Zorgplichten tegen cybercrime

Eric Tjong Tjin Tai & Bert-Jaap Koops[1]

Op 16 en 17 april 2015 vond de Global Conference on Cyber Space 2015 in Den Haag plaats. De bestrijding van cybercrime stond daarbij hoog op de agenda. Cybercrime is wereldwijd een van de grote uitdagingen van het internet, en een terrein waarop Nederland vaak een voortrekkersrol speelt. Meestal richt de aandacht zich op daders en slachtoffers, maar bij een integrale aanpak van cybercrime moeten ook derde partijen worden betrokken, zoals internetaanbieders en softwareontwikkelaars. Kunnen deze derden ook juridisch worden aangesproken als zij hun rol bij de bestrijding van cybercrime verwaarlozen?

1. Inleiding[2]

Tegelijk met de opkomst van internet heeft cybercrime in tal van ingenieuze varianten een grote vlucht genomen. In vele rapporten zijn de diverse vormen geanalyseerd en maatregelen ter bestrijding gesuggereerd.[3] Centraal hierbij staan natuurlijk de daders, maar ook de slachtoffers, die oplettender kunnen zijn en voorzorgsmaatregelen kunnen nemen. Daarnaast wordt er ook vaak op gewezen dat diverse andere partijen zoals Internet Service Providers (ISP's) en softwareleveranciers een bijdrage kunnen leveren. Maar in welke mate zijn zij daartoe ook *verplicht*? Dat is de vraag die in dit artikel centraal staat.[4]

Allereerst beschrijven we kort de relevante factoren en partijen bij cybercrime. Vervolgens behandelen we relevante zorgplichten. Eerst geven we een theoretisch kader over zorgplichten, daarna volgt een positiefrechtelijke beschrijving op hoofdlijnen van zorgplichten op betrokken partijen in vogelvlucht: eerst privaatrecht, dan strafrecht. Dit berust op vergelijkend onderzoek van het recht van Nederland, de Verenigde Staten, Brazilië en Tsjechië. De keuze van deze landen is ingegeven door geografische spreiding en verschillen in rechtstradities en internet-penetratie, zodat een zo gevarieerd mogelijk beeld ontstaat. Vanwege de beperkte ruimte ligt in dit artikel de nadruk op Nederlands en Amerikaans recht, met korte opmerkingen over andere rechtsstelsels.[5] Na een korte tussenconclusie eindigen we met suggesties voor verbetering.

2. Cybercrime als probleem: de rol van derden

Cybercrime kent vele gezichten. Toch zijn er voor veel vormen van cybercrime overlappende oorzaken. Om een goed beeld te krijgen van de bestrijdingsmogelijkheden is daarom een korte analyse van de oorzaken nodig. We concentreren ons op twee vormen van cybercrime, met twee centrale factoren die ook veel andere soorten cybercrime veroorzaken: de infectie van computers met malware en zogenaamde 'botnets' van geïnfecteerde computers.[6]

Een infectie door malware ontstaat primair door twee oorzaken: een gebrekkig veiligheidsbewustzijn bij de gebruiker, en fouten in de software waardoor misdadigers toegang kunnen krijgen tot de computer. Men kan het vergelijken met een bewoner die de deur open laat staan, of een slecht gefabriceerde deur die eenvoudig open te krijgen is zonder sleutel (met de kanttekening dat het functioneren van deuren makkelijker te begrijpen en te beheersen is voor burgers dan computerbeveiliging). Bei-

Auteurs

1. Prof. mr. T.F.E. Tjong Tjin Tai is hoogleraar privaatrecht en prof. dr. E.J. Koops is hoogleraar regulering van technologie, beiden aan *Tilburg University*.

Noten

2. Dit artikel is gebaseerd op een onderzoeksrapport dat is vervaardigd in opdracht van de Nationaal Coördinator Terrorismebestrijding en Veiligheid: T.F.E. Tjong Tjin Tai, D.J.B. op Heij, K.K. e Silva, I. Skorvanek & B.J. Koops, *Duties of care and diligence against cybercrime*, 2015 (te raadplegen via https://repository.uvt.nl. Hierna: Rapport).

3. Bijv. OECD, *Malicious Software (Malware)*, 2008; UNODC, *Comprehensive Study on Cybercrime*, Draft, 2013; N.S. van der Meulen & A.R. Lodder, 'Cybersecurity', in: S. van der Hof, A.R. Lodder & G.J. Zwenne (red.), *Recht en computer*, Deventer 2014, p. 301-318.

4. Zie ook Corien Prins, *NJB* 2007/307, afl. 6, p. 321, en *NJB* 2013/948, afl. 18, p. 1185.

5. Voor uitgebreide beschrijvingen van de buitenlandse stelsels, zie Rapport, par. 5 en 6.

6. Zie voor (veel) meer details Rapport, par. 4, de literatuur in noot 3 hierboven en J.A. Chandler, 'Security in Cyberspace: Combatting Distributed Denial of Service Attacks', *University of Ottawa Law & Technology Journal* 2004, p. 231-261.

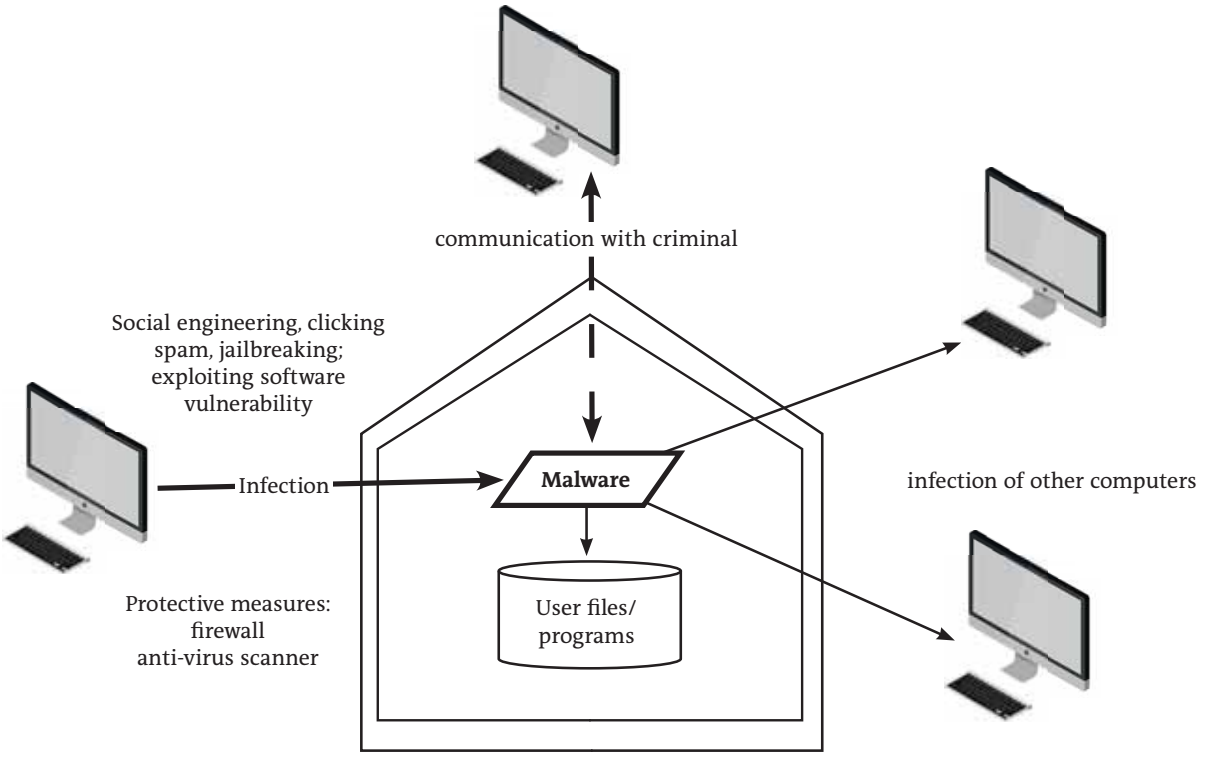
De softwareindustrie is zeer gesloten over hoe veiligheidsfouten blijven ontstaan en niet worden ontdekt

