Sjoerd Rienstra
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
s.w.rienstra@tue.nl

Berry Schoenmakers
Faculteit Wiskunde & Informatica
Technische Universiteit Eindhoven
l.a.m.schoenmakers@tue.nl

Interview Ronald Prins

Zeerecht voor internet

Cybercriminaliteit en cyberoorlog beginnen serieus te worden. Het is echter voor de gemiddelde burger of bestuurder zo onvoorstelbaar en abstract, dat het nog steeds mogelijk is voor een geniale hacker in de Oekraïne om via servers in Australië en Nederland een botnet in de Verenigde Staten op te zetten dat de gegevens van honderdduizenden creditcards en bankrekeningen weet te vangen, met alle gevolgen van dien. Landen gaan zich hier meer en meer tegen verdedigen maar krijgen te maken met ongekende juridische problemen. Van wie is internet? Data in de cloud, waar staan die juridisch, en waar wordt dan de digitale diefstal gepleegd? Tijd voor een gesprek met onze nationale cybercrimefighter Ronald Prins van Fox-IT (Delft). Sjoerd Rienstra en Berry Schoenmakers van de TU/e zochten hem op. Prins is een voorstander van een zeerecht ('cloudrecht') voor cyberspace, waarbij landen het recht hebben om terug te hacken als nationale belangen via internet worden aangevallen. Niet alle juristen en politici zijn al zover.

Hoe ben je als wiskundige hierin terechtgekomen?

"Ik ben in 1995 afgestudeerd als wiskundige en ik vond cryptografie en hacken het allerleukst. Mijn vrouw werkte bij de digitale afdeling van het Nationaal Forensisch Instituut (NFI), en die hoorde dat een van de thema's die daar speelden, de angst was voor de criminele cryptografie. Dus dat criminelen van cryptografische technieken gebruik zouden maken om zichzelf te beschermen. Ze hadden mensen nodig die daar weerstand tegen konden bieden, en dat was ik dan. Dat heb ik vijf jaar gedaan, en dat had in de praktijk niets met wiskunde te maken. Dat ging gewoon met brute kracht: heel snel heel veel wachtwoorden testen, of in het hoofd van de crimineel kruipen en denken wat voor wachtwoord zou hij hierbij gebruikt hebben. Die van zijn telefoon kon je zo uitlezen, en dat was misschien hetzelfde als van zijn spread sheet. Het was meer een beetje 'streetwise clever' zijn — van hoe kom ik bij informatie — dan daadwerkelijk wiskunde inzetten.

Toen ben ik met mijn huidige compagnon, die ook bij het NFI werkte, met Fox-IT begonnen. De wiskundige rode draad die er nog doorheen loopt, is dat we in 2003 een gedeelte van de activiteiten van Philips Crypto hebben overgenomen. Philips Crypto bouwde de producten voor de bescherming van de Nederlandse staatsgeheimen, maar bestaat niet meer. Daardoor bedrijven we nu nog steeds wel wat cryptografie, maar eigenlijk maar weinig. Algoritmes, die we aangeleverd krijgen, stoppen we in de systemen met iets van sleutelmanagement eromheen. We vinden dat soort dingen hier niet uit. Je moet wel goed zijn en er verstand van hebben om dat veilig te kunnen implementeren. Je moet de wiskunde zelf lekker bij de universiteiten laten en niet te veel in de bedrijven, denk ik, maar je moet wel wiskundigen hebben die snappen hoe er mee om te gaan en op veilige manier toe te passen. Je wil niet weten hoeveel succes ik bij het NFI gehad heb, simpelweg doordat de prachtigste protocollen verschrikkelijk slecht geïmplementeerd waren, waardoor ik dingen kon openbreken die nooit open hadden moeten kunnen."

"Er hoeft maar één vent te zijn die snel kan factoriseren en de hele wereld valt uit elkaar."

Waar lag je wiskundige voorkeur?

"Ik had tijdens mijn studie snel affiniteit met discrete wiskunde, omdat het duidelijk was dat daar ook de crypto vandaan kwam. Wat ik zo spectaculair mooi vind aan cryptografie is dat het wiskunde is in de meest zuivere vorm die onmiddellijk en direct een toepassing heeft. Bij andere wiskundige technieken zit daar vaak zo'n fysische laag omheen. Het is daarmee het mooiste vakgebied in de wetenschap dat er is! Er zijn weinig vakgebieden waar je zo diep kunt gaan in pure theorie, die onmiddellijk ook weer terugkomt in je telefoon.

