Centre of Expertise Cyber Security

Praktijkgericht onderzoek naar de cyberveerkracht van organisaties

Lectoren

Prof. Dr. Rutger Leukfeldt
Lector Cybercrime & Cybersecurity
Directeur van het Centre of Expertise Cyber Security

Dr. Marcel Spruit
Lector Cyber Security & Safety

Dr. Peter Roelofsma
Lector Risk Management & Cyber Security

Dr. Gerard Hoekstra
Lector Network & Systems Engineering Cyber Security

Jaarupdate 2024

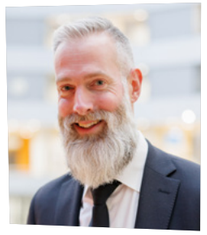
let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

Inhoud

VOORWOORD	3
WIE WE ZIJN	4
WAT WE DOEN	6
CYBER SECURITY & SAFETY	6
CYBERCRIME & CYBERSECURITY	8
NETWORK & SYSTEMS ENGINEERING	10
CYBER SECURITY RISK MANAGEMENT & CYBER SECURITY	12
PHD PROJECTEN	14
ONS TEAM	16
PROJECTENOVERZICHT	18
STAGES VOOR STUDENTEN	24
HIGHLIGHTS 2024	26
VOORUITBLIK 2025	30
BIJLAGE 1: INFOGRAPH 2024	32
BIJLAGE 2: PUBLICATIEOVERZICHT 2024	34

Voorwoord



Het jaar 2024 stond voor het Centre of Expertise Cyber Security (CoECS) in het teken van groei en ontwikkeling. We verwelkomden nieuwe (docent) onderzoekers, startten diverse onderzoeksprojecten en legden stevige verbindingen met het onderwijs. Binnen het SPRONG-expertisenetwerk Cyberweerbaar NL gaven we bovendien extra aandacht aan de talentonwikkeling van onze PhD-kandidaten en junior onderzoekers.

In 2024 hebben we volop ingezet op de verbreding van het Centre of Expertise Cyber Security. Zo richtten we succesvol het nieuwe lectoraat Legal Aspects of Cyber Security (LACS) op, waarin inmiddels meerdere docent-onderzoekers actief bijdragen aan praktijkgericht onderzoek. Daarnaast troffen we de voorbereidingen voor de start van een technisch georiënteerd lectoraat met de werktitel Cybersecurity voor Smart Industry (CSSI).

Ook investeerden we in onze onderzoeksinfrastructuur. In Zoetermeer openden we het Cyber Security Living Lab en breidden we het Human Factor Lab binnen de Dutch Innovation Factory verder uit. Daarnaast verkenden we de mogelijkheden voor een technisch lab op onze locatie in Delft. Deze ontwikkelingen versterken ook de samenwerking met het onderwijs. Studenten draaiden volop mee in onderzoeksprojecten en onze onderzoekers deelden hun kennis actief in het onderwijs.

De samenwerking met externe partners kreeg een extra impuls. Binnen Cyberweerbaar NL werkten we intensiever samen met consortiumpartners. We zetten lopende onderzoeksprogramma's met Thales en de gemeente Zoetermeer voort. Eind 2024 legden we de basis voor een nieuw, langdurig regionaal samenwerkingsprogramma met de gemeente Den Haag. Deze en andere nieuwe samenwerkingen en opdrachten zorgden voor een sterke groei in externe financiering.

We leverden een actieve bijdrage aan het thema 'Digitale Toekomst', een van de drie pijlers van de kennisagenda van De Haagse Hogeschool. Samen met het Centre of Expertise Digital Operations & Finance gaven we dit hogeschoolbrede thema verder vorm en richtten we een AI & Data Sicence Expert Team op, beschikbaar voor de hele hogeschool. Ook startten we een Community of Practice 'Onderzoek en Digitale Toekomst', waarin lectoren en docent-onderzoekers kennis, ideeën en vraagstukken uitwisselen.

In deze jaarupdate zetten we onze belangrijkste resultaten in de schijnwerpers en geven we een inkijkje in ons lopende onderzoek. De wereldwijde ontwikkelingen onderstrepen het belang van ons werk – nu en in de toekomst. We wensen u veel leesplezier en nodigen u van harte uit om met ons in gesprek te gaan over mogelijke samenwerkingen en nieuwe kansen.