de bovengenoemde oorzaken versterken elkaar.

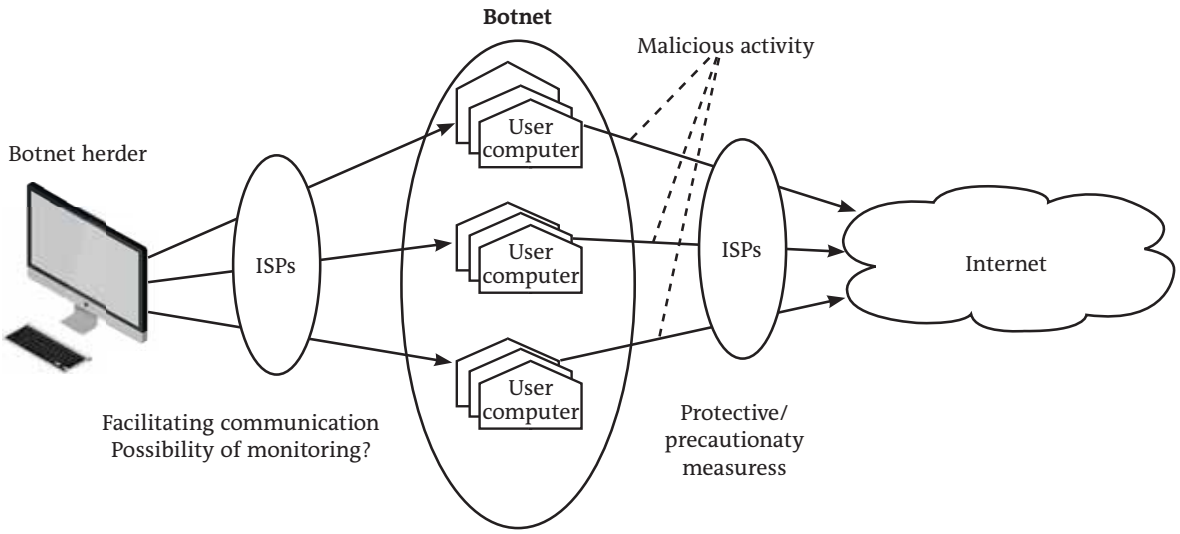
De aanwezigheid van softwarefouten behoeft toelichting.[7] Voor buitenstaanders wekt het verbazing dat bekende software van grote producenten als Microsoft en Adobe zo vaak ernstige fouten blijkt te bevatten die met spoed gerepareerd moeten worden. Praktisch gezien is het echter bijzonder moeilijk om fouten te vermijden. Software is zeer complex en omvangrijk. Daarbij komt dat veiligheidsfouten niet vanzelf naar boven komen bij het testen van software: testen zijn met name erop gericht 'of hij het doet', kortom op functionaliteit. Bovendien eist 'de markt' vooral nieuwe functionaliteit en heeft de aanwezigheid van veiligheidsfouten weinig invloed op aankoopbeslissingen, waardoor de nadruk ligt op snel publiceren van functionaliteit en softwareproducenten weinig prikkels hebben om software zonder veiligheidsfouten op de markt te brengen.[8] Dat neemt niet weg dat er in de softwareindustrie veel aandacht is voor productieverbetering, waarbij ook diverse standaarden zijn opgesteld.[9] Deze zijn evenwel veelal tamelijk abstract en helpen niet evident om daadwerkelijk fouten te voorkomen op de werkvloer.[10] Dit klemt te meer nu veel veiligheidsfouten gevolg zijn van bekende missers zoals 'buffer overflows'. Men zou denken dat in elk geval deze fouten routinematig zouden zijn te voorkomen. Toch is dit mogelijk minder eenvoudig dan het lijkt: er is een grote verscheidenheid aan ontwikkelomgevingen en programmeertalen en toepassingen, waardoor zelfs bekende typen fouten niet altijd gemakkelijk of automatisch kunnen worden herkend. De ontwikkelaar bevindt zich in de positie van de bewoner die een huis geheel ongediertevrij wil afsluiten, terwijl de misdadiger is als de muis die maar één enkel gaatje nodig heeft om binnen te komen. Inmiddels is er een schaduweconomie waar veiligheidsfouten worden 'verkocht' ten behoeve van misbruik.[11]

Ondanks alle inspanningen die tot nu toe worden ondernomen, en die op zichzelf ook wel enig positief effect hebben gehad, zijn er nog behoorlijke aantallen veiligheidsfouten aanwezig. Men kan daaruit concluderen dat de huidige inspanningen onvoldoende zijn – en het dus handiger moet worden aangepakt of meer tijd en geld aan veiligheid moet worden besteed[12] –, of dat de situatie hopeloos is. Vooralsnog lijkt het beter niet voor defaitisme te kiezen. Daarbij kunnen we ook vaststellen dat – anders dan in andere branches – de softwareindustrie zeer gesloten is over hoe veiligheidsfouten blijven ontstaan en niet worden ontdekt. Er is hierdoor geen duidelijk leerproces voor het voorkomen van fouten (zoals wel aanwezig door tuchtrechtspraak in de medische en juridische sector).

Als de computer niet goed beschermd is, kan dit leiden tot infectie met zogenaamde *malware*: kwaadaardige software, die een misdadiger de mogelijkheid geeft de computer te besturen. Men moet dit niet onderschatten: wie een onbeschermde computer aan internet koppelt, loopt het risico dat deze naar verluidt binnen vijftien minuten al is besmet met malware! Malware kan worden gebruikt om de eigenaar te bespioneren, wachtwoorden af te troggelen en geld over te maken, spam te versturen en andere computers te infecteren. Ook kan het worden gebruikt om bestanden te versleutelen, en vervolgens geld te vragen om deze weer vrij te geven: dit heet *ransomware*.



