Prof.dr. Bibi van den Berg en prof.dr. Aske Plaat

Vertrouwd verbonden:
Over een veilige informatiemaatschappij

Universiteit
Leiden

Bij ons leer je de wereld kennen

Vertrouwd verbonden:
Over een veilige informatiemaatschappij

Diesoratie uitgesproken door

Prof.dr. Bibi van den Berg

Hoogleraar Cybersecurity Governance

en

prof.dr. Aske Plaat

Hoogleraar Data Science

tijdens de 445ste dies natalis

op vrijdag 7 februari 2020 in de Pieterskerk.

Universiteit
Leiden

Plaat: Mijnheer de rector magnificus, dank voor uw introductie.
Zeer geachte toehoorders,

Het Nederlands heeft er een nieuw woord bij: Citrixfile. Een Citrixfile ontstaat wanneer mensen op maandagochtend *en masse* naar hun werk gaan, omdat de software waarmee ze vanuit huis via het internet kunnen werken preventief is uitgezet. Vorige week maandag werd op Twitter gesproken over gezellig in de file staan. Gelukkig maar, dat relativerend vermogen. Want we krijgen het wel voor onze kiezen: eerst de ransomware aanval op de Universiteit Maastricht van rond de kerst, en vervolgens dit weer.

Het onderwerp van deze diesrede is, dat heeft u gehoord, cybersecurity. Nu is het op zich best leuk als het onderwerp van een diesrede actueel is, maar dit is wel wat veel van het goede.

Cybersecurity is de laatste jaren een veelbesproken onderwerp geworden. Tot recent was het voor veel van ons een ver-van-mijn-bed show. Dankzij de kwetsbaarheden in Citrix en de steeds frequentere ransomware-aanvallen op bedrijven, ziekenhuizen en universiteiten wordt cybersecurity nu voor ons allemaal een concreet begrip dat raakt aan onze eigen leef- en werkpraktijk. Cybersecurity is één van de grote uitdagingen van deze tijd, en zal in de nabije toekomst alleen maar aan urgentie winnen.

Van de industriële naar de informatiemaatschappij
De wereld waarin we leven wordt meer en meer beheerst door techniek. Onze honger naar kennis en onze drang naar begrijpen, drijven onze economische groei en vergroten onze welvaart. Na de industriële revolutie heeft er een informatierevolutie plaatsgevonden: onze maatschappij is een informatiemaatschappij geworden en steeds grotere delen van de dingen die we elke dag doen worden mogelijk gemaakt of ondersteund door digitale, genetwerkte technologie.

Computers regelen de liftbediening, de verwarming, onze pacemakers, maken schoolroosters, bepalen filmkeuzes, regelen welke advertenties we zien, welke nieuwsberichten, ze helpen ons communiceren met onze vrienden, helpen bij onze partnerkeuze, en ze helpen ziektes op te sporen en medicijnen te ontwikkelen. Zaken van leven en dood worden in toenemende mate door zelfredenerende systemen beslist.

In de dertig jaar dat het internet gemeengoed is geworden, wordt veel van ons moderne leven beïnvloed door de online wereld. Deze vercyberisering voltrekt zich omdat we, als we de keus hebben, steevast een digitaal alternatief kiezen dat makkelijker, beter, of goedkoper is, en zo bijdraagt aan economische groei, aan onze welvaart, en aan ons levensgeluk.

Soms denken we met enige melancholie terug aan een oudere, rustiger tijd, waarin we niet constant met onze telefoon bezig waren, en waarin mensen nog echt aandacht voor elkaar hadden. En vervolgens schrijven we daar een mooie blogpost over die hopelijk veel likes oplevert. En, als we echt te lang op onze telefoon zitten en we willen onze schermtijd beperken, dan installeren we daar toch een app voor?

Wat we er ook van vinden, onze maatschappij zit vol techniek. Maar wat nu als die techniek niet meer werkt, of door criminelen misbruikt wordt?

Een kenmerk van veiligheid is dat we ons pas bewust worden van het belang ervan als zij onder druk staat. In de fysieke wereld kunnen we gevaar waarnemen met onze zintuigen, in de digitale wereld is dat lastiger. Vuur kunnen we zien en voelen, door de lucht vliegende bits niet. In cyberspace weten we vaak niet eens wanneer de veiligheid onder druk staat.

Wat is cybersecurity?
Cybersecurity draait om het veilig maken en veilig houden van gegevens, netwerken en systemen. Uitval en aanvallen van buitenaf, moeten zo min mogelijk voorkomen en de eventuele

gevolgen moeten geminimaliseerd worden. Cybersecurity is een relatief nieuw fenomeen, dat pas is ontstaan na de Tweede Wereldoorlog, en een vlucht nam met de digitalisering van de maatschappij. Helaas is deze digitalisering ook niet onopgemerkt gebleven bij mensen met weinig nobele bedoelingen. Het aantal cyberaanvallen is groot, er is een wapenwedloop tussen de knapste koppen aan de gang, het is big business. De schade als gevolg van cyberaanvallen werd in 2019 tussen de 2 en 4 biljoen dollar geschat (door respectievelijk Juniper Research en Cyber Security Ventures). Dat zijn grote bedragen, het betekent een geschatte schade van tussen de 2 en 4 procent van het wereldwijde bruto product. De schade in Nederland voor 2017 werd door Deloitte op tien miljard euro geschat, tien keer zoveel als de schade veroorzaakt door 'gewone' criminaliteit. De gevolgen van cybercrime zijn dus heel omvangrijk. Als een Nederlandse universiteit geraakt wordt, en nog wel vlak voor de tentamenperiode, komt het opeens heel dichtbij, en hebben ook de mensen van ons eigen ICT Shared Service Centrum een heel drukke kerst. En als u daarna niet meer thuis kunt werken omdat Citrix ontkoppeld is, dan merkt u pas echt in welke mate veiligheid als thema tot in de haarvaten van het internet is doorgedrongen.

