De cyberrevolutie: pak me dan als je kan

Berg, B. van den

Prof.dr. B. van den Berg

De cyberrevolutie: pak me dan als je kan

Universiteit Leiden

De cyberrevolutie: pak me dan als je kan

Oratie uitgesproken door

Prof.dr. B. van den Berg

bij de aanvaarding van het ambt van hoogleraar

Cybersecurity Governance

aan de Universiteit Leiden

op vrijdag 8 juni 2018

Universiteit
Leiden

Mijnheer de Rector Magnificus, zeer gewaardeerde toehoorders,

Inleiding

Stelt u zich voor. Het is het jaar 1800, ergens op het platteland van Engeland. We zien een tafereel dat zo uit een boek van Jane Austen zou kunnen komen. Een picknick van Britse adel die zich vermaakt op een zonovergoten dag. Het gesprek van de dag: de aanleg van een nieuwe spoorlijn, die langs een aantal van de landgoederen van deze edellieden gaat lopen. Sommigen zien voordelen in de komst van de trein. De ontsluiting van andere werelden, een verkleining van afstanden, een vergroting van de sociale realiteit. Anderen zien risico's. Een influx van vreemde mensen die de hechtheid van de plattelandsgemeenschappen zullen doorbreken. Geluidsoverlast, kolendampen, landonteigeningen, economische concurrentie, verschraling van normen en waarden. Om nog maar te zwijgen van allerhande veiligheidsrisico's.

We springen 50 jaar vooruit, naar het jaar 1850. Dezelfde plattelandsgemeente in Engeland. Alles, maar dan ook alles, is anders. Niet alleen door de komst van de trein, maar vooral door de industriële revolutie, die in een halve eeuw het hele aangezicht van de Engelse samenleving veranderde. Rond 1800 woonde meer dan 80% van de Engelse bevolking op het platteland. Rond 1860 woonde meer dan de helft van de bevolking in de stad.[1] Het Georgiaanse Engeland van het begin van de negentiende eeuw was primair een agrarische samenleving. Het Victoriaanse Engeland van het midden van diezelfde eeuw was de eerste geïndustrialiseerde samenleving ter wereld. En de overgang van het één naar het ander voltrok zich in slechts 50 jaar. Een ongekende transformatie in zo'n korte tijd. Een aantal factoren speelde een rol in de snelheid en reikwijdte van deze transformatie: technologische ontwikkelingen, nieuwe transport- en communicatiemiddelen, de opkomst van grootschalige industrie, en veranderingen in het economisch en maatschappelijk bestel. Bij elkaar genomen leidden deze factoren tot wat we nu kennen als de 'industriële revolutie'.

En we spreken dus met recht van een *revolutie*: een ware omwenteling in de manier waarop mensen leefden en werkten, een fundamentele verandering van de structuur van de samenleving. Dit leidde uiteraard tot allerlei maatschappelijke, juridische en economische uitdagingen. De veranderingen gingen zo snel dat men ze amper kon duiden. Michael Crichton - u weet wel, de man van die dinosaurus films - schreef een boek met de titel '*The Great Train Robbery*', over de grote treinroof die in 1855 plaatsvond.[2] In de introductie van dat boek, dat het midden houdt tussen een roman en een populair historisch verslag, schrijft hij over deze periode:

"*De overgang van het agrarische leven leek zich bijna binnen een etmaal voltrokken te hebben; sterker nog, het proces was zo snel dat niemand het echt begreep.*
Victoriaanse romanschrijvers, met uitzondering van Dickens en Gissing, schreven niet over de steden; Victoriaanse schilders verbeeldden amper stedelijke onderwerpen. Er waren ook conceptuele problemen - gedurende een groot deel van de eeuw werd industriële productie gezien als een bijzonder waardevol soort oogst, en niet als iets nieuws of ongehoords. Zelfs de taal bleef achter. Gedurende het grootste gedeelte van de negentiende eeuw betekende 'slum' nog een morsige kamer, en 'urbanisering' betekende verfijnd en modieus worden. Er waren geen algemeen gangbare termen om de groei van de steden te beschrijven, of het verval van delen van die steden.
Daarmee is geenszins gezegd dat de Victorianen zich niet bewust waren van de veranderingen die zich voltrokken in hun samenleving, of dat die veranderingen niet breed - en vaak heftig - bediscussieerd werden. Maar de processen waren nog te nieuw om ze echt te begrijpen."[2] Door de snelheid van veranderingen bleven duidingen van de betekenis ervan achter op de realiteit.

Van 1850 springen we honderdveertig jaar vooruit, naar het jaar 1990. De setting is een kantoorpand in een Westers land. We zien mensen bij de koffieautomaat. Het gesprek van de dag: de komst van het world wide web, dat in 1989 werd gecreëerd.

Het internet bestond toen al bijna twee decennia, maar voor het grote publiek was het nog niet toegankelijk. Met de komst van het world wide web had iedereen sinds kort toegang tot het internet. Informatie van over de hele wereld werd 24 uur per dag, instantaan en overal beschikbaar.

Sommigen zagen in de komst van het internet nieuwe, ongekende mogelijkheden. Net als bij de komst van de trein: de ontsluiting van andere werelden, een verkleining van afstanden, een vergroting van de sociale realiteit. Anderen zagen risico's en gevaren. En die zijn deels vergelijkbaar met de zorgen die we in het eerste tableau tegenkwamen: de erosie van locatiegebonden gemeenschappen, een versnelling in leefritme, het vervagen van cultuurgebonden waarden en identiteiten. En net als bij de komst van de trein gaf ook de komst van het internet zorgen over een trits van veiligheidsrisico's. Daarover later meer.

We springen voor de laatste keer door de tijd. Dit keer 30 jaar vooruit, van 1990 naar 2020. Hetzelfde kantoorpand, dezelfde koffiecorner - men mag hopen met een andere koffieautomaat. Alles, maar dan ook alles, is wederom veranderd. De opkomst van digitale netwerktechnologie, gekoppeld aan cyberspace, heeft in slechts 30 jaar tijd het hele aangezicht van Westerse samenlevingen veranderd. Een tijd lang duidden filosofen en techniekssociologen de opkomst van cyberspace als een nieuwe leefwereld, als een virtuele werkelijkheid die los stond van de fysieke werkelijkheid en juist daardoor ongekende mogelijkheden bood voor nieuwe vormen van interactie, voor experimenten met identiteit[5], zelfs voor een heel nieuw sociaal contract.[6,7] Intussen is de verwevenheid tussen onze online en offline levens echter zo nauw geworden dat die conceptualisering onhoudbaar is gebleken. Virtuele activiteiten gaan naadloos over in offline activiteiten en andersom. Wij leven in een wereld die zo hyperverbonden is, dat het betekenisloos is geworden om te vragen of men online of offline is - we zijn tegenwoordig permanent '*onlife*'.[8] Cyberspace is binnengedrongen tot in de haarvaten van ons bestaan.

Terugkijkend op de afgelopen drie decennia kan men stellen dat er, net als bij de industriële revolutie, sprake is van een ongekende transformatie in zeer korte tijd. Sommigen zouden stellen dat we met de komst van cyberspace wederom een revolutie hebben meegemaakt, de zogenaamde 'cyberrevolutie' (cf. [9]). De vraag die zich daarmee aandient is de volgende: Zijn wij in staat om adequaat te reflecteren op de grootte, de impact en de reikwijdte van die transformatie, van deze 'cyberrevolutie'? Kunnen wij deze radicale verandering al goed genoeg duiden? Of leiden we aan eenzelfde vorm van verwarring die ook de Victorianen tijdens de industriële revolutie kwelde: missen we nog het vocabulaire, de concepten, het overzicht, de afstand in de tijd, om tot een goed begrip te kunnen komen van de betekenis van de 'cyberrevolutie'? Valt deze revolutie te 'vatten'? En zo ja, wat is daarvoor nodig?

