Met de kennis van nu (afscheidsrede Universiteit leiden)

Schmidt, A.H.J.

Met de kennis van nu en door een rechtswetenschappelijke bril: enkele bespiegelingen over de Cyberpest

Afscheidscollege van Aernout Schmidt, als uitgesproken te Leiden op 26 maart 2010

Dames en heren,

ik begin met een halve vergelijking. Hij is afkomstig van Oliver Wendell Holmes Jr. die hem rond 1900 bij een tafelrede gebruikte. Hij luidt als volgt:

"Zoals de rups een cocon spint voor het gevleugelde wezen dat hij nooit zag maar desalniettemin worden zal, zo ..." [einde citaat]

Korter dan via dit geleende beeld kan ik u geen indruk geven van mijn wetenschappelijke basishoudig. Alles wat leeft neemt maatregelen om zich en zijn soort te doen voortbestaan. Die maatregelen moeten evenwel worden genomen met onvolledige kennis: individuen handelen ook zonder dat zij de effecten ervan op zichzelf, op hun gemeenschap en op de omgeving volledig kunnen doorzien, net zomin als zij de invloed van hun omgeving op hun handelen volledig kunnen doorzien. Voor een rups is de beschikbare kennis voornamelijk opgeslagen in zijn DNA. Voor de mens komt daar zijn cultuur bij – en zowel de wetenschapsbeoefening als het recht zijn daarvan onderdelen.

Deze basishouding leidt tot het besef dat na verloop van tijd alles eruit gaat zien alsof het een functie heeft of had. Het Franse vestingdorp *was* er om de vijand te weren, *werd* later in zijn groei beperkt door zijn eigen muren en *is* er anno 2010 nog steeds, maar nu om toeristen te behagen. Voor de wetenschap is het dan de kunst om één en ander in zijn context te beschrijven en te verklaren, en om functies van oorzaken te scheiden.

Dit perspectief is mijn vertrekpunt. De komende minuten gebruik ik om de halve vergelijking te betrekken op mijn vakgebied, informatietechnologie en recht, en om hem af te maken.

Terzijde 1 Intussen ben ik verheugd u hier te treffen bij dit afscheidscollege. Of dat wederkerig zal zijn moet worden afgewacht. Een afscheidscollege is een college, en colleges kunnen verbazend saai zijn, of onbegrijpelijk, of over iets anders gaan dan over wat uw belangstelling heeft. Bovendien is het gebruik van de term afscheidscollege misleidend, omdat ik niet echt uit de faculteit verwijn. Vanaf 22 april verzorg ik bijvoorbeeld het keuzevak Cyberspace & Cyberlaw.

Ik begin met de aankondiging van een vooralsnog denkbeeldige ramp en eindig met enkele overwegingen over of de rechtswetenschap heeft bijgedragen aan het ontstaan van die dreiging en of hij kan bijdragen aan het beteugelen ervan. U merkt het: dat wordt lachen, vanmiddag.

Goed. Ik leg u een fictieve casus voor.

De casusbeschrijving

Een maand geleden werd ik gebeld. Ik nam op en werd door een bandopname uitgenodigd om toets 1 te toetsen. Stel dat ik dat deed en dat me vervolgens door diezelfde bandopname gevraagd was een moment geduld te hebben. En stel dat gedurende de periode dat ik wachtte op de één of andere geheimzinnige wijze mijn mobiele telefoon vanuit Cyberspace is *gehackt*, en wel zodanig, dat hij daarna benut kan worden om, na een teken van buiten, SMS-berichten te zenden aan vijf geselecteerde telefoonnummers uit mijn adreslijst. En stel bovendien, dat op een vergelijkbare geheimzinnige wijze een weerzinwekkend filmpje met kinderpornografische inhoud in het geheugen van mijn telefoon is geplaatst en vervolgens is doorgezonden naar de e-mailadressen van diezelfde personen, ditmaal aangevuld met een misdaadverslaggever – dit alles zonder dat ik dat zelf merk en op een wijze die geen sporen van de *hack* achterlaat op mijn Blackberry. Misschien is het goed om deze vooralsnog fictieve gebeurtenis even te laten inwerken.

Hoe zou *u* zich voelen in mijn plaats, wanneer *'uw'* gedrag in de krant aan de kaak is gesteld en *u* door een vooringenomen Officier van Justitie na *uw* aanhouding aan de tand wordt gevoeld?

Of – erger nog – hoe zou Balkenende zich voelen wanneer dit hem overkwam, één maand vóór de verkiezingen?

Of – wellicht nog erger – hoe zouden *wij* ons voelen wanneer dit soort *hacking* op zeer grote schaal zou voorkomen? En hoe zou de maatschappelijke chaos eruit zien die daar het gevolg van zou zijn?

Laten we eens bezien welke rol is weggelegd voor het recht als instrument van rechtsbescherming voor het slachtoffer. Ik bespreek die rol bij het beschreven drama, maar dan zoals zich dat zou hebben kunnen afspelen op de denkbeeldige Blackberry van Balkenende omdat we dan vermoedelijk beter bij de les blijven.