Maar ook in uw privésfeer duiken cybersecurity-incidenten steeds vaker op. Hoe afhankelijk onze maatschappij van netwerktechnologie is geworden, merken we ook wanneer op Tweede Pinksterdag het pin-systeem van de Albert Heijn uitvalt, wanneer democratische verkiezingen door een buitenlandse mogendheid gemanipuleerd worden, of wanneer 112 uitvalt. Cybersecurity is in de meest letterlijke zin een zaak van leven en dood.

Een multidisciplinair vraagstuk

Cybersecurity combineert twee vakgebieden, de informatica en de veiligheidswetenschap, de vakgebieden van collega Van den Berg en van mijzelf. Cybersecurity gaat in technische zin over vertrouwelijkheid, integriteit en beschikbaarheid of, in het Engels, confidentiality, integrity, en availability, kortweg CIA.

Maar cybersecurity is meer dan alleen een technisch vraagstuk. Het vraagt om een aanpak die zowel technische oplossingen biedt, alsook inzicht in de maatschappelijke, juridische, organisatorische en ethische aspecten van ons gebruik van het internet. Alleen wanneer we een multidisciplinaire blik op dit probleem hebben, valt het in zijn volle rijkdom te begrijpen. Dus is het van belang te kijken naar de beveiliging van systemen, netwerken en data, maar ook naar de rol van mensen, organisaties, politiek, overheid en recht. Precies deze multidisciplinaire aanpak staat centraal in onze Executive Master Cyber Security, waarin onze twee instituten, het Leiden Institute of Advanced Computer Science en het Institute of Security and Global Affairs, samenwerken met de TU Delft en de Haagse Hogeschool.

Technische aspecten van cybersecurity

Om het heden te begrijpen, helpt het vaak om naar het verleden te kijken. Dat geldt ook voor cybersecurity. Want geheimen zijn zo oud als de mensheid, en geheimschrift of cryptografie is zo oud als het schrift. Het oudst bekende geheimschrift komt uit Egypte en dateert uit 1900 voor het begin van onze jaartelling. We weten ook dat de oude Grieken, en de volken in India en Perzië, geheime informatie beveiligden met cryptografie. Men gebruikte onder meer verschuivings- en substitutie methoden. Met deze oude technologie ging nog wel eens iets mis. Sleutels werden gekopieerd, berichten werden onderschept, codes werden gebroken, en kluizen werden gekraakt.

Met de komst van de computer hebben cryptografische principes vleugels gekregen, en met de komst van de zogeheten public-key-methoden hebben we codes gekregen die onbreekbaar zijn voor huidige computers. (En voor het geval huidige methodes door quantumcomputers gebroken kunnen worden doet men nu al onderzoek naar zogeheten post-quantum cryptografie.)

De wiskunde van versleutelmethodes wordt steeds verder geperfectioneerd, en de mogelijkheden om fouten uit software

te halen worden steeds beter, iets waar we ook in Leiden aan bijdragen. Met moderne technologie kunnen we nu veel meer gegevens opslaan en versturen, en we kunnen die ook veel beter beveiligen.

Waarom is cybersecurity dan toch een van de grote vraagstukken van onze informatiemaatschappij? Waarom gaat er dan toch zoveel fout in de praktijk, en kunnen we daar iets aan doen?

Over die vraag willen we u graag iets meer vertellen, en collega Van den Berg neemt u graag mee.

Van den Berg: Techniek heeft inderdaad een steeds belangrijkere rol in ons moderne bestaan. We koppelen alles, maar dan ook alles, aan het internet. Collega Plaat noemde al een reeks van activiteiten die we tegenwoordig in en via cyberspace uitvoeren, van betalen en het delen van persoonlijke informatie via sociale media tot het doen van aankopen en het lezen van boeken. Ook op een hoger maatschappelijk niveau zien we steeds meer verwevenheid tussen de fysieke werkelijkheid en cyberspace. Kritieke infrastructuren worden zo genoemd omdat ze kritiek zijn voor het functioneren van de samenleving. Hun uitval kan leiden tot maatschappelijke ontwrichting. Steeds meer kritieke infrastructuren hangen tegenwoordig aan het internet. Denk aan ziekenhuizen die patiëntgegevens massaal gedigitaliseerd hebben in een patiëntendossier en in toenemende mate medische apparatuur, of soms zelfs de hele operatiekamer, aan het internet koppelen. Of denk aan Schiphol, waar alle procedures, van het inchecken van je koffer en het verwerken van je ticket tot de logistieke afwikkeling van de bagage en de grenscontrole bij de douane, allemaal verlopen via digitale, genetwerkte technologie. Of denk aan Rijkswaterstaat, dat in de afgelopen decennia alle bruggen, alle waterkeringen, en alle waterwerken van Nederland aan het internet heeft gekoppeld, opdat ze op afstand bedienbaar werden. Onder het motto van efficiëntie is nagenoeg de hele kritieke infrastructuur van Nederland, van zorg tot verkeer, en van financiën tot energie, aan cyberspace gekoppeld.