Ondanks vaak slechte implementatie, is de wiskunde in de cryptografie wel degelijk het probleem, en daar zijn we ook doodsbang voor. Je kan op de universiteit het verschil maken tussen veiligheid vandaag en onveiligheid morgen. Er proberen nu veel Chinezen factorisatiemethoden uit te vinden. Er hoeft maar één vent te zijn die snel kan factoriseren en de hele wereld valt uit elkaar. Ga maar een ander vakgebied aanwijzen waar dat ook zo is. En niemand kan nu nog zeggen dat dat nooit zal gebeuren.

Ik vraag wel eens bij de lunch, om de jongens hier wakker te houden, het volgende. Stel, je kan snel gehele getallen factoriseren. Wat ga je dan doen? Als je hard gaat roepen dat je het kan en iemand daagt je uit en je bewijst dat je het kan, dan heb je goede kans dat je morgen dood bent. Dus dat is niet de beste manier. Misschien moet je online anoniem bekend maken dat je het kan en het dan verkopen, maar dan ga je daarna alsnog dood, denk ik! Het is een soort wiskundig analogon van de atoombom in de Tweede Wereldoorlog. Anderzijds, dat soort grote uitvindingen wordt op verschillende plaatsen in de wereld tegelijk gedaan omdat 'de tijd er rijp voor is'. Wetenschappers praten met elkaar, en soms is het stellen of identificeren van het probleem al genoeg. Ik denk daarom dat publiek maken toch de beste optie is om de

Foto: Sjoerd Rienstra

wereldvrede te handhaven. Ook al betekent het misschien dat iemand met alle satellieten in de wereld kan gaan spelen en atoombommen kan laten afgaan. Je weet het in ieder geval en je zult hard gaan werken om er wat aan te doen."

Fox-IT

Hoeveel wiskundigen werken hier?

"Ik denk een groepje van een man of zeven à acht afgestudeerd wiskundigen. Natuurkundigen ook zoiets. Informatici zijn de grootste groep. In totaal werken hier 170 mensen. Hiervan vormt de helft, rond de 85 mensen, de nerds. Een derde zijn de academici, de rest hbo-ers, en een paar gepromoveerden. Als het om de techniek gaat zijn het academici, en verder jongens die echt goed kunnen hacken. Dat gaat niet parallel. Er zijn weinig hackers die van de TU afkomen. Hacken is vaak gewoonweg boerenslimheid. Het is iets waar je veel uren in moet maken. Als je het een half jaar niet meer doet, kan je het niet meer. Hackers, dat is bijzonder volk. Dat zijn jongens die met een normale studie moeite hebben."

Hoe vind je ze?

"Vaak kom je ze online tegen. Tijdens onderzoeken zitten ze ook ergens rond te neuzen. Zo hebben we er een paar gevonden. Die zijn zelfstandig en zitten onderzoek te doen omdat ze het leuk vinden, en die halen we hier naartoe. Maar we ontwikkelen zelf ook software, en sollicitant-programmeurs laten we dan allerlei testjes doen. De Nederlandse kampioenschappen programmeren zijn geweest en wij hadden het beste bedrijventeam. We hadden ook een hoop individuele deelnemers. De puzzeltjes daarvan leggen we weer neer bij degenen die hier komen solliciteren. Bijvoorbeeld het probleem van het analyseren van grote datastromen. Stel, de politie zet een tap op iemand, en er komt allemaal data uit, dan kun je software gaan schrijven om te analyseren wat er allemaal staat, maar dat moet je wel heel erg slim implementeren, anders werkt het uiteindelijk alleen op je thuislijntje maar niet meer daarbuiten. Daar moet je echte programmeerhelden voor hebben die dat efficiënt kunnen. Dus dan zit het meer in de verwerking van bulk dan in de dataminingtrucs."

Doen jullie nog wetenschappelijk onderzoek?

"Waar we een beetje wetenschappelijk onderzoek aan doen, is het detecteren van anomalieën op netwerken. Dus van hackersgedrag dat een afwijking zou moeten zijn van normaal gedrag op een netwerk. We kijken hoe je dat moet modelleren en willen er dan iets voor bouwen dat ook werkt.