De praktijk In Nederland is alleen al het beschikbaar hebben van kinderpornografisch materiaal strafbaar. Het verspreiden ervan is dat ook en wordt doorgaans zwaarder gestraft. De maximumstraf is voor beide delicten onlangs verhoogd tot 8 jaar. Ik ga ervan uit dat zowel het beschikbaar hebben op de Blackberry als het verspreiden via de Blackberry kan worden bewezen op basis van bewaarde telecommunicatieverkeersgegevens. Omdat er geen precedenten zijn waarin de lijsttrekker van een belangrijke politieke partij verdachte is geweest moet ik afgaan op wat de doorsnee kinderpornobezitter overkomt: een aanmerkelijke taakstraf of een bescheiden vrijheidsstraf. Op het eerste gezicht staat Balkenende er niet best voor.

Even tussendoor: in het vervolg zal ik de term *agent* regelmatig gebruiken. Ik bedoel dan computertjes of programma's die zelfstandig handelen. Balkenende's Blackberry is zo'n *agent*, en Cyberspace zit er vol mee.

Het recht Terug naar de casus. Wanneer we het relevante positieve recht nader beschouwen dringen de volgende twee vragen zich op: kan de wet zo worden gelezen dat mag worden aangenomen

1. dat *wat de Blackberry van Balkenende* deed *door Balkenende zelf* is gedaan

   en, zo ja, kan dan worden aangenomen

2. dat *wat de Blackberry van Balkenende* deed *opzettelijk* door Balkenende is gedaan.

Wanneer geen sporen van een *hack* kunnen worden gevonden en ook geen ander overtuigend tegenbewijs wordt gegeven, wordt als bewezen aangenomen dat wat de Blackberry van Balkenende deed *opzettelijk door Balkenende is gedaan.* Dit is vaste rechtspraak die ertoe leidt dat het zogenoemde '*hacker*-verweer' maar zelden gehoor vindt. Ook door een positiefrechtelijke bril zit Balkenende in de puree.

Dit is sneu. Balkenende *weet* domweg dat wat zijn Blackberry heeft gedaan niet door hemzelf is gedaan, en zeker niet opzettelijk. Hij weet niet hoe dat-wat-gebeurd-is heeft kúnnen gebeuren, maar *hij* was het niet. Hij weet dat het OM en de rechter dat-wat-echt-gebeurd-is ook niet weten. Intussen ziet hij *wél* zijn carrière door de goot wegspoelen – de Nieuwe Revu heeft er lucht van gekregen en erover gepubliceerd met beschadigende beeldcitaten. Pauw en Witteman bespreken meesmuilend de mogelijkheid dat hij onschuldig is en laten doorschemeren dat hij *hén* nog meer kan vertellen. Hoogleraren informatica passeren in de media de revue en zeggen allemaal wat anders. Maxime Verhagen staat niet alleen klaar om het lijsttrekkerschap over te nemen zodra *hij, Balkenende,* het neerlegt, maar slaagt er bovendien in de suggestie te

wekken dat Cohen achter de affaire zit. Davids zegt onvoldoende van de casus te weten om een opinie te kunnen geven, laat staan een rechtswetenschappelijk oordeel. Het zou mij niet verbazen wanneer Balkenende onder deze omstandigheden een deel van zijn vertrouwen in de Nederlandse rechtsorde verliest, omdat die hem niet beschermt, maar veroordeelt.

Beschermt waartegen? Tegen twee dingen:

1. ten eerste tegen het ten onrechte door een rechter verantwoordelijk worden gehouden voor gedrag van *agents* die niet naar de instructies van hem, Balkenende handelden

   en

2. ten tweede bescherming tegen het verlies van vertrouwen in de rechtsorde dat zou ontstaan wanneer zulks op grote schaal zou gebeuren. En *dat* dit op grote schaal kan gebeuren zal ik straks laten zien als ik iets zeg over *root kits, botnets* en *bounds checks.* Voorlopig nodig ik u uit om ook zonder nadere onderbouwing met mij mee te denken en deze dreiging als een *reële* dreiging te aanvaarden.

Ik geef u, om één en ander toch alvast een beetje aannemelijk te maken het bericht dat Microsoft mij en vele anderen op 9 maart jongstleden zond als toelichting bij een "critical update" van MS-Office in mijn vertaling*:*

> *"Deze update bevat verschillende verbeteringen om de stabiliteit en de werking te verbeteren. Hij bevat tevens verbeteringen voor kwetsbaarheden die een aanvaller gebruiken kan om de inhoud van het geheugen van uw computer te overschrijven met kwaadaardige programmatuur."* [einde citaat]

De aanhef van dit bericht klinkt bemoedigend maar verhult niet dat de meest populaire tekstverwerker ter wereld op 9 maart jongstleden nog kwetsbaarheden bevatte die kwaadwillende *agents* toestonden om de controle over mijn en uw computer over te nemen (en over de computers van alle andere gebruikers van die tekstverwerker) en er kinderporno in te plaatsen - ik noem maar een voorbeeld.