Maar als de dijkbewaker van Rijkswaterstaat een kering op afstand kan openen of sluiten dankzij de koppeling aan cyberspace, dan kan een hacker dat ook. En dan leidt een digitale kwetsbaarheid ineens potentieel tot fysieke schade (lees: mogelijk zelfs doden) in de offline wereld. Dat is de grootste zorg die overheden hebben op het terrein van cybersecurity. En merk op: het is niet alleen de hacker die een overstroming kan veroorzaken, ook een systeemfout of een menselijke fout kan dat. Of schade ontstaat door een bewuste aanval of door uitval van de systemen waar we afhankelijk van zijn geworden is niet zo belangrijk op het moment van een incident. Het gaat erom dat cyberspace, als ruggengraat van zo veel van de systemen waarvan we afhankelijk zijn, zélf feitelijk ook een kritieke infrastructuur is geworden.

Vier risicogebieden

Rap voortschrijdende digitalisering heeft geleid tot risico's die we nu pas langzaam maar zeker beginnen te overzien. Hoe kunnen we die risico's adresseren? En waar moeten we ons het meeste zorgen om maken?

We bespreken een viertal thema's.

In de eerste plaats zijn er zorgen over de bescherming van kritieke infrastructuren. Die draaien vaak op grote, infrastructurele technologie die speciaal gemaakt is voor een specifiek complex, bijvoorbeeld voor een hele fabriek. Die systemen zijn vaak gebouwd in de jaren '60 en '70 van de vorige eeuw, en nooit ontworpen met internetconnectiviteit voor ogen. Nu ze aan cyberspace gekoppeld worden, is één van de zorgen dat er allerlei kwetsbaarheden in zitten die kwaadwillenden kunnen uitbuiten. Dus moet met terugwerkende kracht de beveiliging van deze cruciale technologieën op orde gebracht worden.

Een tweede thema is cybercrime. Al vrij snel na het opkomen van het internet ontdekten criminelen dat cyberspace zich uitstekend leent voor criminele activiteiten. De anonimiteit en het grensoverschrijdende karakter van cyberspace zorgen ervoor

dat criminelen met een lagere pakkans een grotere groep potentiële slachtoffers kunnen bereiken. Naast klassieke vormen van criminaliteit die we al kenden in de offline wereld, zoals bijvoorbeeld fraude en het delen van kinderpornografisch materiaal, hebben we dankzij de komst van cyberspace ook allerlei nieuwe misdrijven op moeten nemen in het Wetboek van strafrecht. Denk aan hacken en het plegen van DDoS aanvallen. Zonder genetwerkte computers bestaan deze misdrijven niet, nu helaas wel.

Een derde zorg is die omtrent desinformatie en fake news. Na de presidentiële verkiezingen in de VS in 2016 en het Brexit-referendum in datzelfde jaar bleek dat we ons niet alleen zorgen moeten maken om de integriteit van *data* in cyberspace, maar ook om het manipuleren van *informatie*. Deze twee gebeurtenissen lieten zien dat statelijke actoren cyberspace in toenemende mate gebruiken om te interfereren in andere landen. Zorgen over beïnvloeding en de ondermijning van democratische processen of zelfs vrijheid van informatie, nemen daarmee hand over hand toe. De opkomst van Artificial Intelligence, en daarmee van nieuwe technologische mogelijkheden zoals 'deep fakes' past in dit thema: het wordt in toenemende mate ingewikkeld om vast te stellen of informatie echt is of niet, en waar is of niet.

En tot slot zijn er zorgen rondom de opkomst van het Internet der Dingen. Als we in de nabije toekomst alledaagse objecten steeds vaker van internetconnectiviteit gaan voorzien, dan heeft dit grote voordelen (weer die efficiëntie, en gebruiksgemak) maar ook de nodige risico's. We hangen onze fietsen, ons koffiezetapparaat, het speelgoed van onze kinderen, en onze televisies en stofzuigrobots massaal aan het internet. Daarmee komt onze privacy verder onder druk te staan, omdat steeds meer data uit onze persoonlijke levenssfeer letterlijk op straat belanden. Bovendien worden al die apparaten toegangspunten voor kwaadwillenden, die een sterk toenemende 'attack surface' krijgen.

Grote incidenten blijven uit

Onderwijl schrijdt de digitalisering voort. Wonderlijk genoeg blijven echt ontwrichtende incidenten uit. We zien af en toe een grote hack. Denk bijvoorbeeld aan de Sony-hack van 2014, waarbij gegevens van medewerkers van Sony Pictures werden gelekt en een groot gedeelte van de systemen van dit bedrijf werden gewist na het uitbrengen van een komische film over de Noord-Koreaanse leider Kim Jong-un. Of denk aan de al genoemde aanval met ransomware op de Universiteit van Maastricht van vorige maand, die de hele universiteit wekenlang platlegde. In een enkel geval ontstaat er discussie over de vraag wanneer een aanval met malware telt als 'digitaal wapen' en er dus sprake zou zijn van een 'oorlogshandeling' (of niet). Een voorbeeld daarvan is het Stuxnet incident in 2010, waarbij een Iraanse nucleaire faciliteit werd beschadigd met malware. En soms gaan aanvallen door statelijke actoren mis en zijn er wereldwijde cascade-effecten. Dit was bijvoorbeeld het geval met de NotPetya-aanval in 2017. Die aanval werd gepleegd door Rusland en was gericht op Oekraïne, maar verspreidde zich al snel als een uitslaande brand over de hele wereld. Grote bedrijven zoals de Maersk Shipping Company werden er door lamgelegd en de schade liep op tot 10 miljard US dollar. Soms schrikken we even op door een enorm groot datalek, zoals dat van de hotelketen Marriott in 2017, waarbij de gegevens van ongeveer vijfhonderd miljoen mensen werden gestolen. Maar door de bank genomen blijven experts zeggen dat de risico's groot zijn, blijven overheden zich grote zorgen maken, en draait de wereld ondertussen rustig verder. Ook de Citrixfile heeft daarin gelukkig geen verandering gebracht.