"Hacken is vaak gewoonweg boerenslimheid."

Wij kijken daar anders naar dan de gewone wetenschap. Daar ging dat zo. De overheid wil dat er iets gebeurt op cybergebied. De wetenschappers denken dan: 'O dat is mooi, we moeten hackers gaan detecteren', en pakken alle literatuur die er is en gaan gecompliceerde algoritmes nog verder uitwerken en heuristiek ontwikkelen. Daarop wordt zwaar geïnvesteerd. Dan komen ze terug met iets dat best goed werkt op een dun lijntje maar niet op een heel dikke lijn [met een grote datastroom]. En dan denk ik: wat zonde is het dat ze niet gekeken hebben naar hoe ver de industrie eigenlijk is. Er wordt vanuit de wetenschap aangenomen dat er dingen al lang gedaan en getest zijn, terwijl dat niet zo is. En je merkt dan dat waar wij het beste mee scoren bij het detecteren van hackers, de heel pragmatische oplossingen zijn, waar je veel meer mee kunt doen dan wat nu in de prak-

NOS-Teletekstpagina van 10 april 2013

tijk gebeurt. Dat vind ik een bijzonder gat tussen werkelijkheid en wetenschap. De werkelijkheid denkt dat ze de wetenschap nodig heeft om oplossingen te implementeren en de wetenschap denkt: dat zal wel al lang gedaan zijn want dat is zo triviaal. Die gaat met haar studie beginnen op een punt waar wij nog lang niet zijn. Daar zit een gat tussen en dat is eigenlijk waar nu vooral de winst zit."

Cybercriminaliteit

Hoe treedt de Nederlandse overheid op?

"Laat ik zeggen dat ik blij ben met iemand als Jeanine Hennis-Plasschaert als minister van Defensie. Zij leefde als Europarlementariër al in die internetwereld. Ze heeft cybergevoel, ik denk dat dat goed is. Ook goed is minister Ivo Opstelten, die weliswaar zelf niet zo digitaal is, maar wel goed luistert."

Wat doet men verder?

"Als ik nu kijk hoe de Nederlandse overheid bezig is met de cyberproblematiek, dan is er een Cyber Security Raad (CSR) geïnstalleerd. Die staat dus boven het Nationaal Cyber Security Centrum (NCSC). De Raad bestaat uit veertien leden: de Nationaal Coördinator Terrorismebestrijding, vertegenwoordigers van KLPD, AIVD, Defensie, EZ en het College van PG's, vijf vertegenwoordigers van industrie en drie wetenschappers. Die moeten de regering adviseren, en oplossingen bedenken voor de dreiging waar we voor staan. Maar de gedachte dat de oplossing bij de wetenschap vandaan moet komen gaat er bij mij niet in. Crypto kan nog wel wat leuke dingen doen in het verbeteren van de privacy, maar voor de rest komt de wetenschap niet verder dan beschrijven van wat er gebeurt."

Maar hoe zorg je dan dat de burger veilig met internet omgaat?

"Het echte probleem is wellicht psychologisch, maar ik weet niet of het de wetenschap is die daar in gaat helpen. Wat ik waardevoller zou vinden is het gat waar ik het net over had. Er zijn wat welbekende en eenvoudige dingen die je kunt doen om het internet veiliger te maken, maar dan blijkt gewoon dat die niet gedaan worden. En dan gaat het er dus meer om hoe we dat gat opvullen. Dus zorgen dat wat we al lang weten ook gebeurt, zoals een firewall neerzetten, aanzetten en de goede configuratie instellen. Dat is helemaal geen wetenschappelijk probleem, dat is gewoon een keer logisch nadenken.

"De gedachte dat de oplossing bij de wetenschap vandaan moet komen gaat er bij mij niet in."

Ik vind de analogie wel aardig dat je op de autosnelweg niet harder mag rijden dan 120 km/u. Je kunt niet zomaar iets uitvinden waardoor dat vanzelf gebeurt. Je zou kunnen zorgen dat de auto's niet harder kunnen, maar ook dat is te hacken. Op zijn best kun je het gedrag van de mensen beïnvloeden, bijvoorbeeld met strepen op de weg waardoor je denkt dat je harder rijdt dan je rijdt.