Als gezegd ontvangen we dit soort berichten met *critical updates* om de haverklap van *alle* belangrijke softwareproducenten. We hebben een situatie laten ontstaan die zich laat vergelijken met wat voorafging aan de kredietcrisis: we hebben ons op grote schaal afhankelijk gemaakt van ondoorzichtige producten van dubieuze kwaliteit, met alle risico's van dien – risico's die tegenwoordig ook wel systeemrisico's worden genoemd. En ik durf de stelling wel aan dat een *serieuze, goedgeorganiseerde aanval* aanmerkelijk sterkere repercussies hebben *kan* dan de kredietcrisis zoals we die tot nu toe kennen. Tenslotte zal de financiële sector er *zelf* ook het slachtoffer van zijn.

De Cyberpest

Deze dreiging noem ik verder de dreiging van de *Cyberpest*, als aanduiding voor een besmettelijke aandoening die onze hele maatschappelijke orde kan aantasten. Een belangrijke eigenschap van de Cyberpest is dat hij op het moment van toeslaan de bewijzen van zijn eigen oorzaken en werking verloren doet gaan of anderszins verbergt.

Ik vat samen in twee stellingen:

Stelling 1 *Met de kennis van nu ondervinden slachtoffers van Cyberpestaanvallen nauwelijks rechtsbescherming van het positieve recht.*

Onmiddellijk in samenhang hiermee is mijn tweede stelling:

Stelling 2 *Met de kennis van nu kunnen kwaadwillenden in de informatiemaatschappij een Cyberpestepidemie veroorzaken zonder veel risico te worden opgespoord en vervolgd.*

Het Cyberpestrisico lijkt ook in een ander opzicht op wat de kredietcrisis heeft laten zien: wie ondoorzichtige financiële producten koopt zit niet alléén in het schuitje dat de resulterende maatschappelijke storm moet doorstaan, wie ze niet kocht vaart toch mee. Wie ondoorzichtige ICT-producten koopt is niet de enige die zal moeten leven in de erop volgende Cyberpestchaos, dat moeten we allemaal.

Mede daarom denken we over onze rechtsorde niet alleen als instrument voor individuele rechtsbescherming maar ook als een patroon dat zich ontwikkelt gedurende de tijd, een patroon dat we zelf maken en dat aan onze *maatschappelijke* orde stabiliteit kan bezorgen, ook in tijden waarin de omstandigheden zodanig wijzigen dat aanpassingen noodzakelijk zijn.

We zijn met dat laatste beeld vertrouwd. We herkennen het in de rol die we het recht toekennen bij zo uiteenlopende bedreigingen als – ik noem slechts twee andere voorbeelden – de opwarming van de aarde en de ineenstorting van de financiële sector. Ik geef een paar overeenkomsten met de Cyberpestdreiging:

1. Ook op die bedreigingen lijkt het positieve recht geen vat te hebben.
2. Ook bij die bedreigingen verwachten we dat het recht of aanpassingen ervan ertoe zullen bijdragen ze effectief tegemoet te treden.
3. Ook bij die bedreigingen gaat het om grensoverschrijdende belangen waarop ons internationale publiekrecht maar geen werkelijke greep op lijkt te krijgen.
4. Ook bij die bedreigingen zijn het de regelmatigheden in menselijk gedrag die ertoe leiden dat de omgeving zozeer verandert dat *onze rechtsorde* er niet veel langer of maar heel moeizaam in zal kunnen overleven.

Deze vier overeenkomsten geven aan dat bij de Cyberpestdreiging – net als bij de kredietcrisis en bij de opwarming van de aarde – sprake is van wat tegenwoordig wel een systeemdreiging wordt genoemd.

In termen van systeemdreigingen heeft de maatschappelijke orde een deels hiërarchische en deels spaghetti-achtige structuur die is opgebouwd uit hele collecties van regelgeleide gemeenschappen welke door actoren worden gevormd en in stand gehouden. Ik acht het bijzonder aannemelijk dat het vormen en overleven van regelgeleide gemeenschappen een proces is dat zinvol kan worden begrepen als een evolutionair proces dat deels wordt ontworpen door de deelnemende actoren en deels het 'blinde' resultaat is van wat de cultuur en de natuur aan de deelnemende actoren ingeeft om te doen tegen de voorliggende interne en externe bedreigingen, bedreigingen die ze doorgaans maar gedeeltelijk kunnen overzien.

