunicatiesector een migratie waarneembaar van traditionele, meestal analoge, spraakverbindingsprotocollen naar het op digitaal datatransport toegesneden Internetprotocol. Een dergelijke overstap, die ook zal worden toegepast op spraakcommunicatie, zal naar alle waarschijnlijkheid het aantal op de markt beschikbare en betaalbare end-to-end encryptie voorzieningen doen toenemen. Dit zal de eindgebruiker zelf in staat stellen om tot een optimale afstemming te komen tussen risico's, gewenst beveiligingsniveau en kosten, waarbij de aanbieders en andere gebruikers van telecommunicatie niet nodeloos voor hoge lasten komen te staan.

20. Een inhoudelijke wijziging van de telecommunicatiewetgeving op het punt van beveiliging is, ook op Europees niveau, niet noodzakelijk. Aanvullende verplichtingen zouden enerzijds onevenredige kosten met zich meebrengen in verhouding tot de aard en hoeveelheid informatie, anderzijds brengt dit de concurrentiepositie van de telecommunicatiebedrijven in gevaar. Hierbij zij opgemerkt dat in het kader van het «eEurope 2002»-initiatief op Europees niveau al veel aandacht is voor veiligheid van de telecommunicatie infrastructuur en in het bijzonder van netwerken en informatiesystemen, zie bijlage 2[2] voor een overzicht daarvan. Het Nederlandse beleid is in lijn met de ontwikkelingen binnen de Europese Unie en waar nieuwe ontwikkelingen zijn aangekondigd, zal Nederland hierop aansluiten.

21. Burgers, bedrijven en instellingen hebben een eigen verantwoordelijkheid om te bepalen hoe kwetsbaar hun communicatie is voor afluisteren; zich voorts bij de keuze voor een communicatiekanaal[3] van het risico op afluisteren bewust te zijn en dit risico af te wegen alsmede zich zelf afdoende te beschermen tegen afluisteren door het naleven van bepaalde gedragsregels en door het treffen van een combinatie van organisatorische en technische beveiligingsmaatregelen. Het voorgaande geldt mutatis mutandis ook voor de bescherming tegen inbreuken op de integriteit en beschikbaarheid van de desbetreffende informatie.

22. De overheid heeft mede een taak op het gebied van de bewustwording van de eerder genoemde risico's en voorts ten aanzien van de bekendheid met toepasbare beveiligingsmiddelen door het geven van voor-

[1] Dit standpunt is reeds medegedeeld bij de beantwoording op de Kamervragen 64 en 65 (zie voetnoot 3).
[2] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.
[3] Mogelijke vormen van communicatie zijn mondelinge-, radiografische-, telefonische-, schriftelijke- of elektronische informatieoverdracht; het ene daarvoor te gebruiken communicatiekanaal is inherent onveiliger dan het andere.

lichting dienaangaande. Daarnaast dient de overheid zonodig de juridische kaders te creëren en anderszins voorwaarden te scheppen, opdat burgers, bedrijven en instellingen zich ook daadwerkelijk afdoende kunnen beschermen.

23. De overheid draagt zelf verantwoordelijkheid en de verplichting voor een adequate beveiliging van de informatie die zij onder zich heeft. Dit geldt onverkort voor gegevens die van burgers, bedrijven en instellingen afkomstig zijn. Daarnaast bestaan er binnen de overheid categorieën informatie die om uiteenlopende redenen geheimhouding behoeven.

24. Indien de overheid aanschaffingen voor eigen gebruik overweegt, bijvoorbeeld op het vlak van beveiliging, dan zou die vraag stimulerend kunnen zijn voor een bredere markt en normstellend kunnen zijn voor het aanbiedende bedrijfsleven – de overheid als *launching customer*. De overheid kan vanuit die rol partij zijn in platforms zoals standaardisatiewerkgroepen of gebruikersgroepen.