Namens het Centre of Expertise Cyber Security
Rutger Leukfeldt

Over ons

Het Centre of Expertise Cyber Security richt zich op het versterken van de cyberveerkracht van publieke en private organisaties die kwetsbaar zijn voor cyberdreigingen. Aangezien cyberaanvallen steeds geavanceerder worden, is het van groot belang dat organisaties over de juiste kennis en middelen beschikken om zich effectief te beschermen.

Met praktijkgericht onderzoek bieden wij oplossingen voor actuele vraagstukken op het gebied van digitale veiligheid. We werken intensief samen met het onderwijs en het werkveld en hanteren een multidisciplinaire aanpak. Dit levert nieuwe kennis, producten en diensten op die direct toepasbaar zijn en bijdragen aan een veiligere digitale samenleving.

Onderzoeksthema's

Ons onderzoek richt zich op drie kerngebieden:

- **Mens:** welke gedrag- en houdingsaspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten verbeteren?
- **Organisatie:** welke organisatorische factoren zijn van invloed op cyberweerbaarheid en hoe kunnen organisaties hierop inspelen?
- **Techniek:** welke technische aspecten dragen bij aan cyberveerkracht en hoe kunnen technische maatregelen mensen en organisaties helpen om hun cyberveerkracht te verbeteren?

Samenwerking

In het Centre of Expertise Cyber Security werken vier lectoraten samen, elk met hun eigen expertise:

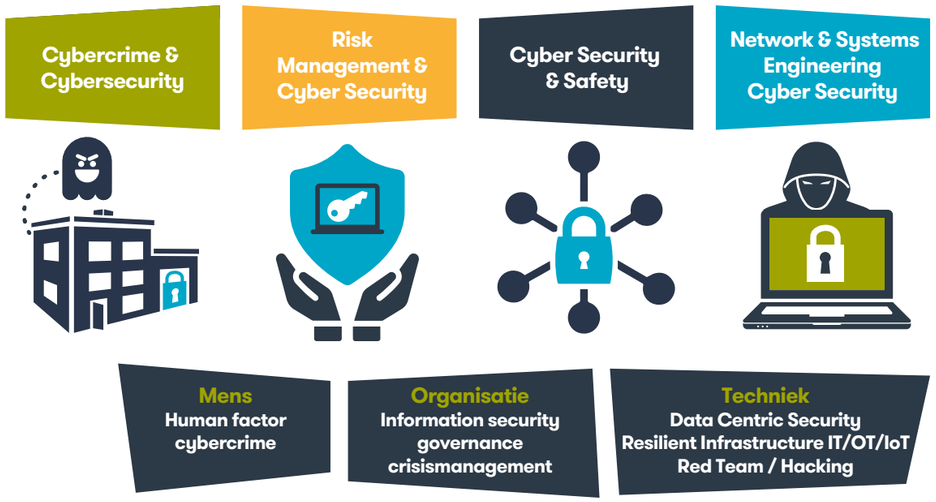
- **Cyber Security & Safety**
- **Cybercrime & Cybersecurity**
- **Risk Management & Cybersecurity**
- **Network and Systems Engineering Cybersecurity**

Door deze verschillende invalshoeken samen te brengen, leveren we een unieke, multidisciplinaire bijdrage aan praktijkgericht onderzoek in cybersecurity. Ons team bestaat uit lectoren, onderzoekers, docent-onderzoekers, projectmanagers en studenten die gezamenlijk werken aan diverse projecten.

Het Centre of Expertise is nauw verbonden met de faculteiten en opleidingen van De Haagse Hogeschool. We werken actief samen met bedrijven, organisaties en andere instellingen. Deze samenwerking biedt organisaties en bedrijven de mogelijkheid om samen met onderzoekers, docenten en studenten nieuwe kennis te ontwikkelen en direct in de praktijk toe te passen.

Ons werk sluit aan bij de kennisagenda van De Haagse Hogeschool, die is opgebouwd rond drie hoofdthema's: Rechtvaardig samenleven, Transitie naar duurzaamheid en Digitale Toekomst. Voor het thema Digitale Toekomst vervullen wij samen met het Centre of Expertise Digital Operations & Finance de trekkersrol binnen de hogeschool. De focus binnen het thema ligt op veiligheid en weerbaarheid en de toekomst van werk. Daarbij staan mens, organisatie en techniek centraal.