(Bron: Rapport)



Een ander gebruik van malware is dat de computer als één van vele wordt bestuurd door de misdadiger: het geheel heet dan een *botnet*. Zo'n botnet geeft controle over grote reken- en communicatiekracht.

Een botnet kan worden misbruikt om grote aantallen spam te versturen, maar ook voor een zogenaamde verstikkingsaanval (DDoS: Distributed Denial of Service). Hierbij word een website overvoerd met communicatieverzoeken waardoor deze onbereikbaar wordt voor gebruikers.

Wat valt hiertegen te doen, naast voorkomen van besmetting van individuele computers? Eén mogelijkheid is grotere inzet van bedrijven om misbruik van hun systemen te voorkomen. Hoewel van particuliere gebruikers weinig deskundigheid verwacht kan worden, kunnen bedrijven in hogere mate hun computers en netwerk bij de tijd houden en controleren op verdachte activiteit. Daarnaast kunnen bedrijven als slachtoffer van DDoS-aanvallen ook extra voorzorgen nemen om hun website robuuster te maken.

Daarnaast zijn ook internetdienstverleners (Internet Service Providers, ISP's) in een positie waarin zij technisch gezien communicatie kunnen monitoren, verdachte patronen ontdekken, geïnfecteerde computers isoleren of hinderlijk verkeer wegleiden.

Als we afzien van de daders zelf en particuliere gebruikers, zijn er dus in elk geval drie partijen die – naast wat zij al doen – nog meer inspanningen zouden kunnen leveren: softwareproducenten, bedrijven en ISP's. Wij concentreren ons hierna op de op hen rustende zorgplichten. We gaan niet zelfstandig in op de rol van ICT-dienstverleners. Hun activiteiten staan namelijk vooral in dienst van een van de drie genoemde partijen, en komen daarmee indirect via deze partijen aan de orde.

3. Zorgplichten als analytisch instrument[13]

Voor de analyse van verplichtingen van andere partijen gebruiken we het concept zorgplichten. In Nederland zijn we inmiddels gewend om te werken met zorgplichten. Dit begrip bestaat echter niet als zodanig in andere landen. Toch is het zinvol zorgplichten als analytisch instrument te gebruiken. Het benadrukt namelijk de primaire eigen verantwoordelijkheid van partijen in de samenleving, en de vooral stimulerende in plaats van regulerende rol die de overheid hierbij zou moeten spelen. Zorgplichten functioneren idealiter in een praktijk die op basis van actuele praktijkervaringen passende, contextuele normen formuleert en deze handhaaft. Het recht kan dit ondersteunen maar dient dit niet te vervangen. Ook in andere rechtsstelsels valt erkenning van dergelijke meer morele en sociale zorgnormen te lezen, ook al worden deze slechts beperkt als rechtsnormen erkend en gehandhaafd.

In deze benadering zijn de aansprakelijkheidsnormen derhalve volgend ten opzichte van de morele en sociale zorgplichten. Uitgangspunt is het vertrouwen in de eigen wens van partijen om hun zorgplichten na te leven; alleen voor ernstige tekortkomingen is ingrijpen van het recht nodig. Hierdoor krijgt de praktijk de ruimte om zelf de optimale normen te ontwikkelen. Een dergelijke praktijk krijgt ondersteuning door onderlinge communicatie, bijvoorbeeld in een beroepsgroep of sociale omgeving.

7. Zie nader R. Warner & R.H. Sloan, 'Vulnerable Software: Product-risk Norms and the Problem of Unauthorized Access', *University of Illinois Journal of Law, Technology & Policy* 2012, p. 45-94 en OECD, *Computer Viruses and Other Malicious Software. A Threat to the Internet Economy,* 2009, p. 109-122. We concentreren ons op standaardsoftware, omdat fouten daarin grootschalig misbruikt kunnen worden.

8. Warner & Sloan 2012, K.R. Pinkney, 'Putting Blame Where Blame Is Due: Software Manufacturer and Customer Liability for Security-Related Software Failure', *Albany Law Journal of Science & Technology* 2002, 13/1, p. 43-82.

9. Bijv. ISO/IEC 27001 (Information Security Management System), ISO/IEC 27034 over *secure software development*, ook ISO/IEC 27014 en ISO/IEC 27018.

10. Vergelijk P.N. Otto, 'Reasonableness Meets Requirements: Regulating Security and Privacy in Software', *Duke Law Journal* 2009, 59/2, p. 309-342.

11. C. Prins, 'Geheime handel in digitale lekken', *NJB* 2014/865, afl. 17, p. 1171.

12. Om deze reden is het ook ontoereikend om erop te wijzen dat producenten de geldende veiligheidsstandaarden moeten naleven: deze zijn kennelijk in de huidige vorm niet effectief.

13. Rapport, par. 3; T.F.E. Tjong Tjin Tai, *Zorgplichten en zorgethiek* (diss. UvA Amsterdam), 2007 en 'Zorg, privaatrecht en publiekrecht: van ondersteuning naar handhaving, en terug', *Recht der Werkelijkheid* 2010, afl. 3, p. 6-25.

4. Relevante privaatrechtelijke zorgplichten

In deze paragraaf bespreken we in vogelvlucht de positie van de drie genoemde partijen.[14] We beginnen met softwareproducenten, waarna ISP's en bedrijven aan bod komen.

4.a. Softwareproducenten

Voor de beoordeling van zorgplichten bij veiligheidsfouten in geleverde standaardsoftware zijn allereerst de gewone contractuele regels relevant. Software kan worden geleverd op basis van koop,[15] waardoor ook het conformiteitsvereiste geldt. Echter ingevolge artikel 7:17 lid 2 BW kan de overeenkomst de verwachtingen van de koper beperken, en dat gebeurt ook: software wordt meestal voetstoots verkocht,

Als de publiekrechtelijke regels activiteit verbieden kunnen we ISP's niet privaatrechtelijk verwijten dat zij weinig doen

'as is'. Het valt te verdedigen dat er niettemin een minimale verplichting is om veiligheidsfouten te vermijden. In het bijzonder ernstige, eenvoudig te voorkomen, veiligheidsfouten zouden dan toch als non-conformiteit kunnen worden aangemerkt. Dan treedt evenwel de volgende verdedigingswal in werking: de aansprakelijkheid is als regel maximaal geëxonereerd.[16] Omdat bij cybercrime meestal geen zaakschade of letselschade optreedt, en de veiligheidsfouten doorgaans niet door opzet of bewuste roekeloosheid van leidinggevenden ontstaan, houden deze exoneraties stand. In de literatuur en jurisprudentie zijn er dan ook niet of nauwelijks voorbeelden van schadevergoeding wegens veiligheidsfouten.[17]

In Amerika is de situatie niet veel anders.[18] De ALI Principles of Software Contracts (2010)[19] §3.05 gaan niet verder dan een dwingendrechtelijke 'implied warranty of no material hidden defects' waarmee de verkoper bekend was. Exoneraties zijn eveneens gebruikelijk, zij het dat deze niet lager mogen gaan dan wat redelijk is gelet op de te verwachten schade (§4.02 ALI Principles). Bijgevolg zijn softwareproducenten praktisch niet aansprakelijk. In ons onderzoek troffen we bijvoorbeeld geen voorbeelden aan van *class actions* voor software alleen.

