Open Universiteit

PROF. DR. IR. H.P.E. (HARALD) VRANKEN

Cybersecurity: pompen of verzuipen

Open Universiteit

PROF. DR. IR. H.P.E. (HARALD) VRANKEN

Cybersecurity: pompen of verzuipen

Vranken HPE (2025). Cybersecurity: pompen of verzuipen.
Open Universiteit, Heerlen, The Netherlands

Cover background photo: Stockcake

INHOUD

Cybersecurity: pompen of verzuipen

Rede

In verkorte vorm uitgesproken bij de openbare aanvaarding van het ambt van hoogleraar Cyber Security aan de Open Universiteit op

vrijdag 14 maart 2025

door prof. dr. ir. H.P.E. (Harald) Vranken

Open Universiteit

Open Universiteit

Geachte meneer de rector magnificus, geachte decaan,
beste collega's, familie, vrienden, bekenden en belangstellenden,
zowel hier aanwezig in Heerlen als online,
fijn dat jullie er allemaal zijn.

Welkom bij mijn inaugurele oratie ter aanvaarding van het ambt van hoogleraar Cyber Security aan de Open Universiteit.

1 Inleiding

De titel van mijn oratie is 'Cybersecurity: pompen of verzuipen'. Wie Van Dale erop naslaat, zal lezen dat 'pompen of verzuipen' een informele uitdrukking is die betekent dat het gevaar groot is: je moet je uiterste krachten inspannen, alles op het spel zetten om de zaak te redden. Dat is een treffende omschrijving voor de uitdaging die cybersecurity aan ons stelt.

1.1 Cybersecurity, wat is dat eigenlijk?

Definitie van cybersecurity

De term 'cybersecurity' is een samenstelling van de Engelse termen 'cyber' en 'security' en duidt op de beveiliging van de zogenaamde cyberspace, de virtuele wereld die zich afspeelt in computersystemen, computernetwerken en het internet.

Van Dale omschrijft cybersecurity als cyberbeveiliging, de beveiliging tegen cyberaanvallen. Er is echter geen universele definitie van cybersecurity [24, 34, 43]. Zo maken sommige bronnen bijvoorbeeld een onderscheid tussen information security en cybersecurity (zoals ISO), terwijl andere bronnen beide begrippen min of meer als synoniem beschouwen [5]. Schatz et al. [43] publiceerden in 2017 een systematisch literatuuronderzoek waarin zij 28 verschillende definities vergeleken uit industrie, overheden en wetenschap. Op basis van lexicale en semantische analyses van de reikwijdte en context van deze definities, werd daaruit de volgende definitie afgeleid: *De aanpak en acties gerelateerd aan processen voor het managen van beveiligingsrisico's die door organisaties en staten worden gevolgd om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en middelen die in cyberspace worden gebruikt, te beschermen. Dit omvat richtlijnen, beleid en verzamelingen van beveiligingsmaatregelen, technologieën, hulpmiddelen en training om de beste*

bescherming te bieden voor de toestand van de cyberomgeving en haar gebruikers. Dat is een brede definitie die vele facetten uit verschillende vakgebieden omspant.

Deze definitie maakt duidelijk dat alleen technische oplossingen niet afdoende zijn. Bruce Schneier, een internationaal gerenommeerde expert op gebied van cybersecurity, verwoordde dit treffend: *If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology* [72]. Naast technische aspecten is er op zijn minst ook aandacht nodig voor het menselijk handelen in digitale processen, alsmede risicomanagement en governance.

Uit bovenstaande definitie volgt ook dat cybersecurity geen doel op zichzelf is, maar een middel om een doel te bereiken, namelijk vertrouwen opbouwen in de betrouwbaarheid van (kritieke) IT-infrastructuur en digitale processen, zelfs als deze worden aangevallen [65, 67].

Interactie tussen virtuele en fysieke wereld

De virtuele wereld van cyberspace speelt zich af in computersystemen en computernetwerken. Het is een abstracte wereld, waarin wij niet fysiek kunnen rondlopen en die wij ook niet met onze zintuigen kunnen waarnemen. We kunnen er slechts mee communiceren via beeldschermen en toetsenborden. Het is de wereld van de informatietechnologie (IT), een ecosysteem dat wij als mensen hebben gecreëerd, waarin we informatie creëren, opslaan, bewerken, gebruiken, uitwisselen en delen. We gebruiken die IT voor verschillende doeleinden, bijvoorbeeld: met elkaar communiceren, zoals e-mail, social media en instant messaging; dienstverlening, zoals internetbankieren, webwinkels en digitale loketten van de overheid; informatie opslaan en toegankelijk maken via het world wide web; en informatie verwerken in de administratieve processen van organisaties.

De virtuele wereld van cyberspace raakt echter in toenemende mate ook aan onze fysieke wereld. Vrijwel alle moderne apparaten, van auto's tot keukenapparatuur, hebben intern een computersysteem om de werking van het apparaat te regelen, en zijn verbonden met het internet waarmee we bijvoorbeeld diagnostische gegevens naar de fabrikant kunnen sturen en software updates kunnen downloaden. Inmiddels zijn er wereldwijd vele miljarden apparaten verbonden in het internet of things (IOT). Verder zien we dat door de toenemende automatisering operationele technologie (OT) wordt gekoppeld aan computernetwerken of het internet. Deze OT-systemen besturen operationele processen in de fysieke wereld, zoals het aansturen van een pomp of een industriële robot en het op afstand uitlezen van een sensor. OT speelt een grote rol in vele sectoren, waaronder chemische industrie, maakindustrie en onze kritieke infrastructuur voor distributie van elektriciteit en gas, drinkwatervoorziening, waterbeheer, transport over land, water en lucht, en betalingsverkeer.

Door deze almaar toenemende digitalisering, automatisering en koppeling met het internet, raken de virtuele wereld en de fysieke wereld steeds meer met elkaar verweven. Cybersecurity is daarom niet alleen noodzakelijk voor de beveiliging van de virtuele wereld van cyberspace, maar ook voor de beveiliging van onze fysieke wereld.

1.2 Herkomst van de term 'cybersecurity'

De term 'cyber' is afkomstig uit het Grieks: het werkwoord $\kappa\upsilon\beta\epsilon\rho\nu\acute{\alpha}\omega$ betekent sturen, besturen of leiden en het zelfstandig naamwoord $\kappa\upsilon\beta\epsilon\rho\nu\acute{\eta}\tau\eta\varsigma$ betekent stuurman, bestuurder of leidsman. De Amerikaanse wiskundige Norbert Wiener (1894-1964) gebruikte aan het eind van de jaren 1940 het woord 'cybernetica' om de besturing van machines en levende organismen door middel van communicatie en terugkoppeling aan te duiden. De term 'cybernetica' en het daarvan afgeleide voorvoegsel 'cyber' werd daarna vaak geassocieerd met humanoïde robots, zoals de Cybermen die in de Britse sciencefictionserie Doctor Who voorkwamen in 1966 [76].

De eerste associatie van de term 'cyber' met computers en het internet wordt toegeschreven aan de Amerikaanse sciencefictionauteur William Gibson (1948-) die de term 'cyberspace' bedacht en gebruikte in zijn korte verhaal Burning Chrome (1982) en later in zijn debuutroman Neuromancer (1984) [24]. In die tijd stond het internet nog in de kinderschoenen en voor Gibson was de term 'cyberspace' destijds een modewoord zonder een concrete semantische betekenis.

De context van de term 'cyber' is gaandeweg verschoven en omvat tegenwoordig niet alleen de virtuele omgeving die zich afspeelt in computersystemen, computernetwerken en het internet, maar ook de objecten en stakeholders in de fysieke wereld die interacteren met die virtuele wereld [5].

De term 'cyber' wordt enerzijds gebruikt als bijvoeglijk naamwoord en anderzijds als voorvoegsel. In het Engels wordt 'cyber' als bijvoeglijk naamwoord gebruikt om te benadrukken dat het gaat om het virtuele domein, zoals in 'cyber space' en 'cyber security'. In het verleden werd aan deze schrijfwijze de voorkeur gegeven [38]. Echter, 'cyber' wordt in toenemende mate gebruikt als voorvoegsel van zelfstandig naamwoorden, zoals 'cyberspace' en 'cybersecurity' [5]. Ook in het Nederlands werd initieel de spelling 'cyber security' gehanteerd, zoals we bijvoorbeeld zien in het 'Nationaal Cyber Security Centrum' (NCSC), een onderdeel van het Ministerie van Justitie en Veiligheid, en de 'Cyber Security Raad' (CSR), een nationaal, onafhankelijk adviesorgaan van het kabinet en bedrijfsleven. Tegenwoordig is 'cybersecurity' echter de gangbare spelling en sinds 2020 opgenomen in Van Dale.

1.3 Leerstoel Cyber Security

Mijn leerstoel is gepositioneerd in de vakgroep Informatica van de faculteit Bètawetenschappen aan de Open Universiteit, en concentreert zich op de technische aspecten van cybersecurity binnen het vakgebied informatica. In die context is cybersecurity gericht op de technische beveiliging van de software en hardware in computersystemen en computernetwerken, en de informatie die zich daarin bevindt. Cybersecurity omvat zowel proactieve methoden voor de preventie, verdediging en detectie van cyberaanvallen, als reactieve methoden voor de bestrijding en herstel van cyberaanvallen.

Mijn leerstoel concentreert zich weliswaar op technische aspecten vanuit de informatica, maar zoekt ook samenwerking met andere disciplines. Zoals ik zojuist al aangaf, is het vormgeven van cybersecurity immers een complex probleem dat een multidisciplinaire aanpak vereist. Pompen of verzuipen houdt dan ook in dat we de krachten van meerdere disciplines moeten bundelen. Een bredere visie op cybersecurity is essentieel.

1.4 Over de oratie

Deze oratie bestaat uit drie onderdelen. Allereerst ga ik in hoofdstuk 2 in op de vraag hoe het met cybersecurity is gesteld. Ik beschouw daarin hoe cybersecurity zich in de afgelopen 50 jaar heeft ontwikkeld en schets een beeld van de huidige stand van zaken omtrent cybersecurity. De conclusie van dat hoofdstuk is dat er weliswaar lichtpuntjes zijn, maar dat cybersecurity een chronisch probleem is waar we maar moeilijk vat op krijgen. In hoofdstuk 3 ga ik vervolgens in op de vraag waarom cybersecurity een chronisch probleem is. Er is geen eenvoudig antwoord op die vraag en vele factoren spelen een rol. Mijn antwoord is dan ook niet uitputtend, maar ik zet de belangrijkste oorzaken op een rij. Tot slot ga ik in hoofdstuk 4 in op de vraag hoe we cybersecurity kunnen verbeteren. Ik zal mijn plannen voor onderzoek en onderwijs op gebied van cybersecurity toelichten. Cybersecurity is een enorm complex en veelzijdig probleem, en het is dan ook een utopie dat mijn leerstoel dit probleem zal oplossen. Maar de ambitie is in elk geval om cybersecurity vooruit te helpen. En de noodzaak daartoe is groot, want zoals ik al aangaf, is het een kwestie van pompen, want anders verzuipen we vast en zeker in de cyberspace.

2 Hoe is het gesteld met cybersecurity?

In dit hoofdstuk geef ik een historisch overzicht van hoe cybersecurity zich heeft ontwikkeld en schets ik een beeld van de huidige stand van zaken omtrent cybersecurity. Daarbij kijk ik achtereenvolgens naar drie aspecten van cybersecurity: incidenten, aanvallers en maatregelen.

2.1 Cybersecurityincidenten

Helaas is het in de virtuele wereld van cyberspace, net zoals in de fysieke wereld, verre van pais en vree. In deze sectie kijken we naar cybersecurityincidenten, gebeurtenissen waarbij cybersecurity onder druk staat. Daartoe beschouw ik eerst gegevens over kwetsbaarheden in computersystemen waardoor cyberaanvallen mogelijk worden. Vervolgens beschouw ik cyberaanvallen die daadwerkelijk hebben plaatsgevonden.

2.1.1 Kwetsbaarheden

In 1999 werd in de VS een programma gestart met als doel om gekende, openbaar gemaakte kwetsbaarheden in computersystemen, met name in software, overzichtelijk in kaart te brengen [31]. Dit programma genaamd 'Common Vulnerabilities and Exposures (CVE)' is sindsdien uitgegroeid tot de de facto internationale standaard [66]. Met een kwetsbaarheid ('vulnerability') wordt een zwakke plek bedoeld in een concreet product die kan worden uitgebuit door een kwaadwillende. Elke kwetsbaarheid die in de CVE-catalogus wordt opgenomen, krijgt een unieke identificatiecode in de vorm CVE-J-N, waarin J het jaartal aanduidt en N het volgnummer. Een voorbeeld is CVE-2021-44228, de beruchte kwetsbaarheid in de loggingsoftware Log4j. Het aantal kwetsbaarheden dat is opgenomen in de CVE-catalogus, stijgt gestaag en bedraagt inmiddels al meer dan 250.000. Elk jaar worden er meer nieuwe kwetsbaarheden gerapporteerd dan in het voorgaande jaar. In 2015 werden zo'n 6.500 nieuwe kwetsbaarheden gerapporteerd. In 2024 waren dat er meer dan 40.000, dus gemiddeld meer dan 100 per dag [79]. Dat zijn flinke aantallen.

De Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) houdt de 'Known Exploited Vulnerabilities (KEV)' catalogus bij. Deze catalogus bevat kwetsbaarheden die daadwerkelijk zijn uitgebuit. Met deze catalogus is pas recent in november 2021 gestart en bevatte initieel 287 kwetsbaarheden. Het aantal kwetsbaarheden dat is opgenomen in de KEV-catalogus, groeit gestaag en bedraagt inmiddels meer dan 1.000 [78].

De kwetsbaarheden in de CVE- en KEV-catalogus bestrijken een breed pallet van verschillende soorten kwetsbaarheden. De 'Common Weakness Enumeration (CWE)' is een lijst en taxonomie van zwakheden die in hardware of software producten kunnen voorkomen [83]. Deze zwakheden ('weaknesses') zijn de onderliggende oorzaken van kwetsbaarheden. Elke zwakheid in de CWE-lijst heeft eveneens een unieke identificatiecode in de vorm van CWE-N, waarin N een volgnummer is. Bijvoorbeeld, aan de genoemde Log4j-kwetsbaarheid (CVE-2021-44228) liggen CWE-917 ('Expression Language Injection'), CWE-400 ('Uncontrolled Resource Consumption'), CWE-502 ('Deserialization of Untrusted Data') en CWE-20 ('Improper Input Validation') ten grondslag.