25. De algemene beschikbaarheid van beveiligingsmiddelen voor eindgebruiker apparatuur is voldoende te noemen uit oogpunt van privacybescherming van de gemiddelde gebruiker. Waar het gaat om grootschalig afluisteren en de daarmee nauw samenhangende mogelijkheden van decryptie door degenen die afluisteren, zijn of komen beveiligingsmiddelen endiensten, zoals bijvoorbeeld TTP/PKI-producten (zie verder), beschikbaar. De regering zal waar mogelijk de beschikbaarheid van dergelijke middelen en diensten bevorderen.

26. De genoemde beveiligingsmiddelen en -diensten zouden, indien gebruikt voor algemene toepassing, voldoende garanties moeten bieden tegen grootschalig afluisteren. Omdat niet zeker gesteld kan worden dat de sterkte van uit het buitenland afkomstige cryptoproducten ten behoeve van overheden uit het land van oorsprong niet is beïnvloed, bieden standaard beveiligingsmiddelen onvoldoende garanties voor specifieke behoefte aan zware beveiliging. Daarvoor dient men aanvullende maatregelen te treffen.

27. De regering is uit oogpunt van beveiliging voorstander van het gebruik van apparatuur waarvan de goede werking en betrouwbaarheid valideerbaar is. Voor de evaluatie en certificatie van apparatuur zijn internationaal gestandaardiseerde criteria en methodieken nodig en beschikbaar. Nederland heeft in 2000 een arrangement ondertekend waarmee de wederzijdse erkenning van zogenaamde Common Criteria-certificaten[1] wordt geregeld tussen een aanzienlijk aantal landen in de wereld. Eerder heeft Nederland zich aangesloten bij een dergelijke regeling ten behoeve van zogenaamde ITSEC-certificaten. De aanschaf en het gebruik van software, inclusief encryptie-software, waarvan de broncode openbaar is[2] zou verder aan de veiligheid van informatiesystemen kunnen bijdragen.

28. Standaard op de markt verkrijgbare encryptie-producten bieden beveiliging tegen meelezen van communicatie door onbevoegden in zijn algemeenheid. Maar, omdat de sterkte van de geleverde encryptie niet altijd vastgesteld kan worden, verdient het aanbeveling om gebruik te maken van encryptie-technieken die openbaar gepubliceerd en bewezen veilig zijn. In gevallen waarbij zekergesteld moet worden dat de sterkte van de encryptie niet beïnvloed is geven deze producten onvoldoende garanties en zou de mogelijkheid om zelfstandig ontwikkelde encryptie aan te brengen in bestaande hardware en software[3] een oplossing kunnen zijn. Voor bepaalde delen van de overheids-

[1] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, may 2000.
[2] Het gaat hier om zogenaamde open source software, het Europees Parlement beveelt het gebruik van open souce encryptie-software aan.
[3] Gedoeld wordt hier op zogenaamde pluggable encryption, waaraan door de Europese Commissie aandacht wordt geschonken.

communicatie is het uit oogpunt van staatsveiligheid noodzakelijk om encryptie-producten geheel onder overheidstoezicht te (laten) ontwikkelen en produceren. Deze apparatuur zou onder omstandigheden ook beschikbaar kunnen komen voor het relevante bedrijfsleven.

Activiteiten

29. Op vele onderdelen van het huidige regeringsbeleid wordt reeds aandacht besteed aan de noodzakelijke verbetering van de veiligheid en betrouwbaarheid van de informatie en communicatietechnologie. Met name zij verwezen naar de pijlers A, D en E (respectievelijk Telecommunicatie-infrastructuur; Regelgeving en ICT in de publieke sector) van de nota De Digitale Delta[1]. Hierna worden reeds lopende activiteiten opgesomd, die een raakvlak hebben met het grootschalig afluisteren en waarbij zonodig accenten op het beleid zijn aangebracht om een betere bescherming daartegen te bieden en voorts activiteiten die zich in de verkennende fase bevinden en waarover besluitvorming nog moet plaatsvinden. In de laatste categorie bevinden zich de punten 37 voor wat betreft de grootschalig uitrol en 40/41. Achtereenvolgens komen maatregelen aan bod op de terreinen maatschappelijke bewustwording, beveiliging openbare netwerken (internet), zelfbeschermingsmiddelen, maatregelen gericht op de publieke sector en verbetering van de rechtsbescherming. Telkens wordt daarbij aangegeven wat de doelstelling is, wat de huidige stand van zaken (status) is en wat het beoogde resultaat is van de beschreven maatregel alsmede waar de verantwoordelijkheid voor de uitvoering van de maatregel ligt en welke de aandachtspunten zijn voor eventuele vervolgacties. De in deze notitie genoemde activiteiten worden in de uitvoering door de verantwoordelijke ministeries onderling op elkaar afgestemd.