Het probleem lost zich deels op doordat internet gewoon wordt. De mensen die nu aan de knoppen zitten zijn wat ouder en zijn nog zonder internet opgegroeid. Straks als onze kinderen aan de macht zijn zal het al beter gaan. Je ziet het aan die overheidsprogramma's: er moeten 40.000 politiemensen opgeleid worden, zodat ze een beetje snappen dat als je een huiszoeking doet je ook de usbsticks meeneemt. Hebben ze net die cursus af dan zijn het opeens micro-SD-kaartjes. Zo moet je continu die mensen opleiden. Maar onze kinderen die leven er gewoon mee en die hoef je niet uit te leggen wat je met een huiszoeking moet meenemen. Dat kost dus twee of drie generaties, en dat is het irritante van de revolutie die nu plaatsvindt. De vraag is of we de tijd hebben totdat de mensen die wel begrijpen hoe je met internet om moet gaan, aan de knoppen zitten."

Is het NCSC een soort Fox-IT?

"Nee, was dat maar zo. Het Centrum, onder de Raad, heeft heel wat rollen. Het is een publiek-private samenwerking met ambtenaren naast bedrijven, maar het gaat nog niet heel hard. De gedachte is dat naast de overheid ook bedrijven die slachtoffer zijn erbij moeten zitten. Dat zijn wij dus niet. Wij zijn gewoon leverancier. Het idee is dat overheid en bedrijven hetzelfde doel hebben en dan samen kunnen optrekken. Jammer genoeg heeft het NCSC meer de rol van expertisecentrum dan wat ik hoopte, namelijk de rol van digitale brandweer. Ze kunnen ook niet uitrukken of optreden. Ze geven adviezen, die ook nog eens niet dwingend zijn, bijvoorbeeld aan gemeentes. Ze zetten dan op hun website dat, op het moment dat je gehackt wordt, het handig is om poort 555 dicht te zetten. Ze mailen dat ook rond en hopen dan dat mensen die aangesloten zijn dat opvolgen.

Wat ik mis is de ambitie om de optredende rol te willen spelen. Als je kijkt hoe Nederland veilig blijft, dan hebben we een leger, een politie, een inlichtingendienst en een brandweer, allemaal instanties die een bepaalde rol hebben. Daarvan heb je in het cyberdomein ook de equivalenten nodig. We hebben een cyberinlichtingendienst bij de AIVD en de MIVD, we hebben een cyberleger bij defensie, we hebben een cyberpolitie, maar we hebben geen cyberbrandweer. *Wij* hebben eigenlijk die brandweerrol, de keren dat wij optreden. Dan gaan we met dertig man naar een organisatie die gehackt is en waarvoor het van het grootste belang is dat ze zo snel mogelijk weer verder kunnen. Vaak is het de verstorende werking die de meeste gevolgen heeft op je continuïteit. Of er dan nog een boef achter

zit die je wel of niet kunt pakken, is eigenlijk voor de getroffen organisatie niet haar primaire zorg. Ik denk dat er daarom ook een rol is voor de overheid om hier iets in te doen. Tot nu toe is de houding, ook vanuit het Centrum, dat het de verantwoordelijkheid is van het bedrijf zelf. Maar ik vind dat niet terecht, want ik heb ook geen eigen brandweer in dit pand zitten voor als er eens brand uitbreekt. Het Centrum (niet de Raad, die vergadert maar een paar keer per jaar) zou dat moeten kunnen doen. Daar zitten wel vier of vijf mensen die je achter een toetsenbord kunt zetten, en die ik ook hier zo zou kunnen plaatsen."

Cyberoorlog

Is de volgende oorlog een digitale?

"Er is wel eens gezegd dat de volgende oorlog een digitale oorlog zal zijn, maar dat is wat overdreven. In een oorlog wil je een land veroveren, en dat zal met alleen een internetoorlog niet lukken. Maar je kan wel een land verschrikkelijk verpesten. Het eerste wat je dan zou doen is zorgen dat niemand meer kan pinnen. Als je drie dagen niet kan pinnen krijg je een bankrun. Maar dat werkt ook maar een dag, want iedereen gaat cash halen en dan is dat ook op. Dan kun je niet meer naar Albert Heijn en kunnen we geen benzine meer tanken. Een land is een puinhoop als je drie dagen lang dat weet uit te zetten. Dat is gewoon te doen, en daarom denk ik, dat als we ooit conflicten krijgen, dat zal gebeuren.