Multidisciplinair onderzoek Centre of Expertise Cyber Security



Cyber Security & Safety

Marcel Spruit, lector Cyber Security & Safety

Marcel Spruit is lector Cyber Security & Safety aan De Haagse Hogeschool. Met zijn uitgebreide ervaring in informatiebeveiliging en cybersecurity leidt hij praktijkgericht onderzoek en draagt hij bij aan de ontwikkeling van onderwijs op dit gebied. Daarnaast doceert hij in diverse masteropleidingen aan De Haagse Hogeschool en enkele universiteiten.

Eerder werkte Marcel onder andere bij Fokker Space in kwaliteitsborging, als universiteit hoofddocent aan de TU Delft en als senior consultant voor cybersecurity bij PBLQ (voorheen Het Expertise Centrum). Zijn onderzoek richt zich op het meten en verbeteren van menselijk gedrag rondom cybersecurity, het analyseren en optimaliseren van cybersecurity in organisaties en de kwalificatie van cybersecurityprofessionals.

“Bij het cyberweerbaarder maken van onze samenleving ligt de nadruk vaak op technische oplossingen, maar dat is niet voldoende. We moeten meer aandacht besteden aan de rol van mensen en hoe we cyberweerbaarheid organiseren.”

Wat doet het lectoraat Cyber Security & Safety?

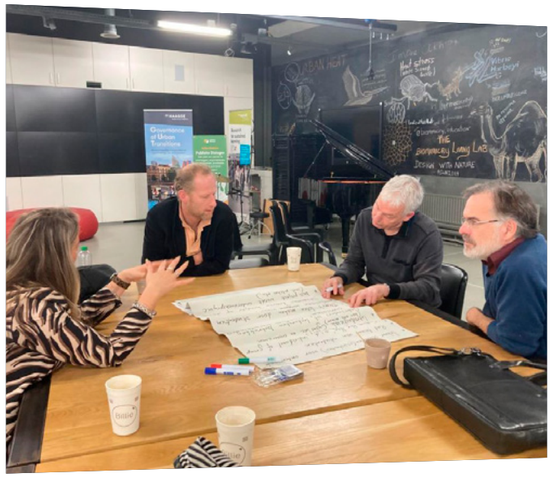
Het lectoraat Cyber Security & Safety doet onderzoek naar methoden en technieken om het cybersecuritygedrag van mensen te meten en te verbeteren – zowel van individuen als van medewerkers binnen organisaties. Daarnaast ontwikkelt het lectoraat manieren om cybersecurity binnen organisaties te analyseren en te versterken, met aandacht voor de rol die kunstmatige intelligentie hierin kan spelen. De focus ligt op zowel publieke als private organisaties. Ook zet het lectoraat zich in voor het versterken van het cybersecurityonderwijs voor professionals.

Het onderzoek binnen het lectoraat is onderverdeeld in vier hoofdthema’s:

1. **Het vergroten van het cybersecurity-bewustzijn bij mensen**
2. **Het versterken van cybersecurity in organisaties**
3. **De rol van kunstmatige intelligentie binnen cybersecurity**
4. **De kwalificatie van cybersecurityprofessionals**

Samenwerking met onderwijs

- Faculteit Bestuur, Recht & Veiligheid: Integrale Veiligheidskunde
- Faculteit IT & Design: HBO-ICT en Master Cyber Security Engineering



Uitgelichte projecten

De impact van Generatieve AI op cybersecurity in de financiële sector

De financiële sector maakt al geruime tijd gebruik van kunstmatige intelligentie. De opkomst van Generatieve AI (GenAI) biedt nieuwe kansen voor innovatieve financiële toepassingen, maar brengt ook extra risico’s met zich mee. Zo kunnen kwetsbaarheden ontstaan die de kans op geavanceerde cyberaanvallen vergroten. In dit project onderzoeken we de impact van GenAI op de cyberweerbaarheid van de financiële sector. Op basis van interviews met experts brengen we de belangrijkste ontwikkelingen, risico’s en kansen in kaart.

- **In opdracht van:** HCLTech
- **In samenwerking met:** Security Delta (HSD)

Digitale veiligheid van Nederlandse gemeenten: een onderzoek naar de cybersecurity van Operationele Technologie

Door nieuwe Europese regelgeving (NIS2) worden gemeenten verplicht om de cybersecurity van hun operationele technologie (OT) op orde te brengen. Het gaat daarbij om systemen die onder andere bruggen, sluizen, gemalen en verkeersinstallaties aansturen. Veel gemeenten maken zich zorgen over hun huidige beveiligingsniveau. In dit project is een enquête afgenomen onder 65 Chief Information Security Officers (CISO’s) van Nederlandse gemeenten. Het doel: inzicht krijgen in de staat van OT-cybersecurity, de getroffen maatregelen en hoe het thema binnen de organisatie is belegd. De resultaten helpen bij het formuleren van ondersteuningsbehoeften en oplossingsrichtingen voor een betere beveiliging van gemeentelijke infrastructuur.