30. Opzetten van een **voorlichtings- en bewustwordingscampagne** rond het thema internetveiligheid[2].
Doel: De campagne, «surf op safe» getiteld, heeft tot doel het bewustzijn van en de kennis over de veiligheidsrisico's bij het publiek te vergroten en aan te geven hoe hiermee kan worden omgegaan. Om de bekendheid van gebruikers met de versleutelingsmogelijkheden van communicatie te vergroten, wordt bij de voorlichting expliciet aandacht geschonken aan de beveiliging van vertrouwelijke informatie.
Status: De campagne loopt en is gekoppeld aan de eveneens lopende campagne «Nederland gaat Digitaal».
Resultaat: Eind 2001, begin 2002 is er meer bekendheid over risico's en beveiligingsmaatregelen bij het publiek.
Verantwoordelijk: Ministeries van Verkeer en Waterstaat en van Economische Zaken.
Aandachtspunten: De kosten van uitvoering belopen 3 miljoen gulden; reeds besloten en gefinancierd uit het Nationaal Actieprogramma Elektronische Snelwegen. Na afloop van de campagne zal een evaluatie plaatsvinden.

31. Stimuleren van het gebruik van de **Code voor Informatiebeveiliging**[3] door onder andere een grotere bekendheid te geven aan het bestaan en het nut er van.
Doel: Meer gebruikmaking van de Code voor Informatiebeveiliging door bedrijven en instellingen. De Code is gebaseerd op een verzameling van de beste praktijkmethoden van informatiebeveiliging, die in gebruik zijn bij vele toonaangevende internationale bedrijven en organisaties. Met behulp van de Code kunnen individuele organisaties komen tot een effectief management van de eigen informatiebeveiliging. Dit is vooral nodig in verband met de organisatie rond het

[1] Brief van de ministers van Economische Zaken, voor Grote Steden en Integratiebeleid en van Justitie en de staatssecretarissen van Verkeer en Waterstaat, van Onderwijs, Cultuur en Wetenschap en van Financiën van 1 juli 1999, Tweede Kamer, 26 643, nr. 1 en de voortgangsrapportage De Digitale Delta van november 2000.
[2] Aangekondigd in notitie De Digitale Delta alsmede in de beleidsnota Kwetsbaarheid op Internet; ook zij verwezen naar internet: *www.surfopsafe.nl*.
[3] Code voor Informatiebeveiliging, een leidraad voor beleid en implementatie, Ministerie van Economische Zaken/Nederlands Normalisatie Instituut; tevens als ISO-standaard geregistreerd onder nummer ISO 17 799.

toepassen van encryptie (veilig sleutelbeheer, voorkomen van inbraken op het netwerk, enzovoort).
Status: Reeds aangekondigde activiteit[1].
Resultaat: Vermindering van de kwetsbaarheid op het niveau van de individuele organisaties.
Verantwoordelijk: Ministeries van Economische Zaken en van Verkeer en Waterstaat.
Aandachtspunten: Geen.

32. Instellen van een **platform** voor activiteiten met betrekking tot het op een hoger pijl brengen van de betrouwbaarheid van internet.
Doel: Stimuleren en faciliteren van publiek-private samenwerking voor informatieuitwisseling en uitwerking van de actielijnen uit de beleidsnota KWINT.
Status: Aangekondigde activiteit in beleidsnota KWINT. De planning is om in maart 2002 van start te gaan met dit platform.
Resultaat: Tot stand brengen van beoogde producten als bijdrage aan het vergroten van de betrouwbaarheid van internet.
Verantwoordelijk: Ministerie van Verkeer en Waterstaat.
Aandachtspunten: Nog niet bekend.