Focus op cybersecurity

Om een antwoord te vinden op die vraag richten we ons op één van de thema's die in de afgelopen jaren het meeste aandacht heeft gekregen: veiligheid *in* en *van* cyberspace, ofwel cybersecurity. Daar waar cyberspace oorspronkelijk niet primair ontwikkeld werd met veiligheid als kernwaarde in het achterhoofd (cf. [10]) bleek al snel dat deze nieuwe virtuele ruimte allerlei veiligheidsvraagstukken met zich meebracht (cf. [10,11,12-14]). Informatie en communicatie via netwerken moet op vertrouwelijke wijze uitgewisseld kunnen worden, zonder dat derden kunnen meelezen of -luisteren (cf. [15,16]). Systemen moeten zodanig beveiligd zijn dat anderen zich niet van buitenaf toegang kunnen verschaffen tot gegevens, of gegevens kunnen ontvreemden of veranderen (cf. [17,18]). En wanneer diensten in toenemende mate via netwerken worden aangeboden, moeten die netwerken robuust zijn, zodat de diensten te allen tijde beschikbaar zijn (cf. [19]).

In de eerste decennia na de opkomst van cyberspace was informatiebeveiliging een aandachtspunt voor de technische wetenschappen.[20-24] In de laatste 15 jaar zien we daarin een kanteling ontstaan. Het veilig maken en houden van systemen is niet

alleen een technisch probleem. Steeds vaker wordt cybersecurity gezien als een nationaal veiligheidsvraagstuk. Dat betekent dat statelijke actoren, overheden, een rol spelen ten aanzien van cybersecurity.[14,25-28] Zij hebben "*de verplichting om zorg te dragen voor de veiligheid van de burgers binnen hun grenzen, en deze verantwoordelijkheid strekt zich ook uit tot cyberspace*"[29]. Gezien het economisch en maatschappelijk gewicht van cyberspace hebben overheden een rol in het maken van wet- en regelgeving, van regulering en governance[30] ten aanzien van bijvoorbeeld de internet infrastructuur[31], of ten aanzien van cybercriminaliteit[32-34]. Daarnaast heeft de overheid de taak om grondwaarden zoals privacy[35-37], vrijheid van meningsuiting[38-44] en het intellectueel eigendom[45,46] te beschermen in cyberspace. Het vinden van een juiste balans tussen deze waarden en de bescherming van de nationale veiligheid blijkt een lastige klus te zijn.[47,48] Hoewel de overheid dus meerdere verantwoordelijkheden heeft in relatie tot cybersecurity, worden er veel vragen gesteld bij het hoe en waarom daarvan, niet in de laatste plaats omdat cyberspace een wereldwijd fenomeen is, terwijl statelijke soevereiniteit en jurisdictie langs territoriale grenzen lopen.[30,49-51]

Merk op dat statelijke actoren niet de enigen zijn die 'iets moeten' met cybersecurity. Bedrijven hebben de taak ervoor te zorgen dat er binnen hun organisatie, en in de ketens van organisaties waarmee zij samenwerken, gewaakt wordt voor de bescherming, de betrouwbaarheid en de vertrouwelijkheid van systemen en data.[52-54] Zij moeten er bovendien voor zorgen dat de mensen die met systemen en data werken voldoende vaardig zijn op het terrein van cybersecurity.[53,55-57]

En ook burgers zien in toenemende mate het belang van privacy en cybersecurity in.[28] Wij leven in een wereld waarin wij als eindgebruikers allemaal elke dag met digitale netwerktechnologie omgaan en ontelbare digitale sporen achterlaten. Het veilig houden van die wereld is een gedeelde verantwoordelijkheid voor een veelheid aan verschillende actoren.

Hoewel dit inzicht steeds breder gedragen wordt, en cybersecurity dus niet langer als een zuiver technisch probleem wordt gezien, roept de verbreding van de conceptualisering van cybersecurity tegelijk ook vragen op: wat verstaan we nu wel en niet onder dit concept? Wat is cybersecurity precies? En welke deelproblemen scharen we nu wel en niet onder deze paraplu?

Om die vragen te kunnen beantwoorden moeten we eerst een stapje achteruit doen. 'Cybersecurity' heeft in de basis iets te maken met veiligheid in, op en van cyberspace. Maar wat is veiligheid eigenlijk, en wat zijn precies de veiligheidsproblemen rondom cyberspace?

Wat is veiligheid?

Wanneer we de vraag opwerpen wat veiligheid is, is het antwoord vaak al snel dat daar geen eenduidig antwoord op is. Veiligheid wordt vaak gelabeled als een 'essentially contested concept' (cf. [58-60]) - een concept dat verschillende, met elkaar botsende betekenissen heeft, waarbij experts het niet eens kunnen worden over welke betekenis de 'echte' betekenis is.[61]

Als filosoof is het mij niet vreemd dat concepten 'essentially contested' zijn. Sommigen zouden zeggen dat de filosofie drijft op concepten die geen eenduidige betekenis hebben. Wat mij wel vreemd voorkomt, is dat er binnen de filosofie weinig geschreven is over het concept veiligheid.[60,62,63] Àls er binnen de filosofie al aan veiligheid gerefereerd wordt, dan is dat vaak in afgeleide zin: als onderdeel van grondrechten voor de mens of als essentieel element bij het begrijpen van armoede bijvoorbeeld.[64] Bovendien valt op dat alleen politiek filosofen aandacht hebben besteed aan veiligheid als thema. Nagenoeg alle politiek filosofen die vandaag de dag over veiligheid schrijven - en dat zijn er verbazingwekkend weinig - bouwen voort op het werk van Jeremy Bentham of Thomas Hobbes.[63] Beiden koppelden veiligheid direct aan de verantwoordelijkheden van de staat. Voor Bentham betekende veiligheid "*bestendigheid van de wet, zekerheid en voorspelbaarheid ten aanzien van eigendomsrechten*".[63] Volgens Hobbes had het individu bij het

sluiten van het sociaal contract een deel van zijn individuele vrijheid opgegeven - namelijk de vrijheid geweld te gebruiken jegens anderen - in ruil voor bescherming door de staat. Het individu werd een burger door vrijheid uit te ruilen voor veiligheid. Veiligheid is daarmee, in de woorden van de hedendaagse politiek filosoof Jeremy Waldron "*het hele punt van de politieke onderneming*"[63] en dus bij uitstek een overheidsverantwoordelijkheid.

Maar het is wel opmerkelijk dat zelfs Hobbes en Bentham geen invulling geven aan het concept veiligheid zelf. Het is het ultieme uitruilmiddel en de basis van de staat, maar wat het concept betekent blijft in het midden.

Dat veiligheid zo weinig aandacht heeft gekregen binnen de filosofie is des te opmerkelijker als men bedenkt hoe centraal de notie van veiligheid is in ons bestaan. Een ontologische of wijsgerig-antropologische duiding van het begrip veiligheid zou dus zeer op zijn plaats zijn. Het voert te ver deze duiding hier diepgravend uit te voeren, maar u kunt ervan op aan dat die in de komende jaren zeker zal volgen.

Laten we voor nu vaststellen dat veiligheid een grondbegrip is voor ons menselijk bestaan. Veiligheid is, onder alledaagse omstandigheden in Westerse landen, eigenlijk de *normaaltoestand*. We voelen ons in ons dagelijkse leven veilig zonder dat we erover nadenken. Juist omdat we ons veilig voelen, zijn we in staat onze aandacht te richten op andere zaken, op werk of sociale relaties, of onze zelfontplooiing. Veiligheid vormt als het ware de basis voor al het andere, en we leven in een veilige toestand zonder erover na te denken.

We worden ons pas *bewust* van veiligheid op het moment dat die veiligheid voor kortere of langere tijd bedreigd of opgeschort wordt, wanneer ons lichamelijke, emotionele of geestelijke zelf wordt blootgesteld aan dreigingen of gevaar. Dan worden we ons bewust van onze kwetsbaarheid, van de risico's die we lopen op schade, aan onszelf, onze dierbaren, onze bezittingen, aan alle zaken die we waardevol achten. Of dan *ervaren* we die kwetsbaarheid en die schade zelfs.

In de afgelopen eeuw zijn we ons in toenemende mate zorgen gaan maken over onze veiligheid, in allerlei domeinen en ten aanzien van allerlei risico's. Van gezondheid tot veiligheid op de weg, van het milieu tot oorlog, van de veiligheid van onze kinderen tot voedselveiligheid, en van terrorisme tot criminaliteit. En laten we veiligheid en cyberspace niet vergeten. We spreken zoveel over veiligheid dat men zou denken dat we permanent *onveilig* zijn. Nu is het niet eenvoudig om te kwantificeren of we tegenwoordig aan meer risico's blootstaan dan vroeger - laten we het erop houden dat we in de afgelopen eeuwen veel manieren hebben gevonden om onszelf beter te beschermen tegen de willekeurige gevaren die het leven met zich meebrengt, maar dat we tegelijk ook veel nieuwe dreigingen en gevaren gecreëerd hebben (cf. [65,66-69]). En dat we collectief minder tolerant geworden zijn voor gevaren en dreigingen[70], vooral wanneer we ze elimineerbaar achten.