- **In opdracht van:** VNG, Informatiebeveiligingsdienst (IBD)
- **In samenwerking met:** Lectoraat Changing Role of Europe (Centre of Expertise Global and Inclusive Learning, De Haagse Hogeschool)

Kwalificatie Cybersecurity mkb

Het midden- en kleinbedrijf (mkb) is kwetsbaar voor cyberdreigingen, vaak vanwege een beperkt beveiligingsniveau en een tekort aan goed opgeleide cybersecurityprofessionals. Dit project richt zich op het in kaart brengen van de taken en benodigde competenties van cybersecurityprofessionals binnen mkb-organisaties. Op basis hiervan worden competentieprofielen opgesteld. Ook wordt onderzocht in hoeverre het bestaande cursus- en opleidingsaanbod aansluit bij deze profielen. Het eindresultaat is een rapport met concrete aanbevelingen voor passende opleidingstrajecten voor het mkb.

- **In opdracht van:** IT Verband Zuid-Holland (ITVZH)
- **In samenwerking met:** Platform voor Informatiebeveiliging (PvIB), Security Delta (HSD), WE-IT, IT Campus Rotterdam

Plannen voor 2025

In 2025 bundelen De Haagse Hogeschool, Connect2Trust en de gemeente Den Haag hun krachten in de strijd tegen cyberdreigingen. Met de oprichting van het Platform Lokaal Cyberweerbaar Den Haag willen de samenwerkingspartners een belangrijke stap zetten richting een digitaal weerbare stad. Dit initiatief wordt mogelijk gemaakt door de subsidieregeling Versterking Cyberweerbaarheid van het Digital Trust Center. In opdracht van IT Verband Zuid-Holland start het lectoraat een nieuw onderzoek gericht op het mkb. Het doel: inzicht krijgen in de huidige en toekomstige behoefte aan IT- en cybersecurityvaardigheden binnen het mkb in Zuid-Holland. Ook onderzoekt het lectoraat hoe het IT- en cyberonderwijs beter kan aansluiten op deze behoeften. Daarnaast dient het lectoraat een subsidieaanvraag in voor een project over veilige digitale infrastructuren van gemeenten. In mei neemt lector Marcel Spruit afscheid van De Haagse Hogeschool. Meer dan twintig jaar heeft hij zich ingezet voor het onderwijs en onderzoek op het gebied van cybersecurity. Tijdens zijn afscheidsseminar kijkt hij terug op twee decennia vol ontwikkelingen, inzichten en maatschappelijke impact.

Cybercrime & Cybersecurity

Rutger Leukfeldt, lector Cybercrime & Cybersecurity

Rutger Leukfeldt is lector Cybercrime & Cybersecurity en directeur van het Centre of Expertise Cyber Security van De Haagse Hogeschool. Daarnaast is hij senior onderzoeker bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) en bijzonder hoogleraar Governing Cybercrime aan de Universiteit Leiden.

Zijn onderzoek richt zich op de menselijke kant van cybercrime. Hij onderzoekt onder andere wie de daders zijn, hoe zij te werk gaan, welke risicoprofielen slachtoffers hebben en hoe de aanpak van cybercrime effectiever kan worden ingericht. Rutger publiceerde meer dan 130 wetenschappelijke artikelen over cybercrime, waaronder ruim 70 peer-reviewed artikelen, 6 boeken en diverse onderzoeksrapporten. Hij is voorzitter van de Cybercrime Working Group van de European Society of Criminology (ESC) en medeoprichter van de jaarlijkse Human Factors in Cybercrime Conference.

“We moeten toe naar een meer empirisch onderbouwde aanpak van cybercrime. Met alleen een goed idee komen we er niet. Cybercrime is ‘here to stay’ en we moeten dus investeren in een goede kennisbasis.”

Wat doet het lectoraat Cybercrime & Cybersecurity?

Het lectoraat Cybercrime & Cybersecurity ondersteunt het mkb, overheden en publieke organisaties in Nederland bij het versterken van hun digitale veiligheid en bewustzijn. Door onderzoek te doen en kennis te delen, werken we aan het verminderen van het aantal slachtoffers van cyberaanvallen en het beperken van de schade die deze aanvallen veroorzaken.