33. Stimuleren van de totstandkoming van een stelsel van **gecertificeerde Trusted Third Party-diensten**.
Doel: Een Trusted Third Party (TTP) is een organisatie die verschillende diensten kan aanbieden op het vlak van de betrouwbaarheid (authenticiteit, integriteit en vertrouwelijkheid) van gegevensuitwisseling. Het kabinet heeft in overleg met marktpartijen randvoorwaarden geformuleerd waaraan TTP-diensten zouden moeten voldoen[2]. Het kabinet stimuleert de totstandkoming van schema's in de markt aan de hand waarvan TTP's zich vrijwillig kunnen laten certificeren. Voor de elektronische handtekening is een schema gereed gekomen. In het wetsvoorstel ter implementatie van de EU-richtlijn elektronische handtekening[3] is voorzien in het kunnen erkennen van dergelijke schema's. Tevens wordt daarin de OPTA aangewezen als toezichthouder op geregistreerde TTP's die certificaten voor de elektronische handtekening aanbieden. Indien een TTP (ook) vertrouwelijkheidsdiensten aanbiedt, kunnen burgers, bedrijven en instellingen daarvan gebruik maken om hun berichten vertrouwelijk te versturen.
Status: Wetsvoorstel elektronische handtekening is aangeboden aan de Kamer[4].
Resultaat: Totstandkoming van TTP's die aan bepaalde kwaliteitseisen voldoen.
Verantwoordelijk: Ministeries van Verkeer en Waterstaat, van Economische Zaken en van Justitie.
Aandachtspunten: Een regeling aangaande de benodigde kosten van de toezichthouder is in voorbereiding.

34. Bevorderen van onderzoek naar en ontwikkeling van nieuwe **informatiebeveiligingsmethoden en -hulpmiddelen**, met name naar de toepasbaarheid van gebruiksvriendelijke en betrouwbare **encryptiesoftware** die inpasbaar is in marktconforme ICT-producten[5].
Doel: Om gemakkelijk te kunnen communiceren is het van belang dat de cryptografie niet te veel drempels in het gebruik opwerpt. Tegelijkertijd dient de aangebrachte encryptie voor langere tijd bescherming te bieden en dus gegarandeerd «sterk» genoeg te zijn en daar waar nodig (voor bijvoorbeeld zware toepassingen) door deskundige derden gevalideerd kunnen worden. Dergelijke encryptiesoftware is nog onvoldoende beschikbaar. Onderzoek moet de toepasbaarheid daarvan aantonen en de ontwikkeling stimuleren.

[1] Beleidsnota Kwetsbaarheid op internet (KWINT), brief van de staatssecretaris van Verkeer en Waterstaat van 9 juli 2001, Tweede Kamer 26 643, nr. 30.
[2] Beleidsnotitie Nationaal TTP-project, brief van de staatssecretaris van Verkeer en Waterstaat van 3 juni 1999, Tweede Kamer, 26 581, nr. 1.
[3] Richtlijn 1999/93/EG.
[4] Tweede Kamer, 27 743, nrs. 1–2.
[5] Zogenaamde pluggable encryption; zie ook nota KWINT paragraaf 7.1.2.

Status: Continuering van onderzoeksinspanningen nationaal en internationaal (Europese 6e kaderprogramma).
Resultaat: Verdergaande ontwikkeling en beschikbaar komen van beveiligingsproducten.
Verantwoordelijk: Ministeries van Verkeer en Waterstaat en van Economische Zaken.
Aandachtspunten: De ministeries van Verkeer en Waterstaat en van Economische Zaken zullen in de gebruikelijke kaders aansturen op verder onderzoek en ontwikkeling op dit terrein.