Hoe moeten we dat cybersecurity vraagstuk dan duiden? En vooral: wat kunnen we doen om cyberspace veilig te maken en te houden?

Plaat: De wereld draait rustig verder, ja, grote catastrofes zijn uitgebleven, maar wel ten koste van naar schatting 4 biljoen dollar per jaar. We horen over het risico van virussen, ransomware, en diefstal van data. De ene na de andere

kwetsbaarheid wordt ontdekt, met angstaanjagende namen als Heartbleed en Spectre. Criminelen zijn ook heel bedreven in social engineering, en phishing mails zijn moeilijk van legitieme mails te onderscheiden. In een recente test aan een Nederlandse universiteit bleek maar liefst 20% van de medewerkers op de link van een nep-phishing mail te klikken.[1]

De vraag die collega Van den Berg stelde intrigeert daarom: als alle computers fundamenteel afgeluisterd en aangevallen kunnen worden, als mensen te manipuleren zijn, waarom hebben we dan tot nog toe toch zo weinig over geslaagde aanvallen gehoord, en doet onze kritieke infrastructuur het nog steeds? Zijn er dan misschien toch geen aanvallen geweest? Voor de beantwoording van deze vragen kijken we naar drie redenen waarom grote cybersecurity-incidenten tot op heden uitgebleven zijn: de techniek, maatschappelijke tegenkrachten, en vereiste kennis.

Gesegmenteerde netwerken

Een eerste reden waarom ontwrichtende incidenten uitblijven, is technisch van aard. Het falen van het ene systeem leidt in de praktijk maar zelden tot kettingreacties omdat de meeste systemen heterogeen zijn, en slechts losjes met elkaar zijn verbonden. Computers kunnen elkaar wel bereiken (dankzij het internet) maar bedrijfskritische toepassingssystemen zelf zijn vaak niet zo innig gekoppeld dat, als er een stopt, de andere er ook mee ophouden. Laten we als voorbeeld een elektriciteitscentrale nemen, met verscheidene generatoren en een distributiesysteem. De generatorsystemen en het distributiesysteem zijn zo ontworpen dat ze onafhankelijk van elkaar kunnen werken. Tussen de systemen zit vaak ook nog een menselijke operator die kan ingrijpen. Bij uitval van een generator kan de rest van de centrale doordraaien.

De analogie met een griepepidemie gaat hier op. Een ziekte zal minder snel verspreiden in een populatie naarmate (1) de resistentie van individuen groter is, (2) naarmate ze minder met elkaar in contact zijn, en (3) naarmate de populatie heterogener is. De diversiteit vergroot de resistentie van de populatie, en zal verspreiding afremmen, zoals onderzoek naar complexe netwerken ons ook leert. In de financiële markten hebben we meerdere keren gezien dat het blind vervangen van menselijke tussenpersonen in een homogene omgeving kan leiden tot een kettingreactie. Hier moeten we van leren bij het ontwerpen van onze digitale, genetwerkte systemen.

Diversiteit van systemen, zoals een mix van verschillende versies van Windows, Linux, en Mac, is een voordeel: het maakt dat uitval van één systeem nog niet leidt tot de uitval van alle andere aangesloten systemen. Bij het ontwerpen van systemen moeten we de verleiding weerstaan om alles gelijk te trekken en om alles direct aan elkaar te koppelen zonder tussenpersoon of intelligente firewall, ook al is dat efficiënter en overzichtelijker. We moeten juist van een veelheid van losse systemen uitgaan, we moeten toegangsrechten segmenteren, en we moeten gebruik maken van tussenpersonen of interfaces. Diversiteit maakt systemen soms minder efficiënt, maar wel een stuk robuuster.

Maatschappelijke respons

Een tweede reden waarom we weinig grootschalige cyberrampen zien, is dat overheden en instanties zich zorgen maken en maatregelen nemen. En dat helpt. Onze kritieke infrastructuur is door de bank genomen beter beveiligd dan die van het midden- en kleinbedrijf of die van individuen. In Nederland is er een Nationaal Cyber Security Centrum, er wordt redelijk geluisterd naar adviezen van de Cyber Security Raad (waar Collega Van den Berg overigens deel van uitmaakt) en er is een nationale Cyber Security Agenda. Overheden, energiebedrijven, telecombedrijven, de financiële sector en grote technologiebedrijven zijn zich bewust van hun maatschappelijke rol en de gevolgen van reputatieschade, en besteden veel tijd en energie om hun systemen goed te beveiligen. Ze hebben deskundigen in dienst die op de hoogte zijn van de laatste ontwikkelingen.

