P.H.P.H.M.C. van Kempen[1]

Editorial

Spyware – over duidelijke strafwetgeving, de rechtsgoedtheorie en een geconcentreerde regeling[2]

DD 2021/62

1. Inleiding

Na intensief onderzoek door zeventien mediaorganisaties uit onder meer Europa, Israël en de Verenigde Staten werd het wereldnieuws dat spyware is gebruikt om succesvol heimelijk binnen te dringen in smartphones van journalisten, mensenrechtenactivisten en kopstukken uit het bedrijfsleven.[3] Aanleiding voor het onderzoek was een gelekte lijst met meer dan 50.000 telefoonnummers van individuen die door klanten van de spywareproducent als personen van belang zouden zijn geïdentificeerd. Op de lijst staan naast personen als de zojuist genoemden vele staatshoofden, regeringsleiders en volksvertegenwoordigers alsmede ambtenaren, rechters, advocaten en vakbondsleiders. Wat betreft Europa gaat het onder meer om de Franse president Emmanuel Macron en voorzitter van de Europese Raad Charles Michel, maar niet duidelijk is of het plaatsen van de spyware bij hen of andere hooggeplaatste functionarissen is geprobeerd of zelfs geslaagd.[4]
Wel is gebleken dat de spyware – het gaat hier om het kwalitatief zeer hoogwaardige programma Pegasus – niet alleen onrechtmatig door dictaturen en andere rechtstatelijk problematische regimes wordt ingezet. Die spyware blijkt, kennelijk via de toegang die zulke overheden hebben, soms ook de georganiseerde criminaliteit ten dienste te staan.[5] Doorgaans hebben private partijen echter nog moeilijk toegang tot Pegasusspyware. Andere software waarmee heimelijk informatie van gebruikers van geautomatiseerde werken (artikel 80sexies Sr) – zoals smartphones, computers en inmiddels bijvoorbeeld ook autosystemen, woningautomatisering en persoonlijke robots – kan worden verzameld, is echter ruim en in toenemende mate voor het grote publiek beschikbaar.[6]

---

1 *Prof. mr. P.H.P.H.M.C. van Kempen is hoogleraar straf- en strafprocesrecht aan de Radboud Universiteit (onderzoekscentrum Staat en Recht/SteR).*

2 Citeerwijze: P.H.P.H.M.C. van Kempen, 'Spyware – over duidelijke strafwetgeving, de rechtsgoedtheorie en een geconcentreerde regeling', *DD* 2021/62.

3 Zie op de websites van onder meer de hierna genoemde media met verdere verwijzingen naar verdere berichtgeving over het zogenoemde Pegasus-onderzoek en het gebruik van de spyware: 'Het Pegasus Project over cyberspionage: alles wat u moet weten', *Knack* 18 juli 2021; 'Spionage-Software Pegasus: Cyberangriff auf die Demokratie', *Die Z*eit 18 juli 2021; 'Comment les données du «Projet Pegasus» ont été analysées', *Le Monde* 18 juli 2021; 'The Pegasus Project: About the Project', *OCCRP* 18 juli 2021; 'The Pegasus Project, NSO's Pegasus: The Israeli Cyber Weapon Oppressive Regimes Used Against 180 Journalists', *Haaretz* 18 juli 2021; 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', *The Guardian* 18 juli 2021; 'The Pegasus Project, A global investigation: Private Israeli spyware used to hack cellphones of journalists, activists worldwide', *The Washington Post* 18 juli 2021. Zie ook 'Pegasus (spyware)' en 'Pegasus Project (investigation)' op Wikipedia (https://en.wikipedia.org/).

4 Zie 'The Pegasus Project, A global investigation: On the list: Ten prime ministers, three presidents and a king', *The Washington Post* 20 juli 2021.

5 'Revealed: murdered journalist's number selected by Mexican NSO client', *The Guardian* 18 juli 2021; zie ook '"It's a free-for-all": how hi-tech spyware ends up in the hands of Mexico's cartels', *The Guardian* 7 december 2020; 'Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families', The New York Times 19 juni 2017.

6 Zie o.a. D. Harkin, A. Molnar & E. Vowles, 'The commodification of mobile phone surveillance: An analysis of the consumer spyware industry', *Crime Media Culture* 2020, vol. 16(1), p. 33-60; C. Parsons e.a., *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry* (Citizen Lab Research Report No. 119), University of Toronto, 2019.

Spyware is een vorm van malware oftewel ongewenste kwaadaardige software. Er bestaan onnoembaar veel vormen van spyware.[7] Mede daardoor is het niet mogelijk om tot een precieze definitie ervan te komen. In de kern betreft spyware programmatuur die de mogelijkheid biedt om heimelijk informatie te verzamelen in geautomatiseerde werken zonder uitdrukkelijke autorisatie van de gebruiker (persoon of organisatie). Hoewel daarbij vaak sprake zal zijn van het doorbreken of listig omzeilen van beveiligingen, vormt computervredebreuk (hacken) niet de essentie van spywaregebruik. Die essentie is er wel in gelegen dat van een persoon heimelijk communicatie wordt gelezen of afgeluisterd, fysieke of online gedragingen worden gevolgd en/of bestanden worden ingezien.
Afhankelijk van de kwaliteit van de spyware kan het gaan om bijvoorbeeld het lezen van tekstberichten en e-mails, volgen van toetsenbordaanslagen, bekijken van documenten, foto's en video's, detecteren van oproepen, inzien van wachtwoorden en bankgegevens, volgen van locatieverplaatsingen en verkrijgen van toegang tot de microfoon en/of de camera van het doelapparaat. De intensiteit van een inbreuk door spyware op een geautomatiseerd werk kan dus sterk van geval tot geval verschillen. Zoals verderop nog nader aan de orde komt, kan spyware bovendien vele verschillende rechtsgoederen – ook wel aangeduid als: rechtsbelangen – raken. De intensiteit van een inbreuk kan dus ook in dat opzicht sterk variëren.
Het strafrecht is als zodanig geen afdoend en zelfs niet het belangrijkste instrument bij het tegengaan van een crimineel fenomeen zoals heimelijk spywaregebruik.[8] Eerst en vooral is ook bij dit soort cybercrime technische en organisatorische preventie cruciaal. Gelet op de in potentie zeer ernstige aard van deze criminaliteit is niettemin evident dat er een rol voor het strafrecht is.[9] In het navolgende ga ik daarom in op de vraag hoe het gebruik van kwaadaardige software en de computervredebreuk die daarbij vaak speelt, strafbaar is gesteld in het Wetboek van Strafrecht. Meer in het bijzonder gaat het er daarbij om of is voorzien in een duidelijke regeling die helder uitdrukking geeft aan het te bestrijden criminele fenomeen van spyware en aan de rechtsgoederen die daarbij in het geding zijn. Daartoe komen onder meer de expressiefunctie van het strafrecht, het legaliteitsbeginsel en de rechtsgoedtheorie aan bod. Mede naar aanleiding van enkele beknopte vergelijkingen met de voor spyware relevante regeling in Sectie 502(c) van de California Penal Code, concludeer ik daarbij dat het web van strafbaarstellingen dat in ons wetboek relevant is voor spyware vanuit al deze invalshoeken tekortschiet. Tegen die achtergrond ga ik uiteindelijk in op de vraag of alle relevante strafbepalingen in één titel in het wetboek bij elkaar zouden moeten worden gebracht. Alvorens nu over te gaan tot een bespreking van diverse van die relevante strafbepalingen, is het voor het begrip nuttig eerst nog enige achtergrondinformatie te geven.

2. Spywaregebruik als diffuus en wijdverbreid fenomeen

Het gebruik van spyware kan variëren van uitermate ernstig tot weinig indringend. De reden daarvoor is dat er grote verschillen bestaan wat betreft de al genoemde intensiteit van inbreuken op geautomatiseerde werken, de ratio van de toepassing van spyware en de rechtsgoederen die daarbij worden geschonden.

7 Zie S. de Schrijver & J. Schraeyen, '"Spyware": onschuldige spionage in cyberspace?', *Computerrecht* 2005/2, p. 3-11; James Grimmelmann, 'Spyware vs. Spyware: Software Conflicts and User Autonomy', *Ohio State Technology Law Journal* 2020, vol. 16(1), p. 25-66 op 27-33.
8 Vgl. de beschouwing daarover in relatie tot ransomware van M.S. Groenhuijsen, 'Ransomware. Een harde noot om te kraken', *DD* 2020/37, p. 513-527.
9 Zie in dezelfde zin voor ransomware Groenhuijsen, *a.w.* voetnoot 8, p. 525-526.

De blootlegging van het misbruik van het Pegasusprogramma illustreert dat spyware zelfs inzetbaar is ter ondermijning van de democratische samenleving, rechtstatelijke waarden zoals journalistieke vrijheid, vrijheid van meningsuiting en rechtsbescherming, en het functioneren van economische systemen. De schadelijke effecten beperken zich dan overigens niet tot gevallen waarin de spyware succesvol wordt toegepast. Reeds de realiteit dat bijvoorbeeld journalisten of politici slachtoffer van spyware kunnen worden, kan een zogenoemd 'chilling effect' hebben, in die zin dat anderen contacten met hen uit de weg gaan. Bovendien kan het ook tot zelfcensuur leiden doordat zij zelf afzien van communicatie met smartphones of computers die voor hun werk van belang is.[10]

Spyware kan voorts een rol spelen bij meer reguliere criminaliteit waarbij bijvoorbeeld de fysieke integriteit, de vrijheid, het kernprivéleven of de vermogenspositie van individuen in het geding is. Zo kan die worden ingezet in relatie tot strafbare feiten zoals moord, belaging en huiselijk geweld (denk aan locatiebepaling en lezen of afluisteren van communicatie), zedendelicten (bijvoorbeeld het overnemen van foto's en video's, meekijken met de camera), identiteitsdiefstal en -fraude (overnemen van persoonsgegevens) en vermogenscriminaliteit (zoals door verkrijging van bankgegevens en wachtwoorden). Zeker van de twee laatste categorieën kunnen ook overheden en ondernemingen het slachtoffer worden.