35. Continuering van de inzet om te komen tot een internationaal erkend Nederlands schema voor het **evalueren en certificeren van ICT-beveiligingsapparatuur**.
Doel: In publiek/private samenwerking wordt in Nederland toegewerkt naar een structuur voor het evalueren en certificeren van ICT-beveiligingsproducten. Het is daarbij de bedoeling dat een erkend evaluatie-instituut aangeboden apparatuur evalueert aan de hand van een internationaal gestandaardiseerde methodiek, de zogenaamde Common Criteria[1]. Bij positief resultaat van de evaluatie ontvangt de desbetreffende apparatuur een certificaat van een erkend onafhankelijk certificatie-instituut. Vooralsnog is TNO de enige partij in Nederland die dergelijke certificaten kan gaan afgeven, naar verwachting vanaf medio 2002. Op dit moment is Nederland nog slechts «gebruiker» van certificaten van andere landen. Het is de bedoeling dat zodra in Nederland certificaten op dit terrein worden afgegeven, deze dan ook erkend worden in andere landen.
Status: Continuering van de inzet om een Nederlands schema in te richten alsmede van de samenwerking met andere landen.
Resultaat: Medio 2002 kunnen naar verwachting ook in Nederland certificaten worden afgegeven. Gestreefd wordt naar een gelijktijdige internationale erkenning van die certificaten.
Verantwoordelijk: Minister van Binnenlandse Zaken en Koninkrijksrelaties.
Aandachtspunten: Geen.

36. De overheid onderzoekt de mogelijkheden om in het kader van het eigen aanschafbeleid het gebruik van **open source software** te bevorderen en voorts van gebruiksvriendelijke **encryptietechnieken**, die inpasbaar zijn in moderne informatievoorzieningen en die tegelijkertijd voldoende valideerbaar zijn op veiligheid en betrouwbaarheid.
Doel: Naast andere mogelijke voordelen leent software waarvan de broncode beschikbaar is zich beter voor het in die software kunnen inpassen van bijvoorbeeld eigen of door derden ontwikkelde beveiliging, zoals encryptiesoftware. Bovendien kan dergelijke software beter en gemakkelijker op onjuistheden en zwakheden gecontroleerd worden. Indien toepassen van gebruiksvriendelijke encryptie bij overheidscommunicatie de norm zou gaan worden, dan wordt de communicatie in zijn geheel veiliger en kan dit tevens een gunstige maatschappelijke uitstraling hebben.
Status: Een begin is gemaakt met het verkennen van de mogelijkheden.
Resultaat: Van deze maatregel kan tevens een positieve uitstraling buiten de publieke sector uitgaan en leveranciers stimuleren om veilige en gebruiksvriendelijke (beveiligings)software te ontwikkelen.
Verantwoordelijk: ministerie van Economische Zaken en minister voor Grote Steden en Integratiebeleid.
Aandachtspunten: Nog niet bekend.

37. Inrichten van een **Public Key Infrastructure** (PKI) ten behoeve van betrouwbare communicatie tussen overheidsorganisaties onderling en

[1] Voor meer informatie over de Common Criteria, zie ook internet *www.commoncriteria.-com.*

