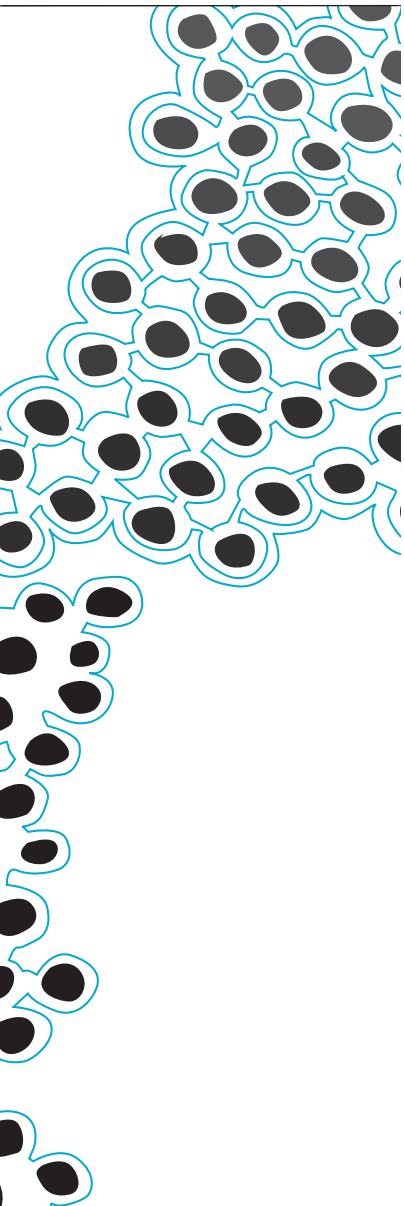
**AFSCHEIDSREDE**
16 APRIL 2021



# KANSEN EN BEDREIGINGEN IN DE VERBONDEN WERELD

**PROFESSOR PIETER HARTEL**

UNIVERSITY OF TWENTE.

PROF. DR. PIETER HARTEL

# AFSCHEIDSREDE

# KANSEN EN BEDREIGINGEN IN DE VERBONDEN WERELD

DOOR DE COVID-19 PANDEMIE IS DEZE REDE NIET UITGESPROKEN.

UNIVERSITY OF TWENTE.

**COLOFON**
Prof. dr.  Pieter Hartel



april 2021



DAMES EN HEREN,
IK WIL U GRAAG MEENEMEN OP MIJN REIS DOOR 50 JAAR GESCHIEDENIS VAN DE INFORMATICA. ZOALS ELKE NIEUWE TECHNOLOGIE HEEFT OOK DE INFORMATICA NIEUWE KANSEN EN BEDREIGINGEN OPGELEVERD EN IK WIL PROBEREN DAAR DE BALANS VAN OP TE MAKEN.

# 1971

Als ik in 1970 Informatica had kunnen studeren was ik dat waarschijnlijk wel gaan doen, maar die studierichting bestond toen nog niet. Ik vond Natuurkunde ook leuk en omdat mijn vrienden aan de Vrije Universiteit in Amsterdam gingen studeren deed ik dat ook. In die tijd was de computer nog geen gemeengoed maar de meeste universiteiten hadden er al wel een. In mijn tweede studiejaar kon ik leren programmeren, en dat leek mij erg leuk. Een van de eerste programmeer opdrachten die wij kregen was het vinden van een oplossing voor de torens van Hanoi. Op de Wikipedia wordt het als volgt uitgelegd:

De Torens van Hanoi is een spel met een aantal schijven. Het spel bestaat uit een plankje met daarop drie stokjes. Bij aanvang van het spel is op een van de stokjes een kegelvormige toren geplaatst van schijven met een gat in het midden. De schijven hebben verschillende diameters, in toenemende grootte. Ze zijn zo geplaatst dat de kleinste schijf bovenop en de grootste onderop ligt.
Het doel van het spel is om de complete toren van schijven te verplaatsen naar een ander stokje, waarbij de volgende regels in acht genomen dienen te worden:

- Er mag slechts 1 schijf tegelijk worden verplaatst.
- Nooit mag een grotere schijf op een kleinere rusten.

Laten we de drie stokjes een kleur geven. De stapel staat op de rode stok en moet naar de groene stok. De derde stok is oranje.
Er is een hele elegante recursieve oplossing voor de torens van

Hanoi. Het idee is dat je het probleem voor N schijfjes kan oplossen als je aanneemt dat je het probleem met een schijfje minder, dus met N-1 schijfjes al hebt opgelost. Dan ziet de oplossing er zo uit: Verplaats N schijven van rood naar groen in drie stappen:

- Verplaats N-1 schijven van rood naar oranje
- Verplaats 1 schijf van rood naar groen
- Verplaats N-1 schijven van oranje naar groen.

In de oplossing wordt twee keer de recursie gebruikt, in de eerste en de laatste stap.

Het was een lastig practicum maar ik had wel de smaak van het programmeren te pakken gekregen. Het leuke van programmeren is dat je onmiddellijk antwoord krijgt van de computer op wat je doet. Als je programma werkt krijg je daar een kick van, en als het niet werkt dan ga je net zo lang zoeken tot je het probleem gevonden hebt.

# 1974

Tijdens mijn studietijd tijd waren er een aantal pioniers in Amsterdam die graag een studie richting Informatica wilden oprichten. Andy Tanenbaum was een van die pioniers. Hij werkte aan de Vrije Universiteit waar ik aan het studeren was. Hij heeft me laten zien hoe leuk de informatica is. Andy was rond 1974 bezig met het schrijven van zijn eerste boek over computerorganisatie, en mijn medestudenten en ik waren zijn proefkonijnen. Wij kregen college uit conceptversies van diverse hoofdstukken. Die hoofdstukken werden natuurlijk niet getypt maar op ponsbandjes gezet, en afgedrukt op de Flexowriter. Toen die ponsbandjes niet meer nodig waren heb ik nog heel lang de plastic doosjes waar ze in zaten gebruikt om schroefjes in te bewaren.

Ik ben op een gegeven ogenblik overgestapt van de natuurkunde naar de wiskunde omdat ik dan meer bijvakken Informatica in mijn programma kon opnemen. Andy was mijn afstudeerdocent en ik heb van hem een 10 gekregen voor mijn afstudeerwerk, daar was ik natuurlijk apetrots op.



# 1978

Voor mijn eerste voltijdse baan ben ik naar Geneve verhuisd waar ik bij Europese centrum voor kern onderzoek (CERN) als systeemprogrammeur aan de slag mocht. Dat was een fantastische ervaring want er was heel veel internationale samenwerking in de hoge-energiefysica, en men had niet alleen computers maar die waren ook met elkaar verbonden via netwerken. Die netwerken waren nog lang zo snel niet als nu maar je kon er al leuke dingen mee doen, zoals email versturen. Het World Wide Web kwam natuurlijk ook van CERN, maar dat was lang nadat ik weg was.

Bij CERN ben ik Bob Hertzberger, mijn tweede leermeester tegengekomen. Ik had toen nog niet het idee dat ik weer terug zou willen naar de Universiteit, maar Bob zag wel wat in mij omdat hij, net als Andy, een van de pioniers was die de Informatica in Amsterdam van de grond wilden krijgen. Bob was op zoek naar mensen die hem daarbij zouden kunnen helpen.