Er is daarnaast gepleit voor productaansprakelijkheid voor software.[20] Naar positief recht is dit niet mogelijk, nu software geen roerende zaak, geen stoffelijk object is (vergelijk artikel 6:187 lid 1 BW juncto artikel 3:2 BW). Daarnaast valt te betwijfelen of zulke aansprakelijkheid wenselijk is. Productaansprakelijkheid is bedoeld voor industriële producten, terwijl software regelmatig door individuen of kleine ontwikkelaars wordt vervaardigd, en bovendien in significante mate ook gratis beschikbaar wordt gesteld (in het bijzonder Open Source Software). In de auto-industrie leidde aansprakelijkheid ertoe dat grote fabrikanten hun veiligheidsbeleid verscherpten. In de versnipperde software-industrie heeft scherpere aansprakelijkheid echter niet vanzelfsprekend dit gevolg, wat er ook toe zou kunnen leiden dat allerlei wenselijke en nuttige initiatieven als Open Source Software en kleine ontwikkelaars worden belemmerd.

Een laatste grond voor aansprakelijkheid zou kunnen zijn de gewone onrechtmatige daad: schending van de zorgvuldigheidsnorm, of naar *common law* de *tort of negligence*. Hoewel wordt gepleit voor een dergelijke tort bij aanbieding van onveilige software,[21] is dit nog geen positief recht. In Amerika lijkt geen ruimte voor een *duty of care* om veilige software aan te bieden, en bovendien kan schending van zodanige *duty* niet leiden tot vergoeding van *pure economic loss*.[22] In Nederland zijn wij wat scheutiger met zorgplichten en vergoeding van zuivere vermogensschade. Niettemin lijkt een claim door een derde niet kansrijk aangezien hij zou moeten bewijzen dat er causaal verband is tussen een concrete veiligheidsfout, en de cybercrime waar hij slachtoffer van is. Bewezen zal moeten worden dat de concrete geïnfecteerde computers betrokken waren bij de cybercrime, en dat deze met malware geïnfecteerd zijn geraakt als gevolg van die concrete veiligheidsfout. Dat laatste lijkt onmogelijk aan te tonen.

De situatie ten aanzien van vérgaande exoneraties is in de meeste landen vergelijkbaar aan wat hierboven is beschreven.[23] Opvallend daarbij is wel dat in Brazilië de stand van zaken anders is. Daar geldt sinds 1990 de Wet voor consumentenbescherming (Fundação de Proteção e Defesa do Consumidor), die consumenten (waartoe ook kleine bedrijven tegenover grote ondernemingen worden gerekend) beschermt tegen gebrekkige producten *en diensten*. Deze aansprakelijkheid kan niet worden uitgesloten (artikel 51). Voor software is dit verbod op exoneratie ook te vinden in artikel 10, §1, II van de Wet 9.609/1988 (Softwarewet). In de praktijk schijnen er echter nauwelijks procedures te zijn tegen softwareproducenten. Dit kan mogelijk worden verklaard uit het boven genoemde feit dat softwareproducenten de verwachtingen voor hun product beperken in de licentieovereenkomst: als er geen gebrek is, is er zelfs onder de Braziliaanse regelgeving geen aanspraak.

4.b. ISP's

ISP's kunnen jegens hun klanten contractuele zorgplichten hebben cybercrime tegen te gaan.[24] De expliciete verplichtingen zijn meestal beperkt, al zou een impliciete verdergaande zorg op basis van artikel 7:401 BW kunnen gelden. Echter ook hier is aansprakelijkheid meestal vérgaand uitgesloten. Wel kiezen bedrijven er regelmatig voor Service Level Agreements af te spreken, die aan het al dan niet behalen van concrete doelstellingen bonus of malus verbinden. Daarmee wordt een beperkte sanctie gekoppeld aan de achterliggende zorgplichten.

ISP's zijn ingevolge artikel 12-15 E-commercerichtlijn 2000/31, geïmplementeerd in artikel 6:196C BW, gevrijwaard voor buiten-contractuele aansprakelijkheid voorzover zij passief blijven ten opzichte van de inhoud die zij doorgeven.[25] Dit ontmoedigt een actievere houding: hoewel veel ISP's graag meehelpen cybercrime te bestrijden,[26] lopen zij juist risico op aansprakelijkheid als zij actief zoeken naar kwaadaardige inhoud of verdachte communicatie. In de U.S.A. is dit 'chilling effect'[27] reden geweest om te bepalen dat goedbedoelde pogingen om bijvoorbeeld kinderporno

te verwijderen niet leiden tot verval van de vrijwaring.[28] Een bezwaar is evenwel dat ISP's hiermee nog geen prikkel hebben om actief te worden.[29] Er gaan daarom stemmen op voor indirecte aansprakelijkheid van ISP's.[30]

Verdergaande aansprakelijkheid lijkt echter vooralsnog geen goed idee.[31] De meeste goedwillende ISP's hebben zelf belang bij bestrijden van cybercrime,[32] maar worden geconfronteerd met regelgeving die dit bemoeilijkt.[33] Het actief monitoren en blokkeren van internetverkeer botst namelijk gemakkelijk met regels inzake netneutraliteit,[34] internettoegang[35] en privacy. Deze regels kennen slechts beperkte uitzonderingen,[36] waardoor ISP's nauwelijks ruimte hebben om creatief te zoeken naar nieuwe maatregelen tegen cybercrime. Let wel: we pleiten niet tegen deze regels als zodanig, het gaat er alleen om dat in de huidige vorm er weinig ruimte wordt gelaten voor wenselijke activiteit van ISP's. Als de publiekrechtelijke regels activiteit verbieden kunnen we ISP's niet privaatrechtelijk verwijten dat zij weinig doen.

