Overzicht van stemmingen in de Tweede Kamer

afdeling **Inhoudelijke Ondersteuning**

aan De leden van de vaste commissie voor Veiligheid en Justitie

datum *20 december 2016*

Betreffende wetsvoorstel:

34372
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)

Eindstemming wetsvoorstel

Het wetsvoorstel is op 20 december 2016 aangenomen door de Tweede Kamer. PvdA, Van Vliet, Houwers, Monasch, VVD, SGP, ChristenUnie en het CDA stemden voor.

Aangenomen en overgenomen amendementen

Artikel I, onderdelen F en G
15 (Tellegen en Van Toorenburg) over de strafbaarheid bij inzet van een virtuele creatie

Met dit amendement beogen de indieners explicieter dan nu in de wet staat geformuleerd een persoon strafrechtelijk te vervolgen indien hij op internet seksuele contacten met minderjarigen zoekt en/of legt met een virtuele fictieve creatie. Strafbaarstelling beperkt zich derhalve niet tot het contact zoeken met een persoon. Een en ander vanzelfsprekend indachtig geldende relevante jurisprudentie. Te denken valt daarbij in het bijzonder aan het «lokfiets-arrest». Indiener onderstreept hierbij dat bewijs dat voortvloeit uit strafrechtelijk onderzoek waarbij gebruik wordt gemaakt van de hiervoor genoemde mogelijkheid, niet per definitie terzijde kan worden geschoven onder verwijzing naar schending van het zogenoemde Tallon-criterium dat in de jurisprudentie is uitgelegd. Het

inzetten van een dergelijk middel maakt niet dat een verdachte per definitie tot andere handelingen wordt gebracht dan die waarop zijn opzet reeds is gericht.
Aangenomen. Voor: PvdA, GroenLinks, D66, Van Vliet, 50PLUS, Klein, de Groep Kuzu/Öztürk, Houwers, Monasch, de VVD, de SGP, de ChristenUnie, het CDA, de Groep Bontes/Van Klaveren en de PVV.

Artikel II, onderdeel U
14 (Recourt en Tellegen) over melding van kwetsbaarheden in geautomatiseerde werken

Dit amendement beoogt om de regel dat kwetsbaarheden in geautomatiseerde werken door de officier van justitie moeten worden gemeld sterker in de wet te verankeren. Het uitgangspunt zijn integere en veilige geautomatiseerde werken. De overheid dient dit te bevorderen. Vanwege de risico's die kwetsbaarheden in een geautomatiseerd werk met zich mee brengen, is de regel dat bekende kwetsbaarheden worden gemeld om de eigenaar van dat werk in staat te stellen die kwetsbaarheid te verhelpen. Het voorliggend wetsvoorstel biedt echter de mogelijkheid om op grond van een zwaarwegend opsporingsbelang een kwetsbaarheid niet te melden. Dit amendement regelt dat de officier van justitie het bevel om een kwetsbaarheid niet te melden pas kan geven na een machtiging hiertoe door de rechter-commissaris. Hiermee wordt een onafhankelijke rechterlijke toets in de wet gebracht waarmee voorkomen kan worden dat de officier van justitie mogelijk te gemakkelijk het opsporingsbelang boven de veiligheid van een geautomatiseerd werk laat prevaleren.
Aangenomen. Voor: PvdD, de PvdA, GroenLinks, D66, Van Vliet, 50PLUS, Klein, de Groep Kuzu/Öztürk, Houwers, Monasch, de VVD, de SGP, de ChristenUnie, de Groep Bontes/Van Klaveren en de PVV.

Verworpen, ingetrokken en/of vervallen amendementen

Artikel I, onderdeel E
Artikel II, onderdelen B, G, L en Q
18 (Van Toorenburg) over herstel van de oorspronkelijke bepaling omtrent een decryptiebevel

Dit amendement herstelt de oorspronkelijke bepaling omtrent een decryptiebevel, enkel richting de verdachte, in het conceptwetsvoorstel zoals de regering dat eerder heeft gestuurd aan de Raad van State.