Nog weer van andere orde zijn de toepassing van zogenoemde *employee monitoring software* door werkgevers of heimelijk geplaatste spyware om een partner geniepig in de gaten te houden. Verder zijn er nog de relatief beperktere privacyschendingen met spyware – waaronder ook onbevoegd geplaatste cookies kunnen vallen – om zicht te krijgen op websitegebruik of koopgedrag door individuen of organisaties.

In het algemeen geldt gebruik van kwaadaardige software als een vorm van cybercrime waar relatief veel mensen slachtoffer van worden.[11] Hoewel precieze cijfers over spyware ontbreken, is duidelijk dat ook daarvan veelvuldig gebruik wordt gemaakt.[12] Volgens cijfers van het CBS en het WODC was 13% van de Nederlanders van 15 jaar en ouder in 2019 slachtoffer van cybercrime, waarbij het ongeoorloofd binnendringen op iemands computer (computervredebreuk, hacken) met 6% het meest voorkwam.[13]

Genoemde cijfers beperken zich tot individuen en hebben geen betrekking op door overheden en bedrijven ondervonden onrechtmatige hacks of spyware.[14] Uit Nederlandse informatie en die van de Europese Unie en van andere landen is echter duidelijk dat de overheid

10 Vgl. S. Woodhams, *Spyware: An Unregulated and Escalating Threat to Independent Media*, Washington: Center for International Media Assistance (CIMA) 2021, p. 18.

11 M.G.C.J. Beerthuizen, T. Sipma & A.M. van der Laan, *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*, WODC Cahier 2020-15, p. 28-30.

12 Zie ter illustratie Europol, 'International Crackdown on Rat Spyware, Which Takes Total Control of Victims' PCS' (Press Release), 29 November 2019 (op: https://www.europol.europa.eu/newsroom/news).

13 WODC, CBS & Raad voor de rechtspraak, *Criminaliteit en rechtshandhaving 2019*, Cahier 2020-16, p. 48. Zie ook, met verwijzingen naar meerdere onderzoeken, Beerthuizen, Sipma & van der Laan, *a.w.* voetnoot 11, p. 24-26, en voorts T. Sipma & E.M.C. van Leijsen, *Slachtofferschap van online criminaliteit. Prevalentie, risicofactoren en gevolgen*, WODC Cahier 2019-18. Zie over eerdere cijfers ook J. Jansen, R. Leukfeldt, J. van Wilsem & W. Stol, 'Onlinegedragingen. Een risico voor hacken en persoonsgerichte cyberdelicten?', *Tijdschrift voor Criminologie* 2013, vol. 55(4), p. 394-408, en voor Europese cijfers C.M.M. Reep-van den Bergh & M. Junger, 'Victims of cybercrime in Europe: a review of victim surveys', *Crime Sci* 2018, vol. 7(5), p. 1-15.

14 Zie wel nog, op basis van een netto steekproef van n=1022 Nederlanders (16-80 jaar), over online veiligheid in zowel de privé- als werksituatie de cijfers in R. van der Grient, N. Schippers & K. Hengstz, *Veilig online 2020*, Ministerie van Economische Zaken en Klimaat/Motivaction.

en het bedrijfsleven in grote en alsmaar toenemende mate met aanvallen en inbreuken op hun cybersecurity te maken hebben.[15] Daarbij gaat het uitdrukkelijk ook om cyberspionage. Dat precieze cijfers ontbreken, heeft er overigens ook mee te maken dat spywareachtige toepassingen bij cybercrime vaak een rol spelen, zonder dat dit uitdrukkelijk in die termen wordt benoemd. Zo wordt bij zogenoemde card-not-present-fraude (CNP) ongeoorloofd gebruikgemaakt van kaartgegevens (nummers, factuuradressen, codes en vervaldatums) die zijn gestolen door middel van onder meer malware voor e-skimming.[16] Met de alsmaar toenemende automatisering van apparaten, die inmiddels een rol spelen in vrijwel alle facetten van het bestaan van individuen, ondernemingen en overheden, neemt het aantal potentiële doelwitten voor computergerichte criminaliteit alleen maar verder toe.[17]

3. Strafbaarstellingen betreffende spyware in het Wetboek van Strafrecht

Gezien het voorgaande is het van belang dat de strafrechtspleging kan beschikken over een helder strafrechtelijk kader voor de bestrijding van crimineel spywaregebruik. Het Wetboek van Strafrecht bevat echter geen strafbaarstellingen die uitdrukkelijk aan 'kwaadaardige programmatuur' of iets dergelijks refereren. Wel zijn er diverse strafbepalingen die in het bijzonder relevant zijn voor crimineel spywaregebruik of daarop in elk geval toepasbaar kunnen zijn. Drie kwesties verdienen daarbij nader aandacht. In hoeverre valt gebruik van spyware binnen de reikwijdte van die strafbaarstellingen? Is uit die strafbaarstellingen voldoende kenbaar dat zij in potentie relevant zijn voor spywaregebruik? En in hoeverre geven die strafbaarstellingen uitdrukking aan de rechtsgoederen die door spywaregebruik worden getroffen?

3.1 *Computervredebreuk (artikel 138ab lid 1 Sr)*

Allereerst relevant is de algemene strafbaarstelling van computervredebreuk in artikel 138ab Sr. Dit delict is in 1993[18] met de eerste Wet Computercriminaliteit in het wetboek gekomen in aansluiting op de strafbaarstelling van huisvredebreuk in artikel 138 Sr.[19] De bepaling beoogt volgens de memorie van toelichting 'het juiste evenwicht te bewaren tussen enerzijds het belang van het vrije gegevensverkeer en anderzijds de bescherming van de persoonlijke levenssfeer. […] Getracht is dit evenwicht te bereiken langs de weg van de beschermwaardigheid van het medium in plaats van die van de gegevens. […] Het gaat hierbij om een uitwerking van het beginsel dat het medium wordt beveiligd.'[20] Centraal staat aldus de bescherming tegen inbreuken op het medium: de eigenlijke computerinbraak. Het eerste lid heeft niet rechtstreeks betrekking op de bescherming van rechtsgoederen die worden geschonden nadat eerst inbreuk op het medium is gemaakt. De bepaling richt zich

15 Zie o.a. Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), *Cybersecuritybeeld Nederland 2021*, Den Haag: 2021; The European Union Agency for Cybersecurity (ENISA), *From January 2019 to April 2020: Cyber espionage, ENISA Threat Landscape*, EU 2020; Federal Office for Information Security (BSI), *The State of IT Security in Germany in 2019*, Germany 2019; Department for Digital, Culture, Media & Sport, *Official Statistics. Cyber Security Breaches Survey 2020*, United Kingdom 26 March 2020.

16 Dit betreft een nog altijd groeiende criminaliteitsvorm, aldus Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020*, European Union Agency for Law Enforcement Cooperation: 2020, p. 9, 42, 51-53.

17 Zie bijv. ook E.E. Bayard, 'The Rise of Cybercrime and the Need for State Cybersecurity Regulations', *Rutgers Computer and Technology Law Journal* 2019, vol. 45(2), p. 69-96 op 69-76.

18 Dat was toen nog als art. 138a Sr; zie *Stb.* 1993/33 (*Kamerstukken* 21551). De strafbaarstelling van computervredebreuk is sinds 1 oktober 2010 opgenomen in art. 138ab Sr; zie *Stb.* 2010/320, 321 (*Kamerstukken* 31560) en laatstelijk gewijzigd per 1 juli 2015; zie *Stb.* 2015/165, 209 (*Kamerstukken* 34034).

19 *Kamerstukken II* 1989-1990, 21551, nr. 3, p. 15 (MvT).

20 *Kamerstukken II* 1989-1990, 21551, nr. 3, p. 4, 15 (MvT).

dus niet op de rechtsgoederen die in essentie bij spyware in het geding zijn, namelijk het heimelijk kennisnemen van communicatie, gedragingen en bestanden. In lijn daarmee is voor strafbaarheid onder artikel 138ab lid 1 Sr niet vereist dat men zich toegang heeft verschaft tot beveiligde gegevens.[21] Wel zal daadwerkelijk toegang moeten zijn verworven tot het medium.[22] Het binnendringen moet dus zijn verwezenlijkt.

'Van binnendringen is', aldus het eerste lid, tweede volzin, 'in ieder geval sprake indien de toegang tot het werk wordt verworven: a. door het doorbreken van een beveiliging, b. door een technische ingreep, c. met behulp van valse signalen of een valse sleutel, of d. door het aannemen van een valse hoedanigheid.' Dit betreft een niet-limitatieve opsomming van vormen van binnendringen. Artikel 138ab Sr definieert dus niet wat onder 'binnendringen' moet worden verstaan. Ook de wetsgeschiedenis is daarover onhelder.[23] Naar normaal spraakgebruik is binnendringen het in een plaats doordringen.[24] De term impliceert dat een zekere weerstand wordt overwonnen.[25] Hoewel binnendringen in velerlei contexten een connotatie van onbetamelijkheid heeft, hoeft daarvan niet noodzakelijk sprake te zijn. Dat binnendringen formeel niet per se wederrechtelijk gedrag impliceert, lijkt ook de opvatting van de wetgever te zijn. Deze heeft 'wederrechtelijkheid' immers voorafgaand aan de term 'binnendringen' als afzonderlijk bestanddeel opgenomen in artikel 138ab Sr.