Het onderzoek binnen het lectoraat richt zich op vier onderzoekslijnen:

1. **De aard en omvang van slachtofferschap**
2. **De aard van cybercriminaliteit**
3. **Het versterken van cyberweerbaarheid**
4. **De aanpak van cybercriminaliteit**

Samenwerking met onderwijs

- Faculteit Bestuur, Recht & Veiligheid: Integrale Veiligheidskunde, LAW en Safety and Security Management Studies
- Faculteit IT & Design: HBO-ICT en Master of Cyber Security Engineering

Uitgelichte projecten

Versterking van cyberweerbaarheid in het mkb met een geautomatiseerde, evidence-based gedragsinterventie

Veel mkb-ondernemers lopen het risico slachtoffer te worden van cyberaanvallen. In de praktijk blijkt het voor hen lastig om structurele stappen te zetten om hun digitale veiligheid te verbeteren en te onderhouden. Het gevaar van cyberaanvallen wordt regelmatig onderschat. Zo leeft vaak het misverstand dat uitbesteding van IT automatisch betekent dat cybersecurity goed geregeld is. Dit project bouwt voort op een eerdere pilotstudie, waarin is onderzocht of een geautomatiseerde kwetsbaarhedenmeting effectief én juridisch toegestaan is als instrument om de digitale weerbaarheid van het mkb te vergroten.

In de huidige fase wordt gewerkt aan de doorontwikkeling van een evidence-based gedragsinterventie die ondernemers stimuleert om drie van de vijf basismaatregelen van het Digital Trust Center (DTC) voor veilig digitaal ondernemen toe te passen:

1. Kwetsbaarheden inventariseren
2. Updates tijdig uitvoeren
3. Bescherming tegen virussen en malware

Ondernemers ontvangen een gepersonaliseerd rapport met concrete adviezen zodra kwetsbaarheden worden gedetecteerd. Het project draagt bij aan de wetenschappelijke onderbouwing van effectieve interventies voor digitale weerbaarheid in het midden- en kleinbedrijf.

- **Gefinancierd door:** CCV City Deal Lokale Weerbaarheid Cybercrime
- **In samenwerking met:** NHL Stenden Hogeschool

Criminele netwerken achter geldezels

De snelle digitalisering van de samenleving zorgt ervoor dat ook criminaliteit steeds vaker online plaatsvindt. Traditionele misdrijven nemen af, terwijl cybercriminaliteit, zoals phishing, hacken en online handelsfraude, toeneemt. Een cruciale schakel binnen deze digitale misdrijven is het witwassen van crimineel geld. Hiervoor maken cybercriminelen vaak gebruik van geldezels — ook wel katvangers of money mules genoemd — om illegale inkomsten weg te sluizen.

Dit onderzoek richt zich op de criminele netwerken die achter geldezelconstructies schuilgaan. Doel is om inzicht te krijgen in de aard, structuur en werkwijze van deze netwerken, en om aanknopingspunten te identificeren voor preventie, verstoring en opsporing. Zo wordt bijgedragen aan een effectieve en integrale aanpak van cybercriminaliteit en gedigitaliseerde criminaliteit.

- **In opdracht van:** Politie
- **In samenwerking met:** NSCR, Operatie Centurion van de Nationale Politie

Naar een toekomstbestendige civielrechtelijke afdoening van online fraude

Het aantal slachtoffers van online fraude blijft stijgen. Naast een strafrechtelijke route kunnen slachtoffers ook civielrechtelijke stappen ondernemen om hun schade te verhalen, bijvoorbeeld via een gerechtsdeurwaarder, rechtsbijstandverzekering of advocaat. De verwachting is dat meer slachtoffers van deze mogelijkheid gebruik zullen maken. Dit onderzoek brengt in kaart hoe de civielrechtelijke afhandeling van online fraude in Nederland verloopt en wat de impact is op slachtoffers, daders en de samenleving. Centraal staat de vraag: Hoe verloopt de civielrechtelijke afdoening van online fraude in Nederland en hoe kunnen de risico’s voor slachtoffers, daders en de maatschappij worden verkleind? Het doel is het ontwikkelen van praktische handvatten voor slachtoffers en maatschappelijke organisaties, zodat civielrechtelijke interventies effectiever en toegankelijker worden.