Indiener betreurt het zeer dat de regering ervoor heeft gekozen dit decryptiebevel te schrappen. De achtergrond en argumenten hiervan zijn reeds opgesomd in het genoemde conceptwetsvoorstel. De regering is daarin uitgebreid ingegaan op de noodzaak en reikwijdte, toepassing, bescherming van grondrechten en de vergelijkbare regeling in andere landen omtrent het decryptiebevel.1 Dit was ook in lijn met eerdere uitspraken van de Minister en toezeggingen naar de Kamer om dit bevel te realiseren.2 In deze toelichting op onderhavig amendement herhaalt indiener dan ook de belangrijkste punten en weerlegt

zij de argumenten van de regering om het decryptiebevel alsnog uit het wetsvoorstel te halen.

Het gebruik van decryptie komt voornamelijk voor binnen bepaalde netwerken van kinderpornogebruikers en -verspreiders. Dit is in het kader van de Rotterdamse proeftuin kinderpornografie aan de orde gekomen. Ook het opsporingsonderzoek in de Amsterdamse zedenzaak bleek dat de verdachte Robert M. grote hoeveelheden kinderpornografie in versleutelde vorm op zijn computer had opgeslagen. Daarnaast is het gebruik van decryptie dienstig in terrorismezaken, de regering verwijst in het conceptwetsvoorstel ook naar de praktijk in Duitsland en het Verenigd Koninkrijk voor de wijze waarop dit in die landen dienstig is.

Juridisch gezien baseert de regering zich op één uitspraak van het Europees Hof voor de Rechten van de Mens, te weten O'Heaney en Mc Guiness tegen Ierland van nota bene zestien jaar terug, 21 december 2000 (!). Daaruit kan overigens niet worden afgeleid dat een decryptiebevel per definitie in strijd is met art. 6 EVRM – dat blijkt thans ook wel uit de brede toepassing ervan in andere landen – maar bleek dat het EHRM de hoogte van de strafbedreiging in het Verenigd Koninkrijk destijds disproportioneel vond. Over de situatie in andere landen is bekend dat thans Frankrijk en het Verenigd Koninkrijk een ontsleutelplicht voor verdachten kennen. Het Verenigd Koninkrijk kent een uitgebreide wettelijke regeling voor wanneer en hoe een decryptiebevel mag worden gegeven, met diverse waarborgen voor rechtsbescherming. In Frankrijk beperkt de wettelijke regeling zich tot strafbaarstelling van het weigeren te ontsleutelen. Australië heeft een wettelijk decryptiebevel ingevoerd dat zich specifiek tot verdachten richt, terwijl in de Verenigde Staten (VS) zich een ontsleutelplicht voor verdachten uitkristalliseert in de rechtspraak, die onder bepaalde voorwaarden verenigbaar wordt geacht met (de vergelijkbare Amerikaanse variant van) het nemo-teneturbeginsel.

De regering heeft, na aandringen van de Tweede Kamer, uitgebreid onderzoek laten doen naar de toepassing van het decryptiebevel in Nederland.3 De conclusie daaruit heeft de opmaat gevormd voor het opnemen ervan in het oorspronkelijke wetsvoorstel. Het WODC concludeert dat een decryptiebevel aan verdachten niet onverenigbaar is met het nemo-teneturbeginsel en hiervoor ruimte bestaat4. Het onderzoek beperkt daarbij zeker niet tot enkel de interpretatie van de regering omtrent de zaak O'Heaney en Mc Guiness tegen Ierland. Toepassing is mogelijk en hangt ervan af hoe het wettelijk wordt vormgegeven (bijvoorbeeld welke soort en mate van dwang kan worden gebruikt) en hoe het in een concreet geval wordt toegepast. Daarin zijn verschillende opties. Het is ook denkbaar om een lagere mate van dwang te kiezen door een weigering om te ontsleutelen niet zelfstandig strafbaar te stellen, maar deze weigering door de rechter te laten meewegen bij beslissingen over bewijs of strafoplegging. Het niet-meewerken aan een decryptiebevel ook kan strafbaar worden gemaakt op basis van artikel 184 Sr (maximaal drie maanden gevangenisstraf) of met een zelfstandige strafbaarstelling met een hogere maximumstraf.