1 https://www.erasmusmagazine.nl/2019/01/24/een-op-de-vijf-medewerkers-trapte-in-mail-virus/

Die ontwikkelingen op cybersecurity gebied gaan snel, aanvallers en verdedigers zijn bijvoorbeeld kunstmatige intelligentie aan het toepassen voor gedragsbeïnvloeding, en collega Van den Berg noemde de *deep fakes* ook al. Kunstmatige intelligentie kan ook gebruikt worden om systemen te beveiligen, bijvoorbeeld met zelflerende firewalls die beter in staat zijn om netwerken af te schermen. Ook vanuit het oogpunt van cybersecurity is het daarom van groot belang dat we ons onderzoek naar kunstmatige intelligentie intensiveren. We zijn dan ook heel blij met de recent in de Delftse dies aangekondigde plannen van de universiteiten en medische centra van Leiden-Delft-Erasmus, waarin een uitgebreide samenwerking van onderwijs en onderzoek in en met kunstmatige intelligentie wordt aangekondigd.

Technische kennis

Een laatste reden waarom grootschalige incidenten tot op heden uitblijven, is het feit dat cyberaanvallen een bepaalde mate van technische kennis vereisen, hoewel het steeds gemakkelijker wordt om malware en exploit kits te kopen. Wanneer criminelen of terroristen er op uit zijn om zo veel mogelijk impact te genereren met zo min mogelijk moeite, dan ligt het soms voor de hand om digitale middelen links te laten liggen vanwege de technische kennis die zij vereisen. Kennis werkt dus vooralsnog als een barrière voor grootschalige, ontwrichtende incidenten.

Helaas is niet voor alle ontwrichtende incidenten technische kennis vereist, want ook fake news en desinformatie kunnen ontwrichtend werken, zoals we hebben gezien bij de uitkomst van het Brexit-referendum en de verkiezingen in de VS. Iedereen kan via social media eenvoudig valse berichten de wereld in sturen, en als die maar slim genoeg in het vat gegoten worden, zorgt de kracht van het netwerk er bijna vanzelf voor dat ze een groot publiek bereiken. Social media-propaganda doet eerder een beroep op sociale kennis dan op technische kennis.

Aan onze eigen universiteit wordt op verschillende plekken onderzoek gedaan naar propaganda in cyberspace. Zo doet nieuwscheckers.nl factchecking van nieuws en social media, doen verschillende groepen onderzoek naar juridische, bestuurlijke en netwerkaspecten van propaganda, en wordt dit jaar in Leiden de tweede MISDOOM-conferentie georganiseerd, het Multidisciplinary International Symposium on Disinformation in Open Online Media. En dit soort onderzoek komt geen moment te vroeg.

De zwakste schakel

Kwaadwillenden zoeken naar de meest lucratieve plek om hun slag te slaan, en zijn op zoek naar de zwakste schakel. Banken en financiële instellingen zijn traditioneel goed beveiligd, en dat geldt ook voor hun cybersecurity. Het is dan ook niet verwonderlijk dat cybercrime zich vaak richt op sectoren die minder goed beveiligd zijn. Dat zijn bijvoorbeeld individuele mensen, ook al is bij ons vaak weer minder te halen. Het is voor een cybercrimineel aantrekkelijk zich te richten op sectoren waar meer te halen is, maar die toch ook minder goed beveiligd zijn, zoals het MKB, ziekenhuizen, en, zoals we onlangs hebben gezien, universiteiten.

Het voorgaande laat zien welke afwegingen kwaadwillenden maken wanneer ze in, of via, cyberspace aanvallen willen plegen. Ten eerste is het namelijk makkelijker en effectiever om een maatschappij te ontwrichten via cyber-propaganda dan goed beveiligde elektriciteitscentrales proberen uit te schakelen. En ten tweede is cybercrime lucratiever wanneer deze zich richt op slecht beveiligde bedrijven, universiteiten en individuen, dan te proberen een goed beveiligde bank binnen te komen.

Wat kunnen we met deze wetenschap? Als universiteit is onze rol het vergroten van kennis en het stimuleren van het maatschappelijke debat. Als wij allen het doelwit geworden zijn van propaganda en cybercrime, dan ligt daar voor ons een maatschappelijke taak. Cybersecurity moet een onderdeel worden van digital skills-onderwijs. Om te begrijpen hoe de digitale wereld werkt, zijn zaken als computational thinking en digitale weerbaarheid essentiële 21st century skills. Universiteiten pleiten hier al jaren voor, en de overheid neemt haar rol nu

in de digitaliseringsagenda primair en voortgezet onderwijs. Of dit voldoende is? Naar mijn idee is er nog een hele weg te gaan met de modernisering van curricula in ons onderwijs en aan onze universiteiten. De LDE-samenwerking op het gebied van kunstmatige intelligentie is een heel goede stap die ik zeer toejuich. Nu kan computational thinking nog een enkel apart vak zijn, spoedig zal deze manier van denken een integraal onderdeel van vele vakken en curricula worden.

Naast digital skills is er natuurlijk een grote behoefte aan gespecialiseerde opleidingen op het terrein van digitalisering, kunstmatige intelligentie en cybersecurity. We noemden eerder al onze eigen Executive Master Cyber Security als mooi voorbeeld daarvan.

Uw Digitale Weerbaarheid
We zien dat cybercrime steeds meer een probleem wordt voor individuen en kleine bedrijven, en dat bewustwording en het vergroten van kennis hard nodig zijn. Daarom, aan het einde van mijn deel, een lesje digitale weerbaarheid, speciaal voor u, om uw cyberweerbaarheid te vergroten. Daar gaan we.