Verschillende organisaties houden ranglijsten bij van welke zwakheden in de praktijk het meest voorkomen of de grootste impact hebben als ze worden uitgebuit. Bekende voorbeelden daarvan zijn de 'CWE Top 25 Most Dangerous Software Weaknesses' [84] en de 'OWASP Top 10 Web Application Security Risks' [95]. Ter illustratie: de top drie van de CWE Top 25 bestaat momenteel uit 'Cross-site Scripting' (CWE-79), 'Out-of-bounds Write' (CWE-787) en 'SQL Injection' (CWE-89). De 'OWASP Top 10' bevat verzamelingen van gerelateerde CWEs. Ter illustratie: de top drie van de 'OWASP Top 10' bestaat momenteel uit: 'Broken Access Control' wat 34 CWEs omvat, 'Cryptographic Failures' wat 29 CWEs omvat, en 'Injection' wat 33 CWEs omvat.

Er zijn diverse andere ranglijsten. Zo is er bijvoorbeeld de 'CWE Most Important Hardware Weaknesses', een lijst met zwakheden in hardware producten. OWASP onderhoudt inmiddels een veelvoud van ranglijsten, onder andere voor verschillende typen applicaties (cloud-native, desktop en mobile), technologieën (IOT, OT, LLMs) en ontwikkelmethoden (DevSecOps, CI/CD, Low-Code/No-Code).

Naast de gekende, openbaar gemaakte kwetsbaarheden zijn er de zogenaamde zero-day kwetsbaarheden. Dat zijn kwetsbaarheden die wel bekend zijn bij aanvallers en mogelijk ook al uitgebuit worden. De kwetsbaarheden zijn echter nog niet bekend bij de software-ontwikkelaars en er zijn dan ook nog geen security updates ('patches') beschikbaar die de kwetsbaarheden verhelpen. Het duurt gemiddeld zo'n 100 dagen voordat er een patch beschikbaar is nadat een zero-day kwetsbaarheid bekend wordt [40]. In die periode zijn gebruikers onbeschermd tegen aanvallen waarin deze kwetsbaarheden worden uitgebuit.

2.1.2 Cyberaanvallen

In de vorige sectie werd duidelijk dat het aantal zwakheden en kwetsbaarheden in computersystemen enorm is en steeds verder toeneemt, hetgeen ruime keuze aan aanvallers biedt om cyberaanvallen te ontwikkelen en uit te voeren waarin deze zwakheden worden uitgebuit. De verscheidenheid aan soorten cyberaanvallen is groot. Het MITRE ATT&CK raamwerk biedt een taxonomie

voor cyberaanvallen [85], waarin cyberaanvallen worden gecategoriseerd op basis van hoe en waarom aanvallen in de praktijk worden uitgevoerd.

In deze sectie schets ik een beeld van cyberaanvallen die daadwerkelijk zijn uitgevoerd. De economische schade en maatschappelijke impact van deze cyberaanvallen is groot, maar de omvang daarvan laat ik in deze analyse verder buiten beschouwing.

Om een eerste, enigszins anekdotisch beeld te schetsen van cyberaanvallen, beschouwen we een greep uit de nieuwsberichten. Dat beeld wordt vervolgens aangescherpt aan de hand van systematische dataverzamelingen.

Een greep uit NOS-nieuwsberichten

Er is een aanhoudende stroom van nieuwsberichten over cyberaanvallen, die variëren van klein tot groot, zowel nationaal als internationaal. Als voorbeeld een greep uit het NOS-nieuws van het afgelopen jaar, waarin verschillende soorten aanvallen de revue passeren.

Om kleinschalig en dicht bij huis te beginnen: In oktober werd bekend dat de organisatie van het Oud-Limburgs Schuttersfeest (OLS) het slachtoffer was geworden van phishing [90]. De aanvaller wist bankrekeningnummers op facturen van leveranciers aan te passen, waardoor er 78.000 euro in verkeerde handen viel. In januari werd de Technische Universiteit Eindhoven getroffen door een cyberaanval, waardoor er een week lang geen onderwijs mogelijk was en tentamens een week moesten worden verschoven [92].

Met name cyberaanvallen waarbij datalekken werden uitgebuit, waren grootschalig. Enkele voorbeelden uit Nederland: In september vond er een digitale inbraak plaats bij de Nederlandse politie [91]. De aanvallers slaagden erin om browsercookies in handen te krijgen, waarmee ze konden inloggen in een politiesysteem. Vervolgens konden ze de adreslijst stelen die wordt gebruikt in Microsoft Outlook. De lijst bevatte de namen, e-mailadressen en soms extra gegevens van bijna alle 65.000 politiemedewerkers. In mei rapporteerde het UWV een datalek waarbij 150.000 cv's ingezien waren en mogelijk gedownload [87]. Enkele voorbeelden met wereldwijde impact: In december werd een groot datalek bij autofabrikant Volkswagen bekend gemaakt [88]. Het bleek dat gegevens van 800.000 eigenaren van elektrische voertuigen waren verzameld bij het downloaden van een gebruikersapp. De gegevens bleken grotendeels onbeschermd en maandenlang toegankelijk te zijn geweest in de cloudopslag van Amazon. In juni werd gemeld dat hackers gegevens van maar liefst 560 miljoen klanten van Ticketmaster hadden gestolen, waaronder adressen, telefoonnummers, creditcardgegevens en ticketaankopen [93]. De hackers boden deze gegevens te koop aan op het dark web voor 500.000 dollar en wilden ook geld om hen ervan te weerhouden om de gegevens vrij te geven.

Zorgwekkend zijn ook cyberaanvallen waarbij niet burgers, bedrijven of organisaties het doelwit zijn, maar waar staten worden aangevallen. In november meldden de gezamenlijke ministers van Buitenlandse Zaken uit Duits-

land, Frankrijk, Polen, Italië, Spanje en het Verenigd Koninkrijk dat Rusland systematisch aanvallen uitvoert op de Europese veiligheidsarchitectuur, waaronder cyberaanvallen [89]. Een alarmbel voor de kwetsbaarheid van onze kritieke infrastructuur was ook het CrowdStrike incident in juni, dat een wereldwijde computerstoring veroorzaakte waardoor onder meer luchthavens en ziekenhuizen werden getroffen [94]. Dit incident betrof weliswaar geen hack of doelbewuste aanval, maar was wel het gevolg van een kwetsbaarheid in security software die werd getriggerd door een software update.

Het beeld dat hieruit volgt is dat het tegenwoordig niet al te best is gesteld met cybersecurity. En helaas moeten we constateren dat dit in de voorgaande jaren ook het geval was. Als we bijvoorbeeld terugkijken naar het nieuws uit 2015, tien jaar geleden, dan zien we een vergelijkbaar beeld. En zelfs als we twintig jaar terugkijken, naar 2005, zien we dat er ook toen regelmatig nieuwsberichten waren over cyberaanvallen en gehackte systemen.

Gegevens over Nederland

Het Centraal Bureau voor de Statistiek (CBS) in Nederland heeft de wettelijke taak om statistieken te maken over een groot aantal maatschappelijke onderwerpen. Daartoe verzamelt het CBS gegevens van personen en bedrijven, met name via enquêtes en uit bestaande registraties. De statistieken van het CBS over cybersecurityincidenten en online criminaliteit laten weliswaar zien dat de recente aantallen incidenten iets lager zijn dan voorheen, maar nog steeds schrikbarend hoog zijn.

Sinds 2017 rapporteert het CBS in de jaarlijkse 'Cybersecuritymonitor' onder meer statistieken over cybersecurityincidenten in Nederlandse bedrijven [59]. Er wordt gekeken naar drie soorten incidenten: uitval van ICT-systemen; vernietiging of verminking van data; en dataonthulling. Het totale aantal incidenten, waaronder zowel incidenten die niet opzettelijk of door eigen toedoen zijn ontstaan als cyberaanvallen van buitenaf, is gedaald. Zo had in 2016 nog bijna 40% van de grootste bedrijven een ICT-veiligheidsincident door een aanval van buitenaf, terwijl dit in 2022 gedaald is tot 18%, waarbij slechts in een derde van de gevallen ook kosten werden gemaakt. Dit echter met de kanttekening dat uitval van een ICT-systeem en datavernietiging weliswaar is afgenomen, maar dataonthulling als gevolg van een cyberinbraak juist is toegenomen.

Het CBS rapporteert in de Cybersecuritymonitor [59] en de Veiligheidsmonitor [60] ook statistieken over online criminaliteit, dat wil zeggen delicten en incidenten die via internet, e-mail of app plaatsvinden. Een voorzichtige positieve ontwikkeling is dat het slachtofferschap van online criminaliteit in 2023 iets is gedaald ten opzichte van 2021, van 17% naar 16%. Die lichte daling komt vooral doordat iets minder mensen slachtoffer werden van computervredebreuk (hacken), en dan met name van hacken van een account; andere online delicten, zoals online oplichting, fraude, bedreiging en intimidatie zijn nauwelijks veranderd. Met name jongeren werden slachtoffer: 18% van de

15- tot 25-jarigen, versus 11% van de 65-plussers. Dat zijn aanzienlijke percentages, ook als we het vergelijken met traditionele criminaliteit: In 2023 werd 20% van de bevolking slachtoffer van traditionele criminaliteit versus 16% van online criminaliteit. De kans dat je slachtoffer werd van online oplichting en fraude (9% van de bevolking) of van hacken (6% van de bevolking) was groter dan dat je fiets werd gestolen (5% van de bevolking).

Internationale gegevens

De European Union Agency for Cybersecurity (ENISA) rapporteert in de afgelopen twee jaar een opmerkelijke escalatie van zowel de verscheidenheid, de aantallen als de gevolgen van cyberaanvallen in de EU [63]. In de periode van juli 2023 tot juni 2024 werden meer dan 11.000 incidenten in de EU geregistreerd. Het merendeel daarvan betrof denial-of-service-aanvallen (41%), ransomware-aanvallen (26%) en data breaches en data leaks (19%).

De effecten van cyberaanvallen zijn grootschalig, met name door digitale monoculturen, concentratie bij grote cloudaanbieders, beperkte cybersecuritycapaciteit en de grootschalige handel in persoonsgevoelige data. Aanvallers zijn voortdurend op zoek naar effectievere manieren om aanvallen uit te voeren en detectie te ontwijken. Recente ontwikkelingen zijn het gebruik van zogeheten living-off-the-land aanvallen, waarbij aanvallers gebruikmaken van legitieme tooling en applicaties, en aanvallen op zogeheten edge devices zoals firewalls, VPN-servers en routers [67].

2.2 Aanvallers

In essentie zou cybersecurity geheel overbodig zijn als mensen nooit kwade opzet hadden of verkeerde keuzes maakten die nadelig uitpakken voor anderen. De moderne psychologie leert ons dat het menselijk gedrag maar zeer ten dele het gevolg is van bewuste, rationele keuzes. Sturende maatregelen die enkel het rationele en bewuste deel van de menselijke geest aanspreken, hebben daarom maar in beperkte mate effect. Vaak zijn het omgevingsfactoren die onbewust het menselijk gedrag beïnvloeden, en sturende maatregelen die hierop aangrijpen zijn niet evident [74]. De mogelijkheid om menselijk gedrag te sturen is desalniettemin een belangrijke component in de multidisciplinaire aanpak voor cybersecurity.

Cybersecurity is de beveiliging tegen cyberaanvallen die worden geïnitieerd door menselijke aanvallers. In deze sectie kijken we naar de motieven van aanvallers, alsmede de gelegenheid en middelen om aanvallen uit te voeren. De gelegenheid om een aanval uit te voeren in cyberspace verschilt enorm van de fysieke wereld. Een aanvaller kan via het internet alle computersystemen ter wereld bereiken die eveneens met het internet verbonden zijn. Een aanvaller kan daarom vanaf elke plek ter wereld een aanval uitvoeren. Het is niet vreemd dat aanvallers daarbij de voorkeur geven aan locaties waar

de kans om gepakt te worden, zo klein mogelijk is. Qua middelen heeft een aanvaller ook ruime keuze. Veel aanvalstools zijn vrijelijk of tegen betaling te verkrijgen op het internet en het dark web, kennis wordt op internetfora gedeeld, en vaak zijn aanvallers ook goed georganiseerd of worden ze ondersteund door staten.

De motieven voor cyberaanvallen komen overeen met de motieven voor aanvallen in de fysieke wereld. Waren in het verleden hackers nog gedreven door nieuwsgierigheid of spanning, tegenwoordig hebben andere motieven de overhand. De belangrijkste motieven achter hedendaagse cyberaanvallen zijn: financieel gewin; het uitdragen van een ideologie, zoals hacktivisme; spionage om gevoelige of vertrouwelijke informatie te verkrijgen; en verstoring of ontwrichting [62]. Bij DDOS-aanvallen gaat het bijvoorbeeld meestal om aanvallers met een ideologisch motief. Bij ransomware-aanvallen en datagerelateerde aanvallen gaat het meestal om financieel gewin.

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschrijft in het 'Cybersecuritybeeld'-rapport over 2024 dat cyberaanvallen in Nederland momenteel voornamelijk afkomstig zijn van statelijke actoren en cybercriminelen [67].

In de huidige turbulente geopolitiek zijn statelijke actoren, waaronder Rusland, China en Noord-Korea, bezig om hun cyberactiviteiten te intensiveren en hun capaciteiten te verbreden. Ze voeren offensieve cyberprogramma's uit via statelijke en niet-statelijke hackersgroepen. Deze hackersgroepen beschikken over financiële middelen, zijn goed toegerust en maken gebruik van geavanceerde technieken. Hun doel is in de eerste plaats spionage en verstoring. Hacktivisten beschikken vaak over minder middelen, maar hebben een sterke motivatie. Hun doelstellingen omvatten vaak ontwrichting en ze gebruiken hacking om een politieke of sociale verandering teweeg te brengen.