voor de communicatie van overheidsorganisaties met bedrijven, burgers en instellingen. Daarvoor is onder andere het landelijk beschikbaar stellen van een **smartcard** ten behoeve van het gebruik van de PKI nodig en moet onderzocht worden of het basisniveau van beveiliging opgetrokken kan en moet worden en voorts of het wenselijk en (financieel) haalbaar is om standaard alle berichten te encrypteren.
Doel: Een belangrijke voorwaarde voor een adequate elektronische dienstverlening betreft de veiligheid van de elektronische communicatie. Een betrouwbaar mechanisme is nodig dat kan zorgen voor dezelfde waarborgen die in de «papieren» wereld gelden. De Public Key Infrastructure[1] (PKI) speelt daarin een hoofdrol door er voor te zorgen dat onder andere de vertrouwelijkheid van communicatie verzekerd is. Met behulp van de PKI-infrastructuur in combinatie met een smartcard voor iedere gebruiker wordt gerealiseerd dat elektronische handtekeningen gezet kunnen worden en dat beveiligde e-mail verstuurd kan worden. Voor beide functies wordt gebruik gemaakt van encryptie. De verwachting is dat als iedereen beschikt over een dergelijke kaart voor communicatie met de overheid, deze kaart ook toegepast zal worden in het verkeer tussen burgers en bedrijven onderling. Het voornemen is de nieuwe elektronische identiteitskaart (eNIK), de opvolger van de huidige door de overheid voor reisdoeleinden uitgegeven identiteitskaart, daarvoor in te zetten. De PKI zal een basisbeveiligingsniveau bieden voor overheidscommunicatie die voldoende is voor de het overgrote deel van het berichtenverkeer. Indien al het berichtenverkeer standaard geëncrypteerd is, heeft dat als voordelen dat er een voorbeeldwerking van uitgaat[2] en dat afluisteren erdoor bemoeilijkt wordt. Deze voordelen moeten worden afgewogen tegen de extra kosten, een groter capaciteitsbeslag op de infrastructuur en het gebruiksgemak.
Status: Activiteit loopt reeds.
Resultaat: In 2002 wordt de basisvoorwaarde voor de PKI gerealiseerd; het centrale deel dat interoperabiliteit waarborgt alsmede de daarbij horende beheersorganisatie. Nadere besluitvorming over de financiering van de grootschalige uitrol zal vóór eind 2002 moeten plaatsvinden. Eind 2002 moet duidelijk zijn of inzet eNIK voor dit doel zowel technisch als organisatorisch mogelijk is. Voor het beproeven van de techniek worden in 2001 en 2002 pilotprojecten uitgevoerd.
Verantwoordelijk: Minister voor Grote Steden en Integratiebeleid.
Aandachtspunten: De eventueel additionele kosten voor het desgewenst optrekken van het beveiligingsniveau in de overheidscommunicatie zijn vooralsnog niet aan te geven.

38. Realisatie van het **Rijksoverheidsintranet** (RYX) met beperkte bescherming. Onderzoeken in hoeverre PKI binnen RYX kan worden ingezet, opdat beveiliging van RYX kan worden opgetrokken.
Doel: RYX biedt de mogelijkheid voor rijksambtenaren om in besloten gebruikersgroepen met elkaar te communiceren. De vertrouwelijkheid die RYX biedt is echter niet meer dan de beslotenheid van de gebruikersgroep en het feit dat de communicatie loopt over een «eigen» vezel van een glasvezelnetwerk. Omdat berichten niet worden geëncrypteerd en via een openbare infrastructuur worden verzonden, is het beveiligingsniveau onvoldoende voor geheime informatie. Wel zal nog worden onderzocht in hoeverre PKI binnen RYX kan worden ingezet, opdat met het eventueel opwaarderen van het basisbetrouwbaarheidsniveau van PKI ook dat van RYX wordt opgetrokken.
Status: In juni 2001 is RYX in gebruik genomen met op dit moment-30 000 aangesloten rijksambtenaren. Eind 2002 moeten alle rijksambtenaren zijn aangesloten. Een beveiligingsplan is opgesteld opdat eenzelfde (hoog) niveau van beveiliging tussen RYX en alle ministeries

[1] Voor de voorbereiding en realisatie is de zogenaamde Task Force PKI ingesteld door de minister voor Grote Steden en Integratiebeleid, zie Kamerstukken II, 1999/2000, 26 387, nr. 5.
[2] De Tijdelijke Echeloncommissie van het Europese Parlement beveelt het standaard toepassen van encryptie om deze reden aan.

zal worden gerealiseerd. Begin 2003 dienen alle onderdelen van RYX te voldoen aan dit beveiligingsplan.
Resultaat: Een mogelijkheid voor beter beveiligde gegevensuitwisseling binnen de rijksdienst.
Verantwoordelijk: Minister voor Grote Steden en Integratiebeleid.
Aandachtspunten: Resultaat van het onderzoek naar de mogelijkheid om het basisniveau van de geboden betrouwbaarheid op te waarderen.