# 1981

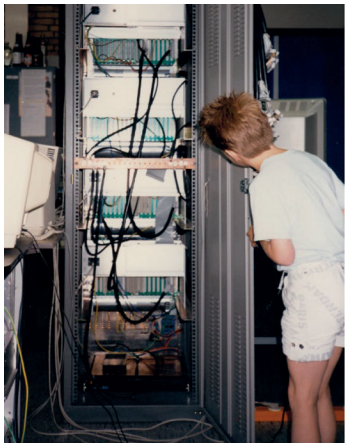
In 1981 ben ik als wetenschappelijk medewerker begonnen bij de Universiteit van Amsterdam om mee te helpen de studie informatica op te bouwen. Ik was verantwoordelijk voor de twee computers van de vakgroep, dat waren VAX 11-750 machines van Digital Equipment, met natuurlijk Unix als besturingssysteem.

Mijn eerste onderwijstaak was het organiseren van het practicum van het vak computerorganisatie terwijl Bob Hertzberger de colleges gaf. We gebruikten er natuurlijk het boek van Andy bij, waarvan ikzelf een van de proefkonijnen was geweest. Op het gebied van didactiek moest ik nog veel leren. De eerste opdracht die de studenten van mij als kersverse docent kregen was natuurlijk de torens van Hanoi. Maar niet in Algol-60, maar in machinecode. Dat is echt een stuk moeilijker, en je kan er best wat uitleg van je docent

bij gebruiken. Ik had toen nog niet bedacht hoe je de studenten op weg kan helpen zonder meteen de oplossing te geven. Dat was op zich niet zo erg maar ik wilde ook niet naar de klachten van de studenten luisteren. Ik vond dat ze het maar moesten kunnen. De studenten hebben toen terecht een boze brief naar de examencommissie gestuurd. Dat was een hele leerzame ervaring. Vanaf dat moment heb ik altijd geprobeerd goed naar de studenten te luisteren.

Met mijn onderzoek wilde het in het begin niet zo vlotten. Er was veel afleiding en ik was er heel goed in om uit te leggen waarom ik ook deze keer weer niet was toegekomen aan wat ik met mijn promotor had afgesproken. Hij verweet mij regelmatig dat ik weer in mijn oude fout was vervallen, maar wat hij precies bedoelde begreep ik pas veel later, toen ik zelf promovendi mocht begeleiden.

Mijn onderwerp, functioneel programmeren, had ik te danken aan mijn derde leermeester, Henk Barendrecht, beroemd Logicus, en schrijver van het standaard boek over de lambda-calculus. Bob's expertise op het gebied van computerarchitectuur en Henk's expertise in de logica waren de essentiële ingrediënten voor het succes van het Nederlandse reductiemachine project waar mijn proefschrift een bijdrage aan was. (Op de foto kijkt mijn zoon Olivier naar de reductiemachine.)





# 1985

Dat reductiemachine project was bedoeld als antwoord op het in 1982 gestarte Japanse vijfde generatieproject waarin nieuwe computerarchitecturen werden ontwikkeld voor kunstmatige intelligentie. Grappig dat we nu, 40 jaar later weer helemaal op de AI-toer zijn. Toen moesten de computers vooral zeer snel worden door het exploiteren van parallellisme. Dat parallellisme moest komen uit programma's geschreven in declaratieve talen. In Japan werd ingezet op logisch programmeren terwijl in Europa vooral werd ingezet op functioneel programmeren.

Ik ga aan de hand van een voorbeeld proberen uit te leggen waarom functioneel programmeren ons toen zo inspireerde. Stel voor dat je een eenvoudige som wil uitrekenen: 5x4-3x2. Je kan van links naar rechts werken, dus eerst 5x4=20 uitrekenen. Dan 3x2=6. En tenslotte 20-6=14. Je kan ook van rechts naar links werken. Dus eerst 3x2=6, en dan 5x4=20, en tenslotte 20-6=14. Het maakt niet uit welke volgorde je kiest: het antwoord is altijd hetzelfde. Maar er is nog een mogelijkheid die je instaat stelt om sneller het antwoord te vinden, namelijk door parallellisme. Als er twee mensen aan de som gaan rekenen, dan kan de ene 3x2=6 uitrekenen terwijl de andere 5x4=20 uitrekent. Dit zijn makkelijke sommen dus de tijdswinst om met meer dan een persoon tegelijk aan het rekenen te gaan is klein. Maar voor echt moeilijke problemen is er tijdswinst te behalen.

Dit parallellisme maakte ons enthousiast om te proberen een speciale computer te bouwen die gigantische tijdswinst mogelijk zou kunnen maken. Na een aantal jaren hard werken van een behoorlijk groot team hebben we computers gebouwd die inderdaad tijdswinst mogelijk maakten. Maar helaas bleek het voor programmeurs lastig om hun programma's zo op te schrijven dat de computer de tijdwinst kon realiseren. Mijn collega onderzoeker Wim Vree had een constructie bedacht de sandwich, waarbij het beleg het parallelle gedeelte voorstelde, en de twee helften van de boterham de rest van de berekeningen. Wim was een van de weinigen die gewoon op papier een programma kon opschrijven

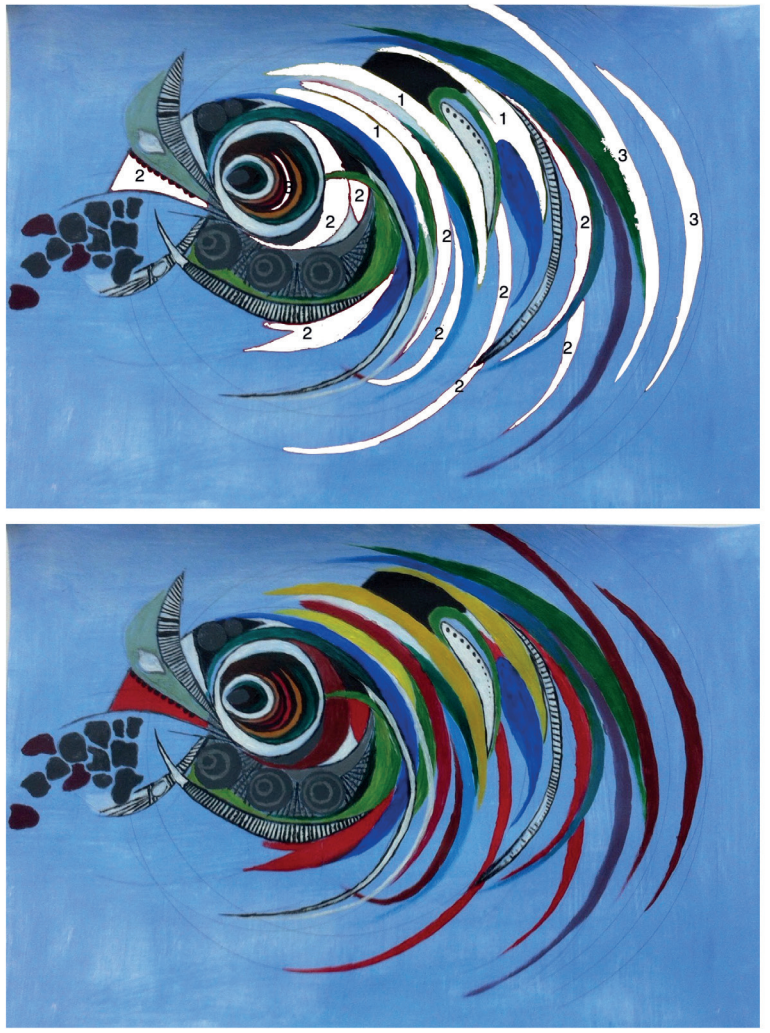
wat meteen werkte. Ik hoefde zijn programma's voor onze parallelle reductie machine alleen maar in te tikken en dan was het klaar. Geen debuggen of niets. Bijna alle andere programmeurs vonden het heel lastig om hun programma's goed op te schrijven, en ook nog zo dat er met parallelisme tijdswinst kon worden behaald. Het is toen uiteindelijk niet goed afgelopen met de AI-droom; ik hoop dat de geschiedenis zich niet gaat herhalen.