De vraag doet zich dan voor wat we bij de Cyberpest als systeemdreiging mogen verwachten van de rechtswetenschap. Mijn derde stelling geeft het antwoord:

Stelling 3 *Bij systeemdreigingen als de Cyberpest mogen we van de rechtswetenschap verwachten dat die eraan bijdraagt dat de noodzakelijke juridische en politieke keuzen* zo *goed mogelijk geïnformeerd kunnen worden gemaakt – dat wil zeggen, met de kennis van nu.*

Ik moet u bekennen dat niet elke collega het op dit punt met mij eens is, vooral niet, wanneer ik probeer aan te

geven dat wij – voorzover het gaat om de gevolgen voor de rechtsorde – de kennis uit andere disciplines mede in onze overwegingen moeten betrekken. Waar ieder het over eens is, is dat we eraan moeten bijdragen dat onze juridische uitspraken zodanig worden geformuleerd, dat de rechtsorde *intern* coherent blijft. *Mijn* stelling aanvaardt dat de rechtswetenschap ook een taak heeft waar het gaat om de *externe* coherentie van de rechtsorde waarover wordt nagedacht.

Het rechtswetenschappelijk zo goed mogelijk informeren bij het onder ogen zien van kritische bedreigingen is helaas niet erg goed ontwikkeld. De rechtswetenschap pleegt traditioneel terug te kijken in de moraalgeschiedenis of omhoog naar de Allerhoogste(n), en een literaire benadering te verkiezen boven een empirische. Dat is, meen ik, de reden dat het empirische onderzoek naar valkuilen van deze soort door ons, juristen, in wetenschappelijke zin is prijsgegeven en – als vanzelfsprekend – door andere wetenschappen wordt veroverd. Ik denk dat we, hier en nu, veel meer kennis beschikbaar hebben die ons kan bijstaan de dreiging van een Cyberpestepidemie te domesticeren dan juristen zich plegen te realiseren. *Wij* komen zelden verder dan het verdedigen van opinies bij sprekende casusposities. (Ik denk dan bijvoorbeeld aan de *informer case* die Hart en Fuller nog verder uit elkaar dreef.)

Maar inmiddels speuren ecologen, economen, sociologen en psychologen het bedoelde gebied theoretisch en empirisch af, en maken aanmerkelijke vorderingen – zowel inhoudelijk als methodisch. Dat de term *moral hazard* een *bij uitstek economische* term is zou ons in dit verband te denken kunnen geven.

Jammer genoeg blijken *zij* doorgaans even mager geïnformeerd over de resultaten van de rechtswetenschap als wij over hún resultaten.

Kortom: ik denk dat een Cyberpestepidemie een reële dreiging is. Ik denk ook dat de Cyberpestdreiging de externe coherentie van onze rechtsorde kan aantasten en om een multidisciplinaire aanpak vraagt, en dat daarbij de analyse door een rechtswetenschappelijke bril niet kan worden gemist. Het ware wenselijk wanneer daarbij over en weer wordt geprofiteerd van de bevindingen van verschillende disciplines die hun eigen bril hebben opgezet en opgezet houden – ook wanneer ze de resultaten van elkaars werk op hun bruikbaarheid beoordelen.

Om op de betekenis hiervan bij de Cyberpestdreiging als systeemdeiging enig zicht te krijgen ga ik in het resterende deel van mijn betoog op zoek naar een antwoord op de vraag wat de rechtswetenschap zou kunnen bijdragen aan het domesticeren van de Cyberpestdreiging en hoe de rechtswetenschap daarbij niet-juridische wetenschapsresultaten kan gebruiken.

Misschien is het goed om dan eerst *door de bril van de informatica* iets te zeggen over de meest gangbare kwetsbaarheden die aan de werking van *agents* in Cyberspace kleven. *Agents* zijn kwetsbaar, of vertonen *vulnerabilities* zoals het spraakgebruik is geworden. Met name alle thans beschikbare systeemprogrammatuur (zoals MS-Windows, en de varianten van Linux en van Unix) vertonen ze. Er is een hele wapenwedloop ontstaan tussen wie die *vulnerabilities* willen misbruiken en wie de gaten willen dichten. Bij die wapenwedloop

ligt het initiatief bij de kwaadwillenden. En aan hun kant, de kant die Hirshleifer als "the dark side of the force" aanduidt is men vergaand gevorderd met het maken van wat *root kits* worden genoemd.

Dit zijn om het kort door de bocht te zeggen programma's die zich nestelen in de kernels van systeemprogrammatuur en die zich niet of nauwelijks laten opsporen. *Root kits* zijn kwartiermakers voor besturing op afstand, voor het uitvoeren van *malware* op commando. Ze zijn zo diep in uw systeem ingedrongen dat ze tot alles bevoegd zijn. Als uw systeem besmet is geraakt wordt het een 'bot' genoemd, omdat het zich vanuit uw gezichtspunt af en toe als een robot gedraagt en iets anders doet dan u verwacht. Bots kunnen in netwerken samenwerken en hun doorgaans bedenkelijke activiteiten heel snel door het botnet van de één aan de ander overdragen. Ze worden er ook steeds behendiger in om de sporen van hun aanwezigheid te wissen en te verbergen. Kortom, ze zijn moeilijk te vinden en te verwijderen. Ze worden vooralsnog vooral gebruikt voor het verspreiden van *spam*, maar er zijn geen technische belemmeringen die hen zouden verhinderen om welk programma dan ook uit te voeren. Met het voortschrijden van de techniek – met name van die spectaculaire producten die tot de artificiële intelligentie worden gerekend – vind ik dat verontrustend.