39. Bij gezamenlijke **aanbestedingen van ICT-diensten** rekening houden met (grootschalig) afluisteren. Waar geen sprake is van gezamenlijke aanbestedingen, zal bezien worden hoe er voor gezorgd kan worden dat het afluisterrisico in de eisen wordt meegenomen.
Doel: Voor het reguliere telefoonverkeer van de overheid is in 2000 een Europese aanbesteding afgerond (OT2000). In het bestek zijn geen andere eisen opgenomen over vertrouwelijkheid dan die welke de aanbieders op grond van de Telecommunicatiewet moeten bieden. Bij eventuele volgende aanbestedingen zullen verplichte beveiligingseisen worden gesteld met het oog op het risico van afluisteren. Dat geldt eveneens voor eventuele komende gezamenlijke aanbestedingen van andere ICT-diensten zoals berichtenverkeer, netwerkdiensten of standaard kantoorautomatiseringspakketten. Indien geen sprake (meer) zal zijn van gezamenlijke aanbestedingen, zal bezien worden hoe er voor gezorgd kan worden dat overheidsorganisaties die zelf de markt op gaan, het afluisterrisico analyseren en daartegen eisen in het bestek opnemen. Hierbij moet vooral gedacht worden aan vereisten met betrekking tot *open source software* en encryptietechnieken alsmede de vereiste dat apparatuur door een deskundige partij geëvalueerd en gecertificeerd moet zijn volgens standaard evaluatiecriteria.
Status: Ten aanzien van een eventuele eerstvolgende aanbesteding overheidstelefonie zal ook het afluisterrisico worden meegenomen.
Resultaat: Duidelijkheid omtrent de wijze waarop generiek aandacht is voor het beveiligingsaspect bij de aanschaf apparatuur door de overheid en welke vereisten dienaangaande bestaan.
Verantwoordelijk: Minister voor Grote Steden en Integratiebeleid.
Aandachtspunten: Vooralsnog geen.

40. Overheidsbrede ontwikkeling en aanschaf van **beveiligingsproducten** zoals beveiligde mobiele en vaste telefonie alsmede werkplek-, email- en laptopbeveiliging.
Doel: In de loop van 2001 is binnen de rijksdienst nagegaan welke apparatuur nodig is om een voldoende peil van beveiliging van de meest gevoelige onderdelen van de overheidscommunicatie te handhaven. Daaruit blijkt dat vooral direct behoefte bestaat aan beveiligde mobiele telefonie (secure-gsm; prioriteit vanwege het veelvuldige gebruik en het afluisterrisico) en voorts aan beveiliging van werkplekken, laptops en e-mailverkeer. Deze apparatuur dient in ieder geval voorzien te zijn van betrouwbare en voldoende sterke cryptografie. In dit verband is tevens onderzoek gaande naar de vervanging van het ministerstelefoonnet en het beveiligd emailen tussen ministers en de ambtelijke top. Nagegaan moet worden of reeds in andere landen voor specifiek gebruik ontwikkelde of te ontwikkelen apparatuur benut kan worden.
Status: Deze activiteit bevindt zich in de verkennende fase.
Resultaat: Veilige verbindingen voor de meest gevoelige onderdelen van overheidscommunicatie (telefonie en gegevensverkeer). De overheidsvraag zou tevens stimulerend kunnen zijn voor een bredere markt.
Verantwoordelijk: Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Aandachtspunten: Besluitvorming dient nog plaats te vinden.