# 1991

Nog steeds geïnspireerd door de elegantie van functioneel programmeren ben ik me steeds meer gaan afvragen of het voor programmeurs misschien makkelijker te maken is goede code schrijven. Ik werkte toen in Southampton waar mijn collega Hugh Glaser het idee had opgevat van "programmeren op nummer". Dat is een programmeer methode die min of meer werkt volgens dezelfde principes als "schilderen op nummer". Het idee is eigenlijk hetzelfde als van de torens van Hanoi: knip een probleem in stukken die je makkelijk kan oplossen, en plak dan de oplossingen weer aan elkaar. We hebben toen een experiment uitgevoerd met studenten als proefpersonen om het succes van de "programmeren op nummer" te meten. De studenten vonden het handig dat de methode hun hielp bij het min of meer mechanisch opdelen van een programmeerprobleem in kleinere stukjes, maar soms ontstonden er te veel stukjes, zodat studenten het overzicht een kwijtraakten. (De foto's hiernaast zijn van een schilderij van Marijke.)

Samen met mijn Amsterdamse collega Henk Muller heb ik het idee van programmeren op nummers voor functioneel programmeren verder uitgewerkt in een leerboek "Functional C". Dit was een avontuur wat me twee jaar heerlijk bezig heeft gehouden. Het boek is helaas geen bestseller geworden. En toen het boek af was heb ik Marijke moeten beloven dat ik nooit meer een boek zou schrijven.





# 1994

Marijke vond het jammer voor mij dat het boek niet lekker liep en had toen ook nog een andere tip voor mij: ga nu eens iets doen waar de mensen wat aan hebben. Gelukkig had een van mijn studenten, Eduard de Jong, een fijn plan. Het idee waar Eduard mee rondliep was: programmeurs vinden het moeilijk om goed beveiligde programma's te schrijven en misschien kan je het makkelijker voor ze maken. Ik dacht toen dat het idee van "programmeren op nummer" hier ook weer van toepassing zou kunnen zijn. Ik zal proberen het idee aan de hand van een voorbeeld uit te leggen.

Stel je wil met de trein van Delft naar Enschede. Dan moet je voordat je instapt je ov-chipkaart scannen en als je uitstapt moet je nog een keer scannen om af te rekenen. Maar als je haast hebt om de trein te halen dan vergeet je soms om te scannen. Nu zijn er toegangspoortjes op het station waar je doorheen moet zodat je niet meer kan vergeten om te scannen maar die zijn er niet altijd geweest. Het is mij herhaaldelijk overkomen dat ik halverwege de reis dacht: heb ik wel gescand? Ik kan het me niet meer herinneren. Dan kon je bij de volgende halte de trein uit en naar de het zuiltje rennen, scannen en hopen dat de trein er nog stond als je weer terug was gerend. De toegangspoortjes zijn er dus vooral voor om mensen eraan te herinneren dat ze voordat ze in de trein stappen iets moeten doen en als ze op de plaats van bestemming zijn aangekomen weer iets moeten doen.

Eduard's idee voor het programmeren van transacties op de smartcard kwam op hetzelfde neer. In plaats van een treinreis maken we een transactie, bijvoorbeeld een betaling. In plaats van het scannen voor het instappen moet de programmeur een beveiligingstap doen, bijvoorbeeld het controleren van een digitale handtekening. En na afloop van de transactie wordt de programmeur ook weer gedwongen om een beveiligingsstap te doen, bijvoorbeeld het zetten van een digitale handtekening. Samen met Eduard heb ik dat idee toen geformaliseerd in de vorm van een functioneel programma en in 1994 gepresenteerd op de eerste editie van de internationale smart card conferentie



CARDIS. Kennelijk had ik een goede indruk gemaakt op de collega-wetenschappers want ik mocht een jaar later de tweede editie van de conferentie in Amsterdam organiseren.

Op dat moment was ik geen onderzoeker op het gebied van parallel functioneel programmeren meer maar een onderzoeker op het gebied van informatiebeveiliging. En het idee om het mensen makkelijker te maken om de juiste dingen te doen zou later nog wel een paar keer terugkomen. Maar waarom was beveiliging eigenlijk interessant?

# 1995

Het commerciële internet zoals wij dat nu kennen is nog maar 25 jaar jong. Voor onderzoek was het Internet al eerder beschikbaar maar pas in 1995 zijn de laatste restricties voor commerciële partijen opgeheven en kon het Internet ook voor zaken worden gebruikt. Het is interessant om te kijken hoe snel nieuwe technologie gemeen goed is. In Amerika heeft het bijna 100 jaar geduurd heeft voordat iedereen een vaste telefoonaansluiting had. Internet en de mobiele telefoon zijn ongeveer 4 x sneller geïntroduceerd. We kunnen dit deels verklaren door het netwerkeffect. Dat is het verschijnsel dat ervoor zorgt dat een dienst meer waarde heeft voor iemand al naar gelang er meer gebruikers zijn die dezelfde dienst al gebruiken. Dus naarmate meer mensen telefoon hebben wordt het interessanter voor andere mensen om ook telefoon te nemen want dan kan je familie, vrienden etc. makkelijk bereiken.

Tech bedrijven zoals Google, Amazon, en Alibaba bestonden 25 jaar geleden nog niet en nu horen deze drie tot grootste bedrijven op aarde. Het Internet en het World Wide Web hebben enorm veel kansen geboden voor nieuwe bedrijvigheid, maar niet zonder nieuwe bedreigingen. Zo heeft de industriële revolutie in de 19e eeuw een gigantische golf van criminaliteit veroorzaakt omdat er bij grote fabrieken ook veel makkelijk te stelen goederen waren opgeslagen. De digitale revolutie heeft ook een nieuwe golf van

criminaliteit mogelijk gemaakt. Waar vroeger de crimineel zijn slachtoffers moest opzoeken kan hij nu rustig van achter de keukentafel via het Internet de halve wereld bereiken. Ik wil daar een voorbeeld van geven.