Het Trendrapport 2009 van GovCert geeft daar voeding aan. Het doet bijvoorbeeld verslag van het oprollen van het 'Sneker botnet,' dat meer dan 100.000 computers onder commando had. Niet door het op te sporen en te vernietigen, maar door een – vergeef me de uitdrukking – snotneus uit Sneek op te pakken toen die het wilde verkopen aan iemand die om andere redenen in de gaten werd gehouden.

Een ironische indruk van de massale onzekerheid die een Cyberpestaanval kan veroorzaken volgde uit de manier waarop de KLPD het Sneker botnet heeft proberen te helpen opruimen: het zond een e-mailbericht aan de getroffenen waarin instructies over hoe de *root kit* kon worden verwijderd. Ik ben benieuwd hoe u zou reageren op een dergelijk bericht. Ik zou het vermoedelijk als gevaarlijk hebben beschouwd en het niet eens hebben geopend.

Dit was het slechte nieuws. Nu over naar het goede.

De beschreven kwetsbaarheden hadden kunnen worden vookómen. Het gaat om een betrekkelijk eenvoudige technische maatregel waaraan *agents* zich zouden moeten houden. We moeten ons daarbij realiseren dat de greep naar de macht door een *agent* over een andere *agent* alleen kan verlopen via code (dat wil zeggen via programma-onderdelen die worden uitgevoerd). Een goedwillend programma is gevoelig voor misbruik wanneer het data in een buffer kopiëert zonder te verifiëren of de weg te schrijven hoeveelheid past in de ruimte die is bestemd voor ontvangst. Wanneer over de grens van die ruimte wordt weggeschreven, kan informatie worden geïnjecteerd op een plaats die later gaat worden uitgevoerd als ware het een programma. Wanneer een kwaadwillende agent van deze eigenschap – die *buffer overflow vulnerability* wordt genoemd – gebruik maakt kan deze de zeggenschap over de goedwillende computer overnemen en een *root kit* installeren. Een eenvoudige en tegelijkertijd effectieve tegenmaatregel is om onmiddellijk voorafgaand aan het wegschrijven van data naar een buffer na te gaan of die informatie in de ervoor gereserveerde ruimte past. Die voorzorg wordt een *bounds check* genoemd.

Dit is geen nieuw idee: in zijn Turing Award Lecture van 1980 – dertig jaar geleden! – zei Hoare er, in mijn vertaling, het volgende over:

> *In elke andere tak van techniek zou het niet in acht nemen van dergelijke elementaire voorzorgen al lang in strijd met het recht zijn geweest.* [einde citaat]

Het is opmerkelijk dat de observatie van Hoare als een elementaire voorzorg tegen het maken van programmeerfouten is bedoeld, geformuleerd in een tijd dat het web er nog helemaal niet was. En dat die voorzorg, achteraf bezien ook bescherming zou hebben geboden tegen de belangrijkste internetkwetsbaarheden van nu.

Eén en ander neemt niet weg dat tot op de dag van vandaag de hierbedoelde elementaire zorgvuldigheid op grote schaal in de wind wordt geslagen bij het inrichten van programmatuur. En het enkele feit dat de marktleidende systeemprogrammatuur, database managementsystemen, *office suites* en *portable document format handlers* niet deze meest voor de hand liggende bescherming bieden dwingt ons onder ogen te zien dat wij, als gebruikers, er weinig anders aan kunnen doen dan een keuze maken: ofwel het deelnemen aan de informatiemaatschappij beëindigen, ofwel het risico aanvaarden. Bij de huidige stand van techniek kunnen

we vaststellen dat de risico's bestaan en toenemen – ook waar het gaat om geregisseerd misbruik op grote schaal – terwijl de lapmiddelen die thans in zwang raken geen aanvaardbare vorm van soulaas bieden.

Ik vat opnieuw samen in een stelling:

Stelling 4 *Het in acht nemen van informaticakennis van vóór 1980 had de dreiging van de Cyberpest kunnen voorkomen.*

We moeten ons dan afvragen of de rechtswetenschap van de waarschuwing van Hoare op de hoogte had moeten zijn en adequate maatregelen had moeten adviseren.