4.c. Bedrijven

Bedrijven zijn in elk geval op twee manieren in staat de eerder in dit artikel besproken vormen van cybercrime te bestrijden: door tegengaan van infecties met malware, en door het nemen van voorzorgsmaatregelen tegen DDoS-aanvallen. Zij zijn hier tot op zekere hoogte ook toe verplicht. Jegens hun eigen klanten zullen zij bescherming moeten bieden tegen DDoS-aanvallen omdat dit leidt tot onderbreking van dienstverlening. Echter opnieuw geldt hier dat de toepasselijke contracten doorgaans geen ongestoorde dienstverlening garanderen, en voorzover er sprake is van wanprestatie de schade grotendeels geëxoneereerd is.[37]

Ingeval van infecties met malware zijn er wel enige sancties. Dit komt namelijk de facto neer op een datalek dat kan leiden tot verlies van privacygevoelige gegevens. In Amerika is hiervoor het middel van *notification duties*, meldplichten, ontworpen.[38] Hoewel een meldplicht geen verdere sanctie met zich brengt,[39] heeft het wel geleid tot grotere activiteit van bedrijven om zulke inbreuken te voorkomen. Onder meer wordt op grote schaal *cyber-insurance* gezocht.[40] Verzekeraars lichten dan bedrijven door op hun veiligheidsbeleid en eisen verbetering waar nodig; bovendien kunnen zij na een inbreuk of DDoS-aanval bemiddelen voor benodigde ICT-expertise. Doordat zij tal van bedrijven zien, beschikken verzekeraars over brede kennis die kan helpen om het algehele veiligheidsniveau te verhogen. Ook in Europa worden dergelijke meldplichten ingevoerd.[41]

14. Rapport, par. 5.

15. HR 27 april 2012, *NJ* 2012/293 *(Beeldbrigade)*.

16. Vergelijk P.H. Blok (red.), *Overeenkomsten inzake informatietechnologie*, Den Haag 2010, p. 112-113 en T. Graaf & C. Stuurman, 'ICT-contracten', in: Van der Hof e.a. 2014, p. 79.

17. Hof Amsterdam 22 november 2001, *Computerrecht* 2002/2, p. 94 *(Kirche in Not vs. Cap Gemini)* betreft aansprakelijkheid voor mislukte automatisering, dat iets anders is dan aansprakelijkheid voor fouten in standaardsoftware. Ook in Amerika is er nauwelijks jurisprudentie.

18. M.L. Rustad & T.H. Koenig, 'The Tort of Negligent Enablement of Cybercrime', *Berkeley Technology Law Journal* 2005, 20/4, p. 1553-1611; J. C. Carle & H.H. Perritt, 'Civil liability on the internet', *GPSolo Magazine* 2006, 23/1, p. 44-47.

19. Deze codificeren grotendeels wat reeds volgt uit jurisprudentie en de Uniform Commercial Code.

20. R.J.J. Westerdijk, *Produktenaansprakelijkheid voor software*, Deventer 1995, M.D. Scott, 'Tort liability for vendors of insecure software: has the time finally come?', *Maryland Law Review* 2008, 67/2, p. 425-484; S.J. Childers, 'Don't stop the music: no strict products liability for embedded software', *University of Florida Journal of Law & Public Policy* 2008, 19/1, p. 125-184; S.W. Brenner, 'Toward a criminal law for cyberspace: product liability and other issues', *Pittsburgh Journal of Technology Law & Policy* 2004, 5, p. [i]-112.

21. W. Dalsen, 'Civil Remedies for invasions of privacy: a perspective on software vendors and intrusion upon seclusion', *Wisconsin Law Review* 2009, p. 1059-1092; Rustad & Koenig 2005.

22. Carle & Perritt, 2006, p. 47, voorzichtiger: Scott 2008, p. 453.

23. M. Kurer e.a. (red.) *Warranties and Disclaimers. Limitation of Liability in Consumer-Related Transactions*, London 2002.

24. L.A.R. Siemerink, *De overeenkomst van Internet Service Providers met consumenten*, Deventer: Kluwer 2007.

25. Zie bijv. HvJ 23 maart 2010, zaken C-236/08-C-238/08 *(Google Adwords)*; nader bijv. N.A.M. van Eijk e.a., *Op weg naar evenwicht: een onderzoek naar zorgplichten op het internet*, WODC, 2010.

26. Ofschoon uit onderzoek ook blijkt dat er 'rogue ISP's zijn die welbewust nalaten veiligheidsmaatregelen te treffen (OECD, *Computer Viruses and Other Malicious Software. A Threat to the Internet Economy*, 2009, p. 102).

27. Vergelijk C. Prins & M.H.M. Schellekens, 'The Chilling-Effect of Liability Law on Initiatives to Enhance the Reliability of On-line Health-Related Information', *European Journal of Health Law* 2004, 11/2, p. 201-208.

28. § 230 Communications Decency Act. Deze uitzondering geldt overigens voor de strafrechtelijke aansprakelijkheid, en geldt niet voor alle soorten inhoud. Over civiele aansprakelijkheid zie Carle & Perritt, 2006.

29. *EU study on the Legal Analysis of a Single Market for the Information Society,* 2009, p. 33, op http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=835.

30. 3J. Peterson, L. Segal, & A. Eonas, 'Global Cyber Intermediary Liability: A Legal and Cultural Strategy', *Pace Law Review* 2014, 34/2, p. 586-630, D. Lichtman & E. Posner, 'Holding Internet Service Providers Accountable', *Supreme Court Economic Review* 2006, 14, p. 221-260.

31. Cf. C. Ziniti, 'The Optimal Liability System for Online Service Providers: How Zeran v. America Online Got it right and web 2.0 proves it', *Berkeley Technology Law Journal* 2008, 23/1, p. 583-616.

32. Zoals blijkt uit diverse vrijwillige initiatieven in de branche, zie Rapport, par. 6.6.3. Ook R.J. Mann, & S.R. Belzley, 'The Promise of Internet Intermediary Liability', *William and Mary Law Review* 2005, 47/1, p. 239-307.

33. A.K. Martin & N.N.G. de Andrade, 'Battling Botnets with Digital Rights in Mind', *European Journal for Law and Technology* 2012, 3/2.

34. In Nederland art. 7.4a Telecommunicatiewet, in Brazilië art. 9 Marco Civil (Wet 12.096/2014). In Amerika heeft de FCC dit principe op 26 februari 2015 aanvaard.

35. Bijv. considerans 29 van Richtlijn 2013/40/EU, en de beslissing van het Franse Cour Constitutionnel 10 juni 2009, no. 2009-580, ook F. La Rue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, UNHRC, 2011, op www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.

36. Rapport, par. 7.4.

37. T.F.E. Tjong Tjin Tai, 'Zorgplichten van banken tegen DDoS-aanvallen', *NJB* 2013/1968, afl. 32, p. 2196-2200.

38. Rapport, par. 5.3.4, zie bijv. L. Rode, 'Data Security Breach Notification Statutes: Does Placing The Responsibility On The True Victim Increase Data Security', *Houston Law Review* 2007, 43/5, p. 1597-1634. Men ziet dit als een vorm van 'regulation through disclosure' (C.R. Sunstein, 'Information Regulation and Information Standing: Akins and Beyond', *University of Pennsylvania Law Review* 1999, 147/3, p. 613-675).