# 2001

Op 11 februari 2001 lanceerde de 20 jaar oude student Jan de Wit uit Sneek het computervirus Anna Kournikova. Dit was de naam van een beeldige Russische tennisspeelster. Jan had het virus in een paar uur in elkaar gezet met behulp van software tools die hij via het Internet had gekregen. In tegenstelling tot wat de naam van het virus suggereerde was er geen plaatje van Anna te zien. In plaats daarvan verzond het virus zichzelf naar alle e-mailadressen in het adressenbestand van het slachtoffer. Miljoenen mensen kregen het virus en dit veroorzaakte niet alleen problemen bij de e-mail servers die de vloed aan e-mails niet meer aankonden maar ook onrust bij de slachtoffers omdat hun adressenbestand kennelijk was gebruikt door het virus.

Jan de Wit was bepaald geen leek op het gebied van computers. Hij werkte in de computerwinkel en hij ging er prat op een verzameling van 7000 virussen te hebben die hij had opgeslagen op 53 CD ROMS. Snel realiseerde Jan zich wat de mogelijke gevolgen zouden kunnen zijn van zijn virus, en hij besloot zichzelf aan te geven bij de politie van Sneek. We kunnen alleen raden naar de reactie van de politiemensen in Sneek maar waarschijnlijk waren ze er niet goed op voorbereid en hadden ze hulp nodig van een digitale expert.

Toen de zaak voorkwam achtte de rechtbank in Leeuwarden bewezen dat de verdachte met opzet een poging had gedaan om schade aan te richten. Op die gronden is de verdachte veroordeeld tot een taakstraf van 150 uur. De verdachte is in beroep gegaan maar de Hoge Raad heeft het beroep verworpen omdat de rechter niet geloofde dat verdachte niet zou hebben geweten dat hij schade zou richten. Hij was immers beroepshalve met computers bezig en



hij was een grote verzamelaar van virussen.
De burgemeester van Sneek was zo onder de indruk van de technische vaardigheden van Jan de Wit dat hij hem een baan aanbood bij de IT-afdeling van de gemeente. Dan weten we dus nu ook waarom IT-projecten van de overheid soms uitlopen en te duur zijn.

Het virus van Jan de Wit kon zich razendsnel verspreiden omdat de ontvanger graag een mooie foto van Anna Kournikova wilde zien, zodat vervolgens geheel automatisch alle contacten van de ontvanger werden verleid met een mail. Dit is dus een slimme combinatie van techniek en verleiding. Het Internet heeft niet alleen gezorgd voor veel nieuwe kansen maar het heeft mensen als Jan de Wit ook onbegrensde mogelijkheden gegeven voor bedreigingen. Ik kom hier zo op terug.

Toen Jan de Wit zijn virus op de wereld lost liet was ik net benoemd tot hoogleraar gedistribueerde systemen aan deze universiteit. In mijn oratie heb ik al duidelijk gemaakt dat gedistribueerde systemen niet mijn eerste belangstelling hadden, maar dat ik vooral aan de beveiliging ervan wilde werken. Heerlijk dat niemand daar mee zat, je hebt als onderzoeker op een universiteit toch wel heel veel vrijheid.

# 2004

Wat ik mij als kersverse hoogleraar niet had gerealiseerd had was hoeveel inspanning er nodig was om onderzoek gefinancierd te krijgen. In die tijd was er nog wel wat geld voor de eerste geldstroom promovendi maar dat droogde snel op en toen was iedereen aangewezen op de betrekkelijk beperkte subsidiepotjes van NWO, STW en de Europese Kaderprogramma's. Gelukkig was ik niet de enige met dit probleem maar mijn collega Bart Jacobs uit Nijmegen wilde ook meer geld voor beveiligingsonderzoek in Nederland. Wij zijn samen op pad gegaan en hebben ongeveer twee jaar in Den Haag gelobbyd om een onderzoeksprogramma

gefinancierd te krijgen, dat Sentinels ging heten. Er zijn drie rondes van dat programma geweest die samen over een periode van 10 jaar 15 M Euro aan subsidie hebben uitgegeven aan naar schatting 30 projecten.

Sentinels heeft niet alleen de wetenschap bevorderd, maar het heeft ook een impuls gegeven aan de economie. Ik heb het natuurlijk over de spin-off Security Matters van Sandro Etalle en zijn twee promovendi Damiano Bolzoni en Emmanuele Zambon. Met z'n drieën hebben ze het bedrijf opgericht om de ideeën te commercialiseren die ze in hun Sentinels projecten hadden bedacht en uitgewerkt. Na 10 jaar hard werken gaf het bedrijf werk aan bijna 100 hoogopgeleide medewerkers en was het wereldmarktleider geworden op het gebied van intrusion detection voor Industrial Control Systems. Dat was een geweldige prestatie van mijn drie collega's. Het heeft ze ook geen windeieren gelegd want in 2018 is Security Matters voor vele miljoenen Euro's aan een Amerikaans bedrijf verkocht.

# 2008

In 2008 kwam collega Marianne Junger bij me langs om eens te praten. Zij was toen hoogleraar sociale veiligheidsstudies, en onderzocht agressie bij kinderen en risicogedrag van jongeren. Het leek haar interessant om na te denken over de rol van het Internet op risicogedrag en criminaliteit. Ik vond dat een goed idee en we hebben de afgelopen 13 jaar leuk samen gewerkt aan wat we nu cybercrime-science noemen.

Het idee dat psychologie en beveiliging gerelateerd zijn was niet nieuw. In hetzelfde jaar dat Marianne mij opzocht schreef Bruce Schneier -- een van de meest beroemde collega's -- in Communications of ACM een artikel over risico perceptie. Hij vergeleek de mens met het een konijn dat ergens rustig zit te eten. Plotseling ziet het konijn een vos. Dan moet het konijn snel een beslissing over het risico nemen: dooreten om niet om te komen van



de honger of wegrennen om niet opgegeten te worden. Konijnen zijn goed in het maken van deze beslissingen want anders zouden ze allang zijn uitgestorven. De mens -- als de meest succesvolle diersoort -- moet dus eigenlijk nog beter zijn in het maken van risico afwegingen. Maar waarom vroeg Bruce zich in het artikel af, zijn wij daar eigenlijk zo slecht in? Waarom schatten we het risico om op een verkeerde link te klikken zo fout in? Waarom kiezen we te gemakkelijke wachtwoorden? Waarom maken we geen backups? Waarom gebruiken we programma's die out-of-date zijn? Waarom doen we alles om een plaatje van Anna Kournikova te zien? Geen van deze vragen kunnen door de techniek worden beantwoord. Maar ze zijn wel fundamenteel voor een goede beveiliging. Het is dus niet voldoende om de techniek goed te beheersen, maar je moet ook goed begrijpen hoe mensen er mee om gaan. Ik had al eerder wat stappen gezet in deze richting toen ik mij afvroeg of je het programmeurs misschien makkelijker zou kunnen maken om het juiste te doen; ik had er zelfs een boek over geschreven....