Stel nu, dat we onze beslissers, de rechters en de politici, door een rechtswetenschappelijke bril zo goed mogelijk willen informeren over de valkuilen die ze kunnen verwachten bij het inzetten van juridische middelen ter bestrijding van de Cyberpest. Ik moet dan eerst even waarschuwen dat de bril van de rechtswetenschap een multifocale bril is. Er zijn twee afstanden waarop kan worden scherp gesteld. Ik noem ze de twee provincies van de rechtswetenschap:

1. De positivistische provincie, hier gaat het om de interpretatie van geldend recht in het licht van gedrag – dit is waar de rechtswetenschap zich onderscheidt van andere wetenschappen, waar zij excelleert en waar zij de interne coherentie van de rechtsorde mee helpt bewaken;

2. De natuurrechtprovincie. Deze provincie van de rechtswetenschap is om veel redenen verdacht, maar komt steevast naar voren wanneer de rechtsorde zelf in moeilijkheden raakt. Ik vermoed dat de rechtswetenschap het scherpstellen op deze afstand zoveel mogelijk tracht te vermijden, hetgeen zou kunnen meebrengen dat we *er niet goed in zijn* en dat hier nog veel te leren valt. Maar dit is ook de provincie waar we een bijdrage kunnen leveren aan de bewaking van de externe coherentie van onze rechtsorde. De stellingname van Van Walsum in de Irak-discussie dat er omstandigheden kunnen zijn die rechtvaardigen om van het volkenrecht af te wijken hoort in deze provincie thuis, net zoals de tweede volzin van ons Plakkaat van Verlatinghe uit 1581 die het regime van Philips de tweede als onaanvaardbaar afwijst. Ik denk dat we deze provincie van de rechtswetenschap in de informatiemaatschappij nogal eens nodig hebben en dat hij het beste kan worden omgedoopt. Het gaat dan om de rechtswetenschappelijke begeleiding van wat ik met een verwijzing naar Scheffer kritische veranderingen van de maatschappelijke orde zou noemen. Reële, revolutionaire veranderingen dus, die ook vanuit de rechtswetenschap eerder om een empirisch-analytisch instrumentarium vragen dan om de metafysische aanpak die nu vooral in zwang lijkt te zijn. Inderdaad, ik doel op het fascinerende instrumentarium zoals dat wordt gebruikt door evolutionair georiënteerde ecologen, economen,

sociologen en psychologen.

Ik nodig u nu uit om met mij door deze bifocale bril te kijken naar de Cyberpestdreiging.

Remedies van het positieve recht

Door de positivistisch geslepen lens ligt het voor de hand na te gaan of er mogelijkheden zijn geweest om iets meer te bereiken langs de lijnen van de gevaarzetting en/of zorgplicht uit het aansprakelijkheidsrecht, en naar de met de maatschappelijke ontwikkelingen meebewegende interpreties van begrippen als *de verkeersopvatting en de risico-aansprakelijkheid uit het civiele* recht, en het voorwaardelijk opzet uit het strafrecht. Uiteindelijk is de gedachte niet absurd dat het openzetten van een kelderluik of het marginaal markeren van een bussluis verwantschap vertonen met het verspreiden van systeemprogrammatuur die kwetsbaar is voor aanvallen van *agents* die *root kits* installeren via *buffer overflow vulnerabilities*. En ook kan men zich afvragen of het verspreiden van dergelijke producten niet kan worden gelijk gesteld met het welbewust nemen van een aanmerkelijk risico. Bij mijn weten is er evenwel geen rechtspraak die deze invalshoek omhelst. In de ICT-praktijk kan dan ook geen traditie worden ontwaard als in de auto-industrie. Wanneer een brandstoftank bij auto-ongelukken bovengemiddeld in brand vliegt of wanneer een gaspedaal een enkele keer blijft hangen wordt de autofabrikant voor eventueel volgende schade aangesproken en zorgt hij er voor om de oorzaken onmiddellijk weg te nemen. Maar wanneer systeemprogrammatuur infectie met Cyberpest toelaat is de schade voor rekening van het slachtoffer – de leverancier gaat in de praktijk doorgaans vrijuit en de veroorzaker is doorgaans onvindbaar.

Ik denk dat dit in beginsel anders kan en anders had gekund – ook met het recht van nu. Ik vat dit op als een teken van kracht van ons positieve recht, al wordt aan dat teken afbreuk gedaan door gebrek aan toepassing. Maar dat is geen kwestie die door de focus van het positieve recht zichtbaar wordt.

Die kwestie wordt wél zichtbaar door de lens die zich richt op kritische veranderingen van de maatschappelijke orde. Daar is het *niet* gebruiken van positiefrechtelijke instrumenten een *alarmsignaal* op zichzelf. Alsdan moeten verklaringen worden gezocht, en moeten relevante verklaringen uit bijvoorbeeld de economie en de sociale wetenschappen niet worden geschuwd.