39. Al kan het helpen voor overheden om kennis op te bouwen, vergelijk F.J. Zuiderveen Borgesius, 'De meldplicht voor datalekken in de Telecommunicatiewet', *Computerrecht* 2011-4, p. 209-218.

40. Rapport, par. 6.6.2, R.M. Peters, 'So You've Been Notified, Now What? The Problem With Current Data-Breach Notification Laws', *Arizona Law Review* 2014, 56/4, p. 1171-1202.

41. Art. 4(3) Richtlijn 2002/58/EG, als herzien door art. 2 sub 4(c) Richtlijn 2009/136, en Verordening 611/2013. Het wetsvoorstel meldplicht datalekken is inmiddels door de Tweede Kamer aangenomen (zie nu *Kamerstukken I* 2014/15, 33662, A). Mogelijk wordt dit wetsvoorstel nog voor de zomer aangenomen.

Bij een zo prevalent delict kan men zich afvragen of van computergebruikers niet tenminste enige vorm van beveiliging kan worden verlangd, voordat ze zich slachtoffer van hacken zouden mogen noemen

Daarnaast hebben de slachtoffers van privacyschending ook recht op schadevergoeding, maar in de praktijk kan het lastig zijn concrete schade aan te tonen.[42] Niettemin zijn er voorbeelden van *class actions*.[43]

5. Strafrechtelijke zorgplichten?

Waar het privaatrecht al weinig expliciete of duidelijk afdwingbare zorgplichten kent voor internetaanbieders, bedrijven of softwareproducenten, valt niet te verwachten dat het strafrecht normen kent die een verantwoordelijkheid van deze partijen inhouden om cybercrime te voorkomen.

Toch zijn er wel enkele vormen van strafrechtelijke aansprakelijkheid die in de buurt komen van een zorgplicht. Ten eerste zijn er culpoze delicten, waarbij iemand bestraft kan worden aan wiens schuld een bepaald gevolg, zoals ernstig letsel, te wijten is. De computercriminaliteitswetgeving kent twee voorbeelden hiervan: culpoze gegevensbeschadiging of virusverspreiding (artikel 350b Sr) en culpoze gemeengevaarlijke computersabotage (artikel 161septies en 351bis Sr). Als aan iemands schuld te wijten is dat een computer geïnfecteerd raakt met malware, kan artikel 350b Sr van toepassing zijn, met een maximale gevangenisstraf van een maand. Volgens Stamhuis is dit alleen (mogelijk) van toepassing op beroepsmatige computergebruikers; hij geeft echter geen criteria wanneer professionele gebruikers strafbaar zullen zijn.[44] Het leerstuk van de *Garantenstellung*[45] suggereert dat personen die zich in een bijzondere positie hebben geplaatst om in te (kunnen) grijpen bij mogelijke misdaden – in ons geval vooral systeembeheerders – aan hogere eisen moeten voldoen dan gemiddelde gebruikers. Wellicht kan artikel 350b daarom worden toegepast op systeembeheerders die aanmerkelijk nalatig zijn in de computerbeveiliging in de organisatie, bijvoorbeeld als zij geen basale, goed beschikbare beveiliging installeren tegen alom bekende *bugs* in de gebruikte systemen. Het Braziliaanse recht kent een vergelijkbare figuur in de 'norma de dever de segundo grau' (tweedegraads rechtsplicht), maar die vergt naast het vermogen om succesvol in te grijpen ook enige rechtsplicht om het resultaat te voorkomen, en die is onder Braziliaans recht niet te construeren.[46] Onder Tsjechisch recht kan dat echter wel, nu een recente Cybersecurity-wet[47] duidelijke en vrij vérgaande plichten oplegt aan professionals die verantwoordelijk zijn voor kritische informatiesystemen. Aanmerkelijke nalatigheid (bijvoorbeeld bij herhaald niet ingrijpen, of niet ingrijpen na waarschuwingen) kan dan voor systeembeheerders leiden tot aansprakelijkheid voor nalatige gegevens- of systeemverstoring onder §232 TZ (Tsjechisch Wetboek van Strafrecht).[48]

Evenzo kan artikel 161septies eventueel van toepassing zijn op verwijtbaar nalatige systeembeheerders in organisaties met kritische systemen die een publiek belang dienen, zoals een ziekenhuis of elektriciteitscentrale, als bijvoorbeeld door een geïnfecteerde computer levensgevaar ontstaat (met maximum gevangenisstraf van een jaar, of twee jaren bij dodelijk gevolg). Het causale verband tussen de nalatigheid, de computerinfectie en het gevolg zal in de praktijk vaak moeilijk aan te tonen zijn, en sowieso zal de lat, voor strafrechtelijke verwijtbaarheid, hoog liggen: een systeembeheerder moet het, ten opzichte van gemiddelde personen in zijn positie, wel behoorlijk bont maken met gebrekkige beveiliging voordat een officier hiervoor zal vervolgen. En waar de lat voor professionals in een bijzondere positie al hoog ligt, zal strafrechtelijke aansprakelijkheid voor andere beroepsmatige computergebruikers, laat staan gewone eindgebruikers, niet aan de orde zijn, ook als zij de computers onder hun beheer slecht of nauwelijks beveiligen. Dat geldt ook voor softwareleveranciers, die weliswaar een zekere beroepsmatige (sociale) plicht hebben hun producten te beveiligen, maar wie computeraanvallen niet strafrechtelijk verweten kunnen worden – het causale verband tussen de nalatigheid (een *bug*) en het veroorzaakte gevolg (een door een misdadiger geïnfecteerde computer) is daarvoor veel te zwak.

Een tweede vorm van strafrechtelijk zorgplicht betreft omissiedelicten: het niet ingrijpen waar dat naar maatschappelijke maatstaven wel verwacht mag worden (bij ernstige gevolgen in situaties waarin handelen mogelijk en niet riskant is). Daarvan zijn geen voorbeelden in de computercriminaliteitsbepalingen.

Ten derde zijn er vormen van accessoire aansprakelijkheid: medeplegen en medeplichtigheid (artikel 47-48 Sr). In combinatie met voorwaardelijk opzet (de ondergrens van opzet) zou je een zekere zorgplicht kunnen construeren: iemand die bewust de aanmerkelijke kans aanvaardt dat hij gelegenheid schept voor een ander om malware te installeren, is medeplichtig aan computervredebreuk (artikel 138ab Sr) of gegevensbeschadiging (artikel 350a Sr). Maar de computerinfectie moet wel duidelijk voorzienbaar en makkelijk te voorkomen zijn, en iemand moet welbewust de aanmerkelijke kans aanvaarden dat anderen de door het beveiligingslek geschapen gelegenheid gaan misbruiken, wil er van medeplichtigheid aan computercriminaliteit met voorwaardelijk opzet sprake zijn. De lat ligt daarbij vermoedelijk niet veel lager dan in de VS, waarbij van 'aiding and abetting' alleen sprake is als de medeplichtige een *mens rea* (kwaad opzet) heeft met kennis van alle elementen van het misdrijf.[49] Vervolging voor een culpoos delict ligt dan toch eerder voor de hand, wat zoals hierboven gezegd slechts in een enkel uitzonderingssituatie het geval zal zijn.