# 2009

Nu werd de vraag nog een slag uitdagender: kan je het misschien makkelijker maken voor niet alleen programmeurs, maar om iedereen juiste dingen te doen? Hier ziet u een foto van mijn Marijke die in een hotel bij Angkor Wat (Cambodia) gevraagd had of er een kamer met een kluisje beschikbaar was. Ja dat was er, en hier was het kluisje! (zie foto volgende pagina)

Marianne en ik zijn eerst begonnen met een overzichtsartikel te schrijven waarin we een brug wilde slaan tussen crime science en informatiebeveiliging. Om uit te leggen wat crime science is herinner ik u aan het spreekwoord "de gelegenheid maakt de dief". Het idee is dat iedereen in principe in staat is om dingen te doen die hij niet zou moeten doen als de gelegenheid maar gunstig is. Wat is het mooie van dat uitgangspunt? Dat je kan proberen om de wereld zo in te richten dat er minder gelegenheid voor criminaliteit is. Bijvoorbeeld als je een ATM in een donker steegje plaatst is dat

vragen om moeilijkheden. Je kan de ATM beter op een drukke en goed verlichte plek neerzetten. Er zijn nog veel meer dingen die je kan doen om de fysieke wereld slimmer in te richten. Wij wilden experimenten gaan doen om te kijken of er ook bewijs kan worden gevonden dat slim inrichten van de digitale wereld effectief zou

We hebben een paar jaar aan het overzichtsartikel gewerkt en helaas is het nooit gepubliceerd geworden omdat de reviewers het niet snapten. De sociale wetenschappers begrepen de techniek niet en de techneuten begrepen de sociale sociaalwetenschappelijke aspecten niet. Het was even vervelend dat we ons onderzoek niet kon publiceren maar gelukkig hebben we daar wat op gevonden.

In 2012 stelde NWO-subsidie beschikbaar voor het oprichten van open access tijdschriften. Wij hebben een aanvraag voor die subsidie ingediend en met internationale collega's het tijdschrift



"crime science" opgericht. Dit is een multidisciplinair tijdschrift met reviewers uit de technische, sociale, en natuurwetenschappen. We hadden natuurlijk ons overzichtsartikel naar ons eigen tijdschrift kunnen sturen maar dat leek ons niet ethisch. Crime science is intussen een van de meest succesvolle Criminologie tijdschriften geworden van de uitgeven Springer.
Ik wil nu graag iets vertellen over de experimenten die onze promovendi hebben gedaan om de digitale wereld slim in te richten.

# 2010

Het eerst project was dat van Trajce Dimkov. Hij deed onderzoek naar de samenhang van fysiek, sociaal, en digitaal beveiligingsbeleid. Een voorbeeld van dergelijk beleid is: verkoopgegevens mogen nooit buiten de organisatie komen. Om dit beleid uit te voeren, moet de IT-afdeling ervoor zorgen dat hackers het systeem van de organisatie niet binnen kunnen dringen. De bedrijfsbeveiliging moet ervoor zorgen dat vreemdelingen het gebouw niet zomaar binnen kunnen komen. En personeelszaken moeten ervoor zorgen dat medewerkers verantwoordelijk omgaan met de hun toevertrouwde informatie.

Trajce deed experimenten waarbij hij de campus van Universiteit als levend laboratorium gebruikte. In een van die experimenten wilde hij nagaan in hoeverre collega's goed op hun laptop passen, want als de vertrouwelijke gegevens van het bedrijf op een laptop staan, dan mag die natuurlijk niet zoekraken of gestolen worden. Trajce had een experiment bedacht waarbij hij 12 laptops aan 12 verschillende, willekeurig gekozen collega's op de universiteit uitleende met een verhaal. Waar hij eigenlijk in geïnteresseerd was is of de mensen wel goed op de laptops zouden passen maar dat kon hij natuurlijk niet verklappen. Dus in plaats daarvan zei hij tegen de mensen die de twaalf laptops in bruikleen hadden dat hij wilde weten of men het fijn vond om ermee te werken. Wat de proefpersonen niet wisten is dat Trajce een aantal studenten had gevraagd om die laptops te stelen. De studenten kregen wat spelregels mee. Ze mochten geen

geweld gebruiken, bijvoorbeeld om een kamer open te breken, maar ze mochten wel een smoesje ophangen. De studenten vonden het helemaal niet moeilijk om die laptops te stelen. Dat was interessant resultaat. Maar bij een experiment gaat er ook nog eens wat mis, en daar kan je veel van leren.

Een van de laptops was uitgeleend aan een promovendus die in een chemisch lab werkte. Nou is een chemisch lab niet een omgeving waar je zomaar je gang kan gaan. Er wordt met gevaarlijke stoffen gewerkt en er staat gevoelige en dure apparatuur waar je voorzichtig mee moet omspringen. Helaas had de promovendus aan wie de laptop was uitgeleend had hem uit voorzorg aan een bureau vastgeketend met een stalen kabel. En het bureau stond in het lab.

De student dieven mochten geen geweld gebruiken en konden dus niet de kabel doorknippen. Maar wat dan wel? Nou heel simpel: je neemt de laptop met bureau en al mee! Dus op een vroege ochtend droegen de studenten een bureau uit het chemisch lab, tussen rinkelend glaswerk door, over de campus, en ons gebouw binnen om het bureau met de laptop voor Trajce's kantoor neer te zetten.

De studenten hadden zich keurig aan de opdracht gehouden maar de directeur van het chemisch lab was heel erg boos op mij. En terecht, want er hadden verschrikkelijke dingen kunnen gebeuren als het mis was gegaan bij de verhuizing van het bureau. Ik heb de directeur moeten uitleggen wat we hadden uitgespookt. Ik heb moeten beloven dat we het nooit meer zouden doen. Ook de directeur van mijn faculteit was boos, maar hij was ook bereid om van het incident te leren. Hoe kan het zijn dat een experiment zulke potentiele risico's met zich meebrengt? Waarom is daar niet opgelet? Het was natuurlijk mijn verantwoordelijkheid als begeleider om de risico's van het onderzoek van mijn promovendi te beheersen en ik was daar duidelijk in tekortgeschoten. Maar ik had ook wel wat hulp kunnen gebruiken en daarin was mijn faculteit tekortgeschoten.

Het is nu de normaalste zaak van de wereld, dat een onderzoek met proefpersonen door een commissie van wijze mannen en vrouwen wordt beoordeeld. Een dergelijke ethische commissie hadden wij niet en als gevolg van het incident heeft mijn faculteit besloten een ethische commissie in te stellen.



# 2017

Het tweede project waar ik iets over wil vertellen is van Elmer Lastdrager. Hij heeft samen met master studenten een experiment gedaan met kinderen. Het onderzoek ging over de mate waarin kinderen zich bewust zijn van de gevaren van phishing. Dat is belangrijk, want er wordt wel veel onderzoek naar phishing onder volwassenen gedaan, maar kinderen zitten ook op het internet, en zijn ook potentiele slachtoffers van phishing. Kinderen hebben misschien nog geen bankrekening maar ze hebben wel een e-mailadres, en een Facebook-account waarvan phishers misbruik kunnen maken.