Wat zijn de oorzaken van het feit dat veiligheid zo'n centraal thema is geworden? Hoe komt het dat we tegenwoordig zo veel over veiligheid praten? Een aantal factoren wordt vaak genoemd, waaronder de opkomst van globalisering[71-73], maar ook de opmars van moderne technologieën die het leven efficiënter en gemakkelijker maken, maar ook allerhande risico's in zich dragen, en afhankelijkheden creëren die er vroeger niet waren.[65,66,68,74] Ook de steeds groter worden complexiteit van systemen wordt als factor gezien[75-77], met meer en grotere risico's tot gevolg. Tot slot moeten we vaststellen dat we met de komst van nieuwe communicatie- en informatiemiddelen allemaal ook steeds meer kennis en besef van risico's hebben, waardoor zorgen om veiligheid wellicht ook toenemen.

Veiligheid als thema binnen de wetenschap

Gezien het feit dat veiligheid een centraal thema in de samenleving is geworden, is het niet verwonderlijk dat ook de wetenschap zich op dit thema heeft gestort. Twee wetenschaps-

gebieden hebben zich, elk op geheel eigen wijze gericht op vraagstukken rondom veiligheid.

Allereerst is daar het domein van de Safety Sciences, dat zich met name in de technische en gezondheidswetenschappen bevindt.[78-84] De Safety Sciences hebben veelal een engineering perspectief op veiligheid: zij houden zich bezig met vragen rondom het veilig maken van complexe systemen, zoals bijvoorbeeld ziekenhuizen, auto's, vliegtuigen of fabrieken, en richten zich met name op niet-intentionele of accidentele schade, bijvoorbeeld door menselijke fouten, door technisch falen of door natuurrampen.[75,85-90] Merk op dat in de Safety Sciences het woord '*safety*' centraal staat, wat duidt op de *bescherming van mensen* tegen allerlei vormen van *gevaar* (cf. [91]). In de Safety Sciences gaat het dus primair om de bescherming van mensen tegen accidentele schade.

Waar de Safety Sciences vooral in de technische en gezondheidswetenschappen thuishoren, is er binnen de sociale wetenschappen aandacht voor veiligheid binnen Security Studies.[58,92-99] Security Studies is een sub-domein van de politieke wetenschappen, ontstaan met de opkomst van de Koude Oorlog. Het richtte zich lange tijd met name op het bestuderen van internationale betrekkingen en het begrijpen van de internationale dynamiek tussen statelijke actoren rondom het behouden, of juist ondermijnen van veiligheid. In de afgelopen decennia is er binnen dit vakgebied gediscussieerd over de breedte van het onderzoeksveld. Nu wordt binnen Security Studies ook in toenemende mate onderzoek gedaan naar conflicten waarin niet-statelijke actoren betrokken zijn, naar terrorisme, en naar cybersecurity. Merk op dat bij de Safety Sciences het woord 'safety' centraal staat, terwijl dat bij Security Studies 'security' is. Dit betekent dat men in dit laatste wetenschapsgebied met name gericht is op het onderzoeken van manieren waarop nationale veiligheid in gevaar kan komen als gevolg van *intentionele* dreiging, zoals bijvoorbeeld door oorlog of conflicten, terrorisme etc. Security Studies richt zich niet zozeer op de bescherming van individuele mensen, maar op de bescherming van de *systemen* en instituties waarbinnen zij leven.

Wat is cybersecurity?
Nu we in kaart hebben gebracht wat veiligheid eigenlijk is en hoe het binnen de wetenschap bestudeerd wordt, kunnen we terug naar de vraag *wat is cybersecurity* eigenlijk? Hoe past *cybersecurity*, als veiligheidsvraagstuk binnen deze framing?

Cybersecurity past binnen deze framing op een aantal manieren. In de eerste plaats past de aandacht voor het onderwerp cybersecurity binnen de brede, sterk toegenomen interesse voor veiligheid in het algemeen. De aandacht voor cybersecurity valt te plaatsen in een tijd waarin mensen in toenemende mate bezig zijn met veiligheid en gevoelens van veiligheid, en waarbinnen de vraag vaak rijst of onze levens vandaag de dag nu meer of minder veilig zijn dan die van vorige generaties.

De aandacht voor cybersecurity past ook bij een aantal terechte zorgen, die we in abstracto al eerder tegenkwamen. We zijn steeds afhankelijker van allerlei complexe technologische systemen, die vanwege hun verwevenheid niet alleen kwetsbaar zijn, maar wanneer zij falen kan dit bovendien een grote, zo niet ontwrichtende impact hebben op ons alledaagse leven. Bovendien zijn er naast maatschappelijke risico's ook significante economische risico's voor bedrijven, organisaties en overheden. En tot slot leiden kwetsbaarheden in en van cyberspace tot reële risico's voor onze fysieke en ideële integriteit. Ik kom hier later nog op terug.

Dat er aandacht is voor cybersecurity is dus begrijpelijk. Maar wat te denken van het concept cybersecurity? Hoe past dit binnen de framing van de notie van veiligheid zoals we die bespraken? Wanneer we kijken naar de manier waarop cybersecurity geduid wordt, dan vallen drie zaken op. In de eerste plaats richt het onderzoek binnen dit domein zich tot op heden bijna zonder uitzondering op *intentionele dreigingen*, op aanvallen, inbraken, verstoringen, spionageactiviteiten en misbruik van systemen die bewust, willens en wetens zijn uitgevoerd door individuen, groepen, of statelijke actoren. In de tweede plaats valt op dat veel van het onderzoek zich richt op het in kaart brengen, kwantificeren en mitigeren van veilig-

heidsrisico's voor *systemen*, aan de infrastructuur van cyberspace, en de data die zich doorheen cyberspace beweegt. Het gaat hier vooralsnog overduidelijk niet (primair) om de bescherming van mensen. Tot slot valt de alomtegenwoordigheid van *risicomanagement* als benaderingswijze voor cybersecurity vraagstukken op. Dit heeft ongetwijfeld te maken met het feit dat cybersecurity haar wortels heeft in de technische wetenschappen, waar risicomanagement een gangbare methode is.

De vraag is nu: is deze conceptualisering, deze afbakening van cybersecurity als domein - gericht op de bescherming van *systemen* tegen *intentionele dreigingen* met *risicomanagement* als belangrijkste methode - de juiste? Zien we daarmee de volledige reikwijdte en impact van de cybersecurity vraagstukken die op ons afkomen? Zou een bredere conceptualisering helpen? En een aanvulling op de methodologische focus? In het laatste deel van deze oratie wil ik graag drie toevoegingen aandragen die het domein mijns inziens zouden verrijken en ons wetenschappelijk arsenaal voor dit vraagstuk zouden versterken: een *methodologische*, een *inhoudelijke* en een *conceptuele* verbreding.

Een nieuwe conceptualisering van cybersecurity
Laten we die drie zaken in volgorde langslopen.

Methodologische verbreding
In de eerste plaats is daar de kwestie van de gebruikte methode, de gereedschapskist waarmee we cybersecurityvraagstukken te lijf gaan. Zoals gezegd is dat op dit moment bijna zonder uitzondering de methode van risicomanagement. Dat is overigens niet alleen het geval binnen cybersecurity - risicomanagement is dè dominante methode geworden om om te gaan met risico's en onzekerheden, binnen bedrijven en organisaties, binnen de overheid, zelfs binnen de universiteit.[100] En dat is het met reden. Risicomanagement heeft ons, dankzij haar praktische benadering van het identificeren, kwantificeren, wegen, mitigeren en evalueren van risico's veel gebracht. Vliegtuigen en auto's zijn er veiliger door, we kunnen de risico's rondom de uitbraak van virale en bacteriële infecties er beter mee in kaart brengen, en het risico op industriële of natuurrampen kan er beter mee begrepen worden.