Een bewezenverklaring van het bestanddeel binnendringen, dat zoals opgemerkt taalkundig en volgens de systematiek van artikel 138ab Sr niet noodzakelijk onbetamelijkheid impliceert, vereist formeel bovendien niet dat een beveiliging is doorbroken of omzeild.[26] Dat geldt zelfs als men van oordeel is dat de vormen van binnendringen onder a t/m d in artikel 138ab lid 1 Sr alle ten minste het omzeilen van een beveiligingseis impliceren en zodoende het bestaan van enige beveiliging veronderstellen. Daaruit kan mijns inziens geen algemeen geldend beveiligingsvereiste worden afgeleid nu het slechts een niet-limitatieve opsomming betreft.[27] Indien de wetgever een zodanig vereiste algemeen beoogde te stellen, had hij dit in de bepaling moeten opnemen. De vraag is overigens of dit veel zou hebben uitgemaakt. Wanneer men beveiliging in ruime zin uitlegt, zal meestal wel in enige zin sprake van een beveiliging zijn. Bovendien zal het bij volledige afwezigheid van het doorbreken of omzeilen van enige beveiliging mijns inziens doorgaans lastig zijn om te bewijzen dat van 'wederrechtelijk' binnendringen sprake is.

Spyware kan op uiteenlopende manieren op een computer of smartphone terechtkomen. Bekend zijn het aanklikken van malafide links op websites of in ontvangen berichten

21 HR 26 maart 2013, ECLI:NL:HR:2013:BY9718, *NJ* 2013/468, m.nt. Reijntjes.

22 HR 9 april 2019, ECLI:NL:HR:2019:560, *NJ* 2019/358, m.nt. Rozemond.

23 Zie B.J. Koops & J.J. Oerlemans, 'Materieel strafrecht en ICT', in: B.J. Koops & J.J. Oerlemans (red.), *Strafrecht en ICT*, Den Haag: Sdu 2018, p. 36-37.

24 De term 'binnendringen' wordt in het Woordenboek der Nederlandsche Taal (WNT) omschreven als 'Tot binnen in eene plaats doordringen, niet zelden met geweld. In allerlei toepassingen, ook van abstracte begrippen.' en in de Dikke van Dale als 'zich (met geweld of wederrechtelijk) toegang verschaffen tot'.

25 Vgl. Keijzer, noot (punt 2) bij HR 22 februari 2011, ECLI:NL:HR:2011:BN9287, *NJ* 2012/62.

26 Zie over het niet (langer) gelden van een beveiligingsvereiste Koops & Oerlemans, *a.w.* voetnoot 23, p. 36-37 (zie daarin ook voetnoot 39 op p. 37). Zie ook *Kamerstukken II* 1991-1992, 21551, nr. 11, p. 17 (Nota n.a.v. eindverslag). Vgl. voorts bijv. Gerechtshof 's-Gravenhage 3 februari 2012, ECLI:NL:GHSGR:2012:BV3397, waarin toegangsverkrijging door het aanpassen van een url in de browserbalk wordt aangemerkt als 'binnendringen met behulp van valse signalen'. Daarbij overweegt het hof dat daarvoor geen beletsel is dat sprake is van een server die niet dermate is beveiligd dat dergelijk binnendringen onmogelijk wordt gemaakt. Opmerkelijk genoeg maakt het arrest niet duidelijk waarom de url-aanpassing wederrechtelijk was.

27 Zie anders A-G Knigge (par. 55-56), conclusie voor HR 22 februari 2011, ECLI:NL:HR:2011:BN9287, *NJ* 2012/62, m.nt. Keijzer (Toxbot). Knigge geeft overigens toe dat dit niet blijkt uit de redactie van de bepaling (vgl. art. 138a oud Sr) en dat de wetgeschiedenis niet eenduidig is. Zie wat betreft de niet-limitatieve opsomming Rb. Rotterdam 27 juli 2016, ECLI:NL:RBROT:2016:9717, waarin het tot een bewezenverklaring op grond van art. 138ab lid 1 Sr komt zonder toepassing van een van de methoden onder a t/m d in deze bepaling.

waardoor heimelijk spyware wordt geïnstalleerd, het zelf downloaden van onbetrouwbare programma's of apps waarin spyware is verborgen en het in reactie op een phishingbericht zelf opgeven van informatie waarmee een derde toegang krijgt om tersluiks spyware te plaatsen. Dergelijke methoden vallen in beginsel onder een van de vormen van binnendringen onder a t/m d in de zin van artikel 138ab lid 1 Sr.[28] In de praktijk is er echter ook allerlei heimelijk spywaregebruik dat niet of niet zonder meer binnen de reikwijdte van de bepaling valt. Dat kan bijvoorbeeld het geval zijn wanneer de gebruiker toestemming heeft gegeven aan een programma c.q. een app om allerlei blind opererende functies te installeren terwijl voor die gebruiker bij de toestemmingsverlenging moeilijk of alleen met aanzienlijke inspanning te doorgronden viel waarvoor precies toestemming werd gegeven. Van binnendringen zal in beginsel evenmin zomaar sprake zijn bij het gebruik door werkgevers op bedrijfsapparatuur van zogenoemde *employee monitoring software* ter controle van werknemers en hun werkzaamheden. Tot slot kan het bestanddeel binnendringen moeilijk te vervullen zijn in gevallen waarin de ene partner de andere heimelijk in de gaten houdt via spyware op een gezinscomputer, -tablet of -smartphone.

Dat het voor artikel 138ab lid 1 Sr draait om het binnendringen en niet om de daaropvolgende onbevoegde aanwezigheid in het medium, vindt bevestiging in het Toxbot-arrest.[29] Oerlemans & Koops wijzen erop dat het (doen) verspreiden of (doen) installeren van een virus volgens dit arrest ook computervredebreuk oplevert wanneer de afzender van het virus niet als zodanig een directe verbinding heeft met het geautomatiseerde werk dat door het virus is geïnfecteerd. Zij menen echter dat er hierbij geen sprake is van binnendringen, omdat daarvoor volgens hen vereist is dat de virusafzender daadwerkelijk met het geïnfecteerde werk communiceert.[30] Anders dan Oerlemans & Koops vereist de Hoge Raad dus niet dat het binnendringen tot een actieve aanwezigheid in het medium leidt. Ook in deze benadering van de Hoge Raad ligt de nadruk dus sterk op het eigenlijke binnendringen (in dit geval van het virus) en niet op vervolgacties.

Opmerking verdient nog dat artikel 138ab Sr – of een andere strafbepaling – niet uitdrukkelijk strafbaar stelt het onrechtmatig aanwezig blijven in een medium na daarin rechtmatig te zijn binnengekomen. Koops & Oerlemans stellen dat men met een creatieve interpretatie zou kunnen betogen 'dat indien iemand die rechtmatig toegang had tot een computer, maar langer verblijft dan toegestaan was, vanaf het moment dat de autorisatie is afgelopen toegang heeft tot de computer met behulp van een valse sleutel of valse hoedanigheid, zodat deze vorm van onrechtmatig verblijf in een computer ook onder 'binnendringen' wordt verstaan.' Zij erkennen dat een zodanige uitleg geen aanknopingspunt in de wetsgeschiedenis vindt maar achten deze wel teleologisch verdedigbaar. Mij lijkt deze benadering problematisch. Taalkundig impliceert zowel het bestanddeel 'binnendringen' als de term 'verwerving van toegang' dat sprake is van een activiteit.[31] Daarvan is geen sprake wanneer iemand zijn aanwezigheid in het werk voortzet door passief te blijven. Binnen

28 Zie bijv. Rb. Rotterdam 10 september 2019, ECLI:NL:RBROT:2019:7259 (met malware binnendringen en vervolgens overnemen van computers); Gerechtshof Den Haag 24 januari 2017, ECLI:NL:GHDHA:2017:81 (met malware binnendringen en vervolgens bankinloggegevens afvangen); Gerechtshof Den Haag 27 oktober 2016, ECLI:NL:GHDHA:2016:3213 (webcamgluurder) (met via nepwebsites verspreide malware binnendringen en vervolgens overnemen van computers en de webcam automatisch beelden naar de eigen computer laten verzenden).

29 HR 22 februari 2011, ECLI:NL:HR:2011:BN9287, *NJ* 2012/62, m.nt. Keijzer (Toxbot).

30 J.J. Oerlemans & B.J. Koops, 'De Hoge Raad bewijst een slechte dienst in high-tech-crimezaak over botnets', *NJB* 2011, p. 1181-1185.