Je ziet ook dat cyber het allemaal op zijn kant lijkt te zetten; je kunt helemaal niet meer denken in termen van leger en politie. Nu kan ons geldsysteem uitgezet worden door een jochie van 16 of 18 op een zolderkamertje, dat net zo ontwrichtend bezig is als een vreemde staat die ons binnenvalt en waarvoor het gepast zou zijn als een leger daarop reageert. Maar het leger zal zeggen dat het geen oorlog is en komt dus niet in actie. Ze zijn er overigens ook de komende vijf jaar nog niet klaar voor. De politie, aan de andere kant, gaat opsporen. Die gaat heel zorgvuldig te werk en zal, in plaats van zo snel mogelijk te handhaven, zorgen dat het juridische proces zorgvuldig verloopt. Dat is verkeerd vakjesdenken. De meest pragmatische oplossing is om het allemaal één te maken, zoals in de Angelsaksische landen. In Amerika wordt de grootste cyberinlichtingendienst ter wereld, de NSA, ingezet om banken te beschermen. Dat is een heel gevoelig onderwerp. Gaan we nu inlichtingendiensten inzetten om banken te beschermen? Is het hun doel om heel internet af te snuffelen om te zien dat een Chinees bezig is om de beurskoersen aan te passen? Toevallig zit daar wel de expertise. Maar met welke bevoegdheden doen ze dat dan? Die asymmetrie die erin zit, dat een paar idioten ontwrichtend voor een heel land kunnen zijn, maakt dat we niet meer in de oude vakjes kunnen denken voor wat we moeten inzetten als een land bedreigd wordt."

Zijn er voorbeelden van hoe het fout ging?

"Je moet oppassen dat je geen *self-fulfilling prophecy* creëert. Zoals dat jongetje van 16, die op Pastebin, het kanaal waar hackers alles op publiceren, had gezegd dat hij KPN, Ziggo en UPC ging platleggen, omdat hij niet blij was dat zij The Pirate Bay blokkeerden. We hadden dat bericht opgepikt, een week voordat het in de krant stond. Na interne analyse concludeerden we dat het een mannetje was waarvoor we geen paniek gaan zaaien. Wat doet het Cybercentrum? Die doen een persbericht uit dat ze op die zaterdag met dubbele sterkte klaarzitten. Tot dan had nog niemand van deze oproep gehoord. Maar gooi je er een persbericht uit dan kan er van alles gebeuren. Hier spelen natuurlijk politieke belangen mee. Stel dat je het, als Centrum, verkeerd inschat en er gebeurt wel wat, dan moet er misschien een minister aftreden.

Het is vergelijkbaar met hoe in de Verenigde Staten op WikiLeaks is gereageerd. Die Assange zou nooit zo 'beroemd' zijn geworden. Webservers zijn net kakkerlakken. Als je er één uit de lucht haalt, krijg je er tien terug. De Amerikaanse overheid heeft het daar duidelijk ook niet goed begrepen. Het is vaak risicomijdend gedrag. Je moet misschien accepteren dat je soms een inbraak hebt. Op de snelweg wordt het ook geaccepteerd dat er soms een ongeluk gebeurt. Ik mis in de digitale wereld de natuurlijke aanmoediging om te streven naar veiligheid, die je wel hebt in de luchtvaart."

Foto: Rijksoverheid

Cloudrecht

Hoe zit dat nu met dat zeerecht voor internet?

"De juristen die de wetten moeten maken lopen hopeloos achter. Die zeggen dat zo'n zeerecht voor internet helemaal niet kan. Uiteraard moeten we dat eerst op VN-niveau regelen, zoals de mariniers bij Somalië. De discussie zou over de inhoud moeten gaan. Als ik zeg dat er nu een computer geld staat weg te halen van Nederlanders en dat we daar iets tegen moeten doen, dan weten de juristen het ook niet. Wat er volgens mij aan de hand is, is dat er een groep mensen is die alleen maar denken in complottheorieën. Dat de overheid voortdurend bezig is om zoveel mogelijk gegevens van mensen te verzamelen, alleen maar om de grote boze overheid te zijn en om controle te krijgen over de burgers.