Krijgt u emails van uw bank (of van uw rector) met het verzoek om op een link te klikken, doe het dan niet. Ziet u een bijzonder fantastisch aanbod op marktplaats of krijgt u een verzoek om geld over te maken via SMS, doe het dan niet. Leest u een bericht op Instagram, Twitter, of Facebook dat precies bevestigt wat u zelf ook al dacht? Trap niet in uw bubble, blijf kritisch. Stop geen USB-sticks van onbekenden in uw computer (en liever ook niet die van bekenden. Wie weet wat ze ermee gedaan hebben). Surf via beveiligde verbindingen, u weet wel, het slotje in uw browser. Zet uw firewall aan, gebruik een virusscanner, en, als u wifi in trein of internetcafé wilt gebruiken, gebruik dan een VPN, zeker als u uw banksaldo checkt. (Weet u niet hoe dat allemaal moet, vraag dan iemand om hulp. U zou er versteld van staan hoeveel leuke contacten er zo tot stand komen.) Installeer security updates op uw computer en telefoon zo gauw ze verschijnen. Gebruik two-factor authentication voor al uw belangrijke accounts. Als het dan toch niet anders kan, probeer dan in ieder geval verschillende wachtwoorden voor verschillende accounts te gebruiken. Maak gebruik van cloud diensten van gerenommeerde IT-bedrijven voor backups en voor samenwerking. (Als de reputatie van een bedrijf op het spel staat is de kans groter dat hun diensten op orde zijn.) En ook: maak geen foto's waarvan u niet zou willen dat uw buren ze zouden zien. Overweeg bij meerdere banken te bankieren, meerdere emailadressen te gebruiken, en als u helemaal zeker wilt zijn kunt u meerdere telefoons gaan gebruiken. Maar als u zover heen bent, dan bent u waarschijnlijk beroepsmatig met beveiliging bezig, aan welke kant van de lijn ook.

We hebben nu enkele technische aspecten de revue laten passeren, die een verklaring kunnen geven waarom cybercrime toch veel voorkomt, waarom er veel *phishing mails* en *fake news* berichten zijn, maar ook waarom we weinig problemen met onze kritieke infrastructuur gezien hebben. Cybercrime en propaganda zijn een probleem van ons allemaal geworden. Wij, en onze democratie, zijn de zwakke schakel geworden. We moeten vaart maken met onderwijs in digitale vaardigheden voor ons allemaal, en we moeten diversiteit koesteren, ook in de digitale wereld, ook al gaat dat daar ten koste van wat efficiëntie.

En nu ben ik benieuwd hoe collega Van den Berg hier vanuit overheid en regelgeving tegen aan kijkt.

Van den Berg: Meer en betere kennis van het gebruik van digitale technologieën kan er zeker aan bijdragen dat eindgebruikers minder vaak slachtoffer worden van cybercrime, van fake news en andere risico's in en van cyberspace. Wie gebruik maakt van het internet moet tenminste een klein beetje besef hebben van de werking èn de gevaren ervan. Net zoals we van van voetgangers verwachten dat ze de verkeersregels kennen en weten hoe ze zich door het verkeer kunnen bewegen met de veiligheid van anderen en zichzelf voor ogen, zo mogen we van eindgebruikers op internet ook verwachten dat zij een basisset aan vaardigheden hebben die ervoor zorgt dat zij

veilig gebruik kunnen maken van genetwerkte technologieën. Digital skills zijn onontbeerlijk geworden in een tijdvak waarin het internet, zoals we eerder gesteld hebben, werkelijk al onze dagelijkse bezigheden ondersteunt of mogelijk maakt.

Digital skills alleen zijn niet genoeg

Dat gezegd hebbende, zie ik ook de nodige beperkingen aan het inzetten op digital skills. In de eerste plaats worden de veiligheidsrisico's via cyberspace elk jaar groter. De kans op slachtofferschap neemt toe doordat er meer criminele activiteit plaatsvindt, en er komen steeds weer nieuwe kwetsbaarheden aan het licht, die telkens op nieuwe manieren voor problemen zorgen. Bij elkaar genomen betekent dit, dat het aanleren van digital skills niet voldoende zal zijn. Immers, de skill set die eindgebruikers nodig hebben, verandert zo'n beetje elk jaar. U kunt proberen om de lessen digitale weerbaarheid van collega Plaat uit uw hoofd te leren, die zullen zeker helpen. Maar ze zijn geen garantie voor de toekomst. Net wanneer u heeft onthouden dat u niet op zomaar op links moet klikken, tuint u in een deep fake. En net wanneer u doorheeft dat u geen geld moet overmaken aan iemand met een zielig verhaal op een dating site, wordt u slachtoffer van Whatsapp-fraude. De snelheid waarmee digitale technologieën zich ontwikkelen is hoog, en daarmee verschuiven de risico's ook in een rap tempo. Dat betekent dat we van burgers en consumenten mogen verwachten dat ze een bepaalde mate van 'basis hygiëne' aan de dag leggen in hun internetgebruik, maar veel meer ook niet.

Een rol voor de overheid

Maar wat dan wel? Heeft de overheid een taak als het gaat om het veiliger maken van cyberspace? Mijns inziens is het antwoord daarop volmondig JA. Merkt u op dat dit geen eenvoudige taak is. Ik bespreek twee redenen waarom het voor de overheid niet gemakkelijk is om invloed uit te oefenen op de veiligheid in en van cyberspace.