31 Zie ook J.M. ten Voorde, in: *T&C Strafrecht*, comm. art. 138ab Sr, aant. 7 (online, actueel t/m 1 febr. 2021), die opmerkt dat computervredebreuk een commissiedelict is, dat slechts door een handelen kan worden verwezenlijkt.

de kaders van de wettekst is er mijns inziens dan ook geen ruimte voor de voorgestelde teleologische interpretatie zonder in een extensieve interpretatie te vervallen die vanuit het legaliteitsbeginsel bezwaarlijk is. Ook los daarvan lijkt mij een zodanige interpretatie lastig nu deze een doelverschuiving impliceert die niet goed aansluit bij artikel 138ab Sr. Bij deze bepaling gaat het zoals opgemerkt 'om een uitwerking van het beginsel dat het medium wordt beveiligd'. De toegang staat dus centraal en niet het heimelijk kennisnemen van communicatie, gedragingen en/of bestanden of het onbevoegd in dat medium aanwezig zijn. Door passief binnen het medium te verblijven na daarin rechtmatig te zijn binnengekomen wordt op dat medium zelf ook geen inbreuk gemaakt. Een en ander ligt mijns inziens anders indien iemand zijn of haar bevoegdheid om het medium binnen te gaan met een ander doel gebruikt dan waarvoor de bevoegdheid is verleend. In dat geval wordt niet rechtmatig toegang genomen tot de computer en kan aldus wel van binnendringen worden gesproken.[32]

Met de nadruk in artikel 138ab lid 1 Sr op het binnendringen, is deze strafbaarstelling weinig toegesneden op het fenomeen spyware. Weliswaar is bij vele vormen van spywaregebruik sprake van binnendringen, zodat de bepaling dan toepasbaar kan zijn, maar aan de essentie van crimineel spywaregebruik raakt die niet. Die essentie is immers juist wel gelegen in het verblijven in het medium en het daarbij heimelijk lezen of afluisteren van communicatie, volgen van fysieke of online gedragingen en/of inzien van bestanden. Dit betekent ook dat de rechtsgoederen die hierbij met kwaadaardige software zoals spyware worden geschonden niet tot uitdrukking komen in artikel 138ab lid 1 Sr.

3.2 *Gekwalificeerde computervredebreuk (artikel 138ab lid 2 en lid 3 Sr)*

De strafbaarstelling in artikel 138ab Sr kent, in het verlengde van het eerste lid over het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk of in een deel daarvan, twee gekwalificeerde vormen van computervredebreuk. De eerste daarvan is gericht op de bescherming tegen computervredebreuk waarbij 'de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van het geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt' (lid 2). Waar het daarbij oorspronkelijk alleen de bescherming van 'opgeslagen gegevens' betrof, beoogt deze gekwalificeerde strafbaarstelling sinds de invoering van de Wet Computercriminaliteit II ook te vrijwaren tegen het aftappen en het opnemen van 'stromende gegevens', dat wil zeggen: gegevens die in een proces zijn van verwerking of overdracht zoals binnenkomende e-mails.[33]

Anders dan voor 'overnemen' en 'opnemen' het geval is, lijkt voor 'aftappen' niet vereist dat de gegevens worden overgebracht op een eigen medium of worden overgeschreven of geprint.[34] Als aftappen geldt 'elke momentane kennisneming van gegevens', 'elke vorm van onderscheppen van gegevensverkeer, dus spraak, geschriften, beelden of data, zonder dat

32 Rb. Midden-Nederland 14 september 2021, ECLI:NL:RBMNE:2021:4419 (gebruikmaking van een rechtmatig verkregen wachtwoord met een ander doel dan het uitvoeren van de aan verdachte toebedeelde werkzaamheden levert computervredebreuk met een valse sleutel in de zin van art. 138ab Sr op); zie in soortgelijke zin maar minder scherp geformuleerd Rb. Den Haag 15 oktober 2019, ECLI:NL:RBDHA:2019:10842 (gebruik door politieagent van autorisatie om politiesystemen te raadplegen voor doeleinden die buiten de grenzen van zijn autorisatie vielen); Rb. Midden-Nederland 20 maart 2019, ECLI:NL:RBMNE:2019:1151 (gebruik door politieagent van inloggegevens voor doeleinden die ver buiten de grenzen van zijn autorisatie vielen).

33 *Stb.* 2006/300, 301 (i.w.tr. 1 september 2006); zie *Kamerstukken II* 1998-1999, 26671, nr. 3, p. 26, 28, 32 (MvT).

34 Zie kennelijk anders J.M. ten Voorde, in: *T&C Strafrecht*, comm. art. 138ab Sr, aant. 9(k) (online, actueel t/m 1 febr. 2021); zie ook J.W. Fokkens, in: *Noyon/Langemeijer/Remmelink Strafrecht*, comm. art. 138ab Sr, aant. 6 (versie: 20 sept. 2017), die mijns inziens ten onrechte opmerkt dat hier daadwerkelijk wordt ontvreemd.

sprake is van vastleggen van deze gegevens.'[35] Hieruit blijkt ondertussen tevens dat het begrip gegevens in overeenstemming met artikel 80quinquies Sr zeer ruim moet worden opgevat. Daaronder kunnen bijvoorbeeld ook camerabeelden en spraakcommunicatie vallen,[36] blijkens het voorgaande in zowel opgeslagen als stromende vorm.
Indien door middel van via computervredebreuk op een geautomatiseerd werk geplaatste spyware heimelijk wordt kennisgenomen van communicatie, gedragingen en/of bestanden, zal dit in beginsel dus binnen het bereik vallen van artikel 138ab lid 2 Sr. Het gaat hierbij echter nog altijd niet om de strafrechtelijke bescherming van de inhoud van de gegevens, nu daarvan slechts sprake is wanneer deze in civielrechtelijke zin aan een rechthebbende toebehoren, bijvoorbeeld vanwege de toepasselijkheid van het auteursrecht of het octrooirecht.[37] De aard van de gegevens – bijvoorbeeld: politiek, journalistiek, economisch of persoonlijk – is dus voor de strafbaarstelling in het tweede lid als zodanig niet relevant. Artikel 138ab lid 2 Sr richt zich dus niet op de bescherming van die rechtsgoederen die in het geding zijn vanwege juist de aard van de met spyware waargenomen gegevens.
De andere gekwalificeerde vorm beoogt te beschermen tegen computervredebreuk via een openbaar telecommunicatienetwerk (lid 3). Onderdeel a daarvan betreft de situatie dat in het verlengde van de hack van dat netwerk een specifieke vorm van gebruiksdiefstal (*furtum usus*) plaatsvindt, te weten: het na die netwerkhack via een particuliere computer, die dus niet ter beschikking staat van het publiek, gebruikmaken van diensten waarvoor anders zou moeten worden betaald.[38] Hier wordt in feite dus tegen een zeer specifieke vorm van vermogenscriminaliteit beschermd. Tot slot heeft onderdeel b betrekking op de toegang na een geslaagde hack van een openbaar telecommunicatienetwerk tot het geautomatiseerd werk van een derde zonder daarbij een beveiliging van die derde te doorbreken.[39] In feite gaat het dan om dubbel binnendringen. De toegangsverwerving bij de derde heeft immers via een oneigenlijke route plaatsgevonden, zodat ook deze als binnendringen valt aan te merken.
Concluderend: het rechtsgoed dat tot uitdrukking komt in artikel 138ab lid 2 Sr is de bescherming tegen handelingen met gegevens tijdens wederrechtelijk verblijf, terwijl dat voor artikel 138ab lid 3 onderdeel a Sr de bescherming tegen een zeer specifieke vorm van gebruiksdiefstal betreft, en voor artikel 138ab lid 3 onderdeel b Sr (zoals ook bij het eerste lid) de bescherming van het medium tegen binnendringen. Deze gekwalificeerde vormen van computervredebreuk hebben dus zeer beperkt betrekking op hetgeen waar het in essentie om gaat bij spywaregebruik, terwijl de rechtsgoederen die door zulk gebruik worden geschonden slechts zeer ten dele naar voren komen.

3.3 *Diverse andere strafbaarstellingen*

Verspreid door het Wetboek van Strafrecht staat er een flink aantal bepalingen die meer specifiek voor bepaalde facetten van spywaregebruik relevant kunnen zijn, ook al richt

35 *Kamerstukken II* 1989-1990, 21551, nr. 3, p. 7, 26 (MvT); daarin wordt dit opgemerkt in relatie tot art. 125g Sv en art. 139c Sr, maar er is geen reden om aan te veronderstellen dat de wetgever een afwijkende definitie voorstaat bij art. 138ab lid 2 Sr.
36 Zie ook A.J. Machielse, in: *Noyon/Langemeijer/Remmelink Strafrecht*, comm. art. 80quinquies Sr, aant. 3 (versie: 1 dec. 2019); Commissie modernisering opsporingsonderzoek in het digitale tijdperk (Commissie Koops), *Regulering van opsporingsbevoegdheden in een digitale omgeving*, s.l. 2018, p. 11, 66-67.
37 Zie J.W. Fokkens, in: *Noyon/Langemeijer/Remmelink Strafrecht*, comm. art. 138ab Sr, aant. 1 (versie: 20 sept. 2017), onder verwijzing naar *Kamerstukken II* 1989-1990, 21551, nr. 3, p. 15 (MvT).
38 *Kamerstukken II* 1991-1992, 21551, nr. 12, p. 3-4 (Tweede nota van wijziging). Vgl. art. 326c Sr, dat betrekking heeft op gebruikmaking van een telecommunicatiedienst voor het publiek zonder volledig te betalen.
39 *Kamerstukken II* 1991-1992, 21551, nr. 12, p. 4 (Tweede nota van wijziging).

geen daarvan zich expliciet op spyware of meer algemeen op kwaadaardige software.[40] Indien spyware tot aantasting van een geautomatiseerd werk of een werk voor telecommunicatie leidt, kan dit strafbaar zijn onder de artikelen 161sexies en 350c Sr (beide doleus) of artikel 161septies Sr (culpoos). Bij aantasting door spyware van opgeslagen gegevens kunnen artikel 350a lid 1 Sr (doleus) of artikel 350b lid 1 Sr (culpoos) van toepassing zijn. Onder deze beide bepalingen kan ook reeds het als zodanig implementeren van spyware in een computerprogramma vallen. Ook programmatuur valt namelijk binnen het begrip 'gegevens' in de zin van artikel 80quinquies Sr.[41] Er is dan sprake van het 'toevoegen van gegevens' (de spyware) 'aan andere gegevens' (de programmatuur op het medium).[42] Het opzettelijk en wederrechtelijk plaatsen van spyware in een medium is dus strafbaar onder artikel 350a lid 1 Sr. Indien de plaatsing culpoos tot stand komt, is volgens artikel 350b lid 1 Sr voor strafbaarheid vereist dat daardoor ernstige schade met betrekking tot andere gegevens wordt veroorzaakt. Daarop gelet lijkt mij de in die bepaling opgenomen strafbaarstelling van 'toevoegen van gegevens' overbodig naast de daarin eveneens opgenomen strafbaarstelling van het worden veranderd of gewist dan wel het onbruikbaar of ontoegankelijk worden gemaakt van gegevens. Het schadevereiste in artikel 350b lid 1 Sr impliceert immers dat van veranderen, wissen, onbruikbaar maken of ontoegankelijk maken sprake zal moeten zijn, nu door voornoemd schadevereiste het culpoos plaatsen van spyware als zodanig niet tot strafbaarheid kan leiden.