Elmer en zijn studenten zijn op een aantal lagere scholen geweest. Ze hebben de kinderen e-mails voorgelegd en getest of ze phishing e-mails van echte e-mails kunnen onderscheiden. De kinderen waren in twee groepen ingedeeld. De ene groep kreeg eerst les in het herkennen van phishing e-mails en werd daarna getest. De andere groep werd eerst getest en kreeg daarna les in het herkennen van phishing. Door de resultaten van de twee groepen met elkaar te vergelijken kan je vaststellen hoe effectief de lesmethode was geweest. Uit het onderzoek is gebleken dat het heel nuttig is om op school over de gevaren van het Internet te praten. Kinderen zijn er erg mee bezig. Ze praten er met elkaar erover, en ze praten er thuis over, en dat draagt allemaal bij aan de bewustwording over mogelijke gevaren.

# 2019

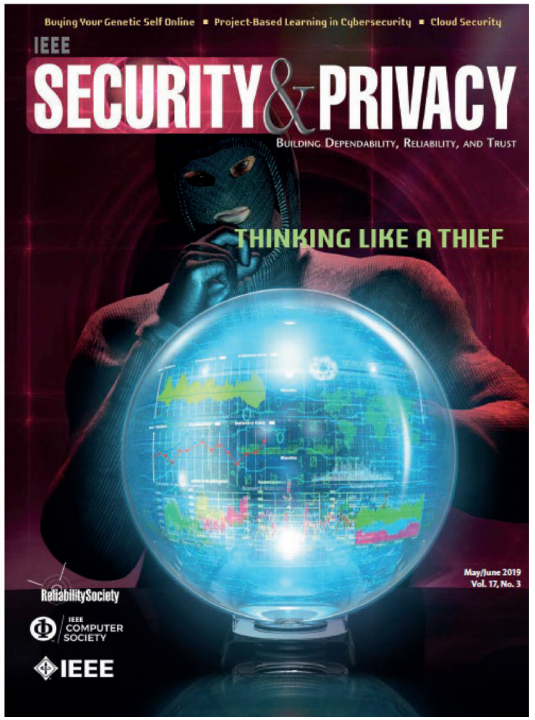
Wat later heb ik zelf in de klas van mijn kleinzoon verteld hoe Kevin Mitnick het met gladde praatjes voorelkaar kreeg om bij allerlei bedrijven binnen te komen. Hij was heel goed in wat hij deed, maar net als andere meesteroplichters heeft Kevin ook een paar keer in de gevangenis gezeten. Ik wilde de kinderen vooral vertellen hoe

makkelijk iemand je wachtwoord te pakken kan krijgen. De kinderen in de klas van mijn kleinzoon wisten hier al veel van, en ze wilden er allemaal tegelijk over vertellen. Ik denk dat Vince en zijn klasgenoten nooit meer hun wachtwoorden met iemand zullen delen, zelfs niet met hun moeder! Ik hoop dat ik in het nieuwe normaal ook iets mag doen in de klas van mijn kleindochter Lotte.

# 2015

We gaan even terug in de tijd. Omdat de wereld zo snel aan het veranderen was dankzij het Internet moesten we natuurlijk ook zorgen dat de studenten passend onderwijs kregen. Samen met Jan van den Berg, mijn collega uit Delft, heb ik een specialisatie Cyber security van de master informatica ingevoerd. We hadden het zo ingericht dat ongeveer de helft van de vakken door Twentse docenten en de andere helft door Delftse docenten kon worden gegeven. Samen hadden we alle expertise in huis die nodig was om een degelijk en modern onderwijsprogramma te maken. Ongeveer twee derde van de colleges ging over harde techniek en een derde ging over de economische, juridische, psychologische, en ethische aspecten van Cyber security. In korte tijd groeide ons programma uit tot de grootste Cyber securitymasteropleiding van Nederland.
Ik heb zelf meegewerkt aan twee nieuwe vakken in de specialisatie. Het eerste vak, cybercrime-science, heb ik samen met Marianne Junger gegeven. Het onderwijs en het onderzoek op dit gebied ging dus hand in hand. Aan de ene kant betekent dit soms experimenteren in het onderwijs maar aan de andere kant worden studenten met de nieuwste resultaten geconfronteerd, en werken ze ook actief mee aan het onderzoek. Vooral dat laatste inspireert de student en de docent enorm. Ik ben er ook erg trots op dat we onze ervaringen met dit vak hebben kunnen publiceren in het meest prestigieuze vaktijdschrift “IEEE security privacy magazine”. De editor was zo onder de indruk van ons werk dat hij van ons artikel het feature artikel van Mei 2019 heeft gemaakt.






# 2016

Het andere vak wat ik heb opgezet was de capstone cyber security. Het idee van dit vak was om de studenten te helpen hun technische kennis zo goed mogelijk te benutten. We deden dat in drie stapjes: eerst moesten de studenten leren om interviews te houden, want als professional kunnen ze hun technische kennis het beste benutten als ze goed weten wat een klant of opdrachtgever nou eigenlijk wil. In de tweede stap leerde de studenten iets over ondernemerschap in cyber security. Dat was natuurlijk gebaseerd op de ideeën van Willem Jonger die als CEO van EIT Digital een hele reeks masteropleidingen had opgebouwd waarin innovatie en ondernemerschap centraal

staat. In de derde stap leerden onze studenten dat de business altijd leidend is. Het bijzondere van de capstone was dat het onderwijs steeds in nauwe samenwerking met bedrijven en organisaties, en op locatie, zoals the Hague Security Delta plaatsvond. Ik denk met de capstone een voorbeeld te hebben gevonden voor de perfecte public private partnership in onderwijs.

# 2013

We gaan voor de laatste keer terug in de tijd. Na ongeveer 15 jaar in Twente te hebben gewerkt was ik toe aan een nieuwe uitdaging. Ik had gemerkt dat als je iets wilde bereiken, dat je daarvoor naar Den Haag moest om te lobbyen. Nu is Nederland klein, maar ook weer niet zo klein. Even van Twente naar Den Haag op en neer kost zo een hele dag. Het leek mij dus handig om een basis in Den Haag te hebben. TNO wilde mij wel een dag in de week hebben en was bereid om een TNO-er voor twee dagen in de week aan de Universiteit Twente uit te lenen. Zo konden we met gesloten beurzen een betere samenwerking tussen de universiteit en TNO organiseren. Ik heb een aantal jaren met veel plezier bij TNO in Den Haag gewerkt.

De mooiste klus die ik voor TNO heb mogen doen is het maken van een training voor INTERPOL in Singapore. Misschien weet u dat in 2008 BitCoin is ontstaan. Dat is een betaalmiddel waar wet en regelgeving lang geen vat op kon krijgen. Het werd dan ook snel populair bij handelaren in drugs en wapens. In 2011 lanceerde Ross Ulbricht de website Silkroad. Dat was een online markt zo ongeveer als marktplaats.nl maar dan bedoeld voor de handel in illegale diensten en producten. Om te zorgen dat de politie geen vat op de marktplaats kon krijgen moesten handelaren en klanten naar de marktplaats toe via het Tor netwerk, en kon je alleen betalen in BitCoin. Dankzij deze twee technieken kon je redelijk anoniem handeldrijven op Silkroad. De FBI en het Team High Tech Crime van de Nederlandse politie waren al redelijk vroeg instaat om greep op dit soort marktplaatsen te krijgen. Zo heeft de FBI in 2013 Silkroad



uit de lucht gehaald. Maar dat was wel een lastige tijdrovend klus. En de politie in de meeste andere landen hadden nog te weinig kennis van deze nieuwe technologie.