"Wat ik mis is de ambitie om de optredende rol te willen spelen."

De gedachte alleen al dat de overheid in iedere computer zou willen meekijken, alsof die politiemensen niets beters te doen hebben!"

Zijn de bestaande juridische begrippen wel toepasbaar?

"Ik praat graag in analogieën, en soms gaan die mis. Juristen hebben daar moeite mee. Een computer staat fysiek in dit land, dus daar kan ik bij, maar de analogie gaat mis dat de fysieke plaats iets zou uitmaken of je rechtsgrond hebt. Je wilt dat de overheid op het internet de rol heeft van de wijkagent die rondrijdt op zijn fiets en een beetje rondkijkt. Op internet vinden we dat eng want we zien die politieagent niet. Cyberspace is wat dat betreft niet symmetrisch. Je kan niet terugkijken. Hoe zie ik nou dat die politieman op mijn computer kijkt, of op die website zit mee te kijken? Als hij door een winkelcentrum patrouilleert dan zie je dat wel. Daar zit volgens mij bij een hoop mensen de angst. Dat de overheid dingen doet die we niet zien. En dat wordt steeds groter, omdat die overheid ook niet zo handig uitlegt

wat ze nu precies doet. Ze is ontzettend weinig transparant op het moment dat het gaat om privacy-inbreuken bij burgers. De discussie tussen voormalig Tweede Kamerlid Arjan El Fassed van GroenLinks en staatssecretaris Fred Teeven over het opvragen van het aantal keren dat de politie Google en Hotmail gebeld heeft om van iemand de inhoud van zijn mailbox te krijgen is kenmerkend. El Fassed wil daar gewoon een gevoel bij krijgen: is elke Nederlander een keer aan de beurt geweest, of is het maar, zeg, twintig keer gebeurd? En Teeven zegt dan: 'Daar maak ik een staatsgeheim van want het zou schadelijk zijn als je weet hoe vaak we dat doen.' Daar is geen enkel goed argument voor want het gebeurt maar tien tot vijfentwintig keer per jaar. En dan gaat het om van huis weggelopen meisjes van 14, die twee weken lang zoek zijn. Dan willen we allemaal dat de politie aan Facebook vraagt wat zo'n meisje de laatste twee weken op Facebook heeft gedaan. Leeft ze nog eigenlijk? Het zijn dat soort vragen. Dat kan Teeven prima uitleggen."

Je kunt instanties als overheid en banken toch niet onbeperkte vrijheid geven?

"Banken en overheid hebben toegang tot veel privé-informatie, maar er is een verschil. Het zijn allebei enge organen, maar ik vind de overheid dan enger omdat we die veel ruimte geven om bepaalde dingen te doen die de rest van de burgers niet mogen. En daar moet dan heel goed toezicht op zijn. Als je bijvoorbeeld in de inlichtingenwereld kijkt, dan hebben we daar een commissie van toezicht op de AIVD. Dat is een aparte groep mensen die verder geen belangen hebben, maar wel alle recht om bij de AIVD binnen te lopen en te kijken wat die allemaal doet.

"Webservers zijn net kakkerlakken. Als je er één uit de lucht haalt, krijg je er tien terug."

Als die dan iemand afluistert, is dan netjes het democratische proces doorlopen zoals we dat in onze democratie met elkaar hebben afgesproken? Dus daar vindt heel veel toezicht plaats. Bij de politie wordt het toezicht door de rechterlijke macht uitgeoefend. Vooraf, voor een aantal bijzondere bevoegdheden kunnen worden ingezet, moet de rechter dat goedkeuren. En bij de zitting gebeurt dat nog eens. Daar kijkt de rechter nog een keer of de rechten van de verdachte niet zijn geschonden. Dus daar vinden veel *checks and balances* plaats. Het hangt dan uiteindelijk wel af van rechters. Ik verwacht dat er een bevoegdheid komt dat de politie in Nederland moet kunnen hacken en daar zullen dan ook diezelfde waarborgen ingebouwd zitten, namelijk dat een rechter van tevoren goedkeuring moet geven.