Het juridische argument dat het decryptiebevel niet mogelijk is, faalt aldus op grond van dit WODC-onderzoek. Het is wél mogelijk, zij het zeer zorgvuldig vormgegeven in de wet. Blijft enkel over de argumentatie van de regering dat het praktisch nauwelijks haalbaar is

en niet zou voldoen aan de behoefte van de opsporingspraktijk. Indiener voegt aan deze argumentatie ook de politieke onwil toe om het decryptiebevel mogelijk te maken.

Indiener concludeert over deze laatste argumenten van de regering als volgt. Het is zeker waar dat opsporingsinstanties zich terughoudend opstellen over de wenselijkheid van gebruikmaking van het decryptie-bevel. Dit is begrijpelijk, gelet op de politieke discussie over dit instrument. Tegelijkertijd heeft het Openbaar Ministerie in haar advies bij onderhavig wetsvoorstel (8 juli 2013) aangegeven dat bij kinderporno-zaken de urgentie aanwezig is om een decryptiebevel te geven. Het OM heeft ook concrete handreikingen gedaan het bevel wettelijk te verbeteren, maar de regering koos ervoor dit plan uiteindelijk niet door te zetten. Er bestaat weinig twijfel over de toepassing van het decryptiebevel in de praktijk: dit zal inderdaad zeer beperkt zijn. Terecht geeft de regering en geven opsporingsinstanties ook aan dat de bewijsvoering en het gedrag van de verdachte belemmerend zal werken. Echter voor die paar gevallen per jaar dát wel een zaak hierdoor kan worden opgelost en mogelijk ernstige misdrijven voorkomen kunnen worden, wil indiener dat politie en Justitie niet belemmerd worden in de toepassing van het decryptiebevel. Ook al is het maar één zaak, de belangen van slachtoffer en samenleving zijn deze keuze waard, volgens indiener. Niet alleen de concrete dreiging van terroristische aanslagen maar ook de afschuwelijke zaak van Robert M. en lessen die daaruit getrokken moeten worden, liggen te vers in het geheugen om dit belangrijke instrument in de strijd tegen criminaliteit, níet in te voeren.

1Zie MvT, p. 47–62, https://www.internetconsultatie.nl/computercriminaliteit.

2Kamerstukken 2011/12, 31 015, nr. 77, p. 6 en Kamerstukken 2011/12, 31 015, nr. 79, p. 6.

3 Idem.

4Het decryptiebevel en het nemo-teneturbeginsel, nopen ontwikkelingen sinds 2000 tot invoering van een ontsleutelplicht voorverdachten?, B.J. Koops, WODC, 305.

Verworpen. Voor: 50PLUS, Houwers, de SGP en het CDA.

Artikel II, onderdeel D

19 (Van Toorenburg) over de bevoegdheid tot doorhalen van misleidende domeinnamen

Het College van Procureurs-Generaal heeft in de consultatieronde geadviseerd een wettelijke bevoegdheid te creëren waardoor het mogelijk wordt te bevelen dat een domeinnaam wordt doorgehaald. De regering heeft hier geen gevolg aan gegeven. Dit amendement strekt ertoe alsnog deze bevoegdheid mogelijk te maken.

Met name in het bancaire internetverkeer kunnen criminelen misbruik maken van internetbezoekers door een domeinnaam te creëren die veel lijkt op die van een bank. Een typefout kan er dan toe leiden dat nietsvermoedend inloggegevens worden ingevuld en criminelen hiermee aan de haal gaan.

De regering geeft aan niet tot doorhaling van domeinnamen over te willen gaan omdat dit niet zal bewerkstelligen dat de website niet meer bereikbaar is. Door een ISP een domeinnaam te laten doorhalen, worden alleen de aangesloten klanten van die ISP beperkt in hun mogelijkheden om de website via die domeinnaam te bezoeken. Indiener erkent dit,

maar stelt vast dat de regering hiermee helemaal níets doet om in elk geval de klanten van de betreffende bank, te beschermen. Dat is zeer zorgelijk en onacceptabel, gelet op het grote aantal slachtoffers jaarlijks van cybercrime en de rol die dergelijke misleidende websites hierin spelen. Met deze wettelijke bevoegdheid worden in elk geval de bezoekers van banken beschermd, hetgeen naar de mening van indiener van groot belang is.