Criminele actoren voeren op grote schaal aanvallen uit en zijn in staat om omvangrijke schade toe te brengen aan digitale processen, zoals met de inzet van ransomware. Hun doel is met name financieel gewin. Hun aanvallen zijn vaak opportunistisch en willekeurig waarbij ze social engineering toepassen. Ze kunnen rechtstreeks van slachtoffers stelen, slachtoffers afpersen, of geld verdienen met de van slachtoffers gestolen informatie. Cybercriminelen zijn in toenemende mate georganiseerd en worden steeds professioneler. Onder cybercriminelen vallen ook hackers die ingehuurd kunnen worden.

Offensieve actoren uit de particuliere sector zijn gespecialiseerd in het ontwikkelen en verkopen van cyberwapens, waaronder zero-day-exploits en kwaadaardige software, aan een verscheidenheid aan klanten, vaak overheden en particulieren. Ze vormen een groeiend probleem vanwege hun vermogen om geavanceerde cybercapaciteiten te bieden aan een breed scala aan klanten.

2.3 Cybersecuritymaatregelen

In deze sectie schets ik hoe securitymaatregelen zich in de afgelopen decennia hebben ontwikkeld. We kunnen cybersecuritymaatregelen op verschillende manieren indelen. We kunnen kijken naar het type maatregel (fysiek, technisch of organisatorisch), de functie (preventie, detectie, response), of het niveau waar maatregelen worden geïmplementeerd en beheerd (management, operationeel of technisch) [44]. Ik focus met name op technologische ontwikkelingen, met een beknopt overzicht van wet- en regelgeving.

2.3.1 Technologische ontwikkelingen

De eerste elektronische computers werden ontwikkeld in de jaren 1940 in de context van de Tweede Wereldoorlog. Dat waren kamervullende rekenmachines. Er waren er wereldwijd maar enkele van en bij security ging het om de bescherming van fysieke toegang met bewakers, hekken en controleposten om diefstal en sabotage te voorkomen.

In de jaren 50 en 60 ontwikkelde de technologie zich snel verder, met onder meer de introductie van geïntegreerde schakelingen, de microprocessor, magnetische opslag, in- en uitvoer via terminals en programmeertalen. Computers deden hun intrede bij universiteiten en particuliere bedrijven. Een belangrijke uitvinding uit die tijd is time-sharing, waarmee het mogelijk werd om meerdere programma's schijnbaar gelijktijdig uit te voeren ('multitasking') zelfs van verschillende gebruikers ('multi-user'). Met time-sharing ontstond een fundamenteel securityprobleem, waarvan we tot op heden last hebben: programma's die gelijktijdig worden uitgevoerd, kunnen elkaar al dan niet opzettelijk in de wielen rijden, met name als ze in hetzelfde geheugen lezen en schrijven. Eind jaren 60 werkte een werkgroep in de VS onder auspiciën van de Defense Science Board aan securitymaatregelen. Het rapport met de bevindingen van die werkgroep, geschreven door Willis Howard Ware, markeert de start van het vakgebied computersecurity [75]. Het Ware-rapport beschrijft niet alleen kwetsbaarheden in hardware, software en communicatie, maar ook maatregelen die we tot vandaag de dag toepassen, zoals: het scheiden van gebruikers en processen met verschillende toegangsrechten; lees-/schrijfrechten op basis van privilegeniveaus; gebruikersauthenticatie; toepassing van cryptografie; logging van transacties; en certificering.

Twee belangrijke ontwikkelingen in de jaren 70 waren de commercialisering van computers en de opkomst van computernetwerken. De uitbreiding van het ARPANET, de ontwikkeling van Ethernet en het TCP/IP-protocol voor packet switching maakten toepassingen mogelijk zoals e-mail (1971), extern inloggen via Telnet (1973) en online nieuwsgroepen zoals Usenet (1978). Het hoofddoel van de netwerkprotocollen was om betrouwbare communicatie mogelijk te maken die bestand was tegen fysieke verstoringen. Echter, er was nauwelijks aandacht voor beveiligingsaspecten zoals authenticatie en inte-

griteit en vertrouwelijkheid van berichten. In 1972 verscheen het rapport van een werkgroep onder auspiciën van de USAF, geschreven door James P. Anderson [57]. Het Anderson-rapport bracht verdere fundamentele beveiligingsproblemen aan het licht, waaronder kwaadwillende gebruikers en een ernstig gebrek aan securitymaatregelen. Het rapport pleitte ervoor dat security vanaf de start bij het ontwerp van systemen ingebouwd moest worden, op basis van een analyse van bedreigingen. Access control, autorisatie, gecontroleerde executie van programma's en de reference monitor waren centrale concepten. Ook het invloedrijke werk van Saltzer en Schroeder over ontwerpprincipes voor security dateert uit die tijd [42]. In de jaren 70 werd ook belangrijke vooruitgang geboekt op gebied van cryptografie, met als mijlpalen de standaardisatie van het DES-algoritme voor symmetrische cryptografie, de uitvinding van publieke-sleutelcryptografie door Diffie en Hellman [13] en het RSA-algoritme van Rivest, Shamir en Adleman [39].

De commercialisering van computers die in de jaren 70 was ingezet, evolueerde verder in de jaren 80 met de komst van de home computer en de personal computer met het Microsoft MS-DOS besturingssysteem. Computernetwerken evolueerden verder tot het internet. De eerste securityincidenten haalden de krantenkoppen, zoals de Morris-worm in 1988. Deze incidenten leidden tot operationalisering van securitymaatregelen, zoals de oprichting van Computer Emergency Response Teams. De focus lag op bescherming van computernetwerken tegen externe bedreigingen, met behulp van netwerkgateways, routers, firewalls en intrusiedetectiesystemen.

In de jaren 90 ontstond het world wide web gebaseerd op de client-serverarchitectuur, wat de wereldwijde uitbreiding van internet verder versterkte. Het gebrek aan securityvoorzieningen in computers en communicatieprotocollen leidde tot verspreiding van malware via e-mailbijlagen, webgebaseerde aanvallen en denial-of-service (DOS) aanvallen. Er werd werk gemaakt van netwerkbeveiliging, zoals de introductie van SSL door Netscape in 1994, SSH als veilig alternatief voor Telnet, VPN, en de toepassing van cryptografie in draadloze netwerken. Ook ontstonden de eerste initiatieven rondom information security management gericht op beveiligingsbeleid in organisaties, zoals de Britse standaard BS 7799 in 1995, als voorloper van de ISO/IEC 27000 serie van standaarden.

De jaren 2000 werden gekenmerkt door de komst van mobiele apparaten, zoals tablets en smartphones. Mobiele en draadloze netwerken zorgden ervoor dat het beveiligen van de randen van netwerken veel moeilijker werd. Ook deden het web 2.0 en sociale media hun intrede, zoals Facebook (2004), YouTube (2005) en Twitter (2006), waarmee de mogelijkheden om aanvallen uit te voeren via social engineering en oplichting flink toenamen. Het beheer van gebruikersaccount en wachtwoorden werd essentieel, en het belang van tweefactorauthenticatie nam toe. Standaarden voor externe authenticatie van gebruikers verschenen, zoals RADIUS. De hoeveelheid malware nam eveneens flink toe. Er ontstonden botnets, waarmee onder andere grootscha-

ligere distributed denial-of-service (DDOS) aanvallen mogelijk werden. Als reactie hierop werd er voortuitgang gemaakt met antivirussoftware, het filteren van netwerkverkeer, load balancing en intrusiepreventiesystemen. De toenemende professionalisering van cybercriminaliteit en door staten ondersteunde actoren, zorgden ervoor dat geleidelijk aan het inzicht ontstond dat het bereiken van volledige beveiliging tegen cyberaanvallen onhaalbaar is en dat het uitgangspunt zou moeten zijn dat je slachtoffer wordt van een cyberaanval.

In de jaren 2010 zette het gebruik van cloudomgevingen verder door, en breidde het internet of things (IOT) zich exponentieel uit. Cybercriminaliteit nam aanzienlijke toe, met name door ransomware en phishing. Het succes van ransomware voor cybercriminelen was mede te wijten aan de introductie van cryptovaluta, waarmee anonieme en onnavolgbare financiële transacties mogelijk werden. De WannaCry ransomware veroorzaakte in 2017 wereldwijd enorme schade. Het cybercrime-ecosysteem professionaliseerde ook met 'as-a-service'-modellen voor het huren van botnets en geavanceerde malware. Er kwamen grootschalige datalekken en door staten gesponsorde cyberspionage aan het licht, onder meer door toedoen van Edward Snowden in 2013. Er vonden zeer geavanceerde aanvallen plaats, zoals Stuxnet in 2010, die gebruikmaakten van zero-day-kwetsbaarheden. Niet alleen de westerse wereld, maar ook staten als China, Rusland, Iran en Noord-Korea ontwikkelden zich tot sterke cybermachten. Als securitymaatregelen raakte het 'zero trust' model in zwang en kreeg security-by-design in softwareontwikkeling via DevOps momentum.

In de jaren 2020 maakte Artificial Intelligence (AI) een enorme ontwikkeling door, en met name generatieve AI is in korte tijd tot vrijwel alle hoeken van de samenleving doorgedrongen. Helaas geldt ook voor AI, net als alle voor andere technologieën, dat er nauwelijks aandacht is besteed aan security.

En om ter afsluiting ook in de nabije toekomst te kijken: we staan waarschijnlijk aan de vooravond van quantumcomputing. In tegenstelling tot onze huidige elektronische computers die werken volgens de principes van de klassieke natuurkunde, werkt een quantumcomputer volgens de principes van de quantummechanica. Quantumcomputing heeft grote impact voor cybersecurity, ten voordele maar ook ten nadele. Quantumcomputing maakt communicatiekanalen mogelijk die niet afgeluisterd kunnen worden, hetgeen een ideaal uitgangspunt is voor het uitwisselen van cryptografische sleutels. Ook maakt quantumcomputing toevalsgeneratoren mogelijk voor het generen van volstrekt willekeurige getallen zonder enige samenhang, hetgeen een essentieel onderdeel is voor betrouwbare cryptografie. Aan de andere kant zijn quantumcomputers in staat om de huidige algoritmen voor publieke-sleutelcryptografie te breken. Deze algoritmen zijn gebaseerd op rekenkundige problemen zoals het ontbinden van grote getallen in priemfactoren of het berekenen van een discreet logaritme. De hoeveelheid tijd die klassieke computers nodig hebben om zulke berekeningen uit te voeren, is gigantisch en daar-

door zijn deze berekeningen praktisch onuitvoerbaar. Met quantumcomputers kunnen deze berekeningen echter wel in relatief korte tijd worden uitgevoerd. Momenteel wordt volop onderzoek gedaan naar post-quantum cryptografie (PQC), die ook voor quantumcomputers onbreekbaar is. Echter, alle huidige toepassingen die gebruikmaken van publieke-sleutelcryptografie, waaronder de beveiliging van vrijwel alle communicatie over het internet, kunnen met quantumcomputers gekraakt worden. Dat is met name problematisch voor geheime of gevoelige informatie die in verkeerde handen is gevallen en nu niet ontsleuteld kan worden, maar straks wel met quantumcomputers.

2.3.2 Wet- en regelgeving

Een wezenlijke ontwikkeling is de nieuwe Europese en Nederlandse wet- en regelgeving omtrent cybersecurity. Het is een gegeven dat wet- en regelgeving achterloopt bij technologische ontwikkelingen. Immers, alvorens een wetsvoorstel opgesteld kan worden, moet de problematiek eerst helder zijn. Als er een wetsvoorstel ligt, duurt het nog enige tijd alvorens het wetsvoorstel is getoetst en in kan gaan. Verder is niet alleen het vormgeven van wetgeving tijdrovend, ook bewustwording en voorbereiding bij bedrijven, uitvoeringsorganisaties, en toezichthouders vergt tijd. Het zal daarom tijd vragen voordat wetgeving daadwerkelijk tot verbetering van cybersecurity kan leiden.

In de afgelopen jaren is in de Europese Unie (EU) vooruitgang geboekt bij het opstellen van beleidskader en het opzetten van structuren en processen rondom cybersecurity [62]. Zo trad de Network and Information Security (NIS1) richtlijn in 2016 in werking, de Cybersecurity Act in 2019 en de EU Cybersecurity Strategy in 2020. Recent volgden onder meer de NIS2-richtlijn in 2023, de Cyber Resilience Act (CRA) in 2024 en de Cyber Solidarity Act (CSOA) in 2025. De NIS2-richtlijn legt wettelijke verplichtingen op aan een groot aantal economische sectoren, waaronder eisen aan securitymaatregelen en het melden van incidenten. De CRA stelt eisen aan hardware en software producten om kwetsbaarheden te voorkomen en aan te pakken tijdens de ontwerp-, productie- en gebruiksfase. Ook zijn er rapportageverplichtingen omtrent actief uitgebuite kwetsbaarheden en ernstige cybersecurityincidenten. De CSOA voorziet in versterkte maatregelen rondom cybersecurityincidenten, zowel qua preventie, detectie en response. Naast deze brede initiatieven zijn er ook diverse initiatieven die toegespitst zijn op specifieke sectoren, zoals de Digital Operational Resilience Act (DORA) voor de financiële sector in 2023, de Artificial Intelligence Act (AIA) en de Digital Services Act (DSA) in 2024. De EU-lidstaten zijn momenteel bezig om deze Europese beleidskaders te implementeren in hun wetgeving.

Het feit dat er wet- en regelgeving is, is op zich goed. Echter, de constatering dat er een wirwar aan wetten en regels dreigt, is een punt van zorg. De tijd zal uitwijzen hoe effectief dit zal bijdragen om cybersecurity te verbeteren.

Daarnaast geldt dat cyberaanvallen niet aan landsgrenzen gebonden zijn.

Een aanvaller kan via het internet in principe vanaf zowat elke plek op aarde een cyberaanval uitvoeren en aanvallers slagen er ook goed in om hun sporen te maskeren. Bovendien hebben cyberaanvallen uitgevoerd door statelijke actoren een geheel eigen dynamiek.