- **In opdracht van/gefinancierd door:** Stichting Achmea Slachtoffer en Samenleving (SASS) en Politie Nederland
- **In samenwerking met:** Slachtofferhulp Nederland, Ministerie van Justitie en Veiligheid, Fraudehelpdesk, CCV, LAVG Gerechtsdeurwaarders B.V., Stichting Achmea Rechtsbijstand, Branchevereniging Horus en Hogeschool Saxion

Plannen voor 2025

In 2025 bouwen we voort op een groot aantal onderzoeken die in 2024 of eerder zijn gestart. Daarnaast starten we nieuwe meerjarige projecten voor diverse opdrachtgevers – daarover binnenkort meer. De samenwerking binnen het SPRONG-expertisenetwerk Cyberweerbaar NL verloopt erg goed. In 2025 vindt de eerste evaluatie plaats. We zetten in op een verdere verdieping van de samenwerking, met als doel om met een aantal partners nog intensiever op te trekken. Een belangrijk hoogtepunt in 2025 is de afronding van de promotietrajecten van meerdere promovendi. Daarmee leveren we als Centre of Expertise Cyber Security voor het eerst gepromoveerde praktijkgerichte onderzoekers af – een mooie mijlpaal!

WAT WE DOEN

Network and Systems Engineering Cyber Security

Gerard Hoekstra, lector Network and Systems Engineering Cyber Security

Gerard Hoekstra is lector Network and Systems Engineering Cyber Security aan De Haagse Hogeschool. Daarnaast werkt hij bij Thales Nederland, waar hij verantwoordelijk is voor oplossingen op het gebied van soevereine cybersecurity.

Gerard heeft tien jaar ervaring in de telecommunicatie-industrie en vervulde daarna verschillende functies binnen Secure Communications & Information Systems bij Thales Nederland. Hij promoveerde aan de Vrije Universiteit op onderzoek dat hij uitvoerde bij het Centrum Wiskunde & Informatica (CWI), waar hij tot 2015 als deeltijd postdoc onderzoeker aan verbonden bleef.

“Denken vanuit het perspectief van een aanvaller is de beste manier om effectief te verdedigen.”

Wat doet het lectoraat Network and Systems Engineering Cyber Security?

Het lectoraat Network and Systems Engineering Cyber Security richt zich op het versterken van cyberweerbaarheid door veilige netwerken en systemen te ontwikkelen. De onderzoekers brengen cyberdreigingen in kaart, ontwikkelen verdedigingsstrategieën en zetten nieuwe technologieën in om aanvallen tijdig te detecteren en effectief te reageren.

De kern van het onderzoek is informatiebeveiliging: hoe kun je systemen ontwerpen die bestand zijn tegen aanvallen, hoe spoor je kwetsbaarheden op via gecontroleerde aanvallen, en hoe leer je van het perspectief van de aanvaller om betere verdediging mogelijk te maken?

De focus ligt op het beschermen van digitale infrastructuren in een wereld waarin IT, OT en IoT steeds meer met elkaar verweven zijn. Het doel is om systemen te ontwikkelen die niet alleen veilig en robuust zijn, maar ook gebruiksvriendelijk en ondersteunend aan samenwerking tussen mensen en organisaties, zonder concessies te doen aan de veiligheid.

Het onderzoek van het lectoraat is opgebouwd rond drie hoofdthema’s:

1. **Data centric security**
2. **Cyberresiliente systemen**
3. **Aanvalstechnieken om beter te verdedigen**

Samenwerking met onderwijs

- Faculteit Bestuur, Recht & Veiligheid: LAW
- Faculteit IT & Design: HBO-ICT/Applied Computer Science, de minor Software Reversing and Exploitation en de master Cyber Security Engineering

Uitgelichte projecten

OT Security: testen van OT Malware

Industriële systemen worden steeds kwetsbaarder voor digitale dreigingen, mede door de toenemende integratie van Operationele Technologie (OT) en IT-systemen. De beveiliging van OT-systemen – die cruciale fysieke processen aansturen – is van vitaal belang voor de (digitale) veiligheid van onze infrastructuren. Dit project richt zich op het versterken van de weerbaarheid van OT-systemen door middel van offensieve beveiligingsmethoden. Centraal staat de ontwikkeling van een stealthy malwarevariant die in staat is OT-systemen aan te vallen. Deze aanpak maakt het mogelijk om detectiemechanismen te testen en te verbeteren.