Indiener hecht waarde aan de voorzichtigheid die de overheid betracht in het ingrijpen in internetverkeer. Daarom stelt ze voor de bevoegdheid tot doorhaling te creëren enkel met betrekking tot bancaire (misleidende) domeinnamen, waarvan is af te leiden dat deze ertoe dienen bezoekers van een bepaalde bankinstelling te misleiden.
Verworpen. Voor: 50PLUS, de SGP, de ChristenUnie, het CDA, de Groep Bontes/Van Klaveren en de PVV.

Artikel II, onderdelen G, L en Q
8 → 11 → **13** (Verhoeven c.s.) over geen gebruik maken van kwetsbaarheden in software

Dit amendement beperkt de bevoegdheid voor de politie om geautomatiseerde werken binnen te dringen, er mag namelijk geen gebruik worden gemaakt van kwetsbaarheden in software. Het binnendringen van geautomatiseerde werken zonder gebruik van kwetsbaarheden in software kan bijvoorbeeld door middel van (spear)phishing technieken, oftewel het sturen van een misleidende email of bericht waarmee een verdachte verleid kan worden om een wachtwoord of logingegevens prijs te geven of om een technisch hulpmiddel zoals een keylogger of andere software te installeren, mits zonder het gebruik van kwetsbaarheden, waarmee vervolgens inloggegevens buitgemaakt kunnen worden. Een andere techniek is social engineering, waarmee door middel van psychologische manipulatie het uitvoeren van handelingen of het openbaar maken van vertrouwelijke informatie, zoals een wachtwoord of inloggegevens, uitgelokt kan worden. Daarnaast zijn technieken mogelijk als brute forcing, dictionary attacks of shoulder surfing.

Cybersecurity experts benadrukken vaak het feit dat de mens de zwakste schakel in ICT-systemen is. Volgens de «Cyber Security Intelli-gence Index 2015» komt 95 procent van alle beveiligingsincidenten voort uit menselijke fouten. Uit meerdere onderzoeken blijkt dat ook de criminelen die zich goed beveiligen steken laten liggen. Een sprekend voorbeeld daarvan is de uitbater van de ondergrondse digitale markt Silk Road.

Het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software is een extra bevoegdheid waarvan de noodzaak niet voldoende aangetoond is. Bovendien is het binnendringen van geautomatiseerde werken door middel van kwetsbaarheden in software een onwenselijke bevoegdheid. Het maakt mensen onveilig omdat kwetsbaarheden in telefoons, tablets en andere apparaten blijven bestaan, waardoor mensen makkelijker slachtoffer kunnen worden van cybercrime. Hiermee zou de overheid een belang krijgen bij onveilige apparaten, zoals laptops, smartphones, wearables en computers en, gezien de brede definitie van «geautomatiseerde werken», ook pacemakers, auto's en medische apparatuur. Dit zorgt ervoor dat hackers die fouten in

software vinden eerder geneigd zullen zijn om gevonden fouten te verkopen aan bedrijven als HackingTeam of Gamma International dan ze te melden aan de maker van de software zodat ze gedicht kunnen worden. Dit kan bijvoorbeeld gaan om een fout in het besturingssysteem van smartphones.

In een tijd waarin vrijwel elk apparaat op het internet wordt aangesloten en onze veiligheid en onze economie steeds meer afhankelijk zijn van veilige ICT-systemen is het belangrijk dat de overheid zich juist inzet voor een veiliger internet. Deze bevoegdheid zou grote schade toebrengen aan onze economie en aan ons vestigingsklimaat. Daarnaast maakt het iedereen gevoeliger voor hacks door criminelen en landen als Rusland en China. Criminelen zullen makkelijker gegevens, zoals medische data, creditcardgegevens of inloggegevens, van gewone mensen buit kunnen maken. Daarom willen de indieners dat de overheid blijft werken aan een veiliger internet, veiligere software en sterke encryptie, alleen dan kunnen mensen veiliger gemaakt worden tegen criminelen en buitenlandse mogendheden.
Verworpen. Voor: SP, de PvdD, GroenLinks, mevrouw Oosenbrug van de fractie van de PvdA, D66, Klein, de Groep Kuzu/Öztürk en Monasch.