Het individuele slachtoffer van een *root kit* infectie, bijvoorbeeld, ondervindt doorgaans – zolang het doel zich beperkt tot het verzenden van *spam* – beperkte hinder of schade van die infectie, meestal merkt hij het niet eens. Dat inmiddels meer dan 90% van de bandbreedte die voor e-mails wordt gebruikt wordt geconsumeerd door *spam* leidt ook niet tot problemen die ergens anders als urgent worden ervaren. De gebruikte capaciteit wordt betaald via de abonnementen van de gebruikers, en de service providers die de capaciteit in- en verkopen zijn gebaat bij een zo hoog mogelijke omzet. Onze telecommunicatiewaakhond, de OPTA, zou aanmerkelijk meer en effectiever tegen *spam* kunnen optreden en daarmee tegen botnets, maar ziet andere kwesties kennelijk als dringender. Met andere woorden, en anders dan waar het gaat over het uitwisselen van door auteursrechten beschermd materiaal, er is eigenlijk niemand die het de moeite waard vindt om te investeren in toezicht of in het voorbereiden en doorzetten van individuele, relatief

kleine en tegelijkertijd buitengewoon moeilijke en onzekere schadeclaims.

Laat ik nog een kort beeld schetsen over hoe de Cyberpestdeiging in onze informatiemaatschappij heeft kunnen postvatten aan de hand van enkele mijns inziens wél relevante, maar niet juridische inzichten die ik domweg in een lijstje opsom. Per inzicht noem ik een handvat voor rechtswetenschappelijke betekenisgeving.

1. Het eerste is sociaalwetenschappelijk van aard en roept het inzicht in herinnering dat wij, en met name regelgevers, de maakbaarheid der dingen plegen te overschatten. Het is daarmee van belang voor de wetgever.

2. Het tweede komt uit de informatica en stelt dat een programmeur zich dient te houden aan de regels van structured programming, waartoe het uitvoeren van bounds check behoort. Juridisch zou dit betekenis kunnen hebben voor de interpretatie van wat we van een zorgvuldige en ter zake kundige programmeur mogen verwachten. Dit inzicht kan worden uitgebreid met een reeks verwante inzichten die ik hier niet noem omdat ze technisch van aard zijn.

3. Het derde inzicht komt uit de economie en zegt dat kennisasymmetrieën (zoals die plegen te bestaan tussen opdrachtgevers, makers en gebruikers van programmatuur) een gevaar kunnen opleveren voor het

vertrouwen tussen partijen en zo een markt kunnen doen instorten. De economie doet hier doorgaans een beroep op effectieve rechtsbescherming bij asymmetrische ad-hoc transacties.

4. Het vierde komt ook uit de economie en zegt dat kennisasymmetrieën (zoals die plegen te bestaan tussen opdrachtgevers, makers en gebruikers van programmatuur) ook een gevaar opleveren voor de overlevingskansen van een bedrijf of organisatie wanneer de benodigde kennis zo zeldzaam is dat er geen markt voor is, terwijl die kennis niet binnen het bedrijf kan worden belegd. De economie doet hier opnieuw een beroep op effectieve rechtsbescherming, ditmaal bij asymmetrische duurcontracten.

5. Het vijfde inzicht komt opnieuw van de economen en zegt dat het prijsmechanisme van de markt niet goed werkt wanneer de voorwaarden daarvoor niet zijn vervuld. De economie doet hier opnieuw een beroep op het recht, waar het recht die voorwaarden zou kunnen scheppen. Hierbij wordt meestal gedacht aan het mededingingsrecht.

   Intussen is de markt met zijn prijsmechanisme in actie gekomen en zien we in de laatste jaren een ontwikkeling in de richting van intermediairs die ons vanuit een centrale plek beveiligde diensten aanbieden. *Softare as a Service* wordt dat genoemd. Meestal zijn aan het gebruik ervan beperkingen verbonden. Deze universiteit, bijvoorbeeld, maakt gebruik van Citrix

en verbiedt de medewerkers om zelf software te installeren. De daaraan verbonden bezwaren worden door economen *moral hazards* genoemd.

6. Het zesde is opnieuw economisch van aard en waarschuwt tegen het ontstaan van een situatie waarin dienstverleners wel concurreren, maar daarbij gebruik blijven maken van een ingeburgerde vorm van marktfalen omdat ze er individueel geen baat bij hebben het algemene probleem aan te pakken. Bijvoorbeeld wanneer ze een bedrijfsmodel hebben dat afhankelijk is van het voortbestaan van de eerder beschreven vulnerabilities. Bij intermediairs is dat vaak het geval. Juridisch komen we hier opnieuw in de buurt van het mededingingsrecht maar ook hier lijkt de maatschappelijke werkelijkheid een evenwicht te hebben gezocht dat een marktfalen inhoudt maar dat niet direct met het mededingingsrecht lijkt te kunnen worden aangepakt.

   Er is een hele industrie ontstaan die er voordeel bij heeft dat de Cyberpestdreiging in stand blijft. Het is in dit verband misschien nuttig om als laatste nog een inzicht te noemen dat hierbij een rol kan spelen.

7. Het zevende inzicht is opnieuw economisch van aard en beveelt aan te voorkomen dat een situatie ontstaat waarin het bijzonder moeilijk is om een gekozen oplossing door een andere te vervangen. Economen

spreken hier van *pad-afhankelijkheid* die tot het vasthouden aan eenmaal gemaakte keuzen kan dwingen. Ook hier is voor het recht op het eerste gezicht weinig ruimte. Het probleem van pad-afhankelijkheid is, dat ook vanuit de vraagzijde de motivering ontbreekt om aanbieders naar andere en betere oplossingen te doen zoeken. Mogelijk kan hier bestuursrechtelijk een aanzet worden gegeven via het aanbestedingsrecht door de overheid, als grootafnemer, een inkoopbeleid te laten voeren dat het vermijden van pad-afhankelijkheden serieus neemt.