INTERPOL is een organisatie waar bijna alle 200 landen van de wereld lid van zijn. Het doel van INTERPOL is de wereld veiliger te maken. Een van de activiteiten van INTERPOL is het ontwikkelen en geven van trainingen. Naar aanleiding van de Silkroad zaak was er behoefte ontstaan bij de lidstaten van INTERPOL om zelf marktplaatsen uit de lucht te kunnen halen. Samen met Mark van Staalduinen van TNO en collega's hebben we in 2015 de eerste training gemaakt en een aantal keren gegeven. Een belangrijk aspect was dat de Cyberafdeling van INTERPOL in Singapore is gevestigd. Van de Universiteit Twente mocht ik een half jaar op sabbatical en Annemarie Zielstra van TNO heeft geregeld dat ik dat sabbatical bij INTERPOL in Singapore mocht doorbrengen.

# 2015

We hadden om de training te ondersteunen een marktplaats nagebouwd die Doarklis heette. (Ik had Silkroad achterstevoren willen schrijven maar ik had een foutje gemaakt). We wilden de marktplaats zoveel mogelijk op een echte marktplaats laten lijken, maar dan kleinschalig zodat de cursisten een goed overzicht zouden hebben. We hebben alle relevante onderdelen van het Internet in een koffer gestopt. De marktplaats draaide op een netwerk van Raspberry PI. Dat zijn kleine Linux computers die maar een paar tientjes per stuk kosten en waar je makkelijk allerlei software op kunt installeren. We hadden een Tor netwerk en een BitCoin netwerk geïnstalleerd en natuurlijk een marktplaats met interessante aanbiedingen van bekende drugdealers, zoals Amsterdam United, en Holland Online. We hadden diverse rollenspellen bedacht voor de cursisten met rollen zoals koper, verkoper, marktmeester, en politie. Het doel van het spel was voor de politie om de identiteit van de andere spelers te achterhalen en voor de andere spelers zo veel mogelijk geld te verdienen zonder gearresteerd te worden.

De techniek van Tor en BitCoin was zo goed dat het eigenlijk niet mogelijk was om met alleen technische middelen de identiteit van iemand achterhalen. Een van de dingen die de politie normaal doet is met het IP-adres van iemand naar de Internet Service Provider (ISP) stappen om ook de naam en het adres te achterhalen. Als mensen communiceren via Tor netwerk dan lukt dit niet meer. De reden hiervoor is dat het Tor netwerk een aantal computers van vrijwilligers als doorgeefluikje gebruikt. Stel voor dat A met zijn webbrowser naar de website van Z wil gaan om drugs te bestellen. Dan kiest het Tor netwerk een aantal doorgeefluikjes, laten we zeggen D, Q en S. Vervolgens stuurt het Tor netwerk de communicatie eerst van A naar D, dan van D naar Q, dan van Q naar S, en tenslotte van S naar Z. Als de politie een internet tap op de marktplaats heeft gezet, dan vindt ze het IP-adres van S. Maar S is alleen maar een doorgeefluik. In principe zou de politie naar de ISP van S kunnen stappen en vragen wie dat is, zijn computer in beslag nemen en bekijken om te ontdekken dat ze eigenlijk Q hadden moeten hebben. Hoe langer de keten hoe meer werk en u begrijpt dat dit niet erg efficiënt is.

Nu zijn politiemensen niet voor een gat te vangen. Als het met technische middelen niet lukt dan zijn er altijd nog wel andere middelen. Bijvoorbeeld als je drugs online bestelt moeten die ook geleverd worden. Dat betekent dat de verkoper naam en adres van de koper moet hebben want anders kan de post het niet bezorgen. Dus wat je kan doen is brievenbussen en postkantoren in de gaten houden om te zien of je ongebruikelijke activiteiten ziet. De trainingen vonden meestal plaats in een paar zaaltjes in een groot gebouw. Ergens in die ruimte moesten de pakjes worden klaar gelegd door de verkoper en weer worden opgehaald door de koper. Het was dus goed mogelijk voor de politie om die ruimtes in de gaten te houden en te zien wie met wat voor pakje bezig was. Natuurlijk begrepen de kopers en verkopers dat ook, en die hadden dan weer manieren gevonden om de politie te ontlopen, bijvoorbeeld door de drugs op de wc te verstoppen. Web hebben allemaal ontzettend veel lol gehad in het spel. Cursisten hebben ook hun nieuwverworven inzichten mee teruggenomen naar hun nationale politieorganisaties. Zo heeft de politie in Maleisië besloten naar aanleiding van de training om ook een team high-tech crime op te richten.



TNO werkte in Singapore samen met INTERPOL maar ook met een aantal universiteiten, waaronder Singapore University of Technology en Design (SUTD). In het eerste gezamenlijke project met SUTD hebben we de training gegeven aan medewerkers van het Singaporese ministerie van defensie en van de cyber security agency. Dat was een leerzame ervaring want deze cursisten hadden veel meer kennis van techniek dan de politiemensen die we tot nu toe getraind hadden. Binnen de kortste keren hadden de cursisten de Raspberry PI's gehackt en al mijn wachtwoorden veranderd. De hackers kregen de volledige controle over de marktplaats en konden gemakkelijk alle kopers en verkopers identificeren. Een mooi voorbeeld van out-of-the box denken.

We hadden op onze marktplaats een Bitcoin netwerk draaien en dat is zoals u waarschijnlijk wel weet een blockchain applicatie. Een blockchain is eigenlijk niet anders dan een slimme combinatie van een aantal technologieën die al heel lang bestaan. Wat het slim maakt is dat voor het eerst in de geschiedenis van de informatica men goed heeft nagedacht over het belonen van gewenst gedrag.

Hoe werkt een blockchain? Het is eigenlijk een groot kasboek waarvan veel kopieën in omloop zijn, en die kopieën zijn allemaal precies hetzelfde. Iedereen kan een kopie bekijken en precies vaststellen wat de waarheid is. Omdat er veel kopieën zijn hoef je ook niet bang te zijn dat je transacties zoekraken. Je transacties kunnen ook niet gehackt worden dan zou de hacker alle kopieën moeten veranderen, wat ondoenlijk is. Hoe zorgt het Bitcoin netwerk ervoor dat al die kopieën hetzelfde zijn? Dat doen de "miners". Dat zijn vrijwilligers die samen verantwoordelijk zijn voor het kasboek. En die miners willen graag meewerken omdat ze ervoor worden beloond. Iedereen die een transactie in het kasboek wil zetten betaalt mee aan het salaris van de miners.