Een grensoverschrijdend vraagstuk

In de eerste plaats is dit het geval, omdat cyberspace grensoverschrijdend is. Cyberspace omspant de wereld. Iedere keer als u een simpele website opzoekt via uw browser, overschrijdt u met gemak drie landsgrenzen, als het er niet meer zijn. Het internet stopt niet bij de grenzen van Nederland. Maar de soevereiniteit en de jurisdictie van de Nederlandse staat stoppen daar wel. Om cyberspace veiliger te maken, zullen landen dus op internationaal vlak moeten samenwerken. Dat leidt uiteraard tot grote uitdagingen, bijvoorbeeld over de vraag welke normen er in cyberspace moeten gelden, en hoe de spanning tussen bijvoorbeeld vrijheid van meningsuiting en privacy of nationale veiligheid en vrijheid van informatie, moeten worden opgelost. Het vastleggen van standaarden, of het scheppen van normen, of het creëren van wet- en regelgeving op allerlei gebieden is dan ook geen kortlopend of gemakkelijk traject. Er is veel onderzoek nodig naar de manier waarop dergelijke standaarden, normen en kaders tot stand komen, of zouden moeten komen. Aan deze universiteit dragen we ons steentje bij door onderzoek te doen naar normen voor statelijk gedrag in cyberspace onder de vlag van het The Hague Cyber Norms Program.

Hoewel het scheppen van standaarden en kaders traag zal gaan, maken we met name in Europa zeker meters in de internationale samenwerking op het terrein van cybersecurity en privacy. De Algemene Verordening Gegevensbescherming (AVG), die sinds 2018 in heel Europa geldt, is een voorbeeld van wet- en regelgeving die bijdraagt aan een veiliger gebruik van cyberspace voor consumenten en burgers. Na jaren sleutelen zijn Europese landen, bedrijven, en belangenorganisaties er gezamenlijk in geslaagd om in die wet vast te leggen hoe alle bedrijven en organisaties die in Europa zaken doen om dienen te gaan met de gegevens en de privacy van eindgebruikers.

Het 'Brussels effect'

Onbedoeld heeft deze ene wet ook wereldwijd effect gehad. We noemen dat het 'Brussels effect.' Omdat internationale internetbedrijven als Google, Microsoft en Facebook zaken willen blijven doen op de Europese consumentenmarkt, passen zij hun gedrag aan aan de vereisten van de in Europa geldende AVG.

En als ze dat eenmaal gedaan hebben voor Europese consumenten, dan gelden die aanpassingen als vanzelf ook voor consumenten in andere delen van de wereld. Facebook gaat immers niet twee diensten aanbieden, eentje in Europa, en eentje in de rest van de wereld. Dat zou kostbaar en inefficiënt zijn. Hoewel de AVG bedoeld was om de rechten van *Europese* consumenten te beschermen,, heeft de implementatie ervan als onbedoeld bij-effect dat de hele wereld beter beschermd wordt op het terrein van privacy en gegevensbescherming. Het Brussels effect laat zien dat de regulatieve kracht van de Europese Unie wereldwijd voor meer veiligheid op internet kan zorgen. Tot op heden is dat, zoals gezegd, nog een onbedoeld bij-effect geweest. Maar hoe veel potentieel schuilt er in dat effect? Zouden we dit bewust kunnen inzetten om, met behulp van regulering, de veiligheid in en van cyberspace wereldwijd te versterken? We hebben in Europa intussen de eerste stappen gezet in het harmoniseren van wet- en regelgeving op het terrein van kritieke infrastructuren. Als we op die weg meters maken, zou het Brussels effect ook ten bate kunnen komen van een verbeterde bescherming van vliegvelden, ziekenhuizen, energienetwerken enzovoort.

Een rol voor de overheid?
Wellicht blijft u na dit pleidooi achter met vraag: maar waaròm zou de overheid juist een rol moeten spelen in relatie tot veiligheid in cyberspace? Kunnen bedrijven dat niet zelf, zonder dat de overheid zich ermee bemoeit? Zou de private sector niet zelf de voortrekkersrol moeten nemen?

De private sector laat te veel liggen
Het antwoord daarop is ja en nee. Cybersecurity op orde krijgen kost veel geld, tijd en mankracht, en wanneer organisaties dat geld geïnvesteerd hebben, is het resultaat dat ze daarmee behalen het *uitblijven* van incidenten. Erger nog, als incidenten na al die investeringen uitblijven, dan kán dat te maken hebben met de tijd en energie die organisaties er in gestoken hebben om hun informatiebeveiliging op orde te krijgen. Maar dat is niet noodzakelijkerwijs het geval. Investeringen in cybersecurity worden door organisaties nog steeds vaak gezien als een 'nice to have', als extra bonus bovenop het primaire proces. Dat ICT intussen onderdeel geworden is van dat primaire proces, en dus bij uitval of een aanval ook het primaire proces direct geraakt wordt, is helaas voor veel organisaties nog niet duidelijk genoeg geworden. Pas na jaren van veelvuldige incidenten zal cybersecurity als vanzelf tot het DNA van gezonde organisaties gaan horen. Op dit moment zijn er nog te veel prikkels die organisaties kunnen afleiden van het investeren in hun eigen cyberveiligheid.