2.3.3 Huidige stand van zaken

In de jaarlijkse 'Cybersecuritymonitor' geeft het CBS een globale indruk van het ICT-beveiligingsniveau van Nederlandse bedrijven aan de hand van statistieken over twaalf basismaatregelen voor cybersecurity, te weten: antivirussoftware, updaten van software/besturingssysteem, authenticatie via soft- of hardwaretokens, beleid voor sterke wachtwoorden, network access control, VPN internetgebruik buiten het bedrijf, encryptie van data, gegevensopslag op andere fysieke locatie, logbestanden voor analyse van incidenten, methodes voor beoordelen van ICT-veiligheid, risicoanalyses en cursussen aan ICT-specialisten. De Cybersecuritymonitor 2023 [59] laat zien dat met name grotere bedrijven maatregelen nemen. In 2022 had meer dan 90% van bedrijven met meer dan 50 werknemers minimaal vijf van deze maatregelen genomen. Bij kleinere bedrijven was dit beduidend lager: 71% bij bedrijven met 10 tot 50 werknemers en 41% van bedrijven met 2 tot 10 werknemers. Daarnaast is er ook variatie per bedrijfstak: in 2022 had bijvoorbeeld 77% van de bedrijven in de ICT minimaal vijf maatregelen genomen, versus 52% van bedrijven in de industrie en slechts 24% van de bedrijven in de horeca. Hoewel de situatie in de afgelopen jaren licht verbeterd is in nagenoeg alle bedrijfstakken, is er nog veel ruimte voor verbetering, met name bij kleinere bedrijven.

Ook internationaal geldt dat nog steeds veel organisaties er zelfs niet in slagen om basismaatregelen te implementeren, zoals een onderzoek van de Amerikaanse National Security Agency (NSA) en de Cybersecurity and Infrastructure Security Agency (CISA) in 2023 uitwees [68]. Dit ondanks het gegeven dat het implementeren van basismaatregelen doorgaans relatief weinig kost: 20% van de kosten kan al voorzien in 80% van de voordelen [58]. Het is paradoxaal dat het merendeel van incidenten niet te wijten is aan het feit dat aanvallers nieuwe of geavanceerde exploits gebruiken om securitymaatregelen te omzeilen, maar aan het ontbreken van basismaatregelen [44].

Hoewel er zeker lichtpuntjes zijn, kunnen we eigenlijk niet anders concluderen dan dat het momenteel niet zo best is gesteld met cybersecurity. We zien dat burgers, private en publieke organisaties en overheden te lijden hebben onder cybersecurityincidenten, en dat het in de afgelopen decennia nauwelijks beter is gegaan. Al jaren wordt wijdverbreid onderkend dat de noodzaak groot is om hier iets aan te doen. Maar ondanks alle inspanningen laten de feiten zien dat we er maar niet in slagen om cybersecurity op orde te krijgen. Dat roept de vraag op waar dat nu aan ligt. In het volgende hoofdstuk ga ik verder in op de oorzaken daarvan.

3 Waarom is cybersecurity een chronisch probleem?

In het vorige hoofdstuk schetste ik dat onze kennis en kunde omtrent cybersecurity zich in de afgelopen 50 jaar, vanaf het ontstaan van het vakgebied eind jaren 60 tot op heden, sterk heeft ontwikkeld. Er is heel wat vooruitgang geboekt op allerlei terrein. Echter, we zagen ook dat het niet evident is om maatregelen in praktijk te brengen, dat cyberincidenten nog steeds aan de orde van de dag zijn en dat de impact van cyberaanvallen zelfs toegenomen is. We kunnen dus wel stellen dat cybersecurity een chronisch probleem is, waar we toch maar moeilijk vat op krijgen. Waar ligt dat aan? In dit hoofdstuk geef ik een antwoord op deze vraag. Er is geen eenvoudig antwoord en vele factoren spelen een rol [69]. Het antwoord is dan ook niet uitputtend, maar ik zet de belangrijkste oorzaken op een rij.

3.1 Een snel veranderende wereld

De informatietechnologie ontwikkelt zich razendsnel op een wijze die we eerder als revolutionair dan als evolutionair kunnen bestempelen. Zie de snelle opmars van het internet, smartphones en heel recent AI als voorbeelden. Het beeld is telkens dat nieuwe technologie beschikbaar komt die snel door gebruikers omarmd wordt. Met de ontwikkeling van die technologie gaan grote investeringen gepaard. Bedrijven die producten ontwikkelen en aanbieden zijn erbij gebaat om snel op de markt te komen en een zo groot mogelijk marktaandeel te veroveren. Hun prioriteit is immers geld verdienen. Security is helaas nog steeds een aspect dat onvoldoende aandacht krijgt bij de ontwikkeling van nieuwe technologie. Elke nieuwe technologie brengt nieuwe zwakheden en kwetsbaarheden met zich mee die door aanvallers uitgebuit kunnen worden. En terwijl we nog aan het worstelen zijn om de security van de huidige technologie op orde te krijgen, doet de volgende generatie technologie al haar intrede. We lopen daarmee voortdurend achter de feiten aan.

Daarnaast ontwikkelen aanvallen en aanvallers ook voortdurend. Er worden dagelijks nieuwe kwetsbaarheden ontdekt in hardware en software producten. Aanvallers zijn inventief en bedenken nieuwe aanvalsvormen. Voorbeelden zijn de opkomst van ransomware, die zich met name in de afgelopen tien jaar sterk heeft uitgebreid [35], en supply chain attacks [62]. Er geldt dus dat niet alleen datgene wat we moeten beveiligen, namelijk IT-systemen en digitale processen, zich razendsnel ontwikkelen en voortdurend veranderen, maar ook datgene waartegen we moeten beveiligen, namelijk aanvallers en aanvallen. Cybersecurity holt daarmee voortdurend achter de feiten aan.

3.2 Tegenstrijdige doelen

Een fundamenteel probleem is verder dat cybersecurity een aantal tegenstrijdige doelen nastreeft. De drie kerndoelen van cybersecurity zijn beschikbaarheid, integriteit en vertrouwelijkheid. Met beschikbaarheid bedoelen we dat IT-infrastructuur beschikbaar moet zijn. Als die doelbewust verstoord wordt, zodat systemen en online diensten niet meer beschikbaar zijn, hebben we een probleem. Met integriteit bedoelen we dat IT-systemen betrouwbaar moeten zijn. We moeten ervan uit kunnen gaan dat IT-systemen niet zomaar aangepast kunnen worden. En tot slot wordt met vertrouwelijkheid bedoeld dat we confidentiële gegevens ook geheim moeten kunnen houden. Het is een groot probleem als bijvoorbeeld wachtwoorden, bedrijfsgeheimen of staatsgeheimen uitlekken en in verkeerde handen vallen.

Met cybersecurity willen we die drie doelen tegelijk beschermen. Een fundamenteel probleem is dat die doelen elkaar deels bijten. Met name staat beschikbaarheid haaks op integriteit en vertrouwelijkheid. Dat is eenvoudig in te zien. Stel je bezit iets kostbaars dat je wilt beschermen. Je wilt bijvoorbeeld niet dat anderen daar weet van hebben (vertrouwelijkheid beschermen), en je wilt al helemaal niet dat anderen dat kunnen manipuleren of ontvreemden (integriteit beschermen). Een oplossing is om de kostbaarheden achter dikke muren te plaatsen. Daar staan ze veilig en kan niemand erbij. Nou hebben we wel een probleem, want als echt niemand erbij kan, kunnen we er zelf ook niet meer bij. Er zit niets anders op dan dat we toch een deurtje moeten maken om erbij te kunnen (om beschikbaarheid mogelijk te maken). En daar beginnen de problemen, want als jij door de deur kan, kunnen anderen dat ook. Je moet die deur gaan beveiligen, bijvoorbeeld door er een slot op te monteren. Nu is de moeilijkheid niet alleen dat dat slot deugdelijk moet zijn, maar ook dat je de sleutel zorgvuldig bewaart. Eigenlijk zijn we nu weer terug bij af. Want in plaats van de kostbaarheden zelf te beschermen, moeten we nu de sleutel beschermen.

In cybersecurity speelt precies ditzelfde probleem. Naast sloten en sleutels hebben we ook te maken met autorisatie: welke partijen hebben rechten om bij bepaalde data of systemen te kunnen of om bepaalde acties uit te voeren. En we moeten daarbij natuurlijk ook kunnen vaststellen wie een partij is. Dat is de authenticatie: het kunnen bevestigen van de identiteit van een gebruiker of een systeem. Het is verre van triviaal om dat goed op orde te krijgen.

3.3 De aard van cybersecurity

Zoals al gesteld in de introductie (zie sectie 1.1) is cybersecurity geen doel op zichzelf, maar een middel om een hoger doel te bereiken, namelijk vertrouwen opbouwen in de betrouwbaarheid van onze IT-infrastructuur en digitale processen, zelfs als deze worden aangevallen. Daarbij doet zich het probleem voor

dat dit hogere doel niet heel concreet is gedefinieerd en ook lastig te vangen is in kwalitatieve of kwantitatieve maatstaven.

Puur vanuit economisch oogpunt is cybersecurity iets waar je liever geen geld aan besteedt. Immers, het voegt in feite nauwelijks iets toe aan bijvoorbeeld de functionaliteit, bruikbaarheid of waarde van systemen. Sterker nog, vaak staan securitymaatregelen de gebruiksvriendelijkheid eerder in de weg. En cybersecurity is verder niet de enige zogenaamde non-functionele eis die we aan systemen stellen. Het is afwegen waaraan tijd en geld te besteden en zaak om de juiste balans te vinden en te behouden.

In de kern is cybersecurity risicomanagement. Het is zaak om risico's in kaart te brengen en in te schatten hoe ernstig en hoe waarschijnlijk deze risico's zijn. Aan de hand daarvan kan bepaald worden hoeveel tijd en middelen besteed zouden moeten worden om de risico's te beteugelen, en welke maatregelen uiteindelijk genomen worden. Daarbij doen zich verdere problemen voor, namelijk dat het lastig aan te geven is wat de huidige risico's zijn, laat staan wat de impact en waarschijnlijkheid ervan is, en onvoorspelbaar wat de risico's in de nabije toekomst zullen zijn. Immers, zowel datgene wat beveiligd moet worden, namelijk onze IT-infrastructuur en digitale processen en onderliggende technologie, als datgene waartegen we moeten beveiligen, namelijk de aanvallers en aanvallen, veranderen voortdurend. Het beste wat we kunnen doen is risicomanagement als een continu proces beschouwen dat voortdurend aandacht vraagt, maar dan nog biedt het geen garantie. Verder geldt dat risicomanagement voor cybersecurity niet universeel is, maar afhangt van de context. Het maakt nogal verschil of je risico's beschouwt in de context van de computer van een consument of van een elektriciteitscentrale.

Aangezien de risico's deels onbekend en onvoorspelbaar zijn, kwamen we al rond 2000 tot het inzicht dat naast cybersecurity in toenemende mate behoefte is aan cyberresilience [48]. Daarbij is de gedachte dat je ervan uit moet gaan dat je slachtoffer wordt van een cyberaanval, en dat je daartegen bestand moet zijn en ervan moet kunnen herstellen. En nog een stap verder is, volgens het idee van antifragiliteit, dat je ervan leert en sterker wordt [73]. In feite moet iedereen en elke organisatie ervan uit gaan dat je slachtoffer wordt. Het is niet de vraag of dat gebeurt, maar wanneer. Het is dan ook cruciaal om plannen en maatregelen gereed te hebben over hoe je de schade kunt beperken en kunt overleven.

In feite moeten we van cybersecurity naar cyberresilience en antifragiliteit nog een stap verder. Als de risico's dermate worden dat ze een te grote dreiging vormen waartegen we ons niet meer adequaat kunnen beschermen, rest er weinig anders dan drastische maatregelen. En dat betekent bijvoorbeeld dat we op kritieke gebieden de afhankelijkheid van IT eerder moeten verkleinen dan vergroten. Dat geldt op meerdere niveaus.

Een eerste voorbeeld is het vermijden van technologie met inherente kwetsbaarheden. We weten al decennialang dat de programmeertalen C/C++ niet memory safe zijn. Ondanks het feit dat er enorm veel onderzoek naar is ge-

daan en vele oplossingen zijn aangedragen, blijft memory safety een uitermate hardnekkig probleem. Zo gaven bijvoorbeeld zowel Microsoft als Google rond 2020 aan dat in het afgelopen decennium 65% tot 70% van de security vulnerabilities in hun software gerelateerd waren aan memory safety [81, 82]. Beide bedrijven hebben geconcludeerd dat de tijd rijp is om over te stappen op modernere programmeertalen die wel memory safe zijn, met name Rust. En dat zet zoden aan de dijk: Google rapporteerde dat het aantal memory safety kwetsbaarheden in Android van 2019 tot 2022 is afgenomen van 76% naar 35%, wat met name toegeschreven wordt aan gebruik van memory-safe programmeertalen.

Een ander voorbeeld is het besluit van minister-president Dick Schoof in augustus om voortaan alle telefoons en elektronische apparaten te verbieden tijdens vergaderingen van het kabinet [86]. Dit om spionagedreiging af te wenden waarbij aanvallers mee kunnen luisteren via gehackte apparaten. Het is een draconische maatregel, maar momenteel wel de enige maatregel die risico's volledig uitsluit, op voorwaarde natuurlijk dat de maatregel ook nageleefd en gehandhaafd wordt. Dat vormt meteen de brug naar een andere factor die bijdraagt aan het chronische probleem met cybersecurity, namelijk de menselijke factor.

3.4 Menselijke factoren

De mens is niet alleen aanvaller, maar de mens is ook de ontwikkelaar en gebruiker van informatietechnologie. De ontwikkelaars van hardware en software producten hebben vaak onvoldoende kennis en middelen om security te implementeren, en dat dan nog los van de inherente beperkingen van technologie. Bij ontwikkeling is het ook essentieel om te beschouwen hoe mensen die technologie of producten gaan gebruiken. Het daarop anticiperen is niet eenvoudig. Er zijn talloze voorbeelden van securitymaatregelen die we hinderlijk vinden en die we het liefst omzeilen. Voorbeelden daarvan zijn het negeren van vragen over het accepteren van cookies op websites, het blindelings goedkeuren van machtigingen bij het installeren van apps, of het wegklikken van onbegrijpelijke beveiligingswaarschuwingen. Er valt nog heel wat te winnen op gebied van 'usable security'. Expertise uit de psychologie en cognitieve wetenschappen zijn van cruciaal belang om te begrijpen hoe bruikbaarheid de security beïnvloedt en vice versa.