Artikel II, onderdeel G
17 → **25** (Van Toorenburg) over vervanging in de artikelen 126nba, 126uba en 126zpa van de achtjaargrens van delicten door zes jaar

Naar aanleiding van het advies van de Afdeling advisering van de Raad van State heeft de regering differentie aangebracht in de voorwaarden voor de toepassing van de in dit wetsvoorstel voorgestelde bevoegdheden. Specifiek voor de toepassing van onderzoekshandelingen waarbij het geautomatiseerde werk wordt binnengedrongen met het oog op het vastleggen of ontoegankelijk maken van gegevens, is in plaats van het vereiste van een misdrijf waarvoor voorlopige hechtenis is toegelaten, gekozen voor een misdrijf waarop een gevangenisstraf van acht jaar of meer is gesteld. Indiener begrijpt de gedachte hierachter, namelijk dat het op afstand binnendringen in een geautomatiseerd werk, gevolgd door het doorzoeken van alle gegevens die in dat werk zijn opgeslagen, een meer vergaande inbreuk op de privacy van de betrokkene oplevert dan wanneer het binnendringen wordt gevolgd door het aftappen van communicatie of stelselmatige observatie. Tegelijkertijd acht indiener de gekozen grens nu evenwel te hoog, omdat hierdoor bepaalde ernstige misdrijven niet binnen het toepassingsbereik van deze bevoegdheid zullen vallen. In het conceptwetsvoorstel zoals aan de Raad van State was gezonden wordt door de regering aangegeven dat bijvoorbeeld bij omvangrijke ernstige fraude de opsporingspraktijk ook in die gevallen de behoefte heeft aan de voorgestelde bevoegdheid, zodat het mogelijk is in voorkomende gevallen een geautomatiseerd werk binnen te dringen en te onderzoeken met het oog op bijvoorbeeld de vastlegging van gegevens. Indiener merkt echter op dat als gevolg van de in het thans voorliggende wetsvoorstel gemaakte keuze voor de achtjaar grens, bij delicten als gewoonteheling (art. 417) witwassen (art. 420bis) en valsheid in geschrifte (art. 225 en 227) de voorgestelde bevoegdheid niet kan worden ingezet. Dat geldt ook voor verduistering vanuit een ambt (art. 359) of bij actieve of passieve ambtelijke omkoping (art. 177 en art. 363). Indiener acht het onwenselijk dat bij dergelijke ernstige misdrijven niet de benodigde

bevoegdheden kunnen worden ingezet om gegevens vast te leggen of ontoegankelijk te maken om deze misdrijven op te lossen. Ook een delict als ontucht met een bewusteloze, dan wel een verstandelijk gehandicapte of kind (art. 247) valt hierdoor buiten de reikwijdte van de hierboven genoemde bevoegdheid. Dat geldt ook voor het aanbieden, verspreiden of bezitten van kinderpornografie (artikel 240b Sr), de verleiding van een minderjarige tot ontucht (artikel 248a Sr) en de «grooming» (artikel 248e Sr). Voor de laatste drie artikelen is de regering voornemens om deze net als het delict gebruik van een botnet (artikel 138ab, derde lid, Sr) apart aan te wijzen in een algemene maatregel van bestuur.1 Gelet op de ernst en het aantal delicten waarop een gevangenisstraf van zes jaar of meer is vereist, waarvan enkele voorbeelden hierboven genoemd door indiener, lijkt het indiener echter verstandig om in de artikelen 126nba, 126uba en 126zpa de achtjaar grens te vervangen door zes jaar. Van Toorenburg
Verworpen. Voor: 50PLUS, de SGP en het CDA.

Artikel II, onderdelen G, L en Q
9 → **21** (Verhoeven) over het bij wet aanwijzen van misdrijven waarvoor bevoegdheid tot binnendringen van een geautomatiseerd werk bestaat