Maar er zitten ook tekortkomingen aan risicomanagement. Ik wil er twee in het bijzonder bespreken. In de eerste plaats werkt risicomanagement het best bij systemen met een beperkte complexiteit, waarbij we veel kennis hebben over mogelijke risico's en het hoe en waarom van hun optreden. Hoe groter de complexiteit van het systeem, des te meer onzekerheden en ruis er optreedt bij het identificeren, kwantificeren en vooral wegen van risico's. Voor het in kaart brengen en behandelen van risico's in cyberspace - een buitengewoon complex system - werpt dit de vraag op of risicomanagement altijd een geschikte methode is. Nu denk ik zeker dat risicomanagement grote merites heeft voor cybersecurity, omdat de wetenschappers die ermee werken binnen dit domein zich bewust zijn van de sterke kanten van risicomanagement, en ook weten waar de beperkingen zitten.

Echter, een tweede tekortkoming aan risicomanagement betreft niet zozeer de methode zelf, maar de wijze waarop de uitkomsten van risicomanagement inventarisaties door beslismakers worden gebruikt. Eén van de meest aantrekkelijke aspecten van risicomanagement is het feit dat het risico's kwantificeert; het geeft op basis van de kans dat een risico zich manifesteert en de impact die het dan zal hebben een indicatie van hoe ernstig risico's zijn. Daarmee worden risico's vergelijkbaar ten opzichte van elkaar. Dit stelt beslismakers in staat keuzes te maken over welke risico's onmiddellijk geadresseerd moeten worden - namelijk de grootste, welke genegeerd kunnen worden - namelijk de kleinste, en welke misschien later eens opgepakt moeten worden - alles er tussenin.

Een nadeel van dergelijke kwantificeringen is dat zij bij beslismakers de illusie kunnen oproepen dat de cijfers keihard zijn, terwijl dit, zeker bij complexe risicoanalyses zoals bijvoorbeeld vaak het geval is binnen de cybersecurity, niet zo is. Beslismakers zien de ruis en de onzekerheid rondom deze

getallen wellicht onvoldoende, en prioriteren dus op basis van ogenschijnlijk harde, objectieve cijfers, die in werkelijkheid de nodige marges in zich dragen.

Een bijkomend nadeel is dat cijfers dwingen, op de volgende wijze: wanneer de vermeend objectieve cijfers eenmaal bij de beslismaker op tafel liggen, is het ongelooflijk moeilijk nog een debat te voeren over *andere* informatie die wellicht relevant zou kunnen zijn voor het maken van een afgewogen besluit. De cijfers geven immers een ogenschijnlijk heldere richting aan. Maar beslissingen kunnen ook gemaakt worden op gronde van bijvoorbeeld een debat over waarden, en welke waarden ons het meest dierbaar zijn.

Juist waar het gaat om afwegingen ten aanzien van risico's is dit een belangrijk element binnen het instrumentarium voor beslismakers. Risico wordt vandaag de dag vaak op basis van kwantitatieve analyses afgewogen, de benaderingswijze die in belangrijke mate gestalte heeft gekregen in de Safety Sciences. Maar wat zouden de sociale en de geesteswetenschappen naast deze benaderingswijze kunnen bieden? In de sociale en geesteswetenschappen bestaan geheel andere conceptualiseringen van risico, die veel meer gericht zijn op een *kwalitatieve* duiding van dit begrip. Zij richten zich bijvoorbeeld op risicopercepties (cf. [57,70,101,102]), of de *politisering* van risico - de manier waarop risico's pas 'ontstaan' wanneer zij in politieke processen als zodanig worden geduid (cf. [11,94,103-105]).

We hebben gezien dat binnen de cybersecurity de methode van risicomanagement een centrale plaats inneemt. Mijns inziens zou dit domein er baat bij hebben wanneer we ook onderzoek zouden gaan doen naar risico's in cyberspace vanuit een meer kwalitatieve benaderingswijze. Bovendien zou het een verrijking zijn van de maatschappelijke en politiek-bestuurlijke discussies over cybersecurity wanneer wij deze niet alleen op basis van gekwantificeerde prioriteringen voeren, maar ook durven voeren op basis van kwalitatieve standpunten ten aanzien van fundamenteel botsende waarden, zoals bijvoorbeeld de spanning tussen transparantie en privacy, of die tussen veiligheid en vrijheid van meningsuiting.

Inhoudelijke verbreding

Naast een *methodologische* verbreding zie ik ook noodzaak tot een *inhoudelijke* verbreding. We zagen eerder dat het onderzoek over cybersecurity zich met name richt op de bescherming van *systemen* tegen *intentionele aanvallen*. Deze focus kan verklaard worden met een verwijzing naar de oorsprong van het veld. Cybersecurity begon als een technisch vraagstuk rondom het veilig maken van systemen en communicatie tegen inmenging van buitenaf. De focus op *intentionele* dreigingen voor *systemen* is blijven bestaan, terwijl de cybersecurity vraagstukken die op ons afkomen daar niet meer helemaal in passen.

In de eerste plaats moeten we niet alleen naar *intentionele dreigingen* kijken in cyberspace, maar ook naar *accidentele gevaren*, zoals bijvoorbeeld de gevolgen van menselijke fouten of systeemfouten. Gezien de toenemende complexiteit van technische systemen wordt de kans op dergelijke fouten met de jaren groter, en vanwege de verwevenheid van systemen neemt de potentiële impact ervan eveneens toe. We hebben allemaal nog vers in het geheugen wat de impact was van de storingen op Schiphol dit voorjaar. De economische en maatschappelijke schade daarvan is niet gering. Toch beschouwen we dergelijke storingen niet als een cybersecurityvraagstuk, maar als een issue voor de IT afdeling. Want er was geen sprake van een aanval maar van uitval. Een kunstmatig onderscheid, zo komt het mij voor. Het centrale punt hier is dat er schade was, veroorzaakt in, door, met behulp van computersystemen. Natuurlijk is het relevant te begrijpen wat de oorzaak daarvan is, en of er sprake is van intentioneel handelen of niet. Echter, tot op heden wordt accidentele schade, zoals de gevolgen van storingen, menselijke fouten of natuurrampen - wat we 'cyber safety' zouden kunnen noemen - bijna volledig uitgesloten als onderzoeksonderwerp binnen dit domein. Dat is zorgwekkend, omdat de consequenties van uitval even groot kunnen zijn als die door een aanval.

In de tweede plaats valt ook aan de exclusieve focus op *systemen* te tornen. Binnen cybersecurity hebben twee thema's in de afgelopen decennia veel aandacht gekregen: de bestrijding van cybercriminaliteit (cf. [106,107-110]) en de bescherming van kritieke infrastructuren (cf. [104,111,112]). Dat is begrijpelijk, want de economische en maatschappelijke impact van cybercriminaliteit is niet gering, en bovendien schaadt het het vertrouwen in cyberspace. Het beschermen van kritieke infrastructuren is belangrijk omdat dit de plek is waarop manipulaties in cyberspace gevolgen kunnen hebben in de fysieke werkelijkheid. Als aanvallers een dam hacken en de sluizen openzetten, kunnen overstromingen veel slachtoffers eisen. Wanneer aanvallers een elektriciteitscentrale stilleggen, kunnen de cascade effecten daarvan ook tot veel maatschappelijke, economische en fysieke schade leiden. Kortom, het bestrijden van cybercriminaliteit en het beschermen van kritieke infrastructuren zijn terechte aandachtspunten.

Bij deze aandachtspunten speelt het veilig maken en houden van *systemen* zoals we gezien hebben een belangrijke rol. Het cybersecurityonderzoek heeft zich in de afgelopen decennia dan ook vooral gericht op twee zaken: op aanvallen die gericht zijn op het verstoren, manipuleren of binnendringen *van* systemen[109,110], zoals bijvoorbeeld hacken, het verspreiden van malware en het plegen van DDoS aanvallen. En op criminele activiteiten *via* systemen[109,110], zoals bijvoorbeeld voor het plegen van diefstal, phishing of fraude. Merk op dat het in beide gevallen gaat om de bescherming van hard- en software, van de digitale infrastructuur waarop cyberspace drijft.