Ik houd ermee op. Ik heb inmiddels 1 relevant inzicht uit de sociale wetenschap, 2 uit de informatica en 4 uit de economie genoemd en zou zo nog wel even kunnen doorgaan. Ik heb voorts tegelijkertijd geprobeerd een eerste indruk te geven van hoe naar die externe inzichten kan worden gekeken door een rechtswetenschappelijke bril.

U begrijpt dat het vinden van een goedgefundeerd advies over hoe de Cyberpestdreiging met juridische middelen tegemoet kan worden getreden geen sinecure is.

Er is nu geen tijd meer om verder te zoeken naar juridische oplossingen voor de Cyberpestdreiging, althans niet in dit college. Ik kan – concluderend – nog wel aangeven waar ik een uitweg verwacht. Eén van de belangrijkste stoorzenders voor een natuurlijke oplossing van veel problemen is het bestaan van

kennisasymmetrieën tussen partijen die iets met elkaar moeten. Dit probleem treedt niet alleen op in de informatica tussen opdrachtgevers en makers. Het doet zich ook voor op de markt, en niet alleen die voor tweedehand auto's. Het treedt naar voren bij vrijwel elke aanbesteding. Het speelt ook wel eens in de rechtspraak. En het doet zich in wederkerige mate voor wanneer verschillende disciplines moeten samenwerken. De meest effectieve, algemene en goed-gefundeerde aanpak van het kennisasymmetrieprobleem zie ik in de methoden van requirements engineering die in de informaticadiscipline zijn ontwikkeld als antwoord op de software crisis van de jaren 70. Ik heb de laatste jaren gemerkt dat de werkwijze die daar voor het formuleren van stelsels van vereisten is ontstaan effectief kan worden vertaald naar een methode die zulke vereisten door een rechtswetenschappelijke bril formuleert. Ik heb ook gemerkt dat deze benadering vruchten draagt in de aanbestedingspraktijk, met name waar technische en functionele specificaties moeten worden beoordeeld. Corvers en ik publiceerden daar vorig jaar nog over. Van der Klaauw en ik gebruiken die aanpak bij onze adviezen en Schmidt jr. zal er bij Croon Davidovich ook aan moeten geloven. Voorlopig zullen we er nog wel even werk aan hebben.

Intussen brengt het opschrijven van dit college me op de inmiddels voor de hand liggende gedachte dat diezelfde aanpak ook wel eens vruchtbaar zou kunnen worden toegepast ten behoeve van het overbruggen van de kennisasymmetrieën die naar hun aard behoren bij interdisciplinaire samenwerking. Iets voor nader onderzoek, lijkt me.

Ik rond af. Voor het formuleren van effectieve juridische instrumenten die waken tegen het uitbreken van een

Cyberpestepidemie is aanmerkelijk meer nodig dan de reflexmatige reactie zoals die in ons huidige politieke klimaat zou kunnen opkomen en die zou aandringen op een direct wettelijk verbod om *agents* die nalaten *bounds checks* uit te voeren in het verkeer te brengen. Zo'n verbod zou hetzelfde gezag kunnen hebben als een wettelijk voorschrift om je oog geopend te houden als de dokter er een medicijn in prutst.

Een rechtsorde kent ook reflexen die zich weinig *kunnen* aantrekken van bepaalde regels. Het formuleren van voorschriften kent nu eenmaal valkuilen van alle mogelijke aard. Kennis daarover bestaat in alle mogelijke disciplines. Voor zover de valkuilen zijn onderzocht en beschreven vanuit andere disciplines kan en moet met die kennis rekening worden gehouden, ook door een rechtswetenschappelijke bril. Ik acht de vraag naar welke resultaten dat zijn en hoe er mee te rekenen een belangrijke vraag en neem mij niet alleen voor daar verder onderzoek naar te doen maar ook om de bevindingen ervan over te dragen in het keuzevak Cyberspace en Cyberlaw zolang ik het mag blijven geven. Zoals de rups een cocon spint voor het gevleugelde wezen dat hij nooit zag maar desalniettemin worden zal, zo spint de rechtswetenschap *regelstelsels* voor een maatschappelijke orde die *zij* nooit zag maar desniettemin mede voortbrengt en bewonen moet. Het ware wenselijk dat dit goed geïnformeerd gebeurde, met de kennis van nu. Ook wanneer die orde een kritische verandering doormaakt. Ik heb gezegd.

A.H.J. Schmidt. Tekst als uitgesproken op 26 maart 2010. Voetnoten en referenties volgen in de meer uitgewerkte 'officiële' uitgave.