Indiener stelt voor om alle misdrijven waarvoor de bevoegdheid tot binnendringen van een geautomatiseerd werk kan worden afgegeven, te regelen in de wet en niet deels bij algemene maatregel van bestuur.
De bevoegdheid tot het binnendringen van een geautomatiseerd werk betreft een vergaande bevoegdheid. Bij de toepassing van dergelijke bevoegdheden geldt dat zij voorzienbaar en controleerbaar dienen te zijn. Zodoende past het niet om ook bij algemene maatregel van bestuur misdrijven aan te wijzen waarvoor deze bevoegdheid kan worden ingezet. Dat dient bij wet geregeld te zijn om de voorzienbaarheid en controleerbaarheid te waarborgen. Indiener acht het, gezien de ernst van de misdrijven, wenselijk dat misdrijven als bedoeld in de artikelen 240b, eerste lid, 248a en 248e van het Wetboek van Strafrecht, oftewel het aanbieden, verspreiden of bezitten van kinderpornografie (art. 240b Sr), de verleiding van een minderjarige tot ontucht (art. 248a Sr) en de «grooming» (art. 248e Sr), alsnog onder de strekking van dit wetsvoorstel vallen.
Verworpen. Voor: SP, de PvdD, GroenLinks, D66, 50PLUS, Klein, de Groep Kuzu/Öztürk, Monasch, de ChristenUnie, de Groep Bontes/Van Klaveren en de PVV.

Artikel II, onderdeel G
20 (Verhoeven) over beperking van de reikwijdte van het begrip geautomatiseerd werk

De indiener beoogt met dit amendement de reikwijdte van het begrip geautomatiseerd werk te beperken. Onder de definitie van een geautomatiseerd werk vallen alle apparaten die zijn aangesloten op het internet of internet netwerk, waaronder pacemakers, MRI-scanners, auto's, teddyberen, tandenborstels, hartslagmeters en smart horloges. Dit is zeer gevaarlijk in een tijd waarin steeds meer apparaten aangesloten worden op het internet die gevoelige (medische) data opslaan of waarvan we afhankelijk zijn voor onze

veiligheid. Het hacken in apparaten kan onvoorziene gevolgen hebben voor de werking van het apparaat. Dit kan gevaarlijke gevolgen hebben als de politie een auto of een medisch apparaat hackt.
Verworpen. Voor: PvdD, GroenLinks, D66, Klein, de Groep Kuzu/Öztürk, Monasch, de Groep Bontes/Van Klaveren en de PVV.

Artikel II, onderdelen U
12 (Verhoeven) over instelling van een commissie van toezicht op de opsporingsdiensten

Indiener wil met dit amendement regelen dat zowel vooraf als achteraf sprake is van zogeheten «systeemtoezicht» op bevoegdheden waarmee op afstand in een geautomatiseerd werk kan worden binnengedrongen. Dit amendement is bedoeld om het toezicht op en daarmee de correcte uitvoering van bevoegdheden door opsporingsdiensten te versterken wanneer zij op afstand een geautomatiseerd werk willen binnendringen.

Het huidige wetsvoorstel regelt terecht de toestemming vooraf door de rechter-commissaris. Vervolgens wordt bij de inzet van de bevoegdheden weliswaar voorgesteld dat alle technische handelingen worden gelogd en opgenomen in het proces-verbaal, maar dat betekent nog niet dat de integriteit van de werking van het technische hulpmiddel en de informatie die daarmee is vergaard ook daadwerkelijk worden getoetst. De integriteit van het binnendringen van een geautomatiseerd werk kan zo ongecontroleerd en ongecorrigeerd blijven wanneer een zaak niet voor de rechter komt, als notificatie ondanks de verplichting daartoe uitblijft, of wanneer de rechter weliswaar ter zitting onregelmatigheden constateert maar daar geen consequenties aan kan verbinden.

De inzet van vergaande en heimelijke bevoegdheden kan alleen dan correct worden uitgevoerd indien sprake is van onafhankelijk en effectief toezicht zowel vooraf als achteraf. Sterk toezicht is ook in het belang van een zaak tegen een verdachte om te voorkomen dat ingezette middelen verloren gaan door onjuiste inzet door opsporingsdiensten. Het door indiener voorgestelde toezicht dient achteraf te worden uitgevoerd door een onafhankelijke, niet onder de politie of het Openbaar Ministerie ressorterende, commissie van toezicht op de opsporingsdiensten (CTOD). Deze onafhankelijke commissie toetst de regels voor het inzetten van onderhavige bevoegdheden aan de artikelen 126nba, 126uba en 126zpa Wetboek van Strafvordering en kan de opsporingsdiensten gevraagd en ongevraagd adviseren over maatregelen die een rechtmatige inzet van bevoegdheden bevorderen.