Artikel 350a lid 3 en 350b lid 2 Sr kunnen relevant zijn wanneer sprake is van het ter beschikking stellen of verspreiden van gegevens – inclusief kwaadaardige software – die (mede) zijn bestemd om schade aan te richten in een geautomatiseerd werk. Spyware kan dus alleen onder deze bepalingen vallen wanneer die geschikt[43] ('bestemd') is om schade aan te richten. Dit zal bij spyware lang niet altijd het geval zijn. Voorts kan onder meer het vervaardigen, verkopen en verspreiden van spyware in diverse situaties strafbaar zijn. Dat kan het geval zijn indien het spyware betreft die geschikt is om computervredebreuk te plegen, grote hoeveelheden spam te veroorzaken of gegevens die worden overgedragen door telecommunicatie of een geautomatiseerd werk af te tappen of op te nemen (artikel 139d lid 2 Sr; spyware als 'technisch hulpmiddel'), om zonder volledig te betalen gebruik te maken van telecommunicatie (artikel 326c lid 2 en lid 3 Sr; spyware als 'gegevens') of om gegevens of geautomatiseerde werken aan te tasten (artikel 350d Sr; spyware als 'technisch hulpmiddel'). Niet alleen valt kwaadaardige software zoals spyware dus onder het begrip 'gegevens', het kan tevens kwalificeren als 'technisch hulpmiddel', zo blijkt uit de wetsgeschiedenis waarin kraakprogramma's, computerprogramma's, virussen, worms en middelen die kunnen worden gedownload als voorbeelden worden genoemd.[44]

Uiteraard kan spyware een rol spelen bij vele strafbare feiten zonder dat het gebruik daarvan constitutief is voor het desbetreffende delict. Zo kan spyware – al dan niet – zijn gebruikt om botnets op te zetten waarmee spam wordt verstuurd (artikel 138b lid 2 Sr), om wederrechtelijk niet-openbare gegevens die zijn opgeslagen door middel van een geautomatiseerd werk over te nemen of door te geven (artikel 138c Sr[45]), om wederrechtelijk

40 Het navolgende beperkt zich tot misdrijven.

41 Zie ook R. van Elst, in: *T&C Strafrecht*, comm. art. 350a Sr, aant. 8b (online, actueel t/m 1 febr. 2021); Koops & Oerlemans, *a.w.* voetnoot 23, p. 31-32.

42 Zie aldus Rb. Rotterdam 24 maart 2009, ECLI:NL:RBROT:2009:BH7551; Gerechtshof Den Haag 27 oktober 2016, ECLI:NL:GHDHA:2016:3213 (webcamgluurder).

43 *Kamerstukken II* 1998-1999, 26671, nr. 3, p. 48 (MvT).

44 Blijkens *Kamerstukken I* 2005-2006, 26671 en 30036 (R 1784), nr. D, p. 12-13 (MvA), kan een computerprogramma (en daarmee mijns inziens ook een spywarefunctionaliteit) als 'technisch hulpmiddel' kwalificeren.

45 Zie voor 'heling' van zulke door misdrijf (zoals via computervredebreuk, art. 138ab Sr) verkregen niet-openbare gegevens art. 139g Sr.

van een persoon een afbeelding van seksuele aard te vervaardigen (artikel 139h Sr), om zich toegang te verschaffen tot kinderpornografie (artikel 240b Sr), om te komen tot een reële bedreiging dat in een geautomatiseerd werk opgeslagen gegevens onbruikbaar of ontoegankelijk zullen worden gemaakt of zullen worden gewist (artikel 317 lid 2 Sr) en om zonder volledige betaling gebruik te maken van telecommunicatie of om gegevens te verkrijgen waarmee dit mogelijk is met het oog op het verhandelen daarvan (artikel 326c Sr). Voorts kan spyware het bestanddeel 'technisch hulpmiddel' invullen wanneer het gaat om het via een computer afluisteren van gesprekken in een woning of elders (artikelen 139a en 139b Sr), om het aftappen of opnemen van gegevens die worden overgedragen door telecommunicatie of een geautomatiseerd werk (artikel 139c Sr[46]) en om het ongemerkt meekijken in een woning, bijvoorbeeld via een overgenomen webcam (artikel 139f Sr). Tot slot merk ik nog op dat er enkele helingachtige artikelen zijn die gedragingen met betrekking tot bepaalde wederrechtelijk verkregen gegevens of afbeeldingen strafbaar stellen (artikelen 139e, 139g, 139h lid 1 onder b en lid 2 onder a, en 273 lid 1 onder 2 Sr). Deze delicten kunnen dus ook van toepassing zijn indien de desbetreffende gegevens door spywaregebruik zijn verkregen.

3.4 *Tussenbeschouwing*

In zekere zin geldt voor de in de subparagrafen 3.2 en 3.3 besproken strafbaarstellingen het omgekeerde als bij de in subparagraaf 3.1 besproken bepaling inzake computervredebreuk. Anders dan bij artikel 138ab lid 1 Sr blijkt uit de meeste van die andere strafbepalingen namelijk voor specifieke rechtsgoederen tamelijk duidelijk dat deze bij overtreding van de bepaling worden getroffen. Weliswaar blijkt nauwelijks of niet dat computervredebreuk en gebruik van kwaadaardige software ook ondermijnend kunnen zijn voor bijvoorbeeld de democratie, journalistiek en economie, maar belangen rondom gegevens, geautomatiseerde werken of de persoonlijke levenssfeer komen wel enigszins tot uitdrukking. Dit betekent echter niet dat de strafbepalingen zich altijd specifiek richten op de rechtsgoederen waar het in de kern het meest om gaat bij spywarecriminaliteit.

Illustratief in dit opzicht is artikel 350a Sr, dat is opgenomen in de Titel over vernieling en beschadiging. Het eerste lid van deze bepaling impliceert zoals opgemerkt dat het strafbaar is om opzettelijk wederrechtelijk spyware te plaatsen. Het rechtsgoed waarop de bepaling zich daarbij direct richt, betreft de bescherming van gegevens. Bescherming van de persoonlijke levenssfeer speelt daarbij hooguit op de achtergrond een rol.[47] Juist die levenssfeer is echter een rechtsgoed dat in bepaalde gevallen het meest wezenlijk wordt getroffen bij spywaregebruik, aangezien het daarmee mogelijk is van een persoon heimelijk communicatie te lezen of af te luisteren, fysieke of online gedragingen te volgen en/of bestanden in te zien. Met spyware kunnen individuen in feite heimelijk worden belaagd. Artikel 285b Sr lijkt daarop als gevolg van jurisprudentiële ontwikkelingen inmiddels onder omstandigheden overigens ook van toepassing te kunnen zijn.[48] Belaging door middel van kwaadaardige software behoort echter zeker niet tot de kern van die bepaling.

46 Ook al is het communicatieapparaat zelf geen 'hulpmiddel' in de zin van art. 139c Sr (zie J.W. Fokkens, in: *Noyon/Langemeijer/Remmelink Strafrecht*, comm. art. 139c Sr, aant. 2 (versie: 1 mei 2007)), de spyware is dit wel, zodat gebruik daarvan op het apparaat onder art. 139c Sr kan vallen.

47 Vgl. J.M. ten Voorde, 'Digitale vermogensdelicten in het Wetboek van Strafrecht', *Ars Aequi* 2018, p. 630-642 op 636, 642, die uitlegt dat de artt. 350a en 350b Sr in het bijzonder strekken tot bescherming van de integriteit van gegevens en van het publieke belang bij bescherming van de informatiemaatschappij.

48 Vgl. HR 21 april 2020, ECLI:NL:HR:2020:673, *NJ* 2020/228 m.nt. Kooijmans; HR 4 november 2014, ECLI:NL:HR:2014:3095, *NJ* 2015/48, m.nt. Reijntjes.