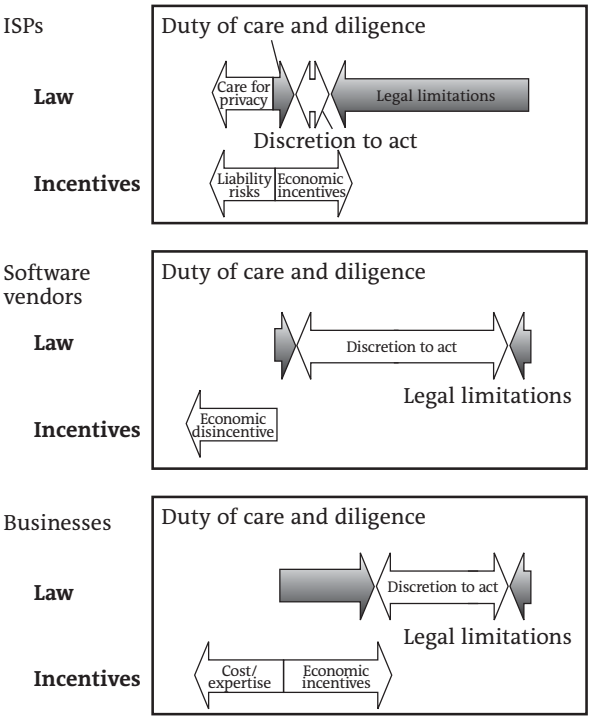
Een laatste categorie betreft een ander type potentiële zorgplicht. Het strafrecht kan ook zekere drempels

invoeren voordat mensen kunnen klagen dat zij slachtoffer van criminaliteit zijn, wat als prikkel kan dienen voor potentiële slachtoffers om zichzelf te beschermen. De Wet computercriminaliteit[50] biedt hiervan een interessant voorbeeld: bij de strafbaarstelling van computervredebreuk (artikel 138a-oud Sr) hanteerde de wetgever een beveiligingseis (hacken was alleen strafbaar wanneer enige beveiliging werd doorbroken), mede om mensen bewust te maken van het belang van computerbeveiliging.[51] Gebruikers, en met name bedrijven, zouden niet mogen klagen als hun computers werden gehackt wanneer zij niet de moeite hadden genomen tenminste enige beveiliging te treffen. Deze interessante vorm van een zorgplicht is echter in 2006 afgeschaft door de beveiligingseis te laten vervallen[52] – iets wat in de literatuur is bekritiseerd.[53] Er valt veel voor te zeggen de beveiligingseis in artikel 138ab opnieuw in te invoeren. Niet alleen kent Richtlijn 2013/40/EU in tegenstelling tot zijn voorganger een beveiligingseis voor de strafbaarstelling van computervredebreuk,[54] maar ook is hacken inmiddels het meest voorkomende delict in Nederland (meer dan fietsendiefstal en voertuigvandalisme!): 5,2% van de Nederlanders was in 2014 slachtoffer van hacken.[55] Bij een zo prevalent delict kan men zich afvragen of van computergebruikers niet tenminste enige vorm van beveiliging kan worden verlangd, voordat ze zich slachtoffer van hacken zouden mogen noemen. Materieel zou een dergelijke beveiligingseis als zorgplicht overigens niet veel uitmaken om (ernstige vormen van) cybercrime tegen te gaan, maar het zou een waardevol signaal kunnen bieden van het belang van computerbeveiliging.

6. Tussenstand

Het voorgaande leert dat in het privaatrecht en strafrecht wel enige zorgplichten tegen cybercrime bestaan, maar deze relatief beperkt zijn en nauwelijks effectief af te dwingen. In schema gebracht is de situatie als volgt. (Zie figuur hiernaast.)

ISP's willen misschien wel, en hebben economische prikkels om zodanig te handelen, maar worden tegengehouden door aansprakelijkheidsrisico's en publiekrechtelijke regels die activiteit verbieden. Softwareproducenten hebben op zichzelf een grote vrijheid om meer te doen tegen veiligheidsfouten, maar worden geconfronteerd met negatieve marktprikkels: een bedrijf dat veel zorg besteedt loopt het gevaar te laat op de markt te komen en te duur te worden. Bij bedrijven lopen de zorgplichten, vrijheid om te



handelen, en economische prikkels grotendeels in de pas, alleen kan de daadwerkelijke uitvoering soms tekort schieten door gebrek aan kennis of door een beperking in het beschikbare budget voor veiligheidsmaatregelen.

7. Mogelijkheden tot verbetering

In het politiek gevoelige speelveld van internetvrijheden, doortrokken van fundamentele principes en economische belangen, stuit iedere aanbeveling al snel op verzet. Uiteindelijk vergt het een politieke afweging om de status quo te veranderen. De hierboven beschreven regels berusten op keuzes waar enige rechtvaardiging voor te vinden is. Men kan ervoor kiezen deze regels te handhaven, en de daardoor onafwendbare aanwezigheid van cybercrime te beschouwen als een onvermijdelijk kwaad. Daartegenover staat dat men er ook voor kan kiezen bepaalde omstandigheden te wijzigen die mogelijk leiden tot het verminderen – doch niet uitroeien – van cybercrime. Wij bespreken kort een aantal mogelijkheden.[56] Deze moeten overigens veelal supra- of internationaal worden uitgevoerd om effectief te zijn.

42. Peters 2014 concludeert dat consumenten effectief weinig remedies hebben. Vergelijk D. van der Zande, 'A penny for your privacy. An analysis of the reimbursements in privacy infringement procedures', masterscriptie Tilburg 2012, op http://njb.nl/blog/import/a-penny-for-your-privacy.9681.lynkx.

43. Bijv. de Sony PSN security breach (https://psnsoesettlement.com/) en de Dropbox breach (http://dockets.justia.com/docket/california/candce/4:2011cv03092/242244).

44. E.F. Stamhuis, 'Criminal Law on Cyber Crime in the Netherlands; General Part', Verona (Italy), 28-30 november 2012, beschikbaar op www.penal.org/sites/default/files/files/RV-11.pdf, p. 21.

45. Noyon/Langemeijer-Remmelink, *Wetboek van Strafrecht* (losbladig), 'Inleiding', aant. 9.

46. Rapport, par. 5.4.4.

47. Wet nr. 181/2014 coll.

48. Rapport, par. 5.5.2.

49. *Rosemond vs. United States*, case no. 12-895, 5 maart 2014.