Uit de eerste onderzoeksfase bleek dat bestaande malwarevarianten onvoldoende effectief waren. Daarom is gekozen voor een herontwikkeling vanaf de basis. Belangrijke innovaties zijn:

- Het toepassen van ARP-spoofing voor Man-in-the-Middle-aanvallen (MiTM)
- De integratie van protocol parsing en replay-functionaliteiten voor de Modbus- en Siemens S7-protocollen
- Verbeteringen in de stealth-eigenschappen van de malware

De ontwikkelde tool bleek in labomgevingen in staat controleverlies en zichtverlies in OT-systemen te veroorzaken, met verhoogde onzichtbaarheid. Usability-tests bevestigen bovendien dat de tool toegankelijk is voor junior security-specialisten.

Het gebruik van geavanceerde taalmodellen om een corpus van binaire exploitatie-uitdagingen te creëren, geschikt voor gebruik in het onderwijs

Vaardigheden op het gebied van offensieve security – zoals reverse engineering en software-exploitatie – zijn essentieel voor het veilig ontwikkelen van software. Studenten oefenen deze vaardigheden doorgaans met kwetsbare programma’s, maar wanneer deze programma’s eenmaal bekend zijn, circuleren oplossingen al snel online.
Dit project onderzoekt hoe geavanceerde taalmodellen kunnen worden ingezet om automatisch unieke binaire exploitatie-uitdagingen te genereren. Elk gegenereerd programma verschilt zodanig van het basisprogramma, dat elke student een eigen, unieke uitdaging krijgt.
Doel is het ontwikkelen van een werkend systeem dat op basis van vooraf gedefinieerde criteria automatisch nieuwe opdrachten genereert, specifiek gericht op gebruik in onderwijs.

Plannen voor 2025

In 2025 zet het lectoraat zich actief in voor de verdere ontwikkeling van offensieve securitytechnieken, met als doel de cyberweerbaarheid van systemen nog beter in kaart te brengen en te versterken. Denk hierbij aan het automatiseren van deze technieken of het optimaliseren ervan voor specifieke technologieën.

Enerzijds richt het onderzoek zich op de doorontwikkeling van de technieken zelf, anderzijds worden ze toegepast op diverse toepassingsgebieden, zoals infrastructuren voor de energietransitie, medische platformen en autonome systemen. Deze activiteiten vinden plaats binnen een breed scala aan samenwerkingen: van nationale en internationale onderzoeksprogramma’s tot partnerschappen binnen De Haagse Hogeschool. Daarbij blijft het lectoraat inzetten op labfaciliteiten, die essentieel zijn voor het testen en verbeteren van de cyberweerbaarheid van praktische systemen.

WAT WE DOEN

Risk Management & Cyber Security

Peter Roelofsma, lector Risk Management & Cyber Security

Peter Roelofsma is lector Risk Management & Cyber Security aan De Haagse Hogeschool. Hij is expert op het gebied van risicomanagement en cybersecurity, met ervaring in uiteenlopende domeinen zoals de gezondheidszorg, smart cities, luchtverkeersleiding, defensie, marine en risicobeheer in verkeerstunnels. Hij publiceerde over onderwerpen als organisatieleren, Shared Mental Models, Safe by Design, AI-coaching en robotica, en besluitvorming in commando- en controlecentra.

Peter promoveerde in cognitieve psychologie en ergonomie aan de Vrije Universiteit Amsterdam en heeft ruime onderwijs- en onderzoekservaring op het snijvlak van psychologie, sociale en culturele wetenschappen, AI en informatica. Voordat hij lector werd aan De Haagse Hogeschool, werkte Peter aan de Technische Universiteit Delft. Daar deed hij onderzoek naar Safety en Security Science binnen het Centrum voor Veiligheid in de Zorg en was hij modulemanager van het vak Health System Management.

“Cascade cyberrisico’s zijn niet alleen een technisch probleem, maar een maatschappelijke uitdaging. Door samen te werken en goed te communiceren, kunnen we veerkrachtige systemen creëren die bestand zijn tegen ernstige cyberdreigingen en de gevolgen van cyberaanvallen verkleinen.”

Wat doet het lectoraat Risk Management & Cyber Security?

Het lectoraat Risk Management & Cyber Security richt zich op de vraag: hoe kunnen organisaties cyberrisico’s effectief beheersen? Daarbij draait het om de besluitvorming rondom risicomanagement, de governance van cybersecurity binnen organisaties, en het voorkomen én beperken van schade door cyberaanvallen.