Maar in de afgelopen twee jaar zien we een nieuwe cyberdreiging van een geheel andere orde opkomen, die niet past binnen de huidige onderzoeksfocus, namelijk de opkomst van misinformatie en *fake news*. Met name de mogelijkheid om sociale media te gebruiken voor het beïnvloeden en manipuleren van meningen en ideeën is een zorgwekkende ontwikkeling. Hoe moeten we die ontwikkeling duiden? Is dit een cybersecurity vraagstuk, en zo ja, wat kunnen we ertegen doen? De maatregelen die we - met veel noeste arbeid en in de loop van meerdere decennia - binnen de cybersecurity hebben ontwikkeld, schieten hier tekort. Het gaat hierbij immers ineens niet meer om de bescherming van *systemen* maar om de bescherming van *ideeën* en *waarden*. Dat betekent dat we nieuwe vormen van bescherming moeten ontwikkelen voor de *contentlaag*, en niet voor de laag van hard- en software. Met de komst van misinformatie is de focus op hard- en software alleen te smal geworden. We zullen ons nu ook moeten buigen over *contentgerelateerde veiligheidsrisico's*.

Dat is overigens niet voor iedereen in het veld een evidente stap. Men zou kunnen stellen dat misinformatie als thema eerder bij buitenlandse inmenging in het algemeen hoort, en daarmee vooral een vraagstuk rondom internationale betrekkingen is, en niet zozeer een cybersecurity vraagstuk. Wellicht is het van belang het concept cybersecurity niet zo breed te definiëren dat ook contentgerelateerde risico's er onderdeel van worden - daarmee wordt het veld immers nog groter en moeilijker te bevatten dan het nu al is.

Toch zou ik een lans willen breken voor misinformatie als nieuw, extra kernthema binnen de cybersecurity. Binnen het onderzoek naar cybercrime zagen we een tiental jaren geleden een vergelijkbare discussie: welke vormen van criminaliteit moeten we nu wel en niet in de definitie van cybercrime opnemen? De beroemde cybercriminoloog David Wall stelde dat we criminele handelingen moeten kwalificeren als verschillende soorten cybercrime door antwoord te geven op de vraag of, en op welke manier, een misdrijf gepleegd had kunnen worden zonder computers en cyberspace. Fraude en diefstal zijn voorbeelden van misdrijven die we ook zonder cyberspace al kenden. Alleen stelen we via cyberspace andere dingen, en de modus operandi is anders dan bij offline diefstal of fraude. Hij noemt deze vormen van cybercrime *misdrijven met behulp van de computer*.[109,110] Hacken en het verspreiden van malware zijn alleen maar mogelijk dankzij het feit dat cyberspace bestaat. Voordat cyberspace er was, bestonden deze misdrijven

nog niet. Wall noemt dit *misdrijven tegen de computer*. Tot slot zijn er *contentgerelateerde misdrijven*, zoals bijvoorbeeld pesten en online geweld. Die zijn niet zozeer gericht tegen machines, maar tegen *mensen*. Ook dit zijn misdrijven die we al kenden voordat cyberspace er was. Maar de schaal en de impact ervan is met de komst van cyberspace wel veranderd.

Merk op dat de eerste twee typen misdrijven, die gericht *tegen* systemen en *via* systemen, nu de kern vormen van cybersecurityonderzoek. Maar Wall neemt contentgerelateerde misdrijven dus ook als formeel onderdeel op in zijn kwalificatie van cybercrime, die daarna de standaard is geworden. Als contentgerelateerde misdrijven wèl meegenomen worden binnen de cybercrime, waarom zouden we contentgerelateerde veiligheidsrisico's dan uitsluiten binnen het grotere veld van cybersecurity?

Men zou kunnen stellen dat misinformatie en *fake news* geen cybersecurityvraagstuk zijn, omdat zij al zo oud zijn als de mensheid. Informatiecampagnes zijn een veelgebruikt onderdeel van conflicten. We gooien al een eeuw lang folders uit vliegtuigen, en proberen burgers al zo lang als er oorlog is te beïnvloeden door het verspreiden van informatie. Maar de misinformatie die we nu zien is van een totaal andere orde. Cyberspace maakt het mogelijk dat statelijke actoren zich mengen in de democratische processen van andere landen op een schaal en met een reikwijdte die geen precedent kent. Via sociale netwerken hebben zij direct en op zeer onopvallende wijze toegang tot burgers in andere landen. Die burgers zijn, juist door het gebruik van het medium dat gekozen is, niet of niet voldoende in staat 'echte' van 'onechte' berichten te onderscheiden. Er zijn dus drie kwalitatieve verschillen tussen de hedendaagse misinformatie en folders uit een vliegtuig gooien: de schaal is vele malen groter, het bereik is vele malen groter, en door de keuze van het kanaal en het gebrek aan poortwachters op dat kanaal is het voor burgers niet langer mogelijk 'news' van 'fake news' te onderscheiden.
Daarom is misinformatie een contentgerelateerd veiligheidsrisico en moet het als cybersecurityvraagstuk worden opgepakt.

Naast de bescherming van kritieke infrastructuren en de bestrijding van cybercrime zou dit thema, gezien de urgentie ervan, een centrale plaats moeten krijgen. Het wordt tijd dat het onderzoek in cybersecurity zich verbreedt, zodat niet alleen systemen als dragers van risico in en via cyberspace worden gezien maar ook mensen. Misinformatie is het thema waarlangs die verbreding kan plaatsvinden.

Theorieontwikkeling
In deze oratie is duidelijk geworden dat cyberspace en cybersecurity beide brede en diffuse concepten zijn. Het is vaak nog onduidelijk wat we met deze concepten bedoelen, en waar de afbakeningen van het veld liggen. Op zichzelf is dit niet verwonderlijk. Cyberspace bestaat pas enkele decennia, en het kost tijd voor we grip krijgen op wat nieuwe fenomenen betekenen en hoe we ze moeten duiden. Toch zou ik er, als derde toevoeging aan het huidige onderzoeksdomein voor willen pleiten dat we meer gaan doen aan theorievorming en conceptuele ontwikkeling binnen het domein van cybersecurity. Tot op heden is dit een veld dat zich karakteriseert door veel toegepast, empirisch werk, met name vanuit een technische achtergrond. Empirisch werk vanuit sociaalwetenschappelijk perspectief blijft helaas achter. Ik hoop dat dit in de komende jaren bij zal trekken.

Wat ook achterblijft is het ontwikkelen van adequate theorieën. Zoals de wetenschapsfilosoof Scott Gordon opmerkt zijn zowel abstracte theorieën als empirische beschrijvingen essentieel voor de wetenschap. Theorieën zonder empirie zijn illusoir, maar empirie zonder theorie is nietszeggend.[114] Binnen het domein van cybersecurity is theorievorming een onderbelichte activiteit. We missen goede conceptualiseringen en afbakeningen. Waar gaat cybersecurity precies over? Welke actoren spelen een rol? Hoe kunnen we ze begrijpen? Wat is de impact van veiligheidsvraagstukken in cyberpace op onze politieke keuzes, op de economie, op onze vrijheden, rechten en plichten?
En daarmee keren we terug naar het begin van deze oratie.
Hoe kunnen we de transformatie die door de komst van cyber-

space geïnstigeerd is duiden? Kunnen we dat al, en kunnen we het afdoende?

Theorieën kunnen ons helpen een *voortschrijdende* duiding van cyberspace en cybersecurity te ontwikkelen, omdat de ontwikkelingen rondom cyberspace ons nopen voortdurend aan herconceptualisering te doen. Tien jaar geleden zagen we cyberspace anders dan we dat nu doen. Tijdens de industriële revolutie duurde het decennialang - zo niet een eeuw lang - voordat duidelijk werd wat de impact was van de transformatie die plaatsvond. Iets vergelijkbaars zal ook voor cyberspace gelden. Maar dat laat onverlet dat we onderwijl wel aan duiding moeten doen. Immers, we maken in het heden ontwerpkeuzes, we ontwikkelen beleid en maken wet- en regelgeving, die sturing bieden en richting geven aan de transformatie die we doormaken. Dat kan niet zonder conceptualisering, zonder theorievorming, zonder abstracte duiding van de impact van de ontwikkeling van cyberspace. Kritische reflectie op de ontwikkeling van en rondom cyberspace, alsmede op de governance en regelgevende systemen die we ten aanzien van cyberspace ontwikkelen, is daarom onontbeerlijk. Juist de sociale en de geesteswetenschappen dienen een rol te pakken naast de technische wetenschappen om die verbeterde conceptualisering te realiseren.