Er zijn veel factoren die een rol spelen bij de mens als gebruiker van informatietechnologie [9]. Mensen zijn niet perfect: we maken fouten; we overtreden onbewust regels en procedures rondom cybersecurity als we deze niet kennen of er niet bewust aandacht aan schenken; soms overtreden we bewust regels en procedures, vooral als securitymaatregelen de gebruiksvriendelijkheid in de weg zitten; we handelen soms irrationeel; en we zijn ons soms niet bewust van risico's of kunnen deze niet goed inschatten. De mens wordt daarom in het algemeen beschouwd als de zwakste schakel in de keten van

cybersecurity. En aanvallers weten dat uiteraard en buiten dat op slinkse wijze uit door middel van social engineering.

We proberen menselijk gedrag te reguleren met wet- en regelgeving. Dat is alleen effectief als mensen ervan weten, als mensen deze willen en kunnen naleven, en dat er gehandhaafd wordt als mensen in gebreke blijven. Daarnaast is ook onderwijs en training noodzakelijk om mensen bewust te maken van de gevaren en hen te leren wat wel en niet te doen. Daarbij spelen ook opvoeding, cultuur en ethiek een rol. Het is bijvoorbeeld gebleken dat niet het gebrek aan kennis of bewustzijn de voornaamste redenen zijn om beveiligingsprocedures niet na te leven in organisaties, maar de impliciete organisatiecultuur [37].

3.5 Technologie

De geschiedenis leert dat we niet goed in staat zijn om technologie te ontwikkelen die robuust is tegen toekomstige securitygevaren. In elk decennium worden nieuwe technologieën geïntroduceerd met nieuwe kwetsbaarheden, terwijl tegelijkertijd de kwetsbaarheden van vorige generaties technologie nog niet verholpen zijn. We moeten gelijktijdig meerdere generaties technologie beheren: Er worden continu nieuwe hardware en software systemen geïntroduceerd; er is een continue stroom van updates en patches van bestaande systemen, waarbij security soms ondermijnd wordt door eisen aan interoperabiliteit en backward compatibiliteit; en we hebben te maken met verouderde 'legacy' systemen die al lang het einde van hun levensduur of einde van de service hebben bereikt, zonder gekwalificeerd personeel. We weten ook niet hoe de technologie van morgen eruit zal zien, en hoe die nieuwe technologie de security van de bestaande technologie zal beïnvloeden, en welke nieuwe aanvalsvormen er zullen verschijnen.

Een tweede aspect van technologie dat roet in het eten gooit, is het feit dat het bij de huidige stand van de techniek vrijwel onmogelijk is om systemen te ontwikkelen waarvan we zeker weten dat ze geen zwakheden of kwetsbaarheden bevatten. De kwaliteit van systemen hangt enerzijds af van hoe goed we ons best doen. We hebben ontwikkelmethoden waarin we in vrijwel elke fase activiteiten kunnen uitvoeren om security te verbeteren. Denk bijvoorbeeld aan formele verificatie, statische codeanalyse van software en dynamische analyse door middel van testen en pentesten. Hoe meer we verifiëren, analyseren en testen, hoe beter de kwaliteit, maar 100% garantie op de afwezigheid van zwakheden of kwetsbaarheden is onmogelijk. En naast theoretische beperkingen, spelen ook praktische beperkingen een rol. We kunnen immers slechts een beperkte hoeveelheid tijd en middelen besteden. En daarnaast geldt dat de gehele keten van toeleveranciers betrouwbaar moet zijn, inclusief de tools die we gebruiken.

En daarmee raken we een derde aspect, en dat is de ongekende complexiteit van systemen. Een computersysteem, of dat nu een desktop, een laptop, een server of een smartphone is, bestaat uit hardware componenten zoals

geheugenchips en een microprocessor. Op die hardware wordt software uitgevoerd, bestaande uit een besturingssysteem en applicaties. Elk van deze hardware en software componenten zijn op zich al enorm complex. En computersystemen zijn via netwerken met elkaar verbonden. Om security te kunnen garanderen, is het vereist dat we de security van elk afzonderlijk onderdeel aantonen, en ook dat het geheel van samenwerkende onderdelen secure is. Dat is een vrijwel onmogelijke opgave.

3.6 Asymmetrie

Een laatste factor die cybersecurity tot een chronisch probleem maakt, is asymmetrie tussen de verschillende stakeholders.

Een eerste vorm van asymmetrie zit tussen aanvallers en verdedigers. De aanvallers zijn in het voordeel: een aanvaller heeft immers voldoende aan één zwakke plek in een systeem die uitgebuit kan worden. Als verdedigers moeten we daarentegen alle zwakke plekken aanpakken. Daarbij speelt zoals we zagen niet alleen dat het aantal zwakke plekken enorm groot is, maar ook dat we niet eens weten dat er zwakke plekken zijn (de 'zero days'). Dat geldt niet alleen voor specifieke producten, maar ook voor de technologie die in deze producten wordt toegepast. Bijvoorbeeld, aanvallers maken tegenwoordig gebruik van de beschikbare AI-tools om aanvallen voor te bereiden en uit te voeren. Om zulk offensief gebruik van AI-tools aan te pakken, is diepgaande kennis van AI vereist. Daarnaast kunnen aanvallers zich snel aanpassen en zijn ze niet gebonden aan enige spelregel; ze zijn niet gebonden aan tijd of plaats en kunnen aanvallen uitvoeren op de meest ongelegen momenten (zie bijvoorbeeld de ransomware-aanval op de Universiteit Maastricht in 2019 net voor Kerstmis) en vanaf elke plek ter wereld; ze hebben alle tijd om een aanval voor te bereiden; ze kunnen grootschalige aanvallen uitvoeren met relatief eenvoudige apparatuur; ze zijn intelligent en beschikken vaak over de modernste technologie en ruime middelen. Er is sprake van een wapenwedloop: we beveiligen onze systemen met nieuwere en sterkere maatregelen, en aanvallers weten die telkens weer te omzeilen of hele andere manieren te vinden om aanvallen uit te voeren.

Een tweede vorm van asymmetrie zit tussen consumenten en producenten van systemen. Als consumenten zijn wij lang niet altijd in staat om te beoordelen hoe goed een systeem beveiligd is. En als we dat niet goed kunnen beoordelen, zijn we ook niet geneigd om ervoor te betalen. Als bij aankoop keuze is tussen een goedkoop en een duur systeem, waarvan het duurdere systeem zogenaamd veiliger is, valt de keuze op het goedkopere systeem. Dit leidt tot de welbekende 'market for lemons', waardoor goedkope maar kwalitatief minderwaardige systemen de overhand krijgen.

Een derde vorm van asymmetrie is dat de ene partij de kosten draagt voor securitymaatregelen, maar dat een andere partij er baat bij heeft. Bijvoorbeeld, als een systeem gehackt is en deel uitmaakt van een botnet dat ge-

bruikt wordt om een DDOS-aanval uit te voeren, heeft de eigenaar van dat systeem er nauwelijks last of weet van; het slachtoffer van de aanval draagt de kosten. Daarnaast geldt ook dat de securityindustrie erbij gebaat is om zichzelf in stand te houden, waardoor er soms eerder sprake lijkt van symptoombestrijding dan problemen bij de basis aanpakken.

3.7 Conclusie

Ik schetste zojuist een niet bepaald rooskleurig beeld van cybersecurity. We leven in een samenleving die vol inzet op digitale transformatie. We gaan steeds meer gebruik maken van informatietechnologie. We zijn er zo langzamerhand volledig afhankelijk van geworden en er is nauwelijks een weg terug. Dat maakt ons enorm kwetsbaar. De factoren die ervoor zorgen dat cybersecurity een chronisch probleem is, zorgen ervoor dat we de strijd niet kunnen winnen. Dan rijst de vraag: wat nu? Het antwoord op die vraag wordt treffend verwoord met een uitspraak van Johan Cruijff (1947-2016): *Als je niet ken winnen, moet je zorgen dat je niet verliest*. We kunnen de slag om cybersecurity weliswaar niet winnen en zullen er nooit in slagen om cybersecurity 100% waterdicht te maken, maar we hebben geen andere keuze dan ons uiterste best te doen om cybersecurity te verbeteren. Het is een kwestie van pompen of verzuipen.

4 Hoe kan cybersecurity verbeteren?

In dit hoofdstuk beschrijf ik hoe mijn leerstoel gaat bijdragen om de toestand van cybersecurity te verbeteren. Ik licht eerst de onderzoeksagenda toe en vervolgens de plannen voor onderwijs.

4.1 Onderzoek

4.1.1 Onderzoekslijn Security & Privacy

De faculteit Bètawetenschappen van de OU heeft in 2024 haar onderzoeksstrategie vernieuwd met als titel 'New Horizons for Science' [70]. Een integraal onderdeel daarvan is het onderzoeksprogramma 'Towards High-quality and Intelligent Systems (THIS)' van de vakgroep Informatica. Dat onderzoeksprogramma omvat vier onderzoekslijnen: Artificial Intelligence onder leiding van professor Natasha Alechina, Computer Science Education onder leiding van professor Erik Barendsen, Software Engineering onder leiding van professor Tanja Vos en Security & Privacy onder mijn leiding. Deze vier onderzoekslijnen zijn nauw aan elkaar verbonden en zijn gericht op de vraag hoe we computersystemen, en met name software en AI, kunnen ontwikkelen die niet alleen correct maar ook veilig ('safe') en beveiligd ('secure') zijn.

De leerstoel Cyber Security staat centraal in de onderzoekslijn Security & Privacy. De leerstoel is er met name op gericht om deze onderzoekslijn verder uit te bouwen en de synergie tussen onderzoekers verder te versterken. De onderzoekslijn heeft tot doel software- en computersystemen te beveiligen, waarbij de nadruk ligt op maatregelen voor het voorkomen en detecteren van en verdedigen tegen bedreigingen. De onderzoekslijn analyseert kwetsbaarheden van moderne ICT-technologieën die een gevaar vormen voor cybersecurity en privacy, en zoekt naar oplossingen om deze te verhelpen. De onderzoekslijn concentreert zich op drie globale onderzoeksvragen:

- Wat zijn kwetsbaarheden die bedreigingen voor security en privacy veroorzaken, en wanneer en waarom doen ze zich voor?
- Hoe kunnen we deze bedreigingen voorkomen of ertegen verdedigen?
- Wat is de invloed van menselijke factoren?

Om een impressie te geven van de onderzoekslijn, beschrijf ik kort het onderzoek van de onderzoekers die werkzaam zijn in deze onderzoekslijn. Mijn eigen onderzoek volgt in de volgende sectie (4.1.2).

Dr. Fabian van den Broek doet onderzoek op gebied van authenticatie [17] en privacy [26]. Zijn onderzoek is onder meer gericht op attribute-based credentials en privacy-preserving technologies. Hij onderzoekt met name oplossingen en implementaties voor authenticatie en identity management, zoals de IRMA/Yivi app, recente ontwikkelingen vanuit de industrie, zoals identity aware proxies en passkeys, en de vernieuwing van de eIDAS en de daarin besloten Europese eID oplossingen.

Dr. Hugo Jonker doet onderzoek naar web security en privacy en is tevens actief op gebied van digitaal-forensisch onderzoek. In zijn onderzoek op gebied van web security en privacy was hij onder meer copromotor van Benjamin Krumnow, buitenpromovendus van Fachhochschule Köln, die in 2023 aan de OU promoveerde op het proefschrift 'Web scrapology: overcoming limits of automating web measurements' [21]. Dit onderzoek is gericht op hoe je geautomatiseerd, op grote schaal en op betrouwbare wijze metingen kunt uitvoeren aan het world wide web. In het digitaal-forensisch onderzoek was hij onder meer copromotor van Vincent van der Meer, buitenpromovendus van Zuyd Hogeschool, die in 2024 aan de OU promoveerde op het proefschrift 'Improving foundations of file recovery: a digital forensics perspective on file fragmentation, timestamps, and JPEG validation' [33]. Dit onderzoek is gericht op hoe je verwijderde bestanden op gegevensdragers zoals harde schijven terug kunt vinden, in het bijzonder gefragmenteerde JPEG-bestanden. Bij beide promoties fungeerde ik als promotor. Tevens doet dr. Jonker onderzoek op gebied van het automatiseren van Open Source Intelligence (OSINT), waarbij data uit diverse bronnen wordt verzameld en gecorreleerd. Een toepassing daarvan is bijvoorbeeld de security van het wetenschappelijk publicatieproces, zoals detectie van onethisch handelen door editors en reviewers rondom citaties en auteurschap.

Dr. Clara Maathuis doet multidisciplinair onderzoek op het raakvlak tussen cybersecurity en AI, waarbij ze zich met name richt op de domeinen defensie en sociale media [27–30]. Haar onderzoek concentreert zich op het bouwen van AI-gebaseerde systemen die verantwoordelijk, veilig, betrouwbaar en mensgericht zijn. Daarbij kijkt ze naar bedreigingen bij toepassing van generatieve AI en LLMs, zoals desinformatie, hallucinaties, en aanvallen. Ook kijkt ze naar hoe generatieve AI en LLM-technologie ingezet kan worden voor detectie van desinformatie en ransomware. Ze doet tevens onderzoek naar aspecten van cybersecurity bij internationale conflicten en verantwoorde, mensgerichte oplossingen in besluitvorming bij militaire operaties.

Dr. Mina Sheikhalishahi doet onderzoek op het snijvlak van privacy en AI, waarbij de uitdaging is om gegevensbescherming te waarborgen zonder afbreuk te doen op de prestaties van AI-modellen [1, 2, 14, 46]. Haar onderzoek is onder meer gericht op de selectie van privacybehoudende features in AI-modellen en federated learning. Een toepassing van haar onderzoek is onder andere privacy en gegevensbescherming in het medische domein, waar een uitdaging is om de balans te vinden tussen de bruikbaarheid en privacy

van genetische gegevens van individuen voor medisch onderzoek. Een andere toepassing is privacy en gegevensbescherming in diensten die gebruik maken van locatiegegevens van personen in gebouwen, door gevoelige informatie over bewegingspatronen te verdoezelen. Recent doet ze ook onderzoek naar betrouwbare AI-modellen die voldoen aan ethische en juridische standaarden. Daartoe onderzoekt ze onder meer de wisselwerking tussen privacy en fairness.

Dr. Stefano Schivo doet onderzoek naar het toepassen van formele methoden voor het analyseren van security (en safety) eigenschappen van systemen, onder meer met behulp van attack trees. Zijn huidige onderzoek is met name gericht op industriële controlesystemen en safety-critical systemen, waarbij hij een hybride benadering toepast door formele modellen aan te vullen met machine learning voor anomaly detection. Een onderdeel daarvan is het creëren van datasets die realistische scenario's simuleren.