50. *Stb.* 1993, 33.

51. Zie B.J. Koops & Th. de Roos, 'Materieel strafrecht en ICT', in: B.J. Koops (red.), *Strafrecht en ICT*, Den Haag: Sdu 2007, p. 31.

52. *Stb.* 2006, 300.

53. Koops & De Roos 2007, p. 32, met verwijzingen.

54. Art. 3 Richtlijn 2013/40/EU, *PbEU* 14.8.2013, L218/8.

55. 5CBS, *Veiligheidsmonitor* 2014, p. 168.

56. Rapport, par. 8. Zie ook, naast de hierboven reeds genoemde literatuur, bijv. S.W. Brenner & L.L. Clarke, 'Distributed Security: A New Model of Law Enforcement', op: http://ssrn.com/abstract=845085; D.A. Barnes, 'Deworming the Internet', *Texas Law Review* 2004, 83/1, p. 279-329, OECD, *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies*, 2012; OECD, 'Proactive Policy Measures by Internet Service Providers against Botnets', OECD Digital Economy Papers, 2012, nr. 199.

We zijn in het algemeen geen voorstander van verdergaande aansprakelijkheden, behalve ingeval van aan opzet grenzende nalatigheid. Voor deze situatie bestaan echter al enkele strafrechtelijke mogelijkheden. Alleen bij grootschalig gebruikte standaardsoftware zou aansprakelijkheid wellicht een nuttig effect hebben, maar dat valt lastig af te grenzen van andere vormen van software en bovendien is het complex dit op internationaal niveau te regelen. Ook blijft dit problematisch voor Open Source Software.

Voor ISP's is het van belang dat de publiekrechtelijke regels meer uitzonderingen toelaten om internetverkeer te controleren en reguleren ten behoeve van bestrijding van cybercrime.[57] Dit moet uiteraard zorgvuldig worden afgewogen tegen belangen als privacy en netneutraliteit. Daarnaast zijn additionele prikkels zinvol, zoals een verplichting voor overheden om te selecteren op veiligheid bij aanbesteding voor ICT-diensten.[58]

Er zou een opener discussie moeten komen over oorzaken en preventiemaatregelen voor veiligheidsfouten

Voor softwareproducenten is het wenselijk een markt voor veiligheid te stimuleren, waarin er bereidheid is om te betalen voor veiligheid, zodat producenten op dat vlak gaan concurreren. Een voorbeeld is verplichte keurmerken voor het niveau van veiligheid. Aanbestedingseisen voor veilige software kunnen daarbij helpen.[59] Daarnaast zou er een opener discussie moeten komen over oorzaken en preventiemaatregelen voor veiligheidsfouten. Meldplichten of verplichte *bounty programs* (beloningen voor *bug*-vinders) kunnen hierbij helpen; een goede regeling voor 'responsible disclosure' (richtlijnen voor hackers om verantwoord veiligheidslekken bij bedrijven te melden) is eveneens belangrijk.[60] Men zou ook kunnen denken aan structureel onderzoek door de Onderzoeksraad voor Veiligheid of een vergelijkbare op te richten instantie: deze raad heeft mogelijkheden om dwingend doch anoniem, zonder sanctie van aansprakelijkheid, te onderzoeken wat oorzaken van veiligheidsgevaren zijn en aanbevelingen te doen. Professionalisering van de softwaresector in lijn met wat bij medici en juristen bestaat is theoretisch interessant doch praktisch waarschijnlijk onhaalbaar. Tot slot kan men denken aan verschillende vormen van aansprakelijkheid of recht op teruggave van onveilige software; deze mogelijkheden achten wij minder wenselijk. Het maakt een tamelijk grote inbreuk op geldende regels en heeft door de grote gevolgen mogelijk contraproductieve effecten. Het valt in dat verband op dat de strenge Braziliaanse regelgeving in feite geen effect lijkt te hebben.

Open Source Software levert daarnaast een lastig probleem op omdat daar niet altijd een duidelijke aanbieder of ontwikkelaar is, en bovendien het opleggen van strengere verplichtingen ertoe kan leiden dat dergelijke software niet langer beschikbaar wordt gesteld.[61] Gelet op het centrale belang van diverse Open Source-producten voor internet[62] is dit onwenselijk en praktisch niet haalbaar. Voor dergelijke producten zou het een mogelijkheid zijn om bedrijven te verplichten of aan te moedigen onderhoudscontracten af te sluiten:[63] daardoor komen er middelen ter beschikking om actiever op zoek te gaan naar veiligheidsfouten en deze tijdig te repareren.

Voor bedrijven lijkt het huidige regelgevend kader reeds behoorlijk op orde. Als men verdere maatregelen zou wensen, zijn denkbaar het opleggen van een indringender security audit (al dan niet als onderdeel van een accountantsrapportage), waarbij ook wordt gelet op wat bekend is van de veiligheid van de gebruikte softwareproducten.[64] Voor specifieke sectoren waar dienstverlening hoogst belangrijk is zou gedacht kunnen worden aan gefixeerde schadevergoeding.

8. Conclusie

Bestrijding van cybercrime door meer actie van diverse indirect betrokken partijen is juridisch nog tamelijk gecompliceerd, en raakt aan vragen van verantwoordelijkheid en vrijheid. Niettemin zijn er maatregelen denkbaar die enig positief effect zouden kunnen hebben. Gelet op de omvang van het probleem lijkt verdere actie door indirect betrokken partijen hoognodig. Het recht kan daarbij een belangrijke rol spelen om hen daartoe nader te stimuleren, in de vorm van afdwingbare zorgplichten, met name voor die partijen die door hun positie in het internet-speelveld goed in staat zijn om (meer) in actie te komen. •

57. Al dan niet naast een uitbreiding van de vrijwaring voor aansprakelijkheid ingeval van zulke pogingen.

58. Zie in het VK: www.cesg.gov.uk/News/Pages/Cyber-Essentials---the-new-cyber-security-standard.aspx.

59. Zie voor het VK: www.cesg.gov.uk/servicecatalogue/cyber-essentials/Pages/cyber-essentials.aspx.

60. Vgl. *Kamerstukken II* 2012/13, 26643, nrs. 264 en 342.

61. Dit geldt ook voor gratis beschikbaar gestelde sofware. Open Source Software is gratis beschikbaar doordat de broncode publiek is, zij het dat er geld gevraagd mag worden voor de gecompileerde, verpakte software.

62. Denk aan de Apache webserver of het Single Sign-On (SSO)-protocol, waar in april 2014 de Heartbleed-*bug* in werd ontdekt.

63. Er zijn al diverse dienstverleners die dergelijke diensten aanbieden.

64. Hiermee zou een prikkel kunnen ontstaan om veiliger producten te kopen, waardoor producenten weer een prikkel krijgen om hun product (nog) veiliger te maken.