De voorgestelde commissie kan bijvoorbeeld controleren of het bevel van de rechter-commissaris niet wordt overschreden, of daadwerkelijk sprake is van logging en dat dat ook wordt opgenomen in het proces-verbaal, en of de soevereiniteit van andere landen niet wordt geschonden. Tevens dient deze commissie te beoordelen of en zo ja welke kwetsbaarheden gebruikt mogen worden waarmee niet alleen criminelen, maar ook niet-verdachte burgers kwetsbaar worden voor hacks.

De voorgestelde commissie van toezicht is een aanvulling op bestaand toezicht door diverse betrokken instanties en verandert niets aan de toetsing zoals deze in individuele gevallen is voorzien door de officier van justitie, de rechter-commissaris en de rechter. Dit voorstel beoogt slechts de door de regering voorgestelde toetsing van met name de naleving van interne procedures door de opsporingsdiensten onafhankelijk te maken van diezelfde opsporingsdiensten die uitvoering zullen geven aan de onderhavige bevoegdheden.
Verworpen. Voor: SP, de PvdD, GroenLinks, D66, 50PLUS, Klein, de Groep Kuzu/Öztürk, Monasch, de ChristenUnie, de Groep Bontes/Van Klaveren en de PVV.

Artikel III
10 → **24** (Van Tongeren) over het aanpassen van de evaluatietermijn
De Wet Computercriminaliteit III introduceert vergaande opsporingsbevoegdheden. De Afdeling advisering van de Raad van State oordeelt dat de proportionaliteit van de voorgestelde bevoegdheid van het heimelijk binnendringen in een geautomatiseerd werk onbewezen is gebleven. Dat levert spanning op met het grondwettelijk en verdragsrechtelijk erkende recht op eerbiediging van de persoonlijke levenssfeer. Zo beschouwd is het van belang om op korte termijn inzicht te krijgen in de aard en omvang van de toepassing van de in dit wetsvoorstel geïntroduceerde bevoegdheden en de beoordeling van deze toepassing door de strafrechter. Daarom zijn indieners van mening dat de evaluatiebepaling moet worden aangepast.
Verworpen. Voor: SP, PvdD, GroenLinks, D66, 50PLUS, Klein, Groep Kuzu/Öztürk en ChristenUnie.

Invoegen Artikel IVa
16 (Verhoeven) over het toevoegen van een horizonbepaling van vijf jaar

De voorgestelde bevoegdheden in het wetsvoorstel computercriminaliteit III waarmee op afstand in een geautomatiseerd werk kan worden binnengedrongen, brengt grote risico's met zich mee. Indiener constateert dat met name het gebruik van kwetsbaarheden in software nadelige gevolgen kan hebben voor alle gebruikers van die software. Dit amendement regelt zodoende dat een horizonbepaling wordt opgenomen ten aanzien van de voorgestelde bevoegdheden waarmee zij na vijf jaar komen te vervallen. Indien uit de wetsevaluatie blijkt dat een voortzetting van deze bevoegdheden verantwoord en wenselijk is, dan heeft de Minister voldoende tijd om een voortzettingsvoorstel aan de Kamer voor te leggen en daarmee continuïteit van de bevoegdheid te garanderen.
Verworpen. Voor: SP, PvdD, GroenLinks, D66, Klein, Groep Kuzu/Öztürk en Monasch.

Moties

22 (Verhoeven c.s.) over het niet inkopen van hacksoftware die gebruikmaakt van onbekende kwetsbaarheden
Verworpen. Voor: SP, de PvdD, GroenLinks, mevrouw Oosenbrug van de fractie van de PvdA, D66, 50PLUS, Klein, de Groep Kuzu/Öztürk en Monasch.

23 (Recourt) over inzetten door opsporingsinstanties van onbekende kwetsbaarheden of software die daarvan gebruikmaakt
Aangenomen. PvdA, GroenLinks, Van Vliet, 50PLUS, Klein, de Groep Kuzu/Öztürk, Houwers, Monasch, de VVD, de SGP, de ChristenUnie, het CDA, de Groep Bontes/Van Klaveren en de PVV.