Met mijn pleidooi voor drie toevoegingen - een gevarieerdere methodologische aanpak, een inhoudelijke verbreding en een verdieping in concepten en theorieën - ben ik aan het einde gekomen van het inhoudelijke deel van deze oratie. Rest mij nog mijn grote dank uit te spreken in de richting van een aantal personen.

Dankwoord
Ik dank het College van Bestuur van de Universiteit Leiden en het bestuur van de Faculteit Governance & Global Affairs voor mijn aanstelling als hoogleraar, en voor het in mij gestelde vertrouwen. In het bijzonder dank ik Kutsal Yesilkagit en Edwin Bakker voor hun inspanningen rondom de totstandkoming van mijn leerstoel.

Zonder leermeesters had ik hier vandaag niet gestaan. In het bijzonder dank ik mijn promotoren Jos de Mul en Valerie Frissen, die mij op vreugdevolle wijze wegwijs maakten in de wetenschap. Ik dank Mireille Hildebrandt voor haar jarenlange rol als mentor en haar vriendschap. Ik heb veel geleerd van Ronald Leenes en Simone van der Hof bij respectievelijk TILT en eLaw. Dank voor de inspirerende samenwerking! En waar zou ik zijn zonder mijn leermeester Jan van den Berg? In elk geval niet in de cybersecurity. Dank daarvoor Jan!

Verder dank ik mijn collega's binnen de Faculteit Governance & Global Affairs, in het bijzonder de toppers Judi Mesman en Sandra Groeneveld. Ik geniet van onze sprankelende samenwerking. Dank ook aan Erwin Muller, onze aankomende decaan, voor de overstap naar Den Haag. Ik heb er zin in!

Het Institute of Security and Global Affairs is de allerleukste werkplek die er bestaat. Het is er altijd spannend - soms net iets te spannend. Ik voel me elke dag opnieuw gezegend met een fantastische groep - dank je wel Dennis, Els, Vlad, Sergei, Daan, Liisi, Ilina, Zine, Marco, Corianne en Tessa. En ik ben dankbaar voor alle geweldige collega's die me omringen in het instituut. Ik zal ze niet alle 85 opnoemen, maar een paar mensen wil ik wel met naam noemen. Dank je wel Antoaneta, Sanneke, Caroline, Marieke, Jelle, Jeanine, Willemijn, Pauline, andere Pauline, Ernst, Liesbeth en Constant. En een bijzonder woord van dank voor Noëlle en Barbara, die mijn baan en mijn hoofd op orde houden.

In de afgelopen jaren heb ik ook met veel plezier samengewerkt met verschillende mensen buiten de Universiteit Leiden. Dank aan de leden van de Cyber Security Raad en de Adviesraad ICT van het Centraal Bureau voor de Statistiek voor de inspirerende vergaderingen. Dank ook aan mijn contacten bij het Ministerie van Justitie en Veiligheid, bij het Ministerie van Buitenlandse Zaken en bij het Ministerie van Onderwijs voor het vertrouwen en de prettige samenwerking.

Een woord van dank aan de studenten die ik in de afgelopen jaren heb mogen lesgeven. Onderwijs geven is één van de leukste dingen die er bestaan en dat komt vooral door jullie. Dank ook aan alle leden van het team van de Bachelor Security Studies en aan dat van de Cybersecurity Academy.

En dan zijn er familie en vrienden. Dank aan mijn ouders, die hier vandaag zitten de glimmen op de eerste rij. Dank aan mijn zus, die er altijd voor me is. Dank aan mijn schoonfamilie, een warm bad, en wat ben ik trots dat mijn schoonvader meeloopt in het cortège. Dank daarvoor. Ik prijs me gelukkig met een warme kring van mensen om me heen. Drie vriendinnen fungeren als ankers in mijn leven. Sienneke, Esther en Ruth, dank voor jullie warmte, energie en wijsheid. En dan is daar mijn gezin: Jonna en Luus. Dank voor alles dat jullie me geven. Het leven is fantastisch met, en dankzij jullie.

Ik heb gezegd.

Referenties

1 P. Bairoch and G. Goertz, "Factors of urbanisation in the nineteenth century developed countries: A descriptive and econometric analysis", *Urban Studies,* vol. 23, pp. 285-305, 1986.

2 M. Crichton, *The great train robbery*. New York: Vintage Books, 1975.

3 J. De Mul, *Cyberspace Odyssee*, 2nd editio ed. Kampen (The Netherlands): Klement, 2003.

4 J. De Mul, "Filosofie in cyberspace: Een introductie", Kampen (The Netherlands): Klement, 2002, pp. 9-44.

5 D. Chandler, "Personal home pages and the construction of identities on the web", 1998.

6 P. Barlow, "A declaration of independence of cyberspace", *The Humanist,* vol. 56, no. 3, pp. 18-19, 1996.

7 D.R. Johnson and D. Post, "Law and borders: The rise of law in cyberspace", *Stanford Law Review,* vol. 48, pp. 1367-1402, 1996.

8 L. Floridi, "The onlife manifesto: Being human in a hyperconnected era" Cham, Heidelberg, New York, Dordrecht, London: Springer Open, 2015.

9 L. Kello, "The meaning of the cyber revolution: Perils to theory and statecraft", *International Security,* vol. 38, no. 2, pp. 7-40, 2013.

10 A. Liaropoulos, "A human-centric approach to cybersecurity: Securing the human in the era of cyberphobia", *Journal of Information Warfare,* vol. 14, no. 4 pp. 15-24, 2015.

11 T. Balzacq and M. Dunn Cavelty, "A theory of actor-network for cybersecurity", *European Journal of International Security,* vol. 1, no. 2, pp. 176-198, 2016.

12 I. Ben-Israel and L. Tabansky, "An Interdisciplinary Look at Security Challenges in the Information Age", *Military and Strategic Affairs,* vol. 3, no. 3, pp. 21-37, 2011.

13 D.-Y. Kim, "Cyber security issues imposed on nuclear power plants", *Annals of Nuclear Energy,* vol. 65, pp. 141-143, 2014.

14 E. Luiijf and K. Besseling, "Nineteen national cyber security strategies", *International Journal Critical Infrastructures,* vol. 9, no. ½, pp. 3-31, 2013.

15 M. Ciampa, *Security Awareness: Applying Practical Security in Your World*. 2013, pp. 304-304.

16 M. Felici, *Cyber security and privacy*. Berlin, Heidelberg: Springer, 2013, pp. 183-183.

17 M. Dunn Cavelty, "Cyber-security", Oxford University Press, 2012.

18 M. Hildebrandt, "Balance or trade-off? Online security technologies and fundamental rights", *Philosophy & Technology,* vol. 26, no. 4, pp. 357-379, 2013.

19 A. Appazov, "Legal aspects of cybersecurity", Copenhagen 2014, Available: http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf.

20 B. Schneier, *Secrets & lies: Digital security in a networked world*, 2 ed. Indianapolis (IN): Wiley Publishers, 2004.

21 L. Hansen and H. Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School", *International Security Studies Quarterly,* vol. 53, no. 4, pp. 1155-1175, 2009.

22 H. Nissenbaum, "Where computer security meets national security" *Ethics and Information Technology,* vol. 7, no. 2, pp. 61-73, 2005.

23 P.W. Singer and A. Friedman, *Cybersecurity and cyberwar: What everyone needs to know*. Oxford (UK): Oxford University Press, 2013.

24 B. Van den Berg and E. Keymolen, "Regulating security on the internet: Control vs. trust", *The International Review of Law, Computers & Technology,* no. 3, 2017.

25 D.J. Betz and T. Stevens, *Cyberspace and the state*. London (UK): Routledge, 2011.

26 D. Clark, T. Berson and H. S. Lin, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*. 2014, pp. 1-134.

27 R.A. Clarke and R.K. Knake, *Cyber war: The next threat to national security and what to do about it*. HarperCollins e-Books, 2010, pp. 304-304.

28 A. Liaropoulos, "Power and security in cyberspace: Implications for the Westphalian state system", in *Panorama of Global Security Environment*, M. Majer, R. Ondrejcsak, V.