Er is nog een ander verschil tussen artikel 138ab lid 1 Sr en veel van de andere strafbepalingen. Waar bij het computervredebreukartikel wel tamelijk evident is dat het gebruik van kwaadaardige software van belang kan zijn in relatie tot de strafbaarstelling, dringt zich bij veel van de andere strafbaarstellingen minder sterk op dat spyware daarvoor mogelijk van betekenis is. Zo wordt zelfs in het specifiek voor het verspreiden en ter beschikking stellen van computervirussen bedoelde artikel 350a lid 3 Sr slechts van 'gegevens' en niet van 'kwaadaardige programmatuur' of iets dergelijks gesproken.
Het op de achtergrond verdwijnen van de strafrechtelijke relevantie van malware c.q. spyware wordt mijns inziens nog versterkt doordat de in het bijzonder voor de bestrijding daarvan relevante bepalingen over het wetboek zijn verspreid. Zoals het voorgaande illustreert levert die versnippering een lastig te doorgronden web van strafbaarstellingen op. Daardoor is de gecombineerde reikwijdte van die strafbaarstellingen moeilijk te bepalen en dus ook of deze in hun gezamenlijkheid het fenomeen van kwaadaardige software en de soms verstrekkende gevolgen daarvan voldoende afdekken. Kortom, de wijze waarop de vervaardiging, verspreiding en toepassing van kwaadaardige software in het wetboek wordt strafbaar gesteld, is problematisch wat betreft de duidelijkheid van de gezamenlijke strafbaarstellingen als geheel en wat betreft de wijze waarop de rechtsgoederen die worden geschonden daarin tot uitdrukking komen.
Met het voorgaande dringt zich de vraag op of het wenselijk is om de strafbaarstelling van gedragingen met kwaadaardige software zoals spyware wezenlijk anders in te vullen en vorm te geven. Met het oog op de beantwoording van die vraag is het nuttig om de regeling in het wetboek op een aantal punten te bezien vanuit een contrapunt. Goed bruikbaar daarvoor is Sectie 502(c) van de California Penal Code.[49] Dit omvangrijke artikel bestaat uit veertien leden.[50] Het behoort in de Verenigde Staten tot de meest ruime en moderne strafbaarstellingen van onder meer computervredebreuk en gebruik van malware zoals spyware.[51] Het gaat er in het navolgende niet om de Nederlandse regeling precies te vergelijken met de strafrechtelijke regeling van de staat Californië. Wel beoog ik in de paragrafen hierna enkele karaktereigenschappen van de Californische regeling in beeld te brengen die vragen doen rijzen omtrent de kwaliteit van de regeling in ons wetboek. Daarbij draait het in het bijzonder om drie onderwerpen: de herkenbaarheid in de delictsomschrijving van onder meer het gebruik van kwaadaardige software zoals spyware als crimineel fenomeen, de kenbaarheid van rechtsgoederen die daarbij in het geding zijn en de keuze voor een geconcentreerde in plaats van een versnipperde regeling.

4. Expressiefunctie en legaliteitsaspiratie: duidelijke strafwetgeving

Uit de voorgaande uiteenzettingen volgt dat bij de voor spyware meest relevante strafbaarstellingen in ons wetboek lang niet altijd onmiddellijk kenbaar is dat het gebruik van kwaadaardige software onder die strafbaarstellingen relevant kan zijn. Daarentegen brengt de regeling in Sectie 502(c) in bepaalde opzichten duidelijk tot uitdrukking wat in feite de verboden gedraging is. Zo is krachtens subsectie (8) degene strafbaar die 'Knowingly

49 Zie voor de tekst van de bepaling de California Legislative Information website (https://leginfo.legislature.ca.gov/) onder: California law > Penal Code (PEN) > Part 1, Title 13, Chapter 5, Section 502 (Amended by Stats. 2019, Ch. 16, Sec. 1. (AB 814), Effective January 1, 2020). Section 502 California Penal Code is ook bekend als de Comprehensive Computer Data Access and Fraud Act.

50 Zie overigens ook Sectie 502(b), waarin vijftien begrippen nader worden gedefinieerd, en Sectie 502(d) e.v., waarin onder meer de toepasselijke sancties zijn opgenomen.

51 Zie het overzicht van relevante wetgeving in de Verenigde Staten op de website van de National Conference of State Legislatures (NCSL) onder 'Computer Crime Statutes' (https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx).

introduces any computer contaminant into any computer, computer system, or computer network.' Reeds uit deze formulering blijkt onmiskenbaar dat het implementeren van kwaadaardige software strafbaar is. Daar komt dan nog bij dat Sectie 502(a)(12) definieert wat moet worden verstaan onder 'computer contaminant'. Blijkens de lange definitie gaat het, kort gezegd, om computerinstructies, zoals wormen en virussen, die onder meer kunnen zijn bedoeld om informatie te doen verzenden. Veel minder spreekt voor zichzelf dat gebruik van kwaadaardige software eveneens strafbaar is onder artikel 350a Sr. Om te begrijpen dat dit het geval is moet men zich immers realiseren dat zulke software onder het bestanddeel 'gegevens' valt, terwijl het in de computer brengen daarvan als 'toevoegen' geldt.
Ander voorbeeld: mede door de versnippering van relevante strafbaarstellingen valt in de Nederlandse regeling minder op dan in die van California dat het vervaardigen, verkopen en verspreiden van spyware in diverse situaties strafbaar is. Het zou al veel verduidelijken wanneer het bestanddeel 'technisch hulpmiddel' in artikel 139d Sr – alsmede in andere bepalingen waarin dit bestanddeel voorkomt en de strafbaar gestelde gedraging met behulp van kwaadaardige software kan worden gepleegd – zou worden vervangen door bijvoorbeeld het bestanddeel 'programmatuur of ander technisch hulpmiddel'. Ter laatste illustratie noem ik dat Sectie 502(c)(9) een expliciete strafbaarstelling bevat van het bewust en zonder toestemming gebruiken van een internetdomeinnaam of een profiel van een andere persoon, onderneming of entiteit om e-mails of posts te verzenden wanneer men daardoor schade toebrengt aan bijvoorbeeld een computer. Ons wetboek kent geen strafbepaling waarin misbruik van zulke namen en profielen is geëxpliciteerd.

Om uiteenlopende redenen is het wenselijk dat strafbepalingen duidelijk maken welke criminele gedragingen of fenomenen zij beogen tegen te gaan. Dit is allereerst aangewezen wil het strafrecht zijn expressieve functie om de maatschappelijke afkeuring van criminele gedrag uit te drukken optimaal kunnen waarmaken.[52] Wanneer voor mensen niet onmiddellijk herkenbaar is welk type activiteiten binnen het kernbereik van een strafbaarstelling ligt, zal de mogelijk communicatieve waarde van de normstelling daarin worden beperkt. Het gaat er dan dus om dat het strafrecht als in beginsel zwaarste instrument om de ontoelaatbaarheid van gedrag formeel te benadrukken, zijn expressieve potentie en in het verlengde daarvan mogelijk preventieve werking niet optimaal benut.
Zonder het belang van de expressieve functie te miskennen, zijn hierbij wel nog enige kanttekeningen op zijn plaats. Allereerst wil het daarnet gestelde niet zeggen dat een strafbepaling noodzakelijk nader omschreven gedragingen dient te bevatten om een sterke expressieve waarde te kunnen hebben. Bij veel materiële delicten – zoals doodslag in artikel 287 Sr – is immers ook zonder nadere specificering van allerlei gedragingen voor vrijwel eenieder uit de strafbepaling wel duidelijk wat niet is toegestaan. Hiervoor bleek reeds dat zulke duidelijkheid er wat betreft crimineel spywaregebruik in veel mindere mate is.
Voorts impliceert het voorgaande niet dat duidelijke benoeming van de criminele gedragingen waartegen de strafbaarstelling zich richt feitelijk veel effect heeft, in die zin dat dit bijvoorbeeld de morele afkeuring van spyware in de maatschappij zal versterken of tot

52 Vgl. J. de Hullu, *Materieel strafrecht*, Deventer: Wolters Kluwer 2021, p. 8, onder verwijzing naar *Kamerstukken II* 2001-2002, 27834, nr. 2, p. 15-16 (Nota criminaliteitsbeheersing). Zie over de communicatieve functie van het strafrecht (en het vaststellen van strafrechtelijke aansprakelijkheid) ook V. Tadros, *Criminal Responsibility*, Oxford: OUP 2007, i.h.b. hst 3. Het gaat mij hier overigens dus niet om de discussie over de rechtvaardiging van strafbaarstelling en dus evenmin om de vraag of gedrag om symbolische redenen mag worden strafbaar gesteld; zie daarover o.a. J. Wilenmann, 'Framing Meaning through Criminalization: A Test for the Theory of Criminalization', *New Criminal Law Review* 2019, vol. 22(1), p. 3-33.

een vermindering zal leiden van spywarecriminaliteit. Dus ook bij het door een duidelijke redactie optimaliseren van de potentieel expressieve en preventieve werking van een strafbepaling kan het effect dat het enkele bestaan van die bepaling in de werkelijkheid heeft gering zijn.
Tot slot benadruk ik dat het belang bij optimalisering van de expressieve waarde van strafbepalingen niet absoluut is. Bij het bepalen van de formulering van strafbaarstellingen kunnen ook andere belangen spelen die van invloed mogen zijn op de redactie van een strafbepaling. Zo zal de strafbaarstelling moeten passen in het systeem van het wetboek en zal deze binnen de strafrechtspleging ook praktisch hanteerbaar moeten zijn.