4.1.2 Onderzoeksagenda: lopend onderzoek

In de afgelopen jaren heeft mijn onderzoek zich op vijf verschillende aspecten van cybersecurity gericht, die ik in deze sectie kort toelicht.

Virtuele security labs

Een eerste onderwerp van onderzoek is de ontwikkeling van een innovatief virtueel security lab: een virtuele, geïsoleerde computeromgeving waarin studenten opdrachten en experimenten kunnen uitvoeren in de rol van zowel aanvaller als verdediger op het gebied van netwerkbeveiliging. Tegenwoordig is virtualisatie een gangbare technologie, maar toen we dit onderzoek startten in 2006 stond virtualisatie nog in de kinderschoenen. Het onderzoek richt zich enerzijds op de technische infrastructuur van zo'n lab en anderzijds op hoe zo'n lab effectief in het onderwijs kan worden ingezet. Het resulterende virtuele security lab wordt inmiddels al ruim 15 jaar gebruikt door onze studenten in de cursus 'Security en IT' van de bacheloropleiding Informatica aan de OU. Jens Haag werkte als buitenpromovendus van de Fachhochschule Köln aan de uitbreiding van het security lab naar een gedistribueerd security lab waarin groepen studenten aan de slag kunnen, en waar studenten ook geautomatiseerd feedback ontvangen. Jens Haag promoveerde in 2018 aan de OU op het proefschrift 'DVCL: a distributed virtual computer lab for security and network education' [16]. In de afgelopen jaren vernieuwden we de infrastructuur van het security lab door gebruik te maken van Docker containers in samenwerking met professor Jörg Keller van de FernUniversität in Hagen, waarbij studenten van de OU en Fernuni ook het lab gebruikten en samenwerkten in internationale teams.

Bruikbare security

Een tweede onderwerp van onderzoek is bruikbare en gebruiksvriendelijke security. In een onderzoeksproject onder leiding van professor Wouter Stol van de faculteit Rechtswetenschappen en in samenwerking met Nederlandse banken, werkte een multidisciplinair team van vier promovendi aan aspecten van online bankieren. Wij deden vanuit informatica daarin mee en samen met professor Marko van Eekelen en promovendus Sven Kiljan onderzochten we aspecten rondom authenticatie. Sven Kiljan promoveerde in 2017 aan de OU op het proefschrift 'Exploring, expanding and evaluating usable security in online banking' [19].

Duurzaamheid

Een derde onderwerp van onderzoek is gericht op duurzaamheid. In de periode 2015-2020 was ik in de toenmalige faculteit MST van de OU een van de grondleggers van het multidisciplinaire onderzoeksprogramma 'Learning and Innovation in Resilient Systems (LIRS)' onder leiding van professor Carolien Kroeze, tegenwoordig rector magnificus van Wageningen University & Research. In het kader van dat onderzoeksprogramma deed ik onderzoek naar het energieverbruik dat nodig is voor het beveiligen van blockchain-applicaties, in het bijzonder cryptovaluta zoals bitcoin. Ik was een van de eerste wetenschappers die aantoonden dat bitcoin mining een enorme hoeveelheid energie vereist. Mijn publicatie 'Sustainability of bitcoin and blockchains' in 2017 [52] was een schot in de roos. De publicatie is inmiddels meer dan 700 keer geciteerd en leidde tot wereldwijde media-aandacht waaronder optredens op tv in het NOS-journaal en radio in BBC Newshour en vermeldingen in The Washington Post [97]. Over de schattingen van het elektriciteitsverbruik van bitcoin is ook in de wetenschappelijke literatuur heel wat debat [32]. De meest betrouwbare schatting is dat vandaag de dag ruim 0,5% van het wereldwijde elektriciteitsverbruik aan bitcoin mining wordt verspild [77]. Een absurde situatie in het licht van klimaatdoelstellingen en duurzaamheid, en des te meer vanuit het oogpunt dat cryptovaluta een voedingsbodem vormen voor cybercriminaliteit [61]. In de afgelopen jaren heb ik samen met OU-onderzoekers dr. Ashish Sai en Elitska Pankovska gewerkt aan de betrouwbaarheid van methoden om energieverbruik in te schatten [41], en naast bitcoin ook het energieverbruik van Ethereum en Filecoin in kaart gebracht [36]. Daarbij werkten we samen met een team van Protocol Labs onder leiding van dr. Alan Ransil, die het onderzoek ook financierde.

Toepassing van AI voor netwerk security

Een vierde onderwerp van onderzoek is gericht op de toepassing van AI in cybersecurity. Reeds in 2015 startte ik onderzoek waarbij we keken naar hoe AI ingezet kan worden voor de analyse van netwerkverkeer. De aanpak

daarbij is om grote datasets van netwerkverkeer te doorzoeken op zoek naar sporen van cyberaanvallen. We gebruiken een deel van de dataset om een AI-model te trainen, en een ander deel van de dataset om te evalueren hoe goed het getrainde model in staat is om anomalieën of cyberaanvallen te detecteren. Een van de uitdagingen in dit soort onderzoek is hoe je aan zulke datasets met realistische data komt. We hebben daartoe samengewerkt met SURF, SIDN Labs en het NCSC, die niet alleen data uit hun netwerken ter beschikking stelden maar ook zowel financieel als met computerfaciliteiten bijdroegen aan het onderzoek. In onderzoeksprojecten hebben we gekeken naar de detectie van botnets in zowel geaggregeerd TCP/IP-verkeer [50] als DNS-verkeer [51], alsmede naar gemengd darknet-verkeer dat verschillende cyberaanvallen bevatte [22]. Ook hebben we onderzoeksprojecten uitgevoerd waarin we netwerkverkeer classificeerden [3], waarin we naar kwetsbaarheden zochten in IOT-netwerken [49], en waarin we data exfiltratie detecteerden [53]. Aan dit onderzoek werkte een groot aantal studenten mee, in de vorm van afstudeeropdrachten van masterstudenten van de OU en Radboud Universiteit, research visits van promovendi waaronder van de University of Jyvaskyla in Finland, en post-doc onderzoeker dr. Hassan Alizadeh.

In deze onderzoeken pasten we een groot aantal methoden en technieken toe uit machine learning en deep learning, gebaseerd op zowel supervised als unsupervised learning. De uitdaging in deze onderzoeken is niet alleen om AI-modellen te trainen die netwerkverkeer op de juiste wijze classificeren, maar ook voldoen aan eisen uit de praktijk. Zo moeten ze grote hoeveelheden netwerkveer nagenoeg realtime kunnen analyseren en snel aangepast en hertraind kunnen worden als de samenstelling van netwerkverkeer verandert. Ook is het van belang om het aantal vals-positieve detecties te minimaliseren en moet inzichtelijk zijn op basis waarvan de modellen tot beslissingen komen. Om hieraan te voldoen, kijken we naar compacte en efficiënte modellen die met een beperkte verzameling features werken. Dit is daardoor een heel andere tak van sport dan de grootschalige large language modellen die voor generatieve AI worden toegepast en momenteel volop in de belangstelling staan.

Toepassing van AI voor software security

Een vijfde onderwerp van onderzoek is eveneens gericht op de toepassing van AI in cybersecurity, maar nu om kwetsbaarheden op te sporen in de broncode van software. We startten dit onderzoek rond 2017, toen dit onderwerp nog in de kinderschoenen stond. De traditionele manier om security kwetsbaarheden in broncode op te sporen is door toepassing van statische codeanalysetools voor static application security testing (SAST). Zulke tools maken gebruik van rulesets waarin patronen zijn vastgelegd om specifieke kwetsbaarheden te kunnen detecteren. De rulesets bepalen in belangrijke mate hoe goed een tool werkt en welke kwetsbaarheden gevonden kunnen worden. Daarnaast speelt het feit dat zulke tools nooit alle kwetsbaarheden kunnen vinden, ener-

zijds omdat dat theoretisch onmogelijk is volgens het theorema van Rice, en anderzijds omdat er praktische beperkingen zijn in de vorm van eisen aan hoeveelheid geheugen en rekentijd en de noodzaak om het aantal vals-positieve detecties te minimaliseren om de tools bruikbaar te maken. Ons onderzoek is gericht op de vraag of de toepassing van AI hier hulp kan bieden. We toonden aan dat het mogelijk is om gangbare kwetsbaarheden op te sporen, zoals SQL-injectie en XSS in PHP-code [20] en buffer overflows in C/C++-code [11]. We maakten daarbij niet alleen gebruik van datasets met gesynthetiseerde broncode, maar ook van broncode uit concrete softwareproducten en konden daarin kwetsbaarheden ontdekken. Recent toonden we ook aan dat vele andere kwetsbaarheden, ook in code in andere programmeertalen zoals C# en Java, hiermee opgespoord kunnen worden [12]. In dit onderzoek werkte ik nauw samen met dr. Arjen Hommersom en ook hier werkte een groot aantal masterstudenten mee tijdens hun afstudeeropdrachten.

In dit onderzoek passen we AI toe als gereedschap, en de uitdaging is met name hoe je broncode van software kunt vertalen naar een verzameling numerieke vectoren, waarbij voldoende informatie van zowel syntaxis als semantiek van de broncode behouden blijft om kwetsbaarheden op te kunnen sporen. We maken daarbij gebruik van methoden en technieken uit de compilertechnologie, zoals het representeren van programmacode in abstract syntax trees en control-flow en data-flow graphs, en moderne AI-technieken zoals graph neural networks.

4.1.3 Onderzoeksagenda: vooruitblik

In het voorgaande gaf ik een overzicht van het onderzoek waaraan ik in de afgelopen jaren heb gewerkt. De onderzoeksagenda voor de komende jaren is deels om dit onderzoek te continueren. Met name de toepassing van AI voor cybersecurity is een speerpunt. Daarnaast is ook deelnemen in multidisciplinair onderzoek een belangrijk aandachtspunt.

Cybersecurity en AI

Zoals geschetst in de voorgaande sectie (4.1.2) is de toepassing van AI voor cybersecurity een speerpunt van mijn onderzoek. Dat richt zich met name op de toepassing van AI in netwerk security en software security.

Op gebied van toepassing van AI in netwerk security zijn er diverse uitdagingen [4, 10, 15, 18, 23, 47]. Veel wetenschappelijk onderzoek waarin netwerkverkeer wordt geanalyseerd met behulp van machine learning, laten uitstekende resultaten zien binnen de context van de datasets die gebruikt zijn om een model te trainen. Echter, als de samenstelling van het netwerkverkeer wijzigt, worden de resultaten snel minder goed. Dat vormt een belemmering voor praktische toepassingen. In mijn onderzoek wil ik daarom kijken naar compacte en efficiënte modellen, die snel hertraind kunnen worden als het netwerkverkeer verandert. Dit vereist een vorm van 'double-loop learning',

waarbij niet alleen een model wordt getraind op basis van huidige data, maar ook wordt geleerd wanneer of waarom hertraining nodig is. Verder wil ik kijken naar gedistribueerde architecturen die bestaan uit meerdere compacte modellen die parallel opereren. Elk model kan daarin toegespitst worden op de detectie van bepaalde type netwerkverkeer.

Op gebied van toepassing van AI in software security zijn er eveneens diverse uitdagingen. De recente opkomst van generatieve AI en LLMs [8] heeft ertoe geleid dat dit deelgebied in een stevige stroomversnelling terecht is gekomen [7, 25, 45, 54–56]. In mijn onderzoek bestudeer ik hoe LLMs kunnen bijdragen aan statische codeanalyse. De insteek daarbij is niet zozeer om te onderzoeken hoe goed LLMs in staat zijn om kwetsbaarheden te ontdekken in programmacode, maar om te onderzoeken hoe LLMs statische codeanalyse kunnen ondersteunen. Daarbij gaat het met name om het kunnen verklaren waar en waarom een stuk programmacode een kwetsbaarheid bevat, en daarmee onderscheid te kunnen maken tussen echt-positieve en vals-positieve detecties. Als we vals-positieve detecties eruit kunnen filteren, opent dat de deur naar een andere afstelling van statische codeanalysetools. In de huidige tools is er immers een balans om het aantal vals-positieve detecties te reduceren omwille van bruikbaarheid, hetgeen ten koste gaat van vals-negatieve detecties ofwel kwetsbaarheden die niet worden gevonden. Ook de combinatie van statische en dynamische codeanalyse kan hierbij helpen, waarbij bijvoorbeeld de resultaten van statische codeanalyse worden gebruikt om testcases te genereren die vervolgens in dynamische analyse worden toegepast. Een volgende uitdaging is om de gedetecteerde kwetsbaarheden geautomatiseerd te kunnen repareren [6]. Zoals we zagen, worden dagelijks nieuwe kwetsbaarheden gevonden in softwareproducten, en automatisering om die kwetsbaarheden te repareren zou een flinke stap vooruit betekenen.

Er zijn diverse andere uitdagende toepassingen van AI in cybersecurity. Een eerste voorbeeld is de toepassing van AI bij threat modelling, waardoor securitymaatregelen reeds meegenomen kunnen worden bij het ontwerpen van systemen in de requirements- en designfase. Een tweede voorbeeld is de toepassing van generative adversarial networks (GANs) in detectie van anomalieën in netwerkverkeer en kwetsbaarheden in programmacode, waarbij realistische datasets worden gegenereerd om detectie en robuustheid van AI-modellen te verbeteren.

Naast de toepassing van AI om cybersecurity te verbeteren, is ook de security van AI zelf een uitdagend onderzoeksonderwerp.

Multidisciplinair onderzoek

Het kwam al diverse keren in deze oratie aan bod dat cybersecurity dermate complex en veelzijdig is, dat een multidisciplinaire aanpak broodnodig is. In mijn onderzoek zoek ik expliciet samenwerking met anderen onderzoekslijnen, zowel binnen het vakgebied informatica als daarbuiten.

Binnen het onderzoeksprogramma van de vakgroep Informatica zijn er

meerdere raakvlakken, zoals: het onderzoek van professor Natasha Alechina op gebied van safe en responsible AI; het onderzoek van professor Stefano Bromuri op gebied van AI en software engineering; het onderzoek van dr. Jesse Heyninck op gebied van kennisrepresentatie; het onderzoek van professor Tanja Vos op gebied van software testen; het onderzoek van dr. Freek Verbeek op gebied van formele verificatie om securityeigenschappen van binary code te bewijzen; het onderzoek van dr. Joshua Moerman op gebied van automata learning; en het digitaal-forensisch onderzoek van professor Harm van Beek.

Ook zijn er raakvlakken met het onderzoek van de vakgroep Informatiekunde, zoals: het onderzoek van professor Arno Nuijten op gebied van governance en menselijk gedrag bij IT-beslissingen; en het onderzoek van dr. Laury Bollen, dr. Tim Huygh en dr. Khoi Nguyen op gebied van IT governance en informatiebeveiliging, waarbij we inmiddels samenwerken met een externe promovendus naar hoe AI kan helpen om dynamische capaciteiten op het gebied van cyberbeveiliging te vergroten of op te bouwen in organisaties.

In mijn onderzoek wil ik ook expliciet aandacht geven aan onderzoekssamenwerking met andere disciplines. Er zijn verbanden met vrijwel alle disciplines waarin onderzoekers aan de OU actief zijn. Ik geef enkele voorbeelden: vanuit managementwetenschappen: risicomanagement alsmede het managen van processen rondom cybersecurity in alle lagen van organisaties; vanuit rechtswetenschappen: wet- en regelgeving rondom cybersecurity, gegevensbescherming en privacy; vanuit sociale wetenschappen: het bewustmaken van mensen van de risico's van cybersecurity door voorlichting, onderwijs en training zodat ze hun gedrag kunnen aanpassen, maar ook bij het nemen van cybersecuritymaatregelen rekening houden met de verschillende gedragingen van mensen; vanuit maatschappijwetenschappen in bredere zin: politieke keuzes die worden gemaakt om onze digitale samenleving weerbaarder te maken, en hoe we privacy beschermen.

4.2 Onderwijs

In opdracht van het Ministerie van Economische Zaken en Klimaat (EKZ) voerden het Platform Talent voor Technologie en Dialogic een onderzoek uit naar het onderwijs en de arbeidsmarkt op gebied van cybersecurity in Nederland. De onderzoeksrapportage [71] vormde de basis voor de brief die de minister van EKZ in mei 2024 aanbood aan de Tweede Kamer met aanbevelingen voor vervolgstappen [96]. Er wordt geconstateerd dat er een groeiende vraag is op de arbeidsmarkt naar cybersecurity expertise, met name naar medior en senior posities, en de verwachting is dat deze vraag zal toenemen. Het is essentieel om in de gehele onderwijsketen, van primair onderwijs tot wetenschappelijk onderwijs, meer aandacht te hebben voor cybersecurity. Daarbij ligt ook een grote opgave bij het Leven Lang Ontwikkelen, aangezien de cybersecurity vraagstukken van vandaag anders zijn dan die van tien jaar geleden.

De Cyber Security Raad (CSR) stuurde aansluitend in juli 2024 een signaalbrief aan de minister van EKZ [80]. Daarin stelt de CSR de onderzoeksresultaten te herkennen, en geeft aandachtspunten en aanbevelingen voor verdere concretisering om de tekorten op de cybersecurity arbeidsmarkt aan te vullen, waaronder gecoördineerde actie in publiek-privaat-wetenschappelijke samenwerking.

De faculteit Bètawetenschappen van de OU biedt momenteel vier masteropleidingen aan op gebied van Informatica en Informatiekunde. De master Artificial Intelligence (AI), de master Business Process Management and IT (BPMIT) en de master Software Engineering (SE) hebben elk een omvang van 60 EC. De master Computer Science (CS) heeft een dubbele omvang van 120 EC en is samengesteld uit onderdelen van de masters AI, BPMIT en SE. In deze master worden al twee cursussen aangeboden op gebied van cybersecurity: de cursus Information Security Management, die gericht is op de managementaspecten van informatiebeveiliging met nadruk op governance en compliance, en de cursus Software Security, die gericht is op technische aspecten van software security met nadruk op security-by-design. Momenteel zijn we een derde cursus aan het ontwikkelen: de cursus Security and AI, die gericht is op toepassingen van AI in cybersecurity alsmede de security van AI-gebaseerde systemen zelf. Ik ben sinds 2020 de programmaleider van de master CS en de master SE en het voornemen is, en dat is al vastgelegd in de Onderwijs- en Examenregeling (OER) voor de komende jaren, dat beide masters gaan bestaan uit een verplicht deel, een keuzedeel waar uit een aantal thematische varianten kan worden gekozen, en een afstudeertraject dat aansluit bij de gekozen variant. In beide masters wordt een security-variant opgenomen. In de master SE bestaat die security-variant uit de cursussen Software Security en Security and AI. Tezamen met het afstudeertraject, kan een student zich in 37,5 van de 60 EC specialiseren op gebied van cybersecurity. In de master CS bestaat de security-variant uit de cursussen Information Security Management, Software Security en Security and AI. Tezamen met het afstudeertraject, kan een student zich in 67,5 van de 120 EC specialiseren op gebied van cybersecurity.

De keuze om een security-variant aan te bieden in de master SE past ook bij de internationale richtlijnen voor het curriculum van software engineering opleidingen, zoals de recente update van de IEEE Guide to the Software Engineering Body of Knowledge [64]. In de master CS past de security-variant met een focus op governance, compliance en technische aspecten van zowel software engineering als AI, uitstekend bij het multidisciplinaire karakter van cybersecurity. En daarnaast geldt uiteraard dat deze onderwijsfocus naadloos aansluit bij de onderzoekfocus.

Naast onderwijs op masterniveau, hebben we ook plannen voor het onderwijs op bachelorniveau. Samen met de collega's uit de vakgroep Informatiekunde en de faculteit Rechtswetenschappen zijn we de mogelijkheid aan het verkennen om een focusprogramma aan te bieden dat bestaat uit een drietal

bachelorcursussen op gebied van cybersecurity, waarin naast management-aspecten en technische aspecten van cybersecurity ook aandacht is voor privacy en gegevensbescherming.

Tot slot worden ook samen met collega's van het OU Business Team mogelijkheden verkend om commercieel onderwijs op gebied van cybersecurity aan te bieden. Een concreet initiatief is de samenwerking met de Route443 Cyber Academy.

5 Dankwoord

Aan het einde van deze oratie wil ik graag een dankwoord uitspreken. Allereerst wil ik het College van Bestuur van de OU en in het bijzonder de rector professor Theo Bastiaens, bedanken voor het in mij gestelde vertrouwen en mijn benoeming tot hoogleraar Cyber Security. Ook wil ik de decaan van de faculteit Bètawetenschappen, professor Petra de Weerd-Nederhof, bedanken voor de ondersteuning. Een bijzonder woord van dank ook aan dr. Bastiaan Heeren, die ten tijde van mijn benoeming vakgroepvoorzitter was van de vakgroep Informatica. Zijn wijze woorden waren een belangrijke bron van inspiratie en namen mijn laatste twijfel weg om te solliciteren.

We begonnen deze dag met een bijzonder geslaagd symposium. Hartelijk dank aan de sprekers, dr. Erik Poll en professor Wolter Pieters van de Radboud Universiteit, en professor Lieven Desmet en dr. Vera Rimmer van de KU Leuven, voor de interessante en inspirerende lezingen. Dank aan collega dr. Fabian van den Broek om het symposium voor te zitten.

Mijn benoeming tot hoogleraar is een belangrijke stap in mijn wetenschappelijke loopbaan. Op de weg daarnaartoe heb ik met veel mensen mogen samenwerken en veel van hen opgestoken. Ik heb in mijn oratie al meerdere namen genoemd. Het is vrijwel onmogelijk om hier en nu iedereen persoonlijk te bedanken. Vergeef het mij als ik u niet apart heb vermeld. Weet dat mijn dank naar u allen uitgaat.

Na mijn studie en promotie aan de Technische Universiteit Eindhoven, ging ik in 1998 als senior wetenschapper aan de slag bij Philips Research in Eindhoven, bij het befaamde NatLab. Ik kijk met veel plezier terug op die tijd en de samenwerking met vele collega's in Eindhoven en Hamburg. De foto van de eerste zelftestbare Philips-chip met Logic BIST die ik kreeg bij mijn afscheid, hangt nog steeds in mijn OU-kantoor aan de muur.

Na mijn vertrek bij Philip Research keerde ik uiteindelijk terug naar de academische wereld en begon ik in 2006 bij de OU. Mijn expertise was voorheen met name op gebied van IC-technologie en testen. Toen ik begon bij de OU kwam ik in aanraking met security, wat niet alleen voor mij maar ook voor de OU nog grotendeels onbekend terrein was. Met trots constateer ik dat in de loop der jaren het onderwijs en onderzoek op securitygebied aan de OU flink is uitgegroeid.

Ik werk inmiddels bijna 20 jaar bij de OU, een hele tijd. In al die jaren heb ik met veel plezier met veel collega's samengewerkt, zowel van de wetenschappelijke als de ondersteunende staf. Ik koester mooie herinneringen aan inmiddels oud-collega's in mijn eerste jaren bij de OU, die mij wegwijs maakten in afstandsonderwijs en in het reilen en zeilen van de OU. In de afgelopen jaren zijn heel wat informatica-collega's gekomen en gegaan; dank dat jullie fijne collega's waren. Dank ook aan alle informatica-collega's van vandaag

de dag. In al die jaren heeft de OU verschillende reorganisaties doorgemaakt waarbij de Informatica-groep als zelfstandige faculteit en als vakgroep in faculteiten met diverse andere vakgroepen was gepositioneerd. Ik heb daarom ook met vele collega's buiten de Informatica-groep gewerkt, wat tot verfrissende en nieuwe inzichten heeft geleid; ik dank jullie allemaal. Ook dank aan de inmiddels lange lijst van studenten waarvan ik de afstudeeropdracht of promotieonderzoek heb mogen begeleiden. Dat was niet alleen heel plezierig, maar ik heb zelf ook veel jullie geleerd.

Een bijzonder woord van dank wil ik uitspreken aan professor Marko van Eekelen, die een belangrijke rol in mijn loopbaan bij de OU heeft gespeeld als vakgroepvoorzitter en decaan. Hij introduceerde mij ook bij de Digital Security group aan de Radboud Universiteit in Nijmegen, waar ik sinds 2014 op basis van detachering voor 0,15 fte werkzaam ben. Ook de vele collega's aan de RU wil ik bedanken voor de fijne samenwerking, de gezamenlijke colleges die we hebben verzorgd, en de goede gesprekken. Ook dank aan de vele afstudeerders die ik heb mogen begeleiden, en aan de bedrijven waarin zij hun afstudeerprojecten uitvoerden, waaronder Fox-IT, NCSC, Northwave, Riscure, Secura, SIDN labs, SURF en TNO.

Tot slot wil ik mij wenden tot mijn familie, vrienden, buurtgenoten en de vele bekenden. Hartelijk dank dat jullie zo'n prettige sociale omgeving bieden. Ik waardeer het zeer om naast mijn wereld van wetenschappelijk onderzoek en onderwijs ook ondergedompeld te worden in jullie vaak totaal verschillende werelden. Mijn allergrootste dank wil ik uitspreken aan mijn ouders, die mij van jongs af aan de mogelijkheid hebben gegeven om te leren en te studeren en mijn eigen weg daarin te vinden. En als laatste mijn dank aan de belangrijkste persoon in mijn leven, mijn echtgenote Jeannine.

Ik heb gezegd.

Referenties

Referenties: wetenschappelijk

[1] M. Alishahi and V. Moghtadaiee, 'Feature selection on anonymized datasets', in *International Conference on Dependable, Autonomic and Secure Computing (DASC)*, IEEE, 2023, pp. 852–859.

[2] M. Alishahi, V. Moghtadaiee, and H. Navidan, 'Add noise to remove noise: Local differential privacy for feature selection', *Computers & Security*, vol. 123, p. 102 934, 2022, Elsevier.

[3] H. Alizadeh, H. Vranken, A. Zúquete, and A. Miri, 'Timely Classification and Verification of Network Traffic Using Gaussian Mixture Models', *IEEE Access*, vol. 8, pp. 91 287–91 302, 2020, IEEE.

[4] D. Arp *et al.*, 'Dos and don'ts of machine learning in computer security', in *31st USENIX Security Symposium (USENIX Security 22)*, 2022, pp. 3971–3988.

[5] R. Azmi and K. Kautsarina, 'Revisiting cyber definition', in *Proceedings of the 18th European Conference on Cyber Warfare and Security (ECCWS 2019)*, Academic Conferences International Limited, 2019, pp. 22–30.

[6] O. I. Al-Bataineh, L. Moonen, and L. Vidziunas, 'Extending the range of bugs that automated program repair can handle', *Journal of Systems and Software*, vol. 209, p. 111 918, 2024.

[7] M. Böhme, E. Bodden, T. Bultan, C. Cadar, Y. Liu, and G. Scanniello, 'Software security analysis in 2030 and beyond: A research roadmap', *ACM Transactions on Software Engineering and Methodology*, 2024.

[8] Y. Cao *et al.*, 'A Survey of AI-Generated Content (AIGC)', *ACM Computing Surveys*, vol. 57, no. 5, pp. 1–38, 2025.

[9] P. Carayon, S. Kraemer, and V. Bier, 'Human factors issues in computer and e-business security', in *Handbook of integrated risk management for e-business: measuring, modeling and managing risk*, J. Ross Publishing, 2005, pp. 63–85.

[10] F. Ceschin *et al.*, 'Machine Learning (In) Security: A Stream of Problems', *Digital Threats: Research and Practice*, vol. 5, no. 1, 2024.

[11] W. De Kraker, H. Vranken, and A. Hommersom, 'GLICE: Combining Graph Neural Networks and Program Slicing to Improve Software Vulnerability Detection', in *Proceedings of 8th IEEE European Symposium on Security and Privacy; DevSecOps Research and Opportunities Workshop (Euro S&PW)*, IEEE, 2023, pp. 34–41.

[12] W. De Kraker, H. Vranken, and A. Hommersom, 'MultiGLICE: Combining Graph Neural Networks and Program Slicing for Multiclass Software Vulnerability Detection', *Computers, Special issue Best Practices, Challenges and Opportunities in Software Engineering*, 2025, MDPI (under submission).

[13] W. Diffie and M. E. Hellman, 'New directions in cryptography', *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, Nov. 1976.