Tarasovic and T. Valasek, eds. Bratislava, Slovakia: Centre for European and North American Affairs, 2011, pp. 541-548.
29 Kovacs, A., & Hawtin, D. Cyber security, cyber surveillance and online human rights. Stockholm: Stockholm Internet Forum on Internet Freedom for Global Development, 2013
30 J.R. Feick and R. Werle, "Regulation of Cyberspace", R. Baldwin, M. Cave and M. Lodge, eds. Oxford (UK); New York (NY): Oxford University Press, 2010, pp. 523-547.
31 L. DeNardis, "The emerging field of internet governance", 2010.
32 S.W. Brenner, "Law in an era of pervasive technology", *Widener Law Journal,* vol. 15, pp. 668-784, 2005.
33 S.W. Brenner, ""At light speed": Attribution and response to cybercrime/terrorism/warfare", *The Journal of Criminal Law and Criminology,* vol. 97, no. 2, pp. 379-476, 2007.
34 C. Czosseck, "State actors and their proxies in cyberspace", K. Ziolkowski, ed. Tallinn: NATO CCD COE, 2013, pp. 1-29.
35 C. Bennett and C. Raab, *The governance of privacy: Policy instruments in global perspective*. The MIT Press, 2006.
36 M. Hildebrandt, *De rechtsstaat in cyberspace?* Nijmegen, 2011.
37 M. Hildebrandt and K. De Vries, *Privacy, due process and the computational turn: The philosophy of law meets the philosophy of technology*. Abingdon (UK); New York (NY): Routledge, 2013.
38 J.M. Balkin, "The future of free expression in a digital age", *Pepperdine Law Review,* vol. 36, pp. 101-118, 2008.
39 J.A. Chandler, "A right to reach an audience: An approach to intermediary bias on the internet", *Hofstra Law Review,* vol. 35, no. 3, pp. 1095-1137, 2007.
40 R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain, *Access denied: The practice and policy of global Internet filtering*. Cambridge, Mass.: MIT Press, 2008.
41 R.J. Deibert and R. Rohozinski, "Liberation vs. Control: The Future of Cyberspace", *Journal of Democracy,* vol. 21, no. 4, pp. 43-57, 2010.
42 R.J. Deibert, R. Rohozinski and M. Crete-Nishihata, "Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war", *Security Dialogue,* vol. 43, no. 1, pp. 3-24, 2012.
43 R. Faris and N. Villeneuve, "Measuring global internet filtering", R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain, eds. Cambridge, Mass.: MIT Press, 2008, pp. 5-28.
44 J. Zittrain and J. Palfrey, "Internet filtering: The politics and mechanisms of control", R. Deibert, J. Palfrey, R. Rohozinski and J. Zittrain, eds. Cambridge, Mass.: MIT Press, 2008, pp. 29-57.
45 M. Hildebrandt and B. Van den Berg, *Information, Freedom and Property*. Abingdon (UK); New York (NY): Taylor & Francis Group, 2016.
46 T. Wu, "When code isn't law", *Virginia Law Review,* vol. 89, no. 4, pp. 679-751, 2003.
47 J. Chandler, "Privacy versus national security: Clarifying the trade-off", I.R. Kerr, C. Lucock and V. Steeves, eds. Oxford: Oxford University Press, 2009, pp. 121-138.
48 S. Landau, *Listening in: Cybersecurity in an insecure age*. New Haven; London: Yale University Press, 2017, pp. 1-221.
49 J. Brito and T. Watkins, "Loving the Cyber Bomb? The dangers of threat inflation in cybersecurity policy", *Harvard National Security Journal,* vol. 3, no. 1, pp. 39-84, 2011.
50 J.L. Goldsmith and T. Wu, *Who controls the Internet? Illusions of a borderless world*. New York: Oxford University Press, 2008, pp. xvi, 224.
51 M. Dunn Cavelty, "Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities", *Science and Engineering Ethics,* vol. 20, no. 3, pp. 701-715, 2014.
52 R. Anderson and T. Moore, "Information security: Where computer science, economics and psychology meet", *Philosophical Transactions of the Royal Society A,* vol. 367, pp. 2717-2727, 2009.

53 M.W. Boyce, K.M. Duma, L.J. Hettinger, T.B. Malone, D.P. Wilson and J. Lockett-Reynolds, "Human Performance in Cybersecurity: A Research Agenda", *Proceedings of the Human Factors and Ergonomics Society Annual Meeting,* vol. 55, no. 1, pp. 1115-1119, 2011.
54 R. Von Solms and J. Van Niekerk, "From information security to cyber security", *Computers and Security,* vol. 38, pp. 97-102, 2013.
55 D.D. Caputo, S.L. Pfleeger, J.D. Freeman and M.E. Johnson, "Going spear phishing: Exploring embedded training and awareness", *IEEE Security and Privacy,* vol. 12, no. 1, pp. 28-38, 2014.
56 S.L. Pfleeger and D.D. Caputo, "Leveraging behavioral science to mitigate cyber security risk", *Computers & Security Security,* vol. 31, no. 4, pp. 597-611, 2012.
57 B. Schneier, "The psychology of security", in *Progress in cryptology: AFRICACRYPT 2008 (First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14, 2008: Proceedings)*, S. Vaudenay, ed. no. 5023) Berlin ; New York: Springer, 2008, pp. 50-79.
58 D.A. Baldwin, "The concept of security", *Review of international studies,* vol. 23, no. 01, pp. 5-26, 1997.
59 P. Bourbeau, "A multidisciplinary dialogue on security", P. Bourbeau, ed. Cambridge (UK): Cambridge University Press, 2015, pp. 1-22.
60 J. Herington, "Philosophy: The concepts of security, fear, liberty, and the state", P. Bourbeau, ed. Cambridge (UK): Cambridge University Press, 2015, pp. 22-45.
61 W.B. Gallie, "Essentially Contested Concepts", *Proceedings of the Aristotelian Society,* vol. 56, pp. 167-198, 1956.
62 E. Rothschild, "What is Security?", *Daedalus,* vol. 124, no. 3, pp. 53-98, 1995.
63 J. Waldron, "Safety and security", *Nebraska Law Review,* vol. 85, no. 2, pp. 455-508, 2011.
64 S. John, "Security, knowledge and well-being", *Journal of Moral Philosophy,* pp. 68-91, 2011.
65 U. Beck, "Living in the world risk society", *Economy and Society,* vol. 35, no. 3, pp. 329-345, 2006.
66 U. Beck, "World at Risk: The New Task of Critical Theory", *Development and Society,* vol. 37, no. 1, pp. 1-22, 2008.
67 P.L. Bernstein, *Against the gods: The remarkable story of risk*. New York: John Wiley & Sons Inc., 1998.
68 A. Giddens, "Risk and responsibility", *The Modern Law Review,* vol. 62, no. 1, pp. 1-10, 1999.
69 D. Lupton, *Risk*, 2 ed. Abingdon (UK); New York (NY): Routledge, 2013, pp. vii, 266 p.-vii, 266 p.
70 P. Slovic, "Perception of risk", *Science,* vol. 236, no. 4799, pp. 280-285, 1987.
71 C.S. Browning and M. McDonald, "The future of critical security studies: ethics and the politics of security", *European Journal of International Relations,* vol. 19, no. 2, pp. 235-255, 2011.
72 A. Burke, K. Lee-koo and M. McDonald, "An ethics of global security", *Journal of Global Security Studies Advance,* vol. 1, no. 1, pp. 64-79, 2016.
73 K.T. Litfin, "Constructing environmental security and ecological interdependence", *Global Governance,* vol. 5, pp. 359-377, 1999.
74 R. Latham, *Bombs and bandwidth: The emerging relationship between information technology and security*. The New Press, 2003, pp. 326-326.
75 C. Perrow, *The next catastrophe: Reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton University Press, 2007.
76 C. Perrow, *Normal accidents: Living with high-risk technologies*. New York: Basic Books, 1984, pp. x, 386 p.
77 K.E. Weick, K.M. Sutcliffe and D. Obstfeld, "Organizing for High Reliability: Process of Collective Mindfulness", A. Boin, ed. London (UK): Sage Publications, 2008, pp. 31-66.
78 T. Aven, "What is safety science?", *Safety Science,* vol. 67, no. 0925, pp. 15-20, 2014.
79 M.D. Cooper, "Towards a model of Safety Culture", *Safety Science,* vol. 36, no. 1993, pp. 111-136, 2000.
80 E. Hollnagel, "Is safety a subject for science?", *Safety Science,* vol. 67, pp. 21-24, 2014.