Ook voor de grote technologiebedrijven zelf geldt dat de kans niet groot is dat zij uit zichzelf zullen bewegen om van cyberspace een veiliger plek te maken. Apple zegt sinds enkele jaren dat het beschermen van uw en mijn privacy haar 'unique selling point' is, en kiest stevig positie in debatten met opsporings- en veiligheidsdiensten over het breken van cryptografische codes voor het verkrijgen van toegang tot Apple-apparaten, en over het inbouwen van achterdeurtjes die gebruikt zouden kunnen worden door die diensten. Maar we zagen vorig jaar dat Mark Zuckerberg geen antwoord gaf op de vragen van het Amerikaanse Congres over de rol van Facebook in het bestrijden van fake news en desinformatie. Facebook wil niet aangemerkt worden als mediabedrijf, met alle verantwoordelijkheden en waarborgen die daarbij horen op het gebied van de kwaliteit van informatie die via haar kanaal wordt aangeboden. In plaats daarvan blijft het liever volhouden dat het slechts een doorgeefluik is voor informatie die eindgebruikers met elkaar delen. Daarmee stelt Facebook zich op als machteloos ten opzichte van een fenomeen waar het, met technische, normatieve en sociale codes, veel meer invloed op zou kunnen uitoefenen. De winst die Facebook maakt op basis van alles wat wij delen, blijft een sterkere prikkel dan de morele en maatschappelijke plicht om cyberspace tot een veiliger plek te maken.

Internet als basisvoorziening
Ofwel: hoewel het logisch is om te stellen dat de private sector zelf verantwoordelijk zou moeten zijn voor betere cybersecurity voor ons allemaal, zijn er talloze redenen waarom het niet waarschijnlijk is dat we op korte termijn verbetering kunnen

verwachten uit die hoek. De overheid dient daarom een sturende rol te pakken ten aanzien van de veiligheid in en van cyberspace. Maar dit is wellicht een wat negatief geformuleerde reden.

Er is echter nog een tweede reden waarom de overheid die rol moet pakken. Zoals we eerder zagen, zorgt de overheid voor de bescherming van kritieke infrastructuren: dìe voorzieningen in de samenleving waarvan uitval zou kunnen leiden tot maatschappelijke ontwrichting. We zagen ook al eerder dat het internet zèlf een kritieke infrastructuur is geworden. Des te meer reden om ervoor te zorgen dat de risico's in en van cyberspace minimaal zijn.

Als het internet in feite een basisvoorziening in ons leven is geworden, dan moeten burgers en consumenten erop kunnen vertrouwen dat het internet dat zij gebruiken veilig is, zelfs als ze helemaal geen kennis zouden hebben van hoe het werkt of welke risico's er eigenlijk zijn. Vergelijk het met voedselveiligheid. Als ik in Nederland naar de supermarkt ga, dan mag ik ervan uitgaan dat het eten dat ik daar koop veilig is, dat ik er niet ziek van wordt. De overheid heeft een belangrijk aandeel in het waarborgen van die voedselveiligheid: er zijn wettelijke eisen en regels voor fabrikanten, er zijn controlerende instanties, en keurmerken. De hele keten van partijen die betrokken is bij de productie, het vervoer en de verkoop van voedsel is aan strenge regels over voedselveiligheid gebonden. De overheid speelt een sleutelrol door regels te maken, te handhaven en regie te voeren.

Voor cyberspace, voor ons gebruik van het internet, hebben we een dergelijke aanpak nog niet ontwikkeld. Cyberspace is pas enkele decennia oud, dus het is ook niet verwonderlijk dat zoiets nog niet bestaat. Maar gezien het belang van cyberspace voor onze samenleving lijkt het me evident dat we moeten werken aan een systeem naar analogie van dat dat rondom voedselveiligheid, of veiligheid op de werkvloer, of productveiligheid, om nog maar een paar voorbeelden te noemen. Een centrale rol voor de overheid is daarbij onontbeerlijk.

Plaat: Als er één ding is dat de lezing van vandaag u heeft laten zien, dan is het dat cybersecurity een complex, gelaagd vraagstuk is. Het is bij uitstek een onderwerp waarin technische aspecten alsook juridische, maatschappelijke, politieke en ethische vraagstukken samenkomen. Een multi- of zelfs interdisciplinaire aanpak is dan ook de enig zinvolle weg om dit ingewikkelde vraagstuk te adresseren. Aan deze universiteit werken technische en gedragswetenschappers samen aan onderzoeksprojecten, zoals bij onderzoek naar fake news, waarin aan dat multidisciplinaire vraagstuk invulling wordt gegeven. Ze geven ook gezamenlijk onderwijs, bijvoorbeeld in de nieuwe Minor Cybersecurity die volgend jaar van start gaat. Om die reden zijn wij trots op het feit dat onze universiteit in Leiden en Den Haag een thuis biedt aan wetenschappers op verschillende vakgebieden die gezamenlijk aan al deze invalshoeken invulling geven. Samen wensen collega Van den Berg en ik de Universiteit Leiden op deze 445e dies van harte geluk met haar verjaardag, morgen.

Wij hebben gezegd.

Prof.dr. Bibi van den Berg

Bibi van den Berg is als hoogleraar Cybersecurity Governance verbonden aan de Universiteit Leiden. Zij staat op de Campus Den Haag aan het hoofd van de onderzoeksgroep Cybersecurity Governance bij het Institute of Security and Global Affairs. Daarnaast is zij lid van de Cyber Security Raad, die het kabinet adviseert op het gebied van cybersecurity in Nederland.

Prof.dr. Aske Plaat

Aske Plaat is hoogleraar Kunstmatige intelligentie aan de Universiteit Leiden, en wetenschappelijk directeur van het Leiden Institute for Advanced Computer Science (LIACS). Hij is geïnteresseerd in adaptieve systemen, *reinforcement learning* en games. Daarnaast is hij mede-oprichter van het Leiden Center for Data Science en initiatiefnemer van het *Program for Society, Artificial Intelligence and Life Science (SAILS)* – het universiteitsbrede programma voor kunstmatige intelligentie.

Universiteit Leiden