Ik vraag me af of een rechter wel kan overzien wat het betekent dat hij daar goedkeuring voor geeft. We moeten daar goed naar kijken. Het is een heel gevoelig onderwerp, om in te kunnen breken in computers van andere mensen die misschien niet eens in Nederland zitten, maar die een delict in Nederland gepleegd hebben. Ik zou graag zien dat daar een gelaagdheid in zit, waarbij de rechter stap voor stap zegt wat mag. Stel, er is een digitale bankroof gaande. Dan zegt de rechter dat je mag gaan terughacken totdat je weet in welk land de computers staan van de hacker. En kom daarna maar terug. En mocht het dan in Duitsland zijn, dan gaan we gewoon op de ouderwetse manier verder. We bellen de Duitse politie op en zeggen: 'Daar staat een computer waar we last van hebben en we moeten wat doen.' En als de Duitse politie dan zegt: 'Doe het maar lekker zelf, dan kost het ons ook geen tijd', dan is het ook goed. Maar die getraptheid is best complex voor een rechter om te begrijpen. Ik vraag me af of je het daar moet leggen. Ik zou me ook kunnen voorstellen dat de politie een commissie van wijze mannen instelt die er wel verstand van hebben, en die je consulteert voordat je een aanvraag doet."

Bestaat internet juridisch wel?

"Je hebt inderdaad het probleem dat je niet weet waar internet juridisch onder valt. Je zal daarom wel naar een vorm van zeerecht moeten gaan, misschien te noemen cloudrecht. Stel je voor dat je data opslaat met een RAID 5-opslagarchitectuur, dus verdeeld over, zeg, vijf computers, waarvan je er maar vier hoeft te kunnen lezen om je data te reconstrueren. Als die vijf computers in vijf verschillende landen staan, en in geen van die computers kun je de data apart lezen, waar staan je gegevens dan? Daar is niets meer van te zeggen. Je zult het moeten definiëren op de manier waarop de gebruiker er naar kijkt. Dus als de gebruiker in Nederland is, dan staat de data in Nederland. Als je wilt, kun je er nog een kwantummechanische metafoor in zien: totdat je een meting doet, kun je ook niet zeggen waar een deeltje is. Dat is dan ook 'overal'. Hier zitten overigens nog meer haken en ogen aan: kun je iemand veroordelen voor het bezit van kinderporno, als dit op telkens iedere harddisk opgeslagen is als ongecorreleerde bitjes?"

Internationaal

Jullie zitten ook in andere landen. Waarom is dat?

"Wij zitten hier, maar kunnen via internet overal bij. We zitten nog met vestigingen in Engeland en in Aruba, maar dat gaan we allemaal stoppen. We zitten op Aruba omdat daar toevallig een bank verschrikkelijk gehackt was, maar je hebt geen eigen lokale entiteit meer nodig om je werk te kunnen doen."

Zeerecht

Het internationale zeerecht omvat een groot aantal verdragen die in de afgelopen eeuwen tot stand zijn gekomen. Wijzigingen en aanvullingen komen sinds de Tweede Wereldoorlog doorgaans tot stand onder de koepel van de Verenigde Naties. Meer dan een halve eeuw is er internationaal geredetwist over de vraag wie de zeggenschap heeft over welk stuk zee. Met het VN-verdrag van 1982 is aan de strijd om de zee een voorlopig einde gekomen. Dit verdrag verdeelt de zee in diverse zones zoals de twaalfmijlszone, de uitgebreide zone, de exclusieve economische zone, de visserijzone en de milieuzone. De twaalfmijlszone is het gebied dat een kuststaat tot zijn territoriale zee mag rekenen. In het VN-gedrag staat het volgende over de rechten van kuststaten op hun territoriale zeeën:

Artikel 25. Rechten van bescherming van de kuststaat
1. De kuststaat kan binnen zijn territoriale zee de maatregelen nemen die nodig zijn om een doorvaart die niet onschuldig is, te voorkomen.
3. De kuststaat kan, zonder rechtens of in feite onderscheid te maken tussen schepen van vreemde nationaliteit, in bepaalde gebieden van zijn territoriale zee de uitoefening van het recht van onschuldige doorvaart van vreemde schepen tijdelijk opschorten, indien die opschorting noodzakelijk is voor de bescherming van zijn veiligheid, met inbegrip van wapenoefeningen. Een zodanige opschorting wordt slechts van kracht nadat zij op behoorlijke wijze is bekendgemaakt.

Bronnen: ecomare.nl en wetten.overheid.nl