Sinds 2008 zijn heel veel mensen aan de slag gegaan om te kijken wat ze met blockchain technologie zouden kunnen doen. Het is net alsof we terug zijn gegaan naar de begintijd van het Internet. Toen wist ook niemand wat je daarmee zou kunnen doen maar nu zouden we niet meer zonder kunnen. Ik heb u al verteld over mijn eerste e-mail in 1978, waarvan ik dacht van nou dat is leuk maar je kan

ook een brief schrijven of opbellen. Ik had niet kunnen vermoeden dat e-mail de killer App van het Internet zou worden. En al helemaal niet dat email een belangrijke pijler zou worden van cyber crime. Inmiddels is wel duidelijk dat criminele marktplaatsen zoals de Silkroad niet mogelijk zouden zijn zonder Bitcoin. Ik denk dat voor criminelen, Bitcoin de killer App van blockchain technologie is. Wat de killer App voor de rest van ons is daar wordt nog naarstig naar gezocht. De balans tussen kansen en bedreigingen van blockchain technologie is dus nog niet gevonden. (Op de foto staan de 2x8 schermen van de Raspberry PI's).




# 2021

Nieuwe technologie opent een wereld van nieuw kansen en bedreigingen. We hebben dat al vaak meegemaakt, eerst met paard en wagen, toen met zeilschepen, de spoorwegen, auto's, telefoon, het Internet, en nu de blockchain. We leven nu in de verbonden wereld, en hebben te maken met nog relatief onbekende kansen en bedreigingen.

Een terechte vraag zou kunnen zijn is de verbonden wereld er in de afgelopen 25 jaar nu veiliger geworden? Ik kan u daar helaas geen goed antwoord op geven om de simpele reden dat we niet instaat zijn om dit goed te meten. Door de politie verzamelde statistieken laten in het algemeen zien dat de criminaliteit in de ontwikkelde landen afgenomen is. Maar cybercrime is waarschijnlijk ondervertegenwoordigd in de politiestatistieken. Dat komt omdat slachtoffers van cybercrime dit vaak niet bij de politie melden en als ze het al melden dan doen ze dat bij organisaties zoals de banken of de fraude helpdesk. Het is helaas nu niet mogelijk om alle vormen van criminaliteit bij elkaar op te tellen en een betrouwbaar inzicht te krijgen in hoe veilig de wereld is. Gelukkig is er nog volop werk voor mijn collega's om criminaliteit beter te leren meten.

Het is ook niet makkelijk om de verbonden wereld zo in te richten dat de voordelen tegen de nadelen opwegen. Ik vind dat ingenieurs daar hard over na moeten denken. Dat betekent niet alleen nadenken over de kansen, maar ook over de bedreigingen. Op de universiteit moeten studenten ook leren over bedreigingen na te denken. Daar wordt in de ingenieursopleidingen die ik ken te weinig aandacht aan besteed. Ik heb geprobeerd in de afgelopen 50 jaar een bijdrage te leveren en ik hoop dat mijn collega's dit werk voortzetten.

# DANKWOORD

Tot slot wil ik graag mijn collega's en studenten bedanken.
Mijn leermeesters Andy Tanenbaum, Bob Hertzberger en Henk Barendregt voor het inspirerende voorbeeld.

De collega's en promovendi van de securitygroep voor het vertrouwen in hun hoogleraar, en speciaal Bertine Scholten en Gert-Jan Laanstra voor de fantastische ondersteuning.

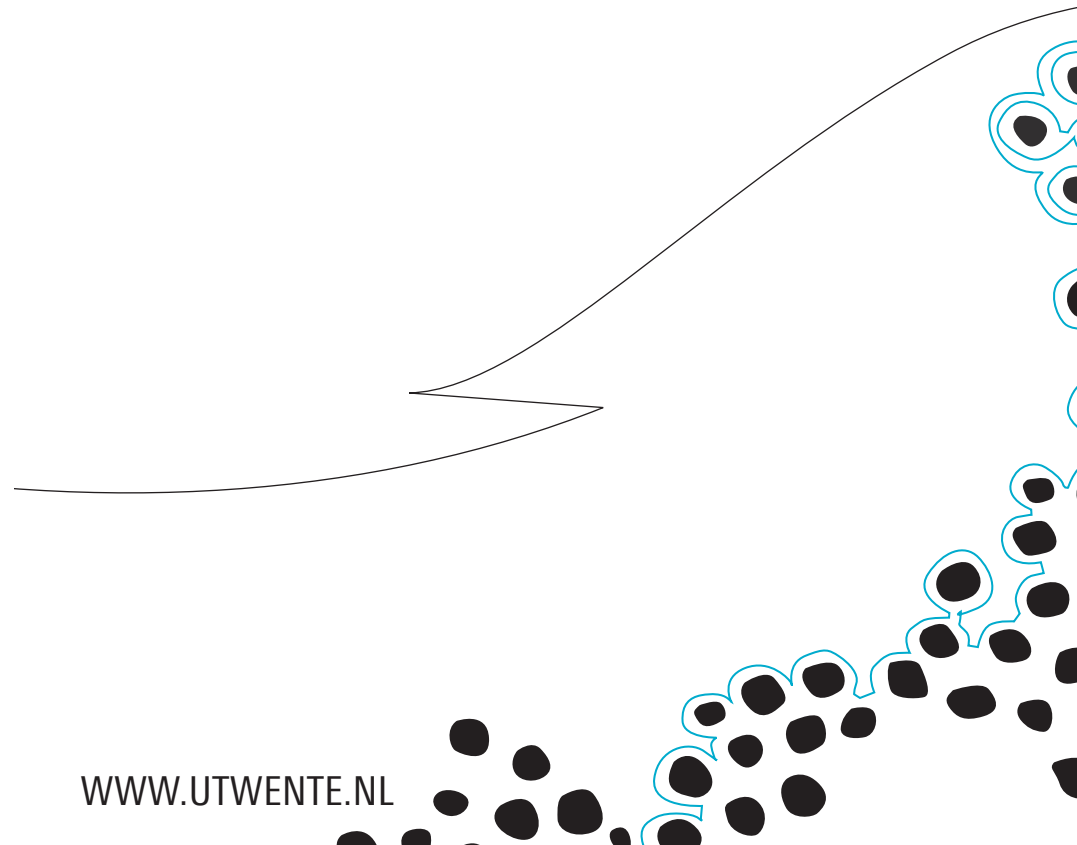
Collega hoogleraren, in het bijzonder Leon Abelman, Peter Apers, Ed Brinksma, Sandro Etalle, Boudewijn Haverkort, Paul Havinga, Hermie Hermens, Johann Hurink, Menno de Jong, Willem Jonker, Marianne Junger, Frank Kargl, Thijs Krol, Andreas Peter, Jacco van de Pol, Arend Rensink, Andrew Skidmore, Maarten van Steen, Mariëlle Stoelinga, Gerard Smit, Raymond Veldhuis, en Roel Wieringa voor de mooie onderzoeksprojecten waar we aan hebben gewerkt.

Het intervisie clubje met Andre ten Elshof, Gijs Krijnen, en Jan Willem Polderman voor het stellen van echt belangrijke vragen.

De vele collega's in Nederland en daarbuiten met wie ik het voorrecht heb gehad om onderwijs en onderzoek te mogen doen.

De studenten van de universiteiten waar ik college heb gegeven omdat je pas echt beseft wat je niet weet als je het probeert uit te leggen.

Marijke voor je liefde en zorg, en omdat je me regelmatig van mijn werk hebt afgehouden om andere leuke dingen te doen.



WWW.UTWENTE.NL