81 A. Hopkins, "Issues in safety science", *Safety Science,* vol. 67, pp. 6-14, 2014.
82 R. Ilan and R. Fowler, "Brief history of patient safety culture and science", *Journal of Critical Care,* vol. 20, no. 1, pp. 2-5, 2005.
83 P. Swuste, C. Van Gulijk and W. Zwaard, "Safety metaphors and theories, a review of the occupational safety literature of the US, UK and The Netherlands, till the first part of the 20th century", *Safety Science,* vol. 48, no. 8, pp. 1000-1018, 2010.
84 P. Swuste, C. Van Gulijk, W. Zwaard and Y. Oostendorp, "Occupational safety theories, models and metaphors in the three decades since World War II, in the United States, Britain and the Netherlands: A literature review", *Safety Science,* vol. 62, pp. 16-27, 2014.
85 D. Alexander, *Confronting catastrophe: New perspectives on natural disasters*. New York: Oxford University Press, 2000, pp. vi, 282 p.
86 M.R. Lakshmi and V.D. Kumar, "Anthropogenic Hazard and Disaster Relief Operations: A Case Study of GAIL Pipeline Blaze in East Godavari of A.P", *Procedia - Social and Behavioral Sciences,* vol. 189, pp. 198-207, 2015.
87 M.F. Lechat, "Natural and man-made disasters", in *Oxford Textbook of Public Health*, vol. 1, W. W. Holland, Ed. Oxford: Oxford University Press, 1984.
88 B. Wisner, "Violent conflict, natural hazards and disaster", in *The Routledge Handbook of Hazards and Disaster Risk Reduction*, B. Wisner, J. Gaillard and I. Kelman, eds. Abingdon, New York: Routledge, 2012, pp. 71-82.
89 B. Wisner, J. Gaillard and I. Kelman, "The Routledge Handbook of Hazards and Disaster Risk Reduction." Abingdon, New York: Routledge, 2012.
90 B. Wisner, J. Gaillard and I. Kelman, "Framing disaster: Theories and stories seeking to understand hazards, vulnerability and risk", in *The Routledge Handbook of Hazards and Disaster Risk Reduction*, B. Wisner, J. Gaillard and I. Kelman, eds. Abingdon, New York: Routledge, 2012, pp. 18-34.
91 E.R. Muller, *Security, safety and criminal justice in the Netherlands: An organizational and legal perspective*. Deventer: Wolters Kluwer, 2012.
92 A. Wolfers, "'National Security' as an ambigious symbol", *Political Science Quarterly,* vol. 67, no. 4, pp. 481-502, 1952.
93 P. Bourbeau, *Security: Dialogue across disciplines*. Cambridge (UK): Cambridge University Press, 2015.
94 B. Buzan, O. Waever and J. D. Wilde, *Security: A new framework for analysis*. Boulder, London: Lynne Rienner Publishers, Inc., 1998, pp. 239-239.
95 M. Bourne, *Understanding security*. 2014, pp. 354-354.
96 A. Collins, *Contemporary Security Studies*, 3 ed. Oxford (UK): Oxford University Press, 2013, pp. 479-479.
97 R.H. Ullman, "Redefining security", *International Security,* vol. 8, no. 1, pp. 129-153, 1983.
98 B. Van den Berg and P. Hutten, "Security and safety", B. Van den Berg and J. Van den Berg, eds. The Hague: Asser Press, Forthcoming.
99 B. Van den Berg and R. Prins, "Security and safety: A conceptual analysis", *Safety Science,* Forthcoming.
100 M. Power, *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos, 2004.
101 R.E. Kasperson *et al.*, "The social amplification of risk: A conceptual framework", *Risk analysis,* vol. 8, no. 2, pp. 177-188, 1988.
102 P. Slovic, *The perception of risk*. Abingdon (UK); New York (NY): Earthscan/Taylor & Francis, Routlegde, 2000, pp. 473-473.
103 M. McDonald, "Securitization and the Construction of Security", *European Journal of International Relations,* vol. 14, no. 4, 2008.
104 C. Aradau, "Security that matters: Critical infrastructure and objects of protection", *Security Dialogue,* vol. 41, no. 5, pp. 491-514, 2010.
105 M. Dunn Cavelty, "From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse", *International Studies Review,* vol. 15, pp. 105-122, 2013.

106 S. Fafinski, W.H. Dutton and H. Margetts, "Mapping and measuring cybercrime", pp. 1-26Accessed on: 12 April 2018Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1694107
107 T.J. Holt and A.M. Bossler, "An assessment of the current state of cybercrime scholarship", *Deviant Behavior,* vol. 35, pp. 20-40, 2014.
108 R. Leukfeldt, "Research agenda: The human factor in cybercrime and cybersecurity." The Hague (The Netherlands): Eleven International Publishing, 2017.
109 D. S. Wall, "Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing", in *The Oxford Handbook on the Law and Regulation of Technology*, R. Brownsword, E. Scotford and K. Yeung, eds. Oxford: Oxford University Press, 2017.
110 D.S. Wall, "The Internet as a conduit for criminal activity", in *Information Technology and the Criminal Justice System*, A. Pattavina, ed. Thousand Oaks, CA (USA): Sage Publishers, 2015, pp. 77-98.
111 S.J. Collier and A. Lakoff, "The vulnerability of vital systems: How "critical infrastructure" became a security problem", M. Dunn and K.S. Kristensen, eds.: Routledge, 2007.
112 M. Dunn Cavelty and J. Giroux, "The good, the bad, and the sometimes ugly: Complexity as both threat and opportunity in the vital systems security discourse", in *World politics at the edge of chaos: Reflections on complexity and global life*, E. Kavalski, ed. Albany, NY: SUNY Press, 2013.
113 R.J. Deibert and R. Rohozinski, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology,* vol. 4, no. 1, pp. 15-32, 2010.
114 S. Gordon, *The history and philosophy of social science*. London, New York: Routledge, 1991.

Prof.dr. Bibi van den Berg (Tietjerksteradeel, 1975)

2017-heden	Hoogleraar Cybersecurity Governance, Institute of Security and Global Affairs (ISGA)
2015-2017	Associate Professor eLaw (Center for Law & Digital Technologies) & Institute of Security and Global Affairs (ISGA)
2015-heden	Lid Cyber Security Raad
2012-2015	Assistant Professor eLaw (Center for Law & Digital Technologies)
2009-2012	Postdoc Tilburg Institute for Law, Technology and Society (TILT), Tilburg University
2004-2009	Promotie Faculteit der Wijsbegeerte, Erasmus Universiteit Rotterdam
1999-2004	Doctoraal Algemene Wijsbegeerte, Erasmus Universiteit Rotterdam

Cybersecurity is een onderwerp dat in recente jaren veel aandacht heeft gekregen. Het kent technische uitdagingen, maar roept ook juridische, bestuurlijke, economische en maatschappelijke en ethische vragen op. Het wetenschappelijk onderzoek binnen de cybersecurity richt zich momenteel veelal op de bescherming van systemen tegen intentionele dreigingen, waarbij risicomanagement een veelgebruikt perspectief is.

In haar oratie pleit Van den Berg voor een verbreding van deze focus in vier opzichten. Ten eerste zou er naast intentionele dreigingen ook meer aandacht moeten komen voor accidentele gevaren, bijvoorbeeld ten gevolge van menselijke fouten of systeemfouten. Ten tweede zou de focus niet alleen moeten liggen op de bescherming van systemen, maar ook op de bescherming van informatie, van de contentlaag. De opkomst van misinformatie en *fake news* tonen de urgentie van het ontwikkelen van dergelijke bescherming aan. Ten derde zou het onderzoek in de cybersecurity methodologisch verrijkt kunnen worden door naast risicomanagement ook gebruik te maken van sociaalwetenschappelijke en geesteswetenschappelijke perspectieven op risico. En tot slot zijn conceptuele helderheid en theorievorming voor dit jonge vakgebied van groot belang. Met de leerstoel Cybersecurity Governance hoopt Van den Berg aan alle vier deze thema's een bijdrage te kunnen leveren.

Universiteit Leiden