Als keerzijde van bovenstaande meer instrumentele invalshoek is er eveneens een rechtsbeschermingsbelang dat erop aandringt dat strafbepalingen duidelijk maken welke criminele gedragingen zij beogen tegen te gaan. Dat belang is gelegen in het Bestimmtheitsgebot. Daarmee impliceer ik niet dat de in paragraaf 3 besproken strafbepalingen daarmee in strijd zouden zijn op de grond dat in die bepalingen niet concreet naar voren komt dat het gebruik van kwaadaardige software binnen de reikwijdte ervan valt. Voor zodanige conclusie is er mijns inziens geen aanleiding, mede erop gelet dat strafbaarstellingen niet gauw als onvoldoende duidelijk, specifiek of voorzienbaar worden aangemerkt door de Hoge Raad en het Europees Hof voor de Rechten van de Mens. Het Bestimmtheitsgebot is echter niet alleen relevant als begrenzing van de wijze waarop gedrag kan worden strafbaar gesteld, in aanvulling daarop hebben de uit het gebot voortvloeiende eisen ook een aspiratieve functie. Het legaliteitsbeginsel scherpt immers ook in dat de wetgever steeds dient te streven naar zo duidelijk, specifiek en voorzienbaar mogelijke materieelrechtelijke strafwetgeving. In dit opzicht blijkt de strafbaarstelling van de vervaardiging, de verspreiding en het gebruik van kwaadaardige software zoals spyware suboptimaal te zijn.

5. Rechtsgoedtheorie: duidelijke kenbaarheid rechtsbelangen (redactiefunctie)

Zoals opgemerkt komen in veel van de relevante Nederlandse strafbaarstellingen verder ook de door spywaregebruik geschonden rechtsgoederen beperkt of niet scherp naar voren. Dit ligt anders voor de regeling in Sectie 502(c). De daaraan voorafgaande Sectie 502(a) maakt – als een soort inleidende bepaling die wij zo niet kennen – kenbaar dat Sectie 502 als geheel strekt ter bescherming van personen, bedrijven en overheidsinstanties tegen manipulatie, interferentie, schade en ongeoorloofde toegang tot rechtmatig gecreëerde computergegevens en computersystemen. Volgens de bepaling is de bescherming van de integriteit van computers, computersystemen en computergegevens van vitaal belang voor de bescherming van de privacy van individuen en voor het welbevinden van financiële instellingen, ondernemingen, overheidsinstanties en anderen die deze computers, systemen en gegevens legaal gebruiken. Hier komen dus zowel individuele als publieke rechtsbelangen tot uitdrukking. Ook in de strafbaarstellingen zelf – in Sectie 502(c) – komen de rechtsgoederen die in het geding zijn soms tamelijk expliciet naar voren. Zo hebben de leden (10) en (11) t/m (14) uitdrukkelijk betrekking op onder meer ‘government computer services’ resp. ‘public safety infrastructure computer system’ apparaten. En in de al genoemde Sectie 502(c)(9) blijkt expliciet dat de strafbaarstelling strekt tot bescherming van internetdomeinnamen en profiel van personen, ondernemingen en andere entiteiten.

Tamelijk algemeen wordt erkend dat het rechtsgoedconcept in het strafrecht in elk geval drie functies vervult.[53] Ten eerste kan de mogelijkheid om tussen verschillende rechtsgoederen te onderscheiden worden gebruikt als een van de criteria om strafbare feiten in te delen en te groeperen (groeperingsfunctie). Mede in het verlengde daarvan kan het rechtsgoed voorts richting geven bij de uitleg van strafbepalingen (interpretatiefunctie). Tot slot lijkt als algemeen aanvaard – maar, gelet op de mogelijkheid om het begrip rechtsgoed zeer ruim uit te leggen, niet noodzakelijk wezenlijk beperkend – uitgangspunt te gelden dat alleen de bescherming van rechtsgoederen het strafbaar stellen van gedragingen kan rechtsvaardigen (legitimeringsfunctie). Dat de wetgever zich al dan niet expliciet met een strafbaarstelling op bepaalde rechtsgoederen richt, heeft dikwijls invloed op de vormgeving van de delictsomschrijving.[54] Dat wil echter nog niet zeggen dat het rechtsgoed zich daarbij ook steeds duidelijk laat identificeren in de strafbepaling.[55] Hier is dan ook vooral de vraag van belang of de rechtsgoedtheorie tevens vereist dat strafbaarstellingen duidelijk maken welke rechtsgoederen zij beogen te beschermen.

De literatuur biedt geen duidelijk antwoord op die vraag. Wel laat Esser zien dat rechtsgoederen vaak duidelijker tot uitdrukking komen in de bestanddelen van materiële delicten, krenkingsdelicten en concrete gevaarzettingsdelicten en dus in mindere mate in die van formele delicten en abstracte gevaarzettingsdelicten.[56] Deze onderscheidingen zijn echter diffuus en het gaat mijns inziens bovendien ook om niet meer dan een algemeen beeld. Zo is uit de vaak als formeel delict aangemerkte strafbaarstelling van diefstal in artikel 310 Sr met de zinssnede 'enig goed dat […] aan een ander toebehoort wegneemt' mijns inziens tamelijk duidelijk af te leiden dat deze bepaling strekt tot bescherming van het vermogen. Evenzo valt uit het formele delict meineed in artikel 207 Sr goed te begrijpen dat dit de (eed als waarborg voor) waarheid beoogt te beschermen. De conclusie die Esser uiteindelijk trekt komt erop neer dat het articuleren en toetsen van de kwaliteit van de relatie tussen het strafwaardige gedrag en het met de strafbaarstelling te beschermen rechtsbelang 'een wezenlijk onderdeel van het rechtsbelangenconcept' vormt en 'daarmee als vanzelf een belangrijk aspect bij de legitimatie van strafwetgeving' is.

Deze conclusie onderschrijf ik voor zover die vaststelt wat het rechtsgoedconcept veronderstelt. Wat dat betreft kan de conclusie zelfs een stap verder gaan. Mijns inziens is namelijk verdedigbaar dat het concept – als een vierde functie – ook meebrengt dat het rechtsgoed dat een strafbaarstelling beoogt te beschermen duidelijk uit de wet identificeerbaar dient te zijn voor de strafbepaling (redactiefunctie). Die duidelijkheid kan expliciet uit de bestanddelen van de bepaling zelf volgen, maar bijvoorbeeld ook impliciet uit de context van de groep strafbepalingen waarin de strafbaarstelling is opgenomen. Het rechtsgoedconcept impliceert een zodanig kenbaarheidsvereiste in die zin dat zonder vervulling ervan de optimale verwezenlijking van voormelde drie functies van het concept wordt bemoeilijkt. Positief geformuleerd: realisatie van de redactiefunctie bevordert de verwezenlijking van de drie andere functies. Duidelijke kenbaarheid van het beschermde rechtsgoed draagt immers bij aan het onderscheid tussen groepen strafbare feiten (groeperingsfunctie), biedt

53 Zie o.a. De Hullu, *a.w.* voetnoot 52, p. 68-70; L.B. Esser, *De strafbaarstelling van mensenhandel ontrafeld. Een analyse en heroriëntatie in het licht van rechtsbelangen* (diss. Leiden), Den Haag: Boom juridisch 2019, i.h.b. p. 4-6 en hst. 2; V.E. van de Wetering, S.A. Eckhardt & S.R. Bakker, 'De rol van het achterliggende rechtsgoed van strafbepalingen bij de beoordeling van de strafwaardigheid van gedrag', *DD* 2018/13, p. 138-167; A.J. Machielse, 'Enige opmerkingen over het rechtsgoed, *DD* 1979, p. 24-43; T. Hörnle, 'Theories of Criminalization', in: M.D. Dubber & T. Hörnle, *The Oxford Handbook of Criminal Law*, p. 679-701 op 686-687.

54 Zie daarover Esser, *a.w.* voetnoot 53, p. 40-42.

55 Zie daarover ook Machielse, *a.w.* voetnoot 53, p. 40-43.

56 Esser, *a.w.* voetnoot 53, p. 38-46. Overigens spreekt Esser van rechtsbelang in plaats van rechtsgoed, maar hij ziet tussen de termen geen principieel onderscheid (p. 13).

nadere houvast voor de rechter bij het uitleggen van de delictsomschrijving (interpretatiefunctie) en zorgt ervoor dat de legitimering van de strafbaarstelling in de bepaling zelf tot uitdrukking komt (legitimeringsfunctie). Daarmee is echter niet gezegd dat het ook wenselijk is de rechtsgoedtheorie in absolute termen voor het strafrecht te erkennen. Juist omdat toepassing van een dergelijke sterke rechtsgoedtheorie de Typizität (d.w.z. de typische eigen en dus beperkte portée[57]) van strafbaarstellingen zal intensiveren, kan deze de wetgever belemmeren wanneer het erom gaat meer diffuse strafrechtelijk relevante fenomenen onder een strafbaarstelling te brengen.
Op zichzelf lijkt van zo'n diffuus fenomeen ook sprake bij het gebruik van kwaadaardige software. Dat neemt echter niet weg dat de rechtsgoederen die in het geding zijn bij het gebruik van onder meer spyware duidelijker dan thans het geval is zouden kunnen doorklinken in de toepasselijke strafbaarstellingen zonder aan de reikwijdte ervan af te doen. Dit is onder meer mogelijk door het heimelijk plaatsen van kwaadaardige software in dergelijke expliciete termen strafbaar te stellen in een afzonderlijke bepaling. Daarbij kunnen dan verschillende gekwalificeerde vormen worden opgenomen. Een daarvan zou het via die software heimelijk kennisnemen van communicatie, gedragingen en/of bestanden kunnen zijn. Verdere gekwalificeerde vormen zouden kunnen worden ingericht naar de gevolgen van het heimelijk kwaadaardig softwaregebruik. Daarbij valt te denken aan het veroorzaken van gevaar voor of teweegbrengen van ernstige inbreuken op de persoonlijke levenssfeer of vrijheid, op de journalistieke vrijheid, op de automatiseringsinfrastructuur van overheden en ondernemingen en/of op politieke, constitutionele, economische of sociale structuren.