41. Inrichten van een faciliteit voor de gezamenlijke ontwikkeling en verwerving van **betrouwbare cryptografische toepassingen** voor de overheid.
Doel: Veel encryptieproducten die thans in gebruik zijn bij de overheid zijn aan vervanging toe. Voor nieuwe communicatiemogelijkheden moeten nieuwe beveiligingsproducten ontwikkeld worden. Mogelijke toepassing van gebruiksvriendelijke encryptie op werkplekken en in netwerken wordt thans bestudeerd, mede in samenspraak met het aanbiedende bedrijfsleven (de crypto-industrie). Uit oogpunt van veiligheid, standaardisatie, kosten en bundeling van expertise op dit terrein is het gewenst dat behoeftestelling en verwerving van dergelijke apparatuur centraal wordt gecoördineerd. Ook wordt bezien of samenwerking, incidenteel dan wel op meer structurele basis, met andere landen op dit punt onder bepaalde voorwaarden denkbaar is. Prioriteiten op de korte termijn zijn genoemd onder ontwikkeling en aanschaf van beveiligingsproducten in nauwe samenhang met onder meer de projecten van Public Key Infrastructure en Rijksoverheid Intranet. Nader onderzoek moet uitwijzen waar en in welke sectoren op termijn de behoeften liggen en hoe deze zonodig op elkaar af te stemmen zijn. Voorstelbaar is dat de genoemde cryptofaciliteit niet alleen kan fungeren als *smart buyer* voor de overheid, maar ook overleg heeft met andere behoeftestellers aan zware cryptografie, bijvoorbeeld grote internationaal opererende bedrijven en instellingen, teneinde te bezien of de behoefte die daar bestaat zou kunnen convergeren met de behoefte van de Nederlandse overheid.
Status: Thans nog in verkennende fase.
Resultaat: Oprichting van een cryptofaciliteit op basis van nadere besluitvorming.
Verantwoordelijk: Ministers van Binnenlandse Zaken en Koninkrijksrelaties en voorts andere betrokken bewindslieden.
Aandachtspunten: Vooralsnog geen.

42. In internationaal verband aandacht vragen voor **verbetering van de rechtsbescherming** van burgers, bedrijven en instellingen tegen grootschalig afluisteren. Aangesloten kan worden bij in gang gezette ontwikkelingen binnen de Europese Unie.
Doel: Verkrijgen van rechtsbescherming op een tenminste met Nederland vergelijkbaar en voor Nederland aanvaardbaar niveau.
Status: Het standpunt van de regering met betrekking tot de rechtsbescherming tegen grootschalig afluisteren zal worden ingebracht bij de onderhandelingen in de Europese Unie over de maatregelen die zijn aangekondigd in de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de regio's van 26 januari 2001 (COM 2000, 890): De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden. De onderhandelingen daarover zijn in het najaar van 2001 gestart.
Resultaat: Opname van een tekst met betrekking tot rechtsbescherming van burgers, bedrijven en instellingen tegen grootschalig afluisteren in het Kaderbesluit dat in het kader van de eerdergenoemde mededeling door de Europese Commissie wordt voorbreid.
Verantwoordelijk: Ministerie van Justitie.
Aandachtspunten: Geen, is onderdeel van lopende activiteiten.

Europese Unie

43. Het Europees Parlement heeft bij resolutie van 5 september 2001 het eindrapport van de Tijdelijke Commissie Echelon-interceptiesysteem,

gevoegd als bijlage 3[1], aanvaard. Het Europees Parlement dringt daarin onder meer bij de lidstaten van de Europese Unie aan op een groot aantal maatregelen.

44. Nederland lijkt redelijk goed toegerust op de maatregelen die het Europees Parlement voorstaat, in het bijzonder door de voorzieningen in de nieuwe Wet op de inlichtingen- en veiligheidsdiensten. Het Nederlandse standpunt met betrekking tot de rechtsbescherming zal worden ingebracht in de te verwachten onderhandelingen in de Europese Unie over een reactie naar aanleiding van de genoemde resolutie van het Europees Parlement met als doel het verwerven van steun voor het Nederlandse standpunt. Vervolgens zal een Europees gedeeld standpunt kunnen worden uitdragen in internationale gremia.

45. Het Europees Parlement roept bedrijven op om vermoedens van economische spionage te melden aan de geëigende instanties. Vooral internationaal opererende bedrijven en instellingen zouden tegen het verschijnsel kunnen zijn aangelopen, maar deze hebben veelal onvoldoende kennis en zijn in de regel niet snel geneigd om met dergelijke vermoedens naar buiten te treden. Sommige bedrijven kennen een meldingsplicht, bijvoorbeeld bedrijven die defensie orders uitvoeren. Teneinde inzicht te krijgen op vermeende en daadwerkelijke inbreuken en de achtergronden daarvan, staat de overheid tevens open voor meldingen van andere bedrijven en instellingen.

[1] Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer.