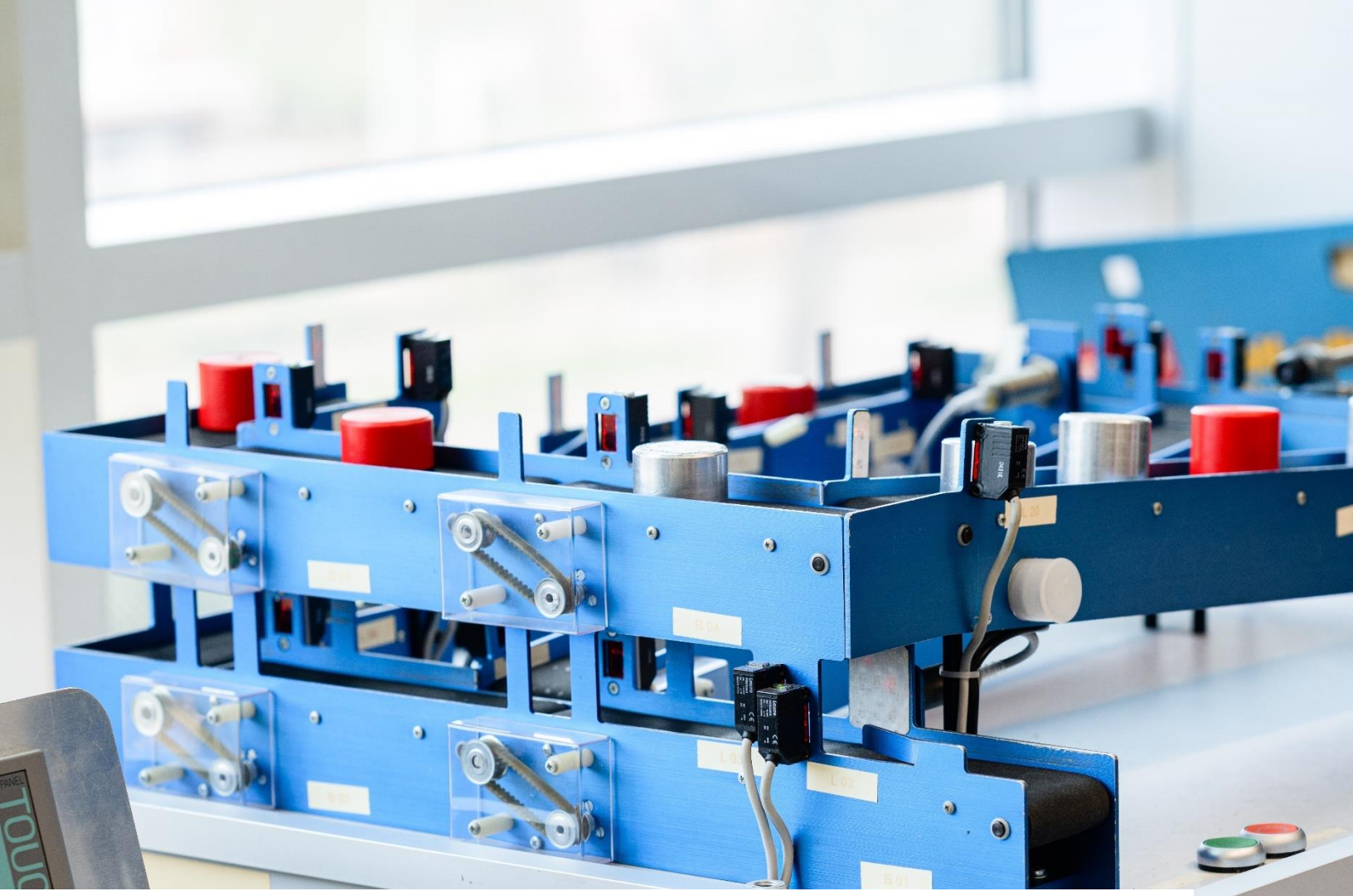


Mogelijkheid en Kwetsbaarheid, de Techniek Ondersteunt

Lectorale rede Gerard Hoekstra

Lectoraat Network and Systems Engineering Cyber Security

20 November 2025

DE HAAGSE HOGESCHOOL

Lectorale rede in verkorte vorm uitgesproken bij de publieke aanvaarding van functie van lector Network and Systems Engineering Cyber Security aan het Centre of Expertise Cyber Security, Haagse Hogeschool 20 november 2025.

Mogelijkheid en kwetsbaarheid, de techniek ondersteunt

Van elektrische fietsen tot energiemanagementsystemen: digitale netwerken en systemen zijn overal. Thuis, op het werk en in de samenleving worden we omringd door complexe systemen. Nieuwe technologieën creëren mogelijkheden die voorheen ondenkbaar waren: van autonoom navigerende drones tot algoritmen die ziektebeelden beoordelen. Digitalisering houdt onze maatschappij draaiende en versterkt de concurrentiekracht van onze economie. Tegelijkertijd digitaliseert ook de criminaliteit: technologie waar we afhankelijk van zijn, kan met verkeerde bedoelingen worden ingezet.

Tijdens zijn intreerede belicht Gerard de onderzoeksfocus en plannen van zijn lectoraat. Hij laat zien hoe praktijkgericht onderzoek kan bijdragen aan betrouwbare netwerken en systemen voor mensen en organisaties.

Inhoud

Motivatie

Waar Nederland zijn geld mee verdient

Zijn de (Tweede kamer) verkiezingen van 29 oktober gegaan over waar Nederland zijn geld (in de toekomst) mee verdient? Scheidend president van De Nederlandsche Bank (DNB), Klaas Knot, vond dat de verkiezingen hierover zouden moeten gaan[1] en dan met name hoe we het zullen moeten hebben van arbeidsproductiviteitsgroei langs de weg van investeringen in innovatie en onderwijs.

Het is de vraag in hoeverre digitalisering en automatisering een rol kan spelen in het verhogen van onze arbeidsproductiviteit. De Rabobank beantwoordde deze vraag al eens met stelligheid[2]: de arbeidsproductiviteit in de zakelijke dienstverlening krijgt “een boost” door digitalisering. Vanwege onder andere de krappe arbeidsmarkt zou er geen andere oplossing zijn.

Figuur 1: *De Nederlandsche Bank (DNB). - Foto: Shutterstock*

Door verdere digitalisering zal onze afhankelijkheid van digitale netwerken en systemen steeds verder worden vergroot. Tegelijkertijd zullen nieuwe technologieën nieuwe mogelijkheden bieden. Deze combinatie van toenemende afhankelijkheid en technologische veranderingen vormt de noodzaak voor cyber security maatregelen. Om onze productiviteit en concurrentiepositie te behouden of te verbeteren zullen we dus moeten investeren en vernieuwen op het gebied van cyber security. Hiermee kunnen maatregelen getroffen worden om digitale dreigingen te weerstaan en/of de invloed ervan te beperken, zodanig dat de risico’s beheersbaar zijn. Op deze manier maakt cyber security digitalisering voor organisaties mogelijk. Omgekeerd helpen de opbrengsten van veilige digitalisering om cyber security niet alleen als kostenpost te zien. Digitalisering en cyber security zijn hierin onlosmakelijk verbonden.

[1] ‘De verkiezingen moeten gaan over de vraag waar Nederland z’n geld mee verdient’ - NRC, 25 juni 2025.
[2] Digitalisering in de zakelijke dienstverlening: een boost voor de arbeidsproductiviteit - Rabobank, 2 juli 2025.

Veiligheid

Naast de Nederlandse concurrentiepositie en arbeidsproductiviteit is ook het belang te onderscheiden van de continuïteit van overheidsdiensten en de vitale sectoren. Door het snelle ontwrichtende effect van bijvoorbeeld energie-uitval op de maatschappij[3] is het belang van de continuïteit van deze voorziening vanzelfsprekend. Als gevolg van de energietransitie - dat de overgang vormt van het gebruik van fossiele brandstoffen naar hernieuwbare bronnen - is ook hier sprake van een toenemende afhankelijkheid van digitale systemen. Energie uit zon en wind kent een wisselende beschikbaarheid en grote fluctuaties die opgevangen zullen moeten worden door andere systemen die tevens digitaal geregeld worden zoals Energy Storage Systems (ESS).

Het doel[4] is dat Nederland eind 2032 met windenergie op zee 21 GigaWatt (GW) opwekt. Deze hoeveelheid energie komt overeen met 16 procent van de energie die Nederland dan nodig heeft en komt overeen met ongeveer 75 procent van het huidige elektriciteitsverbruik. Om in 2050 klimaatneutraal te zijn zal 70 GW op zee door windmolens geleverd moeten worden. Ondanks de tegenvallers met windpark Nederwiek 1-A[5], zal de capaciteit in 2050 om energie op de wekken op de Noordzee een substantieel deel zijn van de behoefte aan elektrische energie. De digitale netwerken en systemen die deze energiebron van formaat mogelijk maken zullen ook op de lange termijn goed beschermd moeten worden tegen cyberdreigingen[6].

Deze energietransitie vindt plaats op een moment dat de digitale dreiging tegen Nederland groot is (Cybersecurity Beeld Nederland 2024[7]). Deze combinatie van factoren onderstreept het belang voor van cyber security voor de maatschappij.

Dit belang van cyber security voor de maatschappij laat zich aan de hand van energievoorziening goed illustreren maar is te generaliseren naar overheidsdiensten en andere vitale sectoren, bijvoorbeeld openbaar vervoer, drinkwatervoorziening, luchtvaart, en de financiële sector.

Figuur 2: *Foto Windmolenpark voor de kust van IJmuiden. - Foto: Shutterstock*

[3] Veiligheidsbevordering en vitale sectoren | Veiligheidsbevordering | AIVD, geraadpleegd 23 oktober.
[4] Doelstellingen - Wind op zee, geraadpleegd 23 oktober 2025.
[5] https://www.nrc.nl/nieuws/2025/10/31/geen-enkel-bedrijf-wil-windpark-nederwiek-in-de-noordzee-bouwen-wat-gebeurt-hier-a4911508, geraadpleegd 31 oktober 2025.
[6] FLECS: Digitale Weerbaarheid voor Offshore Wind, geraadpleegd 23 oktober 2025.
[7] Cybersecuritybeeld Nederland 2024 | Nationaal Coördinator Terrorismebestrijding en Veiligheid, geraadpleegd 23 oktober 2025.

Digitalisering

Vaak wordt digitalisering in verband gebracht met het automatiseren van menselijke handelingen en het reduceren van werkgelegenheid: "*AI als banenkiller*"[8]. In een eerdere studie[9] van het Centraal Bureau voor de Statistiek (CBS) is gebleken dat een hogere arbeidsproductiviteit behaald wordt met meer gebruik van ICT-toepassingen. Zo gaat export gepaard met een hogere graad van digitalisering en daarmee een concurrerendere internationale positie van bedrijven. De bedrijven die automatiseren met bijvoorbeeld robotica of AI hebben, volgens het CBS, een hogere werkgelegenheid dan bedrijven die deze technologieën niet toepassen.

Vooruitkijkend naar 2030 wordt gesteld in het "Future of Jobs Report 2025"[10] - uitgevoerd door het World Economic Forum - dat de sterkst transformerende trend voortkomt uit digitale technologische ontwikkelingen met in het bijzonder AI en informatieverwerking.

Volgens UvA-hoogleraar Henk Volberda (Amsterdam Business School)[11] - verantwoordelijk voor de dataverzameling van dit onderzoek – gaat de arbeidsmarkt structureel veranderen tussen 2025 en 2030. Zo verwacht 60 procent van de werkgevers dat de bedrijfsvoering tegen 2030 vanwege digitalisering "ingrijpend " zal veranderen. Met als effect dat 9 miljoen banen naar verwachting zullen verdwijnen, maar ook 19 miljoen banen gecreëerd worden.

Het zal nog moeten blijken of deze aantallen banen in werkgelegenheid zullen verdwijnen respectievelijk gecreëerd worden. Toch lijkt de houding gerechtvaardigd om juist deze vernieuwingen te omarmen in plaats van te vrezen voor de intrede van nieuwe technologieën die onze manier van werken gaan veranderen.

Het digitale dilemma

Zoals omschreven door Van Rijsewijk[12] is de uitvinding van elke technologische ontwikkeling tegelijk een wonder en een ramp. Nieuwe mogelijkheden worden

[8] Artificial intelligence wordt banen-killer - Computable.nl, geraadpleegd 21 oktober 2025.
[9] Digitalisering bij bedrijven en de relatie met export, productiviteit en werkgelegenheid - Digitalisering - Internationaliseringsmonitor | CBS, 2023-III, geraadpleegd 17 november 2025.
[10] The Future of Jobs Report 2025 | World Economic Forum, January 2025.
[11] In 2030 neemt AI werk grotendeels over: slechts een derde blijft mensenwerk - Universiteit van Amsterdam, geraadpleegd 31 oktober 2025.
[12] R. van Rijsewijk ,Cyberrisico als kans, 2016.

gecreëerd, maar ook nieuwe problemen en wellicht rampen zullen plaatsvinden. Neem de uitvinding van een vliegtuig. Digitale technologie is hierin niet anders.

Het toegankelijk maken van informatie, het verkrijgen van betere inzichten en het op basis daarvan nemen van betere beslissingen wordt ondersteund door nieuwe digitale technologie. Die technologie levert voordelen voor bedrijven, overheden, consumenten maar natuurlijk ook voor criminelen en andere actoren met kwalijke bedoelingen.

Dit digitale dilemma is nadrukkelijk van toepassing op de activiteiten van het lectoraat Network and Systems Engineering (NSE) van het kenniscentrum cyber security van de Haagse Hogeschool: de techniek ondersteunt zowel nieuwe mogelijkheden als nieuwe kwetsbaarheden. Het vinden van deze kwetsbaarheden, toepassen van maatregelen en effectief samenwerken vormt de kern van de technische activiteiten van het lectoraat.

Figuur 3: *Voor-en nadelen digitalisering: nieuwe geavanceerde productiemogelijkheden, maar ook het risico om gehackt te worden.*

Digitale risico's

Criminelen zullen gemotiveerd zijn om nieuwe (digitale) technologieën in te zetten voor een crimineel verdienmodel of om andere belangen te dienen. Bij het ontbreken van aandacht voor de risico's van technologie bij legitieme gebruikers zullen kwetsbaarheden ontstaan die kunnen leiden onbeheersbare schade.

Een voorbeeld van nagenoeg onbeheersbare schade voor een bedrijf is wat Jaguar Land Rover (JLR)[13] is overkomen van eind augustus tot oktober 2025. Een cyberaanval heeft geleid tot een circa 5 weken durende productiestop, een omvang die 5000 Britse organisaties treft en qua financiële schade de grootste (ca. 2.2 Miljard Euro)[14] is in de Britse historie ten gevolge van cybercriminaliteit. Op 25 september heeft de Britse overheid aangegeven JLR financieel te ondersteunen met onder andere een lening ter hoogte van ca. 1.7 Miljard Euro[15].

[13] Jaguar Land Rover production severely hit by cyber attack, geraadpleegd 24 oktober 2025.
[14] Cyber Monitoring Centre Statement on the Jaguar Land Rover Cyber Incident – October 2025 – CMC, geraadpleegd 24 oktober 2025.
[15] Government backs Jaguar Land Rover with £1.5 billion loan guarantee - GOV.UK, geraadpleegd 12 november 2025.

Het is een misverstand dat schade voorkomen kan worden door het nemen van cyber security maatregelen. De vier vermogens, corresponderend met de vier doelen van weerbaarheid, zoals beschreven door Van der Kleij[16] kunnen wel helpen om de risico's te beheersen: voorbereiden, reageren, herstellen en aanpassen. In ieder van deze doelen spelen ook technische aspecten een rol.

Figuur 4: *Jaguar Land Rover (JLR) getroffen door cyberaanval met de grootste cyberschade in de Britse geschiedenis tot gevolg. - Foto Shutterstock*

In het voorbereiden op een cyber incident is het van belang technische ontwikkelingen te volgen. Nieuwe technologieën die voordelen leveren kunnen opgenomen worden bij voldoende kennis van de beperkingen en kwetsbaarheden ervan. Belangrijk hierbij is hoe gereageerd moet worden bij een mogelijk incident. In het vaststellen van een incident en de wijze van reageren kan technologie een belangrijke bedrage leveren en kan voortdurend geïnnoveerd worden. Tijdens het herstellen van een cyber incident kan technologie ondersteunen door de hersteltijd te bekorten en systemen opnieuw beschikbaar te krijgen. In het vermogen om aan te passen is het doel om een hoger niveau van weerbaarheid te behalen en tevens technologische vernieuwingen door te voeren die de (toekomstige) manier van werken en de mens kunnen ondersteunen dit hogere niveau te realiseren.

Bijzondere belangstelling voor de hacker

De cyberrisico's die bedrijven, overheden en consumenten lopen zouden onze belangstelling moeten opwekken in plaats van angst inboezemen. Het gedrag van hackers is interessant om daders beter te begrijpen vanuit het oogpunt van criminologie, maar ook vanuit technisch perspectief.

Zoals beargumenteerd door van Rijsewijk[17] is het belangrijk de digitale dreigingen te kennen: wie zijn deze actoren, wat is hun motivatie, wat zijn hun middelen en hoe worden deze ingezet? Afgezien van leed en schade schuilt achter een succesvolle hack niet zelden menselijke creativiteit en technisch vernuft. De nieuwsgierigheid naar deze creativiteit en innovatieve technieken is de drijfveer om tot nieuwe invalshoeken en kennis te komen. De kennis van de digitale dreigingen kan vervolgens worden ingezet om beter risico's in te schatten en de passende maatregelen te nemen.

[16] R. van der Kleij, Nu veiligheid er niet meer is, lectorale rede, 8 mei 2025.
[17] R. van Rijsewijk ,Cyberrisico als kans, 2016.

Het ethische digitale dilemma

Van huiswerk en boodschappen tot gezondheidszorg en landbouw – ons dagelijks leven wordt radicaal veranderd door data, algoritmes en AI. De keerzijde van technologische vernieuwing door digitalisering is niet enkel het cyberrisico dat van toepassing is. De vraag of digitalisering werkelijk tot een verbetering leidt voor de mens en wat de invloed is van toenemende digitalisering wordt geadresseerd in het onderzoek van hoogleraar Tamar Sharon[18] van de Radboud Universiteit.

Hoe digitalisering onze levens verandert en hoe de invloed van ‘big-tech bedrijven’ te beteugelen is vormt de drijfveer om aan Europese regulering bij te dragen zodat technologie de mens en de maatschappij dient. De documentaire “The Digital Dilemma”[19] illustreert deze invloeden en geeft ook weer hoe digitalisering menselijke interactie kan wegnemen die waardevol wordt gevonden.

Figuur 5: *Boodschappen doen: met het automatiseren van de handelingen bij de kassa (rechts) vervalt ook menselijke interactie (links) die juist gewaardeerd kan worden. - Foto’s Shutterstock.*

Nationale en Europese reguleringen voor digitale technologieën zijn belangrijke elementen om de publieke waarden te borgen en de belangen van de maatschappij te beschermen. De uitwerking en toepassing van deze Nationale en Europese reguleringen voor technische netwerken en systemen is belangrijk voor het lectoraat omdat maatregelen worden voorgeschreven die noodzakelijk zijn om cyberrisico’s beter te beheersen. Bijvoorbeeld technische oplossingen om systeemgedrag te monitoren maar ook de wettelijke verplichting om digitale apparaten veilig ontwerpen en te houden.

[18] https://www.ru.nl/en/people/sharon-t, geraadpleegd 24 oktober 2025.
[19] The Digital Dilemma - AmmodoDocs, geraadpleegd 24 oktober 2025.

Netwerken en systemen

Het lectoraat Network and Systems Engineering (NSE) Cyber Security is onderdeel van het Centre of Expertise Cyber Security (CoECS) van de Haagse Hogeschool(HHs). Het NSE lectoraat voert technische praktijkgericht wetenschappelijk onderzoek uit naar de cyber security aspecten van netwerken en systemen.

Netwerken en systemen worden aangetroffen op allerlei plaatsen waar ze met het toenemen van technische complexiteit zich niet beperken tot toepassing door bedrijven of overheden. Een systeem kunnen we definiëren als een samenstelling van onderdelen die samenwerken om een functie te realiseren die mensen en/of organisaties in staat te stelt een bepaald doel te bereiken. De netwerken zorgen dan vervolgens voor de verbindingen in en tussen de systemen.

Met het toenemen van de complexiteit van technische oplossingen treffen we overal netwerken en systemen aan die vatbaar zijn voor cyberrisico's, bij grotere en kleinere bedrijven, bij de overheid en bij consumenten.

Het lectoraat NSE concentreert zich nadrukkelijk op de cyber security aspecten van de volgende technologieën:

1. **Informatie Technologie (IT)**
   Systemen die gebruikt worden voor het verzamelen, verwerken, opslaan en distribueren van informatie. Dit kan een werkstation zijn of een complexe cloud infrastructuur.
2. **Internet of Things (IoT) oplossingen**
   IoT oplossingen bestaan uit aan het Internet verbonden apparaten die specifieke IoT protocollen implementeren, zoals bijvoorbeeld een robotstofzuiger dit kan doen met het MQTT-protocol.
3. **Operationele Technologie (OT)**
   Systemen bestaande uit Industrial Control Systems (ICS) voor het besturen en monitoren van processen in bijvoorbeeld productie-omgevingen in de industrie.
4. **Embedded technologie**
   Embedded technologie kent een nauwe integratie van hardware en software en is ontworpen voor een specifieke taak met daarop toegespitste functionaliteit en (beperkte) systeembronnen, zoals de besturing van een drone.

Deze technologieën, afzonderlijk of een combinatie, worden in de praktijk aangetroffen in netwerken en systemen.

Netwerken en systemen bij publieke en private organisaties

Bij overheden en bedrijven wordt in toenemende mate gebruik gemaakt van IT-infrastructuur die deels berust op cloud[20] technologie van bekende aanbieders zoals Microsoft, Amazon en Google. Deze cloud oplossingen worden vaak voor kantoorautomatisering van bijvoorbeeld ministeries en andere overheden en organisaties gebruikt. Volgens een rapport van de rekenkamer[21] is het gebruik van de (publieke) cloud bij de Rijksoverheid toegenomen. Cloud technologie biedt veel voordelen zoals voor Ukraine - de belangrijkste data kon worden verplaatst naar de cloud - is gebleken, maar ook risico's waaronder continuïteit van dienstverlening en gegevensbescherming. Met het delen van infrastructuur door meerdere gebruikers ontstaat eenvoudigweg het risico dat de scheiding tussen deze gebruikers onvoldoende is, bijvoorbeeld door een kwetsbaarheid[22].

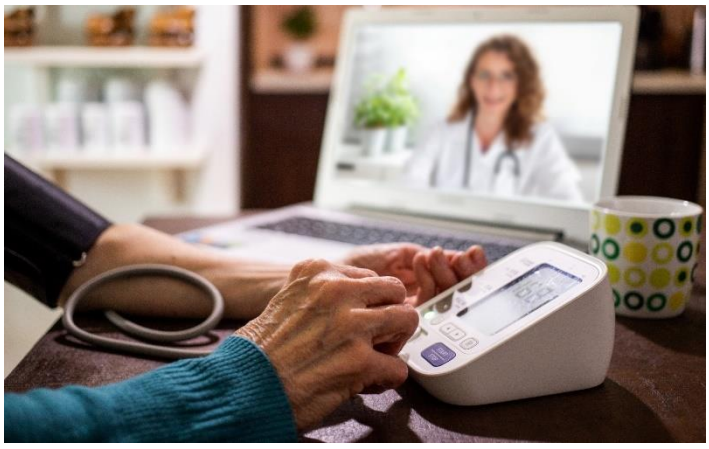
Figuur 6: *Google datacentrum, Eemshaven. - Foto: Shutterstock.*

Bij private non-profit organisaties zoals ziekenhuizen brengt digitalisering – Digitale zorg - veel veranderingen met zich meer en vormt het een noodzakelijk instrument om de zorgkosten te kunnen beheersen. Door digitalisering kunnen patiënten door middel van continue monitoring thuis met IoT – voor deze toepassing ook wel het Internet of Medical Things (IoMT) genoemd - sensoren informatie verstrekken ten behoeve van de behandeling in het ziekenhuis. Bijvoorbeeld met bloeddrukmetingen[23]. Zo kunnen mensen thuis verblijven, is het mogelijk ziektes eerder op te sporen en kunnen zo de

[20] Het via het Internet gebruik maken van hardware en software voor opslag, verwerking en distributie van gegevens. De hardware kan zich op iedere locatie bevinden en daarmee ook de gegevens.
[21] Algemene Rekenkamer, Het Rijk in de cloud, https://www.rekenkamer.nl/site/binaries/site-content/collections/documents/2025/01/15/het-rijk-in-de-cloud/Het+Rijk+in+de+cloud.pdf , 15 januari 2025.
[22] Dutch hacker: all Microsoft Entra ID tenants at risk - Techzine Global, geraadpleegd 31 oktober 2025.
[23] Continue monitoring: innovatie van de toekomst - UMC Utrecht, geraadpleegd 31 oktober 2025.

zorgkosten worden verminderd. Dit bevestigt het onderzoek[24] van het UMC Utrecht. In drie landen (Nederland, Oostenrijk, Duitsland) zijn 787 mensen met diabetes 2 gevraagd naar hun voorkeur voor klinisch onderzoek vanuit huis. De conclusie is dat een onderzoek met een veilige behandeling, korte duur, geen reistijd en contact via video het meest aantrekkelijk is. De bereidheid om aan een klinisch onderzoek deel te nemen zou zo kunnen toenemen van 56 procent naar 89 procent als de onderzoeken meer vanuit huis kunnen plaatsvinden.

Ook digitaliseert een ander deel van de zorgketen, diagnose apparatuur in het ziekenhuis kan de gegevens van een MRI-scan in de Amazon cloud opslaan en analyseren[25]. Met AI kunnen de gegevens van de MRI-scanners vervolgens op ziektebeelden geanalyseerd worden. Ondanks het enthousiasme voor AI worden bij toepassing in de zorg wel kanttekeningen geplaatst[26] over de tijdswinst die door specialisten gerealiseerd wordt. Desondanks is het aannemelijk dat AI en digitalisering door technologische vorderingen een grote rol zullen spelen in de zorgketen van de toekomst.



Figuur 7: *Patiëntmonitoring met bloeddrukmeter. Foto: Shutterstock*

De uitdaging voor deze keten ten aanzien van cyber security is dat een verplaatsing plaatsvindt van een vertrouwde afgebakende omgeving – het ziekenhuis met diens eigen informatiesystemen – naar de omgeving buiten het ziekenhuis. Voorbeelden hiervan zijn de IoMT sensoren die via het thuisnetwerk van de patiëntgegevens aan de informatiesystemen van de specialisten leveren, of MRI-scanners die gegevens opslaan in de cloud om deze vervolgens met AI te verwerken tot een diagnose. Het is uiteraard van belang dat de privacy van deze medische gegevens gewaarborgd is en dat de diagnose van ziektebeelden niet door hackers beïnvloed kan worden. De zorgsector is een populair doelwit voor hackers[27] voor cyberaanvallen van bijvoorbeeld pro-Russische hacktivisten[28] en van ransomware (gijzelsoftware) criminelen[29].

---

[24] Kopanz J, Lagerwaard B, Veldwijk J, et alDo people prefer to take part in a clinical trial from home or come to site? A discrete choice experiment in type 2 diabetes mellitus, BMJ Open 2025;15:e107737. doi: 10.1136/bmjopen-2025-107737.

[25] Philips on AWS: Case Studies, Videos, Innovator Stories, geraadpleegd 31 oktober 2025.

[26] 'Het is hoogzomer voor AI, maar de herfst komt eraan' | medischcontact, geraadpleegd 31 oktober 2025.

[27] De DDoS-aanval en de digitale weerbaarheid van ziekenhuizen | medischcontact, geraadpleegd 31 oktober 2025.

[28] Nederlandse ziekenhuizen doelwit van DDoS-aanvallen | Nieuwsbericht | Nationaal Cyber Security Centrum, geraadpleegd 31 oktober 2025.

[29] Cyberaanvallen | AVG-Helpdesk voor Zorg en Welzijn, geraadpleegd 31 oktober 2025.

De Europese NIS2-richtlijn[30] is van toepassing op diverse sectoren waaronder ziekenhuizen en een verscherpte versie van de eerdere Network and Information Security (NIS)-richtlijn. In Nederland is de Europese NIS richtlijn geïmplementeerd als Wbni. In Nederland wordt de Europese NIS2 omgezet in de Nederlandse Cyberbeveiligingswet[31] (Cbw) die naar verwachting in het tweede kwartaal van 2026 in werking zal treden. Hiermee zal wetgeving van kracht worden die de digitale en economische cyberweerbaarheid moet versterken voor een bredere set van sectoren. Dat zijn niet alleen zeer kritieke sectoren zoals energievoorziening en gezondheidszorg maar ook kritieke sectoren zoals post- en koeriersdiensten en afvalstoffenbeheer.

Bij private organisaties hangt het af van de sector en de grootte van de organisatie of de NIS2 van toepassing is. Bijvoorbeeld in de chemische industrie kunnen bedrijven die onderdeel vormen van een logistieke keten direct of indirect te maken krijgen met de aankomende Cbw. Naar schatting zullen 8.000 bedrijven direct door deze nieuwe regelgeving getroffen worden en 50.000 - 100.000 bedrijven indirect[32].

Bij productieprocessen van chemische stoffen wordt veelvuldig gebruik gemaakt van Operationele Technologie (OT) die voor besturing Industrial Control System (ICS) toepast. Voor het aansturen en bewaken van productieprocessen wordt veelvuldig gebruik gemaakt van ICSs die samengesteld zijn uit specifieke hard- en software en uitgevoerd zijn als Programmable Logic Controller (PLC).

PLCs worden in allerlei organisaties voor procesbesturing gebruikt en daarmee ook in zeer kritische sectoren variërend van de energievoorziening, waterzuivering, bagage-afhandelingssystemen van luchthavens en bij productieprocessen in de automotive-industrie.

Figuur 8: *Operationele Technologie (OT) zoals gebruikt voor procesbeheersing en monitoring. - Foto: Haagse Hogeschool.*

Een belangrijk verschil tussen OT en andere technologieën is de levenscyclus en het gebruik ervan. Doorgaans zijn OT-systemen ontworpen voor een aanmerkelijk langere levensduur van 10 tot 30 jaar, in tegenstelling tot een levensduur van IT-systemen van 3 tot 5 jaar. Ook het gebruik van OT-systemen is anders dan IT-systemen. OT-systemen maken veelal onderdeel uit van een productieketen die 24/7 actief is en niet zomaar stilgezet kan worden. Het

[30] NIS2 Directive: securing network and information systems | Shaping Europe's digital future, geraadpleegd 31 oktober 2025.
[31] Cyberbeveiligingswet (NIS2-richtlijn) | Over het NCSC | Nationaal Cyber Security Centrum, geraadpleegd 31 oktober 2025.
[32] Chemie on Tour: cyberveiligheid in de chemische logistiek, geraadpleegd 31 oktober 2025.

beveiligen van OT-systemen en het implementeren van de NIS2 richtlijn is niet zo eenvoudig als het uitvoeren van een paar maatregelen. Het vergt volgens senior onderzoeker van dit lectoraat Eric ten Bos[33] een zorgvuldige planning om een verlies aan inkomsten door stilstand of door een cyberaanval te beperken.

Bij IT-systemen zou een medewerker in de avonduren nog een e-mail kunnen versturen en zou men kunnen spreken van een iets minder voorspelbaar gebruik van het netwerk. Bij OT is het netwerkverkeer voorspelbaarder en repeterend. Deze en andere verschillen maken het noodzakelijk om een andere benadering te kiezen voor cyber security van OT. Juist de koppeling tussen beide technologieën is van cruciaal belang. Malware – kwaadaardige software gericht op het verstoren van computers – kan zich via e-mail een bedrijf binnendringen om vervolgens zich te richten op het verstoren van OT-systemen.

Stuxnet[34] is een beroemd voorbeeld van industriële malware dat succesvol gebruik wist te maken van kwetsbaarheden in (Windows) IT om op zoek te gaan naar verbonden OT en deze vervolgens te ontregelen.

Naast de toepassing van OT in industriële omgevingen kunnen ook genetwerkte IoT sensoren worden gebruikt - aangeduid als Industrial IoT (IIoT) - als aanvulling met een afzonderlijk ecosysteem van sensoren, applicaties en netwerken. Het cyberveilig houden van deze gemengde infrastructuren is een uitdagend vraagstuk en vergt duidelijke handelingsperspectieven als een cyberaanval zich voordoet.

In samenwerkingsverbanden tussen overheden en private organisaties wordt eveneens een verscheidenheid van technologieën toegepast en in dit verband is het Drone2Go samenwerkingsproject[35] interessant en illustratief. Hierin werken Rijkswaterstaat, Brandweer, Inspectie Leefomgeving en Transport, Douane, Kustwacht en de Nederlandse Voedsel-en Warenautoriteit samen met kennisinstellingen en private partijen. Het doel is om een netwerk van op afstand bestuurde drones te hebben die op initiatief van gebruikers kunnen uitrukken bij ongevallen en ook gebruikt kunnen worden voor inspecties.

De drone is een duidelijke illustratie van hoe technologie nieuwe mogelijkheden creëert. Al in 2017 zijn in de “Robotic and Autonomous Systems Strategy”[36] van de Amerikaanse landstrijdkrachten – US Army - de bijdragen hiervan omschreven onder andere als “Performing missions impossible for humans”. Inmiddels hebben we als maatschappij nader kennis kunnen maken met deze systemen en kunnen vaststellen ze

[33] Eric ten Bos, Risicogestuurd patchen maakt complexiteit security beheersbaar - Computable.nl, publicatiedatum 04 november 2024.
[34] D. Kushner, The Real Story of Stuxnet, IEEE Spectrum, feb 2013, updated 20 juni 2025. https://spectrum.ieee.org/the-real-story-of-stuxnet
[35] https://www.rijkswaterstaat.nl/zakelijk/innovatie/informatievoorziening/gebruik-van-drones-bij-rijkswaterstaat/drone2go , geraadpleegd 31 oktober 2025.
[36] https://mronline.org/wp-content/uploads/2018/02/RAS_Strategy.pdf, geraadpleegd 31 oktober 2025.

steeds belangrijker worden o.a. voor defensietoepassingen[37], inspectie van windmolens[38] en transport van donororganen[39].

Hiermee voeren drones als technologie taken uit voor mensen die anders niet mogelijk zijn. Voor de veilige inzet van autonome systemen zijn de uitdagingen divers: veel systemen maken gebruik van embedded technologie die specifiek ontwikkeld is voor de

Figuur 9: *Drone voor inspectie van energie-infrastructuur. – Foto: Shutterstock*

betreffende toepassing. Hiermee zijn de beschikbare systeembronnen veelal beperkt tot wat nodig is om de kerntaken van deze systemen te verrichten en beperkt ten behoeve van efficiënt energiegebruik. Daarmee is de ruimte beperkt voor het naderhand aanbrengen van aanvullende cybersecurity functionaliteit. Voor het aansturen van deze systemen wordt gebruik gemaakt van netwerkverbindingen en in toenemende mate van AI. Dit maakt deze autonome systemen tot een interessant doelwit om te hacken, door het overnemen van de besturing, het beïnvloeden van het navigatiesysteem, het storen van de netwerkverbindingen, het veranderen van de te nemen beslissingen of het op een andere wijze aantasten van de bedoelde functionaliteit.

Een interessant aspect dat samenwerkingsverbanden treft in het geval van het Drone2Go project is de manier waarop informatie wordt uitgewisseld tussen betrokken organisaties. In deze samenwerkingsverbanden is het nadrukkelijk de bedoeling dat beeldmateriaal (van autonome systemen) voor een verscheidenheid van toepassingen gebruikt kan worden. Wel dient een juridische grondslag aanwezig te zijn en deze kan bepaalde informatie-uitwisseling wel toestaan en andere niet. Bovendien kan de noodzaak daartoe afhangen van veranderende omstandigheden, naarmate de ernst van een situatie toeneemt kan het noodzakelijk zijn meer organisaties te betrekken en

[37] Defensie zoekt bedrijven voor maken en verbeteren van drones | Nieuwsbericht | Rijksoverheid.nl, geraadpleegd 31 oktober 2025.
[38] Windturbine-inspecties – dutch drone solutions, geraadpleegd 31 oktober 2025.
[39] ANWB test een jaar medische dronevluchten tussen ziekenhuizen Zwolle en Meppel - Tweakers, geraadpleegd 31 oktober 2025.

extra informatiestromen toe te staan. Een technische oplossing waarin bepaalde informatie gedeeld – en natuurlijk ingetrokken - kan worden tussen bepaalde partijen conform een vooraf vastgesteld juridisch kader kan zorgen dat altijd binnen de toegestane juridische kaders de juiste informatie gedeeld kan worden. Deze technische oplossingen kunnen zorgen dat snelle en effectieve samenwerking plaatsvindt. Langs deze weg kan technologie het “wegnemen van schotten” realiseren tussen (overheids)organisaties zoals geformuleerd in prioriteit 2 voor het delen van gegevens in de Nationale DigitaliseringsStrategie (NDS)[40].

Het voorbeeld van Drone2Go is illustratief, maar zeker niet het enige samenwerkingsverband waarin de juiste informatie delen tussen organisaties belangrijk is om slagvaardig te handelen. Deze behoefte is in algemene vorm in een verscheidenheid van samenwerkingsvormen te vinden waarin slagvaardigheid gewenst is, zoals tegen luchtvaartterrorisme[41] en cyberdreigingen[42]. In beide gevallen is snelheid van belang om de risico’s beter te beheersen en zal in zeker mate geautomatiseerd delen hieraan bij kunnen dragen.

Het werken met informatie in afgesloten compartimenten kan in zo’n geval samenwerking bemoeilijken. Het onderbrengen van informatie in afzonderlijke delen wordt ook aangeduid als perimeter security of network security en richt zich op het beveiligen van de infrastructuren zelf zodat de informatie die daarin opgeslagen en verwerkt wordt beveiligd is door bijvoorbeeld firewalls en andere maatregelen om moeilijk het compartiment binnen te kunnen dringen.

Met Data Centric Security (DCS) wordt een andere benadering gekozen: de informatie wordt beveiligd door deze bij de bron te vercijferen. Partijen die deze informatie nodig hebben kunnen vervolgens de sleutels ontvangen om de informatie te ontcijferen. Een manier die past bij de mantra “encrypt everything” van HHs alumnus en CTO van Amazon, Werner Vogels. Met deze methode verschuift de controle van het toegang geven tot de informatie naar het verstrekken van de juiste sleutels.

Netwerken en systemen bij consumenten

Bij consumenten voltrekt zich tevens een digitale transformatie. Allerlei apparaten in ons dagelijks leven elektrificeren en digitaliseren. Dit betreft voertuigen (zoals fietsen en auto’s), verbonden apparaten (zoals robotstofzuigers en robotgrasmaaiers) en huiselijke installaties (warmtepompen, zonne-installaties, energieopslag systemen (ESS)).

[40] NDS Prioriteit 2: Data- Digitale Overheid, geraadpleegd 31 oktober 2025.
[41] https://www.nctv.nl/onderwerpen/r/renegade-regeling, geraadpleegd 7 november 2025.
[42] https://www.nctv.nl/onderwerpen/p/programma-cyclotron, geraadpleegd 7 november 2025.

Figuur 10: *Fiets met elektronisch schakelsysteem. - Foto Shutterstock*

Schijnbaar eenvoudige voorwerpen in ons dagelijks leven zijn verrassend complexer dan we ons wellicht vaak bewust van zijn. Zo zijn bepaalde fietsen uitgerust met een Shimano Di2 elektronisch schakelsysteem.

Met dit systeem kan de elektronische derailleur het schakelproces sneller en nauwkeuriger laten verlopen en aangestuurd worden door een draadloze verbinding van de handvatten aan het stuur. Onderzoekers hebben kwetsbaarheden van dit systeem gevonden[43] waarmee het mogelijk was om het schakelgedrag te beïnvloeden. Bovendien konden de signalen tussen de bediening en de derailleur worden gestoord door middel van jamming. Bij gebruik door professionele wielrenners[44] zou de invloed van deze kwetsbaarheden kunnen toenemen en het belang om systemen te manipuleren. Korte tijd na de publicatie heeft de fabrikant de veiligheid naar eigen zeggen verbeterd in een update[45] voor *'enhanced security for wireless communication between the shifter and the rear derailleur of the Di2 System'* en hebben samengewerkt met de onderzoekers die de kwetsbaarheden gevonden hadden. Hiermee is het een goed voorbeeld van cyber weerbaarheid door de samenwerking met de onderzoekers op te zoeken en kort na publicatiedatum de firmware update te publiceren.

Een ander systeem waarmee vele consumenten bekend zijn is de robotstofzuiger. Onderzoekers Dennis Giese en Daniel Wegemer hebben reverse engineering op een specifiek model toegepast[46] dat door middel van een app bestuurd kon worden en gepresenteerd bij het Chaos Communication Congress (CCC) in 2017. De robotstofzuiger bleek voor een IoT apparaat van veel rekenkracht voorzien te zijn en verrassend

Figuur 11: *De robotstofzuiger als sensorplatform met cloudverbinding in onze thuisomgeving. Foto: Shutterstock*

[43] MakeShift | Proceedings of the 18th USENIX Conference on Offensive Technologies, geraadpleegd 7 November 2025.
[44] Vijftien jaar Shimano Di2: deze veranderingen bracht elektronisch schakelen teweeg | WielerFlits, geraadpleegd 13 november 2025.
[45] https://bike.shimano.com/support-and-service/faq/DI20A.html, geraadpleegd 7 november 2025.
[46] https://dontvacuum.me/talks/34c3-2017/34c3.html , geraadpleegd 7 november 2025.

goed beveiligd. Het maakte gebruik van een variant van het besturingssysteem Ubuntu Linux zoals ook voor PCs wordt gebruikt. Ondanks de goede beveiliging bleek de stofzuiger veel informatie te verzamelen en vercijferd door te sturen naar de cloud van de fabrikant – verscheidene megabytes per dag. De doorgestuurde data omvatte gegevens zoals Wi-Fi netwerken met bijbehorende paswoorden en kaarten van de betreffende fysieke omgeving (bijv. kamers van het huis).

Deze gegevens blijven op het apparaat beschikbaar, ook na een herstel naar fabrieksgegevens. Mocht de stofzuiger gebruikt worden doorverkocht, dan beschikt de volgende gebruiker dus ook over de Wi-Fi naam en passwordgegevens van de vorige eigenaar. Bij het eerste gebruik verbond de stofzuiger zich direct tot de app op de telefoon van de gebruiker, daarna bleken de commando's van de app van de gebruiker via de cloud terug in de thuisomgeving bij de robotstofzuiger terecht te komen. Dit onderzoek heeft tot betere inzichten geleid over de informatie die 'eenvoudige' huishoudelijke producten verzamelen en doorsturen naar het Internet. Bovendien is het door het 'rooten'[47] van het systeem door de onderzoekers mogelijk geworden om alle cloud interactie te omzeilen en het product lokaal te kunnen gebruiken[48]. Op deze manier is – tot genoegen van vele onderlegde gebruikers - voor een breed scala van stofzuigers de mogelijkheid ontstaan om grotere controle te krijgen over het systeem zonder deze afhankelijkheid van de cloud. In NRC Broncode[49] geeft Timo Nijssen aan te willen dat: *"fabrikanten niet meer elk apparaat nodeloos 'slim' maken, dan hebben ze ook geen last van een updateplicht".* In dit artikel wordt duidelijk dat fabrikanten in sommige gevallen ook ongewenste functionaliteiten implementeren zoals het verschijnen van reclame op displays van huishoudelijke koelkasten. In ieder functioneel deel van een systeem kan een cyber security kwetsbaarheid ontstaan, dus ook in deze 'feature'. Eerder is door de Autoriteit Consument & Markt (ACM) en de Rijksinspectie Digitale Infrastructuur (RDI) vastgesteld dat fabrikanten meer moeten doen om slimme apparaten werkend en veilig te houden[50]. Het is te hopen dat de fabrikant van genoemde huishoudelijke apparaten wel veiligheidsupdates blijft doorvoeren op diens 'slimme koelkast', anders zou deze reclame feature wel eens een dubbel ongewenst effect kunnen bewerkstelligen.

Naast huishoudelijke systemen neemt ook het aantal andere digitale installaties in de woning toe. Warmtepompen worden verbonden aan het Internet voor diagnose/onderhoud op afstand. WarmteTerugWin (WTW) systemen kunnen eenvoudig via ebus interfaces worden aangestuurd om door middel van een aangesloten sensornetwerk CO2-en vocht afhankelijke regelingen toe te passen. Zonneomvormers

[47] Het hoogste toegangsniveau van een systeem.
[48] https://valetudo.cloud/pages/general/supported-robots.html , geraadpleegd 7 november 2025.
[49] https://www.nrc.nl/nieuws/2025/11/07/plots-weet-mijn-robotstofzuiger-niet-meer-waar-hij-is-a4912044#/krant/2025/11/08/#502, geraadpleegd 8 November 2025.
[50] https://www.acm.nl/nl/publicaties/acm-en-rdi-fabrikanten-en-verkopers-moeten-meer-doen-om-slimme-apparaten-werkend-en-veilig-te-houden, geraadpleegd 10 november 2025.

kunnen via een Internetverbinding gedetailleerde informatie geven over de dagopbrengst, prestaties van afzonderlijke panelen en vele andere technische gegevens. Digitalisering van deze installaties biedt duidelijke voordelen en men zou de invloed van kwetsbaarheden als beperkt kunnen beschouwen: mocht de warmtepomp weigeren vanwege een cyberaanval dan kan dit vervelend zijn, maar heeft nog niet een ontwrichtend effect op de maatschappij als het een enkele woning betreft. Echter, gelijktijdige aansturing van een groot aantal apparaten in deze sector is een denkbaar scenario dat het elektriciteitsnet zou kunnen destabiliseren[51]. De cyberweerbaarheid van deze apparaten in woningen is dus wel degelijk van algemeen belang en vandaar dat initiatieven worden ondernomen om de cyberweerbaarheid van deze systemen te vergroten, waaronder een oproep voor strengere controle op omvormers[52]. Met de opkomst van Energy Storage Systems (ESS) voor thuisopslag van energie (bijvoorbeeld in woningen) kan hetzelfde effect ontstaan en is eveneens de cyberweerbaarheid van belang.

Naast de energiesector maakt ook de automotive industrie een grote verandering door. Enerzijds door elektrische aandrijflijnen en anderzijds door een toenemende digitalisering van deze ‘platformen’.

Figuur 12: : *Installatie van een EV-lader met Energieopslag systeem (ESS) voor thuisgebruik. Foto: Shutterstock*

[51] https://topsectorenergie.nl/documents/1055/TKI_Cyberzon_WEB_v2-2.pdf, geraadpleegd 7 november 2025.
[52] https://solarmagazine.nl/nieuws-zonne-energie/i41478/zonne-energiesector-vraagt-strenge-controle-op-cyberveiligheid-omvormers, geraadpleegd 22 oktober 2025.

In de thuisomgeving van consumenten is de auto daarom nog een complex systeem erbij geworden. Auto-industrie toeleveranciers Valeo[53] en ZF Friedrichshaven[54] spreken beiden van een revolutie resp. transformatie van voertuigen naar Software-Defined Vehicles (SDV) in de toekomst. Volgens ZF worden er in moderne premium voertuigen 150 miljoen regels (software) code gebruikt, tien maal zoveel als tien jaar geleden. De SDV wordt gevormd door krachtige computers, zogenaamde high-performance computers zodat meerdere systemen, zoals remmen, besturing, demping digitaal kunnen worden aangestuurd. Valeo geeft aan dat iedere nieuwe auto in 2024 een computer op wielen is met 200 miljoen regels code – 33 keer meer dan een Boeing 787. Met het toenemen van de complexiteit van voertuigen met de hoeveelheid code lijnen neemt eveneens het belang van cyber security toe.

De van toepassing zijnde internationale standaard ISO/SAE 21434[55] beschrijft dan ook eisen voor deze SDVs met: regelmatige, veilige software updates, intrusion detection systems en encrypted communication protocols. Hiervoor is het nodig om systemen aan boord van de SDV te segmenteren, moeten veilige protocollen gebruikt worden en moet regelmatig een pentest[56] worden uitgevoerd om kwetsbaarheden te vinden voordat deze misbruikt kunnen worden. Deze kwetsbaarheden zullen blijven ontstaan, daarmee is het onderhoud van de systemen over diens levensduur en het continue updaten van de systemen van belang zodat het voertuig zich blijft gedragen wat we er als consument van verwachten.

Figuur 13: *ZF Driving Intelligence van ZF Friedrichshaven voor Software-defined Vehicles bij de IAA Mobility 2021 motor show in München, Duitsland- September 6, 2021. – Foto: Shutterstock*

[53] Everything you need to know about the Software Defined Vehicle (SDV) | Valeo, geraadpleegd 7 november 2025.
[54] Software-defined Vehicle (SDV) - ZF, geraadpleegd 22 oktober 2025.
[55] ISO/SAE 21434:2021(en), Road vehicles — Cybersecurity engineering, geraadpleegd 7 november 2025.
[56] Het gecontroleerd aanvallen van systemen door ethische hackers om kwetsbaarheden te vinden voordat kwaadwillende hackers deze kwetsbaarheden kunnen gebruiken.

Bijdrage lectoraat Network and System Engineering Cyber Security

Het doel van het lectoraat NSE is om enerzijds bij te dragen aan het versterken van de cyberweerbaarheid van publieke en private organisaties met bijbehorende producten en diensten. Anderzijds wil het lectoraat bijdragen aan de ontwikkeling van relevante kennis voor het werkveld en aan de opleiding van toekomstig talent dat studeert aan de HHs. Dit wordt bereikt door het uitvoeren van praktijkgericht technisch wetenschappelijk onderzoek. Het lectoraat Network and Systems Engineering Cyber Security richt zich hierbij op drie verbonden onderzoekslijnen:

1. **Aanvalstechnieken om beter te verdedigen**

Door netwerken en systemen gecontroleerd aan te vallen, kunnen we zwakke plekken in de beveiliging blootleggen. Dit helpt ons om kwetsbaarheden te vinden en nieuwe technieken te ontwikkelen die dreigingen sneller opsporen en de cyberweerbaarheid van netwerken en systemen verbeteren.

2. **Cyberweerbare infrastructuren**

Praktische infrastructuren maken gebruik van verschillende technologieën, zoals IT, OT en IoT, die elk een andere aanpak nodig hebben. Door het uiteenlopende karakter van deze technologieën is het moeilijker om dreigingen te herkennen en hierop te reageren. We onderzoeken methoden die enerzijds gericht zijn op het veilig gebruik van systemen en anderzijds op het detecteren en bestrijden van aanvallen op deze systemen.

3. **Data centric security**

Om netwerken en systemen beter te beschermen, moeten we niet alleen de omgeving beveiligen, maar vooral de informatie zelf. Traditioneel richt beveiliging zich op het compartiment waar de gegevens zijn opgeslagen, zoals met firewalls. Voor het transporteren van gegevens tussen twee compartimenten kan dan bijvoorbeeld gebruik worden gemaakt van een VPN zodat de informatie tijdens het transport is beveiligd om vervolgens, na verwijdering van de beveiliging, in het nieuwe compartiment te worden opgeslagen. Het beveiligen van gegevens in compartimenten biedt beperkte veiligheid en kan onhandig zijn. Als iedere minuut telt kan de beschikbaarheid van de juiste

informatie doorslaggevend zijn. Data centric security kan ervoor zorgen dat de juiste informatie op het juiste moment toegankelijk is voor de juiste mensen, zonder concessies te doen aan veiligheid of gebruiksgemak.

Aan deze drie onderzoekslijnen werken onderzoekers die deelnemen aan nationale en internationale onderzoeksprojecten. De opgedane kennis wordt bijgedragen aan het onderwijs van de HHs, toegepast in de praktijk en in verder onderzoek voortgezet. Publiek private samenwerking kan zo worden gerealiseerd met bedrijven en andere kennisinstellingen op een verscheidenheid van gebieden. Technische cybersecurity onderwerpen passend bij de onderzoekslijnen worden onderzocht en toegepast.

Inspiratie van de te onderzoeken onderwerpen wordt opgedaan door samenwerking in de praktijk met kennispartners en publieke en private organisaties, in combinatie met Nationale (zoals de NWO National Cybersecurity Research Agenda IV[57]) en Internationale (ENISA[58], ECCC[59], ITEA4) research agenda's en strategieën.

Onderzoekslijn aanvalstechnieken

Het doel van deze onderzoekslijn is om diepgaande kennis op te doen over technieken om kwetsbaarheden van netwerken en systemen te vinden. Als onderdeel van deze onderzoekslijn worden hulpmiddelen gemaakt om netwerken en systemen te kunnen binnendringen en beïnvloeden. Op deze manier kunnen kwetsbaarheden worden gevonden voordat deze door andere, ongewenste, partijen worden gebruikt. Zo worden ontwikkelaars in staat gesteld om deze kwetsbaarheden op te lossen en/of vergelijkbare dreigingen te detecteren en hierop te reageren. Het uiteindelijke doel is een hogere weerbaarheid tegen cyberdreigingen van systemen en netwerken. Door te denken vanuit het perspectief van een hacker kan worden bijgedragen aan een betere verdediging. Deze onderzoekslijn kan hiermee bijdragen aan een uitbreiding van de reeds bestaande minor "Software Reversing and Exploitation"[60]. De benadering bij deze minor is om het perspectief – vanuit technisch oogpunt - van een aanvaller beter te begrijpen om te bepalen hoe de systemen cyberweerbaarder gemaakt kunnen worden. Dit aan de hand van binaire-en geautomatiseerde kwetsbaarheden analyse. Reverse engineering – het ontleden van een systeem - is hierbij een proces dat de inzichten over hoe systemen werken enorm kan vergroten ten aanzien van:

1. Het vernuft van het systeem. Praktische netwerken en systemen in hard- en software realisaties, maar ook malware kunnen vernuftig samengesteld zijn en

[57] NCSRA-IV - FINAL, geraadpleegd 10 november 2025.
[58] Home | European Union Agency for Cybersecurity, geraadpleegd 11 november 2025.
[59] Strategic Agenda - European Cybersecurity Competence Centre and Network, geraadpleegd 11 november 2025.
[60] Kies op maat - Software Reversing and Exploitation, geraadpleegd 7 november 2025.

geven nieuwe inzichten over de creativiteit van de makers waarvan we zelf weer kunnen leren.

2. De kwetsbaarheden van het systeem en hoe deze opgelost kunnen worden.

Afhankelijk van de toegang tot het systeem - fysiek of op afstand - en mogelijke ontwerpgegevens ervan, kan een verscheidenheid van hulpmiddelen worden ingezet om op bovenstaande gebieden te leren. Een goed voorbeeld van het succesvol toepassen van reverse engineering technieken zijn de eerder genoemde werkzaamheden van Giese en Wegemer[61]. Na het afgaan van verscheidene mogelijkheden wist men door een subtiele kortsluiting van de applicatieprocessor deze in FEL-mode (programmeermodus) te krijgen waardoor de software uit het geheugen 'gedumpt' en het systeem vervolgens 'geroot' kon worden, waarmee volledige toegang tot het systeem kon worden verschaft[62]. Vergelijkbaar met het uit elkaar halen van een radio om zo de werking beter te begrijpen kan men ook netwerken en systemen ontleden en onderzoeken om ervan te leren en de cyberweerbaarheid naar een hoger niveau te brengen.

Figuur 14: *Het openen van een radio als herkenbare (?) manier om te onderzoeken en leren van systemen. Foto: Shutterstock.*

Onderzoeksvragen binnen deze onderzoekslijn zijn onder meer:

1. **Vulnerability analyse**: Welke nieuwe ontwikkelingen zijn er om snel kwetsbaarheden te vinden? Kan het vinden van kwetsbaarheden geautomatiseerd worden? Welke methoden zijn inzetbaar voor praktische toepassing?
2. **Innovatieve pentesten:** Welke Innovatieve methoden voor het niet-gedetecteerd binnendringen netwerken en systemen kunnen toegepast worden?
3. **Technologie-specifieke kwetsbaarheden:** op welke manier kunnen kwetsbaarheden van specifieke technologieën zoals van Operationele Technologie (OT), Internet of Things (IoT) of cloud infrastructuur gebruikt worden?

Het beoogde toepassingsgebied van de te ontwikkelen technieken is gericht op de netwerken en systemen in de praktijk zoals deze aangetroffen worden bij publieke en private organisaties en consumenten.

[61]

[62] https://media.ccc.de/v/34c3-9147-unleash_your_smart-home_devices_vacuum_cleaning_robot_hacking#t=585, geraadpleegd 7 november 2025.

Gezien de brede toepassing van IT infrastructuren is het vinden van kwetsbaarheden van praktische relevantie. Hulpmiddelen zoals AI assistenten[63] zijn reeds enige tijd beschikbaar maar tot nu toe van beperkte waarde gebleken voor de uitgevoerde onderzoeken. Deze oplossingen zullen verder verbeteren. Het evalueren van de effectiviteit van deze middelen blijft hiermee onderdeel van deze onderzoekslijn zonder daadwerkelijk AI modellen te ontwikkelen. Voor het vinden van kwetsbaarheden in cloud infrastructuren zal nader onderzoek gedaan worden naar de kwetsbaarheden in Infrastructure as Code (IaC) templates, waarmee servers, netwerken en databases in code kunnen worden geconfigureerd. Het grote voordeel van deze IaC templates is de snelheid waarmee infrastructuren ontplooid kunnen worden, het risico van misconfiguraties moet beheersbaar worden gemaakt. Dit is de motivatie voor het ontwikkelen van kennis om deze misconfiguraties snel op te sporen die anders over het hoofd worden gezien. In deze onderzoekslijn ligt de nadruk op het vinden van de kwetsbaarheden, terwijl in de lijn van cyberweerbare infrastructuren onderzoek verricht wordt naar het snel kunnen herstellen van gevonden misconfiguraties.

Een ander te onderzoeken onderwerp van praktische relevantie met betrekking tot cloud infrastructuren is hoe de kwetsbaarheden van toepassingen in de cloud gevonden kunnen worden. In hoeverre zijn AI modellen vatbaar voor manipulatie en kunnen de uitkomsten van deze modellen veranderen zonder dat dit wordt opgemerkt? Voor bijvoorbeeld modellen die gebruikt worden voor de beoordeling van informatie van medische sensoren of diagnose systemen is dit uitermate relevant en een onderwerp voor verder onderzoek.

In het onderzoeksvoorstel DROBOTIZE[64] zal het NSE lectoraat binnen deze onderzoekslijn onderzoek doen naar de cybersecurity kwetsbaarheden van autonome systemen die in groepsverband opereren en uitgerust zijn met AI functionaliteit om als individueel platform en in groepsverband taken uit te voeren. In het bijzonder zullen de inspanningen gericht zijn op het vinden van kwetsbaarheden van de betreffende systemen voor manipulatie, jamming en spoofing. Gezien de reeds beschreven, brede toepassing van autonome systemen zal het onderzoek binnen deze onderzoekslijn zich niet beperken tot het DROBOTIZE project maar zal ook aansluiting worden gezocht op andere instrumenten.

Op het onderwerp van technologie-specifieke kwetsbaarheden wordt door het lectoraat onderzoek gedaan naar OT-malware voor representatieve OT installaties en naar kwetsbaarheden in IoT systemen. In de onderzoeksvoorstellen over Cyberweerbare Gemeentelijke Infrastructuren[65] en Cyberweerbare energie ketens zal deze kennis en ervaring nader toegepast worden.

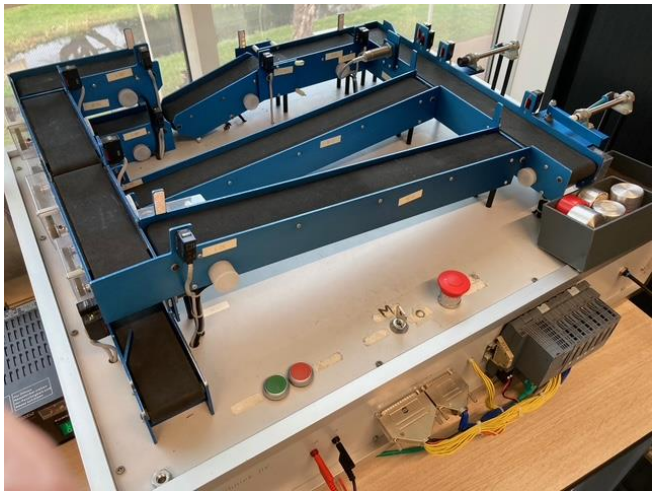
---

[63] https://kali-gpt.com/, , geraadpleegd 7 november 2025.
[64] ITEA 4 · Project · 24006 Drobotize, , geraadpleegd 11 november 2025.
[65] Project Cyberweerbare Gemeentelijke Infrastructuren | NWO-SIA Projectenbank, , geraadpleegd 11 november 2025.

Op het gebied van bijvoorbeeld industriële en medische toepassingen komen gemengde infrastructuren voor van informatie technologie met operationele-en IoT technologie. Zo kan een kwetsbaarheid in een IT systeem behulpzaam zijn voor het misbruiken van een kwetsbaarheid van een OT/IoT systeem. Dit vergt een integrale aanpak voor het onderzoeken van gecombineerde kwetsbaarheden in gemengde infrastructuren en hoe deze combinatie kan zorgen voor een systeemkwetsbaarheid.

Onderzoekslijn cyberweerbare systemen

Het doel van deze onderzoekslijn is om aan de hand van de opgedane kennis en ervaring van aanvalstechnieken systemen en netwerken beter weerbaar te maken tegen cyberdreigingen. In de voorgaande onderzoekslijn wordt van een breed scala aan praktische systemen onderzocht wat mogelijke kwetsbaarheden zijn van technologieën in een verscheidenheid van toepassingen waarin deze afzonderlijk of in combinatie worden toegepast.



Figuur 15: *Operational Technology (OT) sorteerband voor cyberweerbaar OT onderzoek. Foto - Dua Güven, Haagse Hogeschool.*

Onderzoeksvragen binnen deze onderzoekslijn zijn onder andere:

1. **Veilig gebruik van infrastructuur:** Hoe kan een technische oplossing helpen om een systeemconfiguratie veilig te gebruiken?
2. **Detecteren van dreigingen:**
   Op welke wijze kunnen cyberdreigingen in netwerken en systemen in een vroeg stadium vastgesteld worden? Is het mogelijk met nieuwe technologieën, zoals AI, beter detectie uit te voeren? Hoe zou detectie voor specifieke technologieën (zoals IoT) kunnen worden toegepast? Hoe kan de detectie van verschillende technologiedomeinen gecombineerd worden, zodanig dat dreigingen beter integraal kunnen worden vastgesteld?
3. **Respons op en herstel van dreigingen:** welke maatregelen kunnen genomen worden om dreigingen tegen te gaan? Wat zijn de handelingsperspectieven? Kan een technische oplossing beslissingen ondersteunen voor organisaties met beperkte (lokale) cyber security expertise?

Onderzoekslijn Data Centric Security

Zoals eerder beschreven is Data Centric Security (DCS) een andere benadering voor informatiebeveiliging: de informatie zelf wordt beveiligd in plaats van het compartiment waarin de informatie zich bevindt. De informatie wordt bij de bron vercijferd en de encryptie zorgt ervoor dat de confidentialiteit en integriteit kan worden gegarandeerd. Vervolgens kunnen de vercijferde gegevens worden opgeslagen op een plaats waar deze gedeeld kunnen worden met alle beoogde gebruikers zonder dat cyber criminelen de gegevens kunnen inzien. Hiermee kan informatie worden opgeslagen en getransporteerd zonder dat deze direct inzichtelijk is. Deze benadering stelt vele eisen aan een systeem, bijvoorbeeld ten aanzien van het veilig uitvoeren van de encryptie, decryptie, het veilig aanmaken, opslaan en verdelen van encryptiesleutels en het verdelen van de vercijferde gegevens over meerdere opslaglocaties.

Tegenover deze en andere vraagstukken levert een DCS systeem de volgende voordelen:

1. **Snelheid**: vercijferende gegevens kunnen snel toegankelijk zijn voor gebruikers, het beschikken over de juiste sleutel is al voldoende om de opgeslagen informatie te kunnen ontcijferen.
2. **Controle**: controle kan gegeven worden op verscheidene niveaus van toegang. Een gedetailleerde controle kan zorgen dat binnen de gewenste grenzen informatiedeling kan plaatsvinden (om onder verschillende omstandigheden aan de geldende wettelijke kaders te voldoen). Mocht het bovendien nodig zijn om met nieuwe gebruikers informatie te delen dan is het delen van de juiste encryptiesleutel voldoende.
3. **Flexibiliteit**: de vercijferde informatie kan in principe overal worden opgeslagen, in cloud infrastructuren of andere, zelfs meerdere, opslaglocaties.
4. **Zicht op gebruik**: bij voldoende maatregelen om de gegevens veilig te vercijferen kan de aanname gemaakt worden dat alleen de gebruikers die de bijbehorende sleutel hebben ontvangen voor informatie deze hebben kunnen gebruiken. Om zicht op (mogelijk) gebruik van gegevens te hebben kan het sleutelgebruik worden bewaakt.

De onderzoeksvragen die binnen deze onderzoekslijn worden gesteld zijn:

1. **Beveiliging eindpunten:** op welke wijze kunnen de eindpunten van de informatiestromen (de producenten en consumenten) beveiligd worden en zijn de maatregelen haalbaar in de praktijk?
2. **Sleutel management:** hoe kunnen de encryptiesleutels veilig worden aangemaakt, opgeslagen en verdeeld? Is het mogelijk om met beperkte interactie over het juiste sleutelmateriaal te beschikken?
3. **Koppeling meerdere domeinen:** Hoe kunnen meerdere domeinen gekoppeld worden in een gedistribueerd systeem?

Aangezien deze technologische aanpak ten dienste moet staan van gebruikers en mogelijkheden binnen de van toepassing zijnde juridische kaders, biedt deze onderzoekslijn ook voldoende aanknopingspunten voor gemeenschappelijk onderzoek op het gebied van technische en juridische vraagstukken voor informatiedeling.

Praktijkgericht onderzoek voor en met de praktijk

In deze entreerede heb ik uiteengezet wat de motivatie is van het lectoraat om bij te dragen op het gebied van toegepast technisch cyber security onderzoek voor veilige digitalisering in de praktijk. Het is van essentieel belang dat wet- en regelgeving waarborgen biedt zodat technologie de economie en maatschappij ook daadwerkelijk dient. Het lectoraat neemt deze m.n. Nationale en Europese reguleringen daarom als een randvoorwaarde.

Het lectoraat heeft een brede belangstelling voor digitale technologieën die in de praktijk worden toegepast voor private/publieke partijen en consumenten. Dit varieert van OT/IoT systemen tot cloud technologie.

Het lectoraat richt zich nadrukkelijk op de drie beschreven onderzoekslijnen. Hierdoor kan goed begrip van de gedetailleerde werking van systemen en netwerken worden opgedaan, iets dat onderzoekers en studenten helpt om doeltreffende beveiligingsmaatregelen te ontwikkelen en te valideren middels toegepast onderzoek. Samengewerkt wordt met andere lectoraten die zich richten op het gebruik van technologie voor een bepaald doel, waarbij het lectoraat NSE dan de technische cyber security aspecten onderzoekt. Een vergelijkbare samenwerking vindt plaats in de praktijk waarbij systemen voldoende cyber security waarborgen moeten bieden. Verder zal het lectoraat technisch toegepast onderzoek combineren met onderzoek op andere gebieden binnen cyber security, zoals veiligheid, criminologie, risicomanagement en juridische aspecten.

Op deze manier kan enerzijds worden bijgedragen aan technisch onderzoek dat relevant is in de (technische) praktijk en anderzijds aan een integrale benadering van cyber security.