6. Naar een geconcentreerde samenhangende regeling

Aansprekend aan de Californische regeling is mijns inziens tot slot dat de voor computervredebreuk en het vervaardigen, verspreiden en gebruik van kwaadaardige software relevante strafbepalingen in beginsel bij elkaar staan in de Secties 502(a) t/m (k) van de California Penal Code. Dat die Penal Code en het Nederlandse Wetboek van Strafrecht op vele punten fundamenteel van elkaar verschillen, neemt niet weg dat beide een opbouw aan de hand van delictsgroepen kennen. De California Penal Code illustreert daarmee dat een dergelijke opbouw er niet noodzakelijk aan in de weg hoeft te staan strafbaarstellingen aangaande computervredebreuk en kwaadaardige software bij elkaar in een samenhangende regeling onder te brengen. Zodanige geconcentreerde in plaats van versnipperde regeling heeft belangrijke voordelen.
Een eerste pluspunt is dat een geconcentreerde regeling beter duidelijk kan maken tegen welke criminele gedragingen en fenomenen de daarin opgenomen strafbaarstellingen zich richten. Zodanige regeling kan dus bijdragen aan de kenbaarheid van de strafbaarheid van computervredebreuk en het vervaardigen, verspreiden en gebruiken van kwaadaardige software. Daartoe is niet per se vereist dat elk van de strafbaarstellingen afzonderlijk tot uitdrukking brengt op welk specifiek crimineel fenomeen deze betrekking heeft. Waar de relevante bepalingen thans immers veelal op zichzelf staan binnen titels die grotendeels niets met computercriminaliteit te maken hebben, zullen zij binnen een geconcentreerde regeling in de context van het geheel fungeren en dus profiteren van de kenbaarheid die uit de totaliteit van de regeling naar voren komt. Zoals hiervoor al aan de orde kwam, is het zowel vanuit de expressiefunctie van het strafrecht als het Bestimmtheitsgebot wenselijk

57 Zie C. Kelk, 'Atypisch handelen en de grenzen van de delictsomschrijving', in: C. Kelk, *De kunst van een human strafrecht*, Den Haag: Boom juridisch 2018, p. 179-194 op 183-185.

dat duidelijk kenbaar is dat de voor het fenomeen van computervredebreuk en kwaadaardige software relevante strafbepalingen inderdaad daarop betrekking hebben.[58]
Voorts is hier ook de rechtsgoedtheorie relevant. Zoals uiteengezet komen de rechtsgoederen die bij computervredebreuk en handelingen met kwaadaardige software zoals spyware worden geschonden, niet scherp en hooguit zeer beperkt tot uitdrukking in de daarvoor relevante strafbepalingen.[59] Daarnaast fungeren die strafbepalingen in titels waarin vaak andere rechtsgoederen centraal staan dan die het meest relevant zijn voor deze vormen van computercriminaliteit.[60] Dit bemoeilijkt het kunnen vaststellen van de bij de computergerichte delicten relevante rechtsgoederen nog verder. Bovendien vertroebelt het ook de consistentie en toegankelijkheid van die titels zelf en verstoort dit het toch al enigszins willekeurige onderscheid tussen titels. Deze verschillende problemen zouden goeddeels kunnen worden opgelost door te voorzien in een geconcentreerde regeling voor computervredebreuk en kwaadaardige software. Daarin zouden de verschillende binnen dit criminaliteitsfenomeen met elkaar samenhangende relevante rechtsgoederen bescherming kunnen vinden. Dit zou dan bijvoorbeeld op een soortgelijke manier mogelijk zijn als waarop de bepalingen in het Tweede Boek, Titel XXII voor het fenomeen diefstal via diverse strafbaarstellingen uiteenlopende rechtsgoederen beschermen. Niet alleen de regeling zelf maar ook de systematiek van het wetboek als geheel zou daarmee winnen vanuit het gezichtspunt van de rechtsgoedtheorie. Het zou immers tot een betere verwezenlijking leiden van in het bijzonder de interpretatiefunctie, legitimeringsfunctie en redactiefunctie.[61]
Voorts zou een geconcentreerde regeling voor computervredebreuk en kwaadaardige software aanzienlijk toegankelijker kunnen zijn dan het huidige systeem. Het vergt bijzondere inspanning om het thans versnipperde web van strafbaarstellingen te hanteren bij de opsporing, vervolging en berechting van spywarecriminaliteit. Het systeem is daarmee niet alleen inefficiënt in het gebruik, het vergroot ook de kans op fouten en het onbenut laten van mogelijkheden die erin liggen verscholen. Dit is onder meer het geval omdat de gecombineerde reikwijdte van de strafbaarstellingen moeilijk valt vast te stellen doordat deze over het wetboek zijn verspreid en doordat ook niet onmiddellijk zichtbaar is welke strafbaarstellingen in potentie relevant zijn. Bijgevolg kan het – zeker omdat zich op cyberterrein doorlopend nieuwe ontwikkelingen voordoen – een hele uitdaging zijn om te bepalen in hoeverre en in welke mate de in potentie relevante strafbepalingen in hun gezamenlijkheid het fenomeen van kwaadaardige software en de soms verstrekkende gevolgen daarvan voldoende afdekken. Het is dan ook niet verwonderlijk dat het openbaar ministerie eerder al heeft bepleit om zelfs alle cybercrimedelicten in één titel op te nemen. Dit zou ten goede komen aan de toegankelijkheid, de werkbaarheid en het in onderlinge samenhang toepassen van de daarvoor relevante strafbepalingen.[62]
Ook Ten Voorde stelt de vraag waarom er niet voor is gekozen cybercrime in één titel te regelen.[63] In kennelijke aansluiting op de rechtsgoedtheorie hecht hij er daarbij belang aan om strafbaarstellingen over hetzelfde onderwerp te bezien vanuit het gemeenschappelijk belang dat de strafbaarstellingen op het betreffende terrein trachten te dienen. Meer algemeen vanuit de systematiek van het wetboek betoogt Wolswijk in relatie tot de vraag of het

58 Zie hiervoor paragraaf 4.
59 Zie hiervoor paragraaf 5.
60 Zie daarover ook de uitgebreide uiteenzetting van Ten Voorde, *a.w.* voetnoot 47, p. 630-642.
61 Zie paragraaf 5.
62 College van procureurs-generaal, 'Advies implementatie richtlijn aanvallen op informatiesystemen', 21 maart 2013 (blg-382470; bij *Kamerstukken II* 2014-2015, 34034, nr. 3 (MvT)). Vgl. Ten Voorde, *a.w.* voetnoot 47, p. 642.
63 J.M. ten Voorde, 'Het Wetboek van Strafrecht ter discussie', in: B.J.G. Leeuw e.a. (red.), *Leidse gedachten voor een modern straf(proces)recht*, Den Haag: Boom juridisch 2017, p. 21-43 op 34-35.

wetboek herziening behoeft onder meer dat 'computerdelicten' opnieuw doordenking verdienen.[64] Op zichzelf zou het mogelijk zijn om de versnipperde regeling van cybercrime in het wetboek voor een geïntegreerde herziening op beperkte schaal in aanmerking te laten komen. De Hullu benadrukt dat toegankelijkheid, consistentie en stelselmatigheid ook dan primaire aandachtspunten behoren te zijn.[65] Deze worden zijns inziens gestimuleerd door een samenhangende regeling die als geheel bij de tijd is. Relevant daartoe lijkt mij dat juist wanneer de relevante bepalingen bij elkaar staan in een titel, de waarde van het geheel al gauw groter zal zijn dan de som der delen. In de context van het samenhangende geheel wordt immers mede de betekenis van elk van de afzonderlijke bepalingen beter duidelijk, ook wat betreft het verboden criminele fenomeen en de te beschermen rechtsgoederen waarop deze betrekking hebben.

Hoewel deze bijdrage zich specifiek richt op computervredebreuk en vervaardiging, verspreiding en toepassing van kwaadaardige software waaronder in het bijzonder spyware, meen ik dat de vele besproken argumenten meebrengen dat inderdaad het hele samenstel van computergerichte delicten opnieuw doordenking verdient. Daarbij dient dan ook te worden bezien hoe overlapping met andere – veelal klassieke – delicten kan worden voorkomen dan wel kan worden opgelost via de samenloopregeling. Een afzonderlijke regeling betekent eveneens dat er niet aan zal kunnen worden ontkomen om onder meer te onderscheiden tussen strafbare feiten die zijn gericht tegen computertechnologie (zoals computervredebreuk en gebruik van kwaadaardige software) en andere strafbare feiten. Hoewel het voor bepaalde strafbare feiten arbitrair zal zijn of zij wel of niet als computergerichte delicten moeten worden aangemerkt, zal dit naar mijn verwachting toch een aanzienlijk inzichtelijker en hanteerbaarder stelsel opleveren dan waarvan thans sprake is. Zodanige verbetering lijkt mij, ook gezien de vele technologische ontwikkelingen die ons nog te wachten staan, meer dan wenselijk.

64 H.D. Wolswijk, 'Herziening van het Wetboek van Strafrecht?', in: E. Gritter (red.), *Modern strafrecht*, Deventer: Wolters Kluwer 2019, p. 35-46 op 43-44.

65 J. de Hullu, 'En straks op weg naar een geïntegreerde herziening van het Wetboek van Strafrecht?', in: T. Kooijmans e.a. (red.), *Op zoek naar evenwicht* (Liber amicorum Groenhuijsen), Deventer: Wolters Kluwer 2021, p. 339-350; De Hullu, *a.w.* voetnoot 52, p. 545-554.