[14] A. Fathalizadeh, V. Moghtadaiee, and M. Alishahi, 'On the privacy protection of indoor location dataset using anonymization', *Computers & Security*, vol. 117, p. 102 665, 2022, Elsevier.

[15] G. Fernandes, J. J. Rodrigues, L. F. Carvalho, J. F. Al-Muhtadi, and M. L. Proença, 'A comprehensive survey on network anomaly detection', *Telecommunication Systems*, vol. 70, pp. 447–489, 2019, Springer.

[16] J. Haag, 'DVCL: A distributed virtual computer lab for security and network education', Ph.D. dissertation, Open Universiteit, 2018.

[17] W. Hu, F. van den Broek, B. Jacobs, and P. Wolters, 'Attribuut-gebaseerde elektronische handtekeningen en de eIDAS-verordening', in *Digitalisering en conflictoplossing (Serie Onderneming en Recht deel 130)*, Wolters Kluwer, 2021, pp. 293–315.

[18] M. M. Issa, M. Aljanabi, and H. M. Muhialdeen, 'Systematic literature review on intrusion detection systems: Research trends, algorithms, methods, datasets, and limitations', *Journal of Intelligent Systems*, vol. 33, no. 1, p. 20 230 248, 2024, De Gruyter.

[19] S. Kiljan, 'Exploring, expanding and evaluating usable security in online banking', Ph.D. dissertation, Open Universiteit, 2017.

[20] J. Kronjee, A. Hommersom, and H. Vranken, 'Discovering software vulnerabilities using data-flow analysis and machine learning', in *Proceedings of the International Conference on Availability, Reliability and Security (ARES)*, ACM, 2018, p. 6.

[21] B. Krumnow, 'Web scrapology: Overcoming limits of automating web measurements', Ph.D. dissertation, Open Universiteit, 2023.

[22] S. Kumar, H. Vranken, J. Van Dijk, and T. Hamalainen, 'Deep in the Dark: A Novel Threat Detection System using Darknet Traffic', in *Proceedings of the 2019 IEEE International Conference on Big Data; 3rd International Workshop on Big Data Analytic for Cybercrime Investigation and Prevention (Big Data / BDACIP)*, IEEE, 2019, pp. 4273–4279.

[23] J. Lansky *et al.*, 'Deep learning-based intrusion detection systems: A systematic review', *IEEE Access*, vol. 9, pp. 101 574–101 599, 2021.

[24] M. Lehto, 'Phenomena in the cyber world', in *Cyber Security: Analytics, Technology and Automation*, Springer, 2015, pp. 3–29.

[25] Y. Liu *et al.*, 'VulDetectBench: Evaluating the Deep Capability of Vulnerability Detection with Large Language Models', *arXiv preprint arXiv:2406.07595*, 2024.

[26] R. Luijben, F. van den Broek, and G. Alpár, 'Security requirements for proctoring in higher education', in *Global Engineering Education Conference (EDUCON)*, IEEE, 2024, pp. 1–5.

[27] C. Maathuis and S. Chockalingam, 'Risk assessment of large language models beyond apocalyptic visions', in *Proceedings of the 23rd European Conference on Cyber Warfare and Security*, Academic Conferences International Limited, vol. 23, 2024, pp. 279–286.

[28] C. Maathuis and I. Kerkhof, 'Navigating the First Year of the Ukrainian Battlefield: Machine Learning vs. Large Language Models', *Journal of Information Warfare*, vol. 23, no. 2, 2024.

[29] C. Maathuis, 'Human centered explainable AI framework for military cyber operations', in *Military Communications Conference (MILCOM)*, IEEE, 2023, pp. 260–267.

[30] C. Maathuis, 'Trustworthy human-autonomy teaming for proportionality assessment in military operations', in *International Conference on Applied Artificial Intelligence (ICAPAI)*, IEEE, 2024, pp. 1–8.

[31] D. E. Mann and S. M. Christey, 'Towards a common enumeration of vulnerabilities', in *2nd Workshop on Research with Security Vulnerability Databases*, 1999, p. 9.

[32] E. Masanet, A. Shehabi, N. Lei, H. Vranken, J. Koomey, and J. Malmodin, 'Implausible projections overestimate near-term Bitcoin CO2 emissions', *Nature Climate Change*, vol. 9, pp. 653–654, Sep. 2019, Nature.

[33] V. van der Meer, 'Improving foundations of file recovery: A digital forensics perspective on file fragmentation, timestamps, and JPEG validation', Ph.D. dissertation, Open Universiteit, 2024.

[34] L. Neil, J. M. Haney, K. Buchanan, and C. Healy, 'Analyzing cybersecurity definitions for non-experts', in *International Symposium on Human Aspects of Information Security and Assurance*, Springer, 2023, pp. 391–404.

[35] H. Oz, A. Aris, A. Levi, and A. S. Uluagac, 'A survey on ransomware: Evolution, taxonomy, and defense solutions', *ACM Computing Surveys*, vol. 54, no. 11, pp. 1–37, Jan. 2022, ACM.

[36] E. Pankovska, A. Sai, and H. Vranken, 'Determining Optimal Incentive Policy for Decentralized Distributed Systems Using Reinforcement Learning', in *Proceedings of 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, IEEE, 2023, pp. 1–5.

[37] A. Pollini *et al.*, 'Leveraging human factors in cybersecurity: An integrated methodological approach', *Cognition, Technology & Work*, vol. 24, pp. 371–390, 2022, Springer.

[38] R. Ramirez and N. Choucri, 'Improving interdisciplinary communication with standardized cyber security terminology: A literature review', *IEEE Access*, vol. 4, pp. 2216–2243, 2016, IEEE.

[39] R. L. Rivest, A. Shamir, and L. Adleman, 'A method for obtaining digital signatures and public-key cryptosystems', *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978, ACM.

[40] Y. Roumani, 'Patching zero-day vulnerabilities: An empirical analysis', *Journal of Cybersecurity*, vol. 7, no. 1, pp. 1–13, Nov. 2021.

[41] A. Sai and H. Vranken, 'Promoting rigor in blockchain energy and environmental footprint research: A systematic literature review', *Blockchain: Research and Applications*, vol. 5, no. 1, p. 100 169, 2024, Elsevier.

[42] J. H. Saltzer and M. D. Schroeder, 'The protection of information in computer systems', *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278–1308, Sep. 1975.

[43] D. Schatz, R. Bashroush, and J. Wall, 'Towards a more representative definition of cyber security', *Journal of Digital Forensics, Security and Law*, vol. 12, no. 2, pp. 53–74, 2017.

[44] M. Schulze and J. Silomon, 'Revisiting past cyber security recommendations: Lessons we have failed to learn', in *Proceedings of the 23rd European Conference on Cyber Warfare and Security (ECCWS 2024)*, Academic Conferences International Limited, 2024, pp. 461–468.

[45] T. Sharma *et al.*, 'A survey on machine learning techniques applied to source code', *Journal of Systems and Software*, vol. 209, p. 111 934, 2024.

[46] M. Sheikhalishahi, A. Saracino, F. Martinelli, and A. La Marra, 'Privacy preserving data sharing and analysis for edge-based architectures', *International Journal of Information Security*, vol. 21, pp. 79–101, 2022.

[47] A. Thakkar and R. Lohiya, 'A survey on intrusion detection system: Feature selection, model, performance measures, application perspective, challenges, and future research directions', *Artificial Intelligence Review*, vol. 55, no. 1, pp. 453–563, 2022.

[48] V. Tzavara and S. Vassiliadis, 'Tracing the evolution of cyber resilience: A historical and conceptual review', *International Journal of Information Security*, vol. 23, no. 2, pp. 1–25, 2024.

[49] E. Van Es, H. Vranken, and A. Hommersom, 'Denial-of-Service Attacks on LoRa WAN', in *Proceedings of the International Conference on Availability, Reliability and Security; International Workshop on Security and Forensics of IOT (ARES/IOT-SECFOR)*, ACM, 2018, p. 17.

[50] J. Van Roosmalen, H. Vranken, and M. Van Eekelen, 'Applying Deep Learning on Packet Flows for Botnet Detection', in *Proceedings of the Symposium on Applied Computing (SAC)*, ACM, 2018, pp. 1629–1636.

[51] H. Vranken and H. Alizadeh, 'Detection of DGA-generated domain names with TF-IDF', *Electronics, Special Issue Design of Intelligent Intrusion Detection Systems*, vol. 11, no. 3, p. 414, 2022, MDPI.

[52] H. Vranken, 'Sustainability of bitcoin and blockchains', *Current Opinion in Environmental Sustainability*, vol. 28, pp. 1–9, Oct. 2017.

[53] D. Willems, K. Kohls, B. Van der Kamp, and H. Vranken, 'Data exfiltration detection on network metadata with autoencoders', *Electronics, Special Issue Network Intrusion Detection Using Deep Learning*, vol. 12, no. 12, p. 2584, 2023, MDPI.

[54] H. Xu *et al.*, 'Large language models for cyber security: A systematic literature review', *arXiv preprint arXiv:2405.04760*, 2024.

[55] Y. Yao, J. Duan, K. Xu, Y. Cai, Z. Sun, and Y. Zhang, 'A survey on large language model (LLM) security and privacy: The good, the bad, and the ugly', *High-Confidence Computing*, vol. 4, p. 100 211, 2024.

[56] X. Zhou, S. Cao, X. Sun, and D. Lo, 'Large language model for vulnerability detection and repair: Literature review and the road ahead', *ACM Transactions on Software Engineering and Methodology*, Dec. 2024.

Referenties: boeken/rapporten

[57] J. P. Anderson, 'Computer Security Technology Planning Study, ESD-TR-73-51, Vol. I and II', Deputy for Command and Management Systems HQ Electronic Systems Division, 1972.

[58] Canadian Centre for Cyber Security, 'Baseline Cyber Security Controls for Small and Medium Organizations', Feb. 2020.

[59] Centraal Bureau voor de Statistiek (CBS), 'Cybersecuritymonitor 2023', 2024.

[60] Centraal Bureau voor de Statistiek (CBS), 'Veiligheidsmonitor 2023', 2024.

[61] Chainalysis, 'The 2024 Crypto Crime Report: The latest trends in ransomware, scams, hacking, and more', Feb. 2024.

[62] European Union Agency for Cybersecurity (ENISA), '2024 Report on the State of Cybersecurity in the Union', Dec. 2024.

[63] European Union Agency for Cybersecurity (ENISA), 'ENISA Threat Landscape 2024: July 2023 to June 2024', Sep. 2024.

[64] IEEE Computer Society, 'Guide to the Software Engineering Body of Knowledge v4.0', 2024.

[65] International Telecommunication Union (ITU), 'Guide to Developing a National Cybersecurity Strategy - Strategic engagement in cybersecurity, 2nd Edition', 2021.

[66] MITRE Corporation, 'CVE 25th Anniversary Report', Oct. 2024.

[67] Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), 'Cybersecuritybeeld Nederland 2024', Oct. 2024.

[68] National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), 'Cybersecurity advisory: NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations', Oct. 2023.

[69] P. C. van Oorschot, *Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, Second Edition*. Springer, 2021.

[70] Open Universiteit (OU), Faculty of Science, 'New Horizons for Science: Updated Research Strategy 2023-2027', 2024.

[71] Platform Talent voor Technologie en Dialogic, 'Onderzoeksrapportage Onderwijs en Arbeidsmarkt Cybersecurity', 2024.

[72] B. Schneier, *Secrets & Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.

[73] N. Taleb, *Antifragile : things that gain from disorder*. Random House, 2012.

[74] W. Tiemeijer, *Hoe mensen keuzes maken: De psychologie van het beslissen*. Amsterdam University Press, 2011.

[75] W. H. Ware, 'Security Controls for Computer Systems, tech. report R-609-PR', RAND, Defense Science Board Task Force on Computer Security, 1972.

Referenties: overig

[76] BBC, *The Vocabularist: How we use the word cyber*, [Online], March 15, 2016.

[77] Cambridge Centre for Alternative Finance (CCAF), *Cambridge Bitcoin Electricity Consumption Index (CBECI)*, [Online].

[78] CISA, *Known Exploited Vulnerabilities Catalog*, [Online].

[79] CVEdetails, *Common Vulnerabilities and Exposures Catalog*, [Online].

[80] Cyber Security Raad (CSR), *CSR signaalbrief cybersecurity arbeidsmarkt*, [Online], 4 juli 2024.

[81] Google Security Blog, *Memory Safe Languages in Android 13*, [Online], December 1, 2022.

[82] Microsoft Security Response Center, *We need a safer systems programming language*, [Online], July 18, 2019.

[83] MITRE Corporation, *Common Weakness Enumeration*, [Online].

[84] MITRE Corporation, *CWE Top 25 Most Dangerous Software Weaknesses*, [Online].

[85] MITRE Corporation, *MITRE ATT&CK*, [Online].

[86] NOS, *Afluistergevoelige smartphones verbannen uit ministerraad: 'Had veel eerder gemoeten'*, [Online], 23 augustus 2024.

[87] NOS, *Datalek bij UWV: 150.000 cv's ingezien en mogelijk gedownload*, [Online], 10 mei 2024.

[88] NOS, *Datalek bij Volkswagen: 'Gegevens 800.000 auto-eigenaren op straat'*, [Online], 27 december 2024.

[89] NOS, *Duitsland vermoedt sabotage na kapotte zeekabels, wijst op Russische dreiging*, [Online], 19 november 2024.

[90] NOS, *Hacker knoeit met facturen: Limburgs Schuttersfeest voor 78.000 euro gedupeerd*, [Online], 19 oktober 2024.

[91] NOS, *Hackers bij politie kaapten inlogsessie van medewerker*, [Online], 8 november 2024.

[92] NOS, *Hackers TU Eindhoven 'op heterdaad betrapt', onderwijs maandag hervat*, [Online], 15 januari 2025.

[93] NOS, *Moederbedrijf Ticketmaster bevestigt datalek*, [Online], 1 juni 2024.

[94] NOS, *Wereldwijd problemen door computerstoring: onder meer luchthavens en ziekenhuizen getroffen*, [Online], 19 juli 2024.

[95] OWASP, *OWASP Top Ten*, [Online].

[96] Rijksoverheid, *Aanbiedingsbrief bij onderzoeksresultaten kwalitatieve en kwantitatieve tekorten cybersecurity professionals*, [Online], 14 mei 2024.

[97] H. Vranken, *Homepage of Harald Vranken*, [Online].