Onderzoekers ontwikkelen (AI-)modellen, tools en werkwijzen waarmee organisaties risico’s kunnen inschatten en beheersen, en analyseren hoe bedrijven en instellingen effectief reageren op incidenten. Ook de rol van overheid en publiek-private samenwerking is een belangrijk aandachtspunt: hoe versterken we samen de digitale weerbaarheid?

Het onderzoek binnen het lectoraat richt zich op drie hoofdthema’s:

- **Shared risk management**
- **Security operation centers**
- **Adaptieve learning community**

Samenwerking met onderwijs

- Faculteit IT & Design: HBO-ICT
- Faculteit Bestuur, Recht & Veiligheid: Integrale Veiligheidskunde, LAW en Safety and Security Management Studies

Uitgelichte projecten

RISKMATE: AI-Coach voor cybersecurity risicomanagement - *for the SOC of the future*

In dit project ontwikkelen we een proof-of-concept (PoC) van RISKMATE: een spraakgestuurde AI-coach die individuen en organisaties ondersteunt bij het omgaan met cybersecurity-uitdagingen. De coach werkt via empathische, real-time gesprekken en past zich aan op basis van zowel emotionele als informatieve behoeften van de gebruiker. De ontwikkeling van RISKMATE bestaat uit meerdere stappen:

- Literatuuronderzoek en een diepgaande analyse van publicaties van het European Union Agency for Cybersecurity (ENISA), waarbij we onder andere kijken naar sentiment en stress-veroorzakende taal.
- De bouw van een PoC AI-coach die gebruikmaakt van de nieuwe OpenAI Realtime API. Deze technologie maakt vloeiende spraakinteractie mogelijk met instelbare toon, spreektempo en onderbrekingsmogelijkheden.
- Integratie van kennis uit de Risk Management Roadmap (RMR) van het Nationaal Cyber Security Centrum (NCSC).
- Toepassing van inzichten uit de cognitieve psychologie, vertaald naar een gedeeld mentaal model binnen cybersecurityteams.

- **Gefinancierd door:** ITVZH en seed funding
- **In samenwerking met:** mboRijnland, Pinewood, Infinity IT, SURF, Cyberweerbaar NL, TAPS BV, Allianz, het Human Factor Lab, TAPAEMEA, DataFiber, Audit and Risk Solutions, en andere partners in de Dutch Innovation Community

Cyber Security Living Lab (CSyLL)

Sinds 2023 is het Cyber Security Living Lab gevestigd in de Dutch Innovation Factory in Zoetermeer. De officiële opening vond plaats in november 2024. Het lab biedt een experimentele werkomgeving voor innovatie in cybersecurity risk management, gebaseerd op de Living Lab-methodologie.

Het Cyber Security Living Lab is een experimentele werk-, leer- en onderzoeksomgeving en slaat de brug tussen onderwijs, onderzoek en en praktijk. Studenten doen hier waardevolle praktijkervaring op en bedrijven krijgen ondersteuning bij het beheersen van hun cybersecurityrisico’s. Tegelijkertijd draagt het lab bij aan de vernieuwing van het cybersecurityonderwijs én de professionele praktijk. Een belangrijk speerpunt is de ontwikkeling van een eigen Security Operations Center (SOC/SIEM), gericht op dreigingsmonitoring, incidentrespons en gedeeld risicobeheer (shared risk management). Het Cyber Security Living Lab stimuleert kennisuitwisseling tussen wetenschappelijk onderzoek, het bedrijfsleven, overheden en de samenleving. Deze samenwerking leidt tot vernieuwende oplossingen voor actuele en toekomstige cyberbeveiligingsvraagstukken. CSyLL is een initiatief van De Haagse Hogeschool en komt tot stand in nauwe samenwerking met partners uit het onderwijs, onderzoek en de praktijk. Samen bouwen zij aan een betrokken gemeenschap van studenten, docenten en professionals die zich inzet voor een weerbare digitale samenleving.

- **Gefinancierd door:** IT Verband Zuid-Holland
- **In samenwerking met:** mboRijnland, Infinity IT, Cyberweerbaar NL, TAPS BV, Allianz, het Human Factor Lab, TAPAEMEA, DataFiber, Audit and Risk Solutions, en andere partners in de Dutch Innovation Community

Plannen voor 2025

In 2025 breiden we ons onderzoeksteam verder uit met twee nieuwe PhD-trajecten. Voor deze trajecten werven we actief fondsen. In september start het eerste PhD-project binnen de bredere onderzoekslijn over Usability & Security, met als doel: toegankelijke authenticatieoplossingen in e-Health-toepassingen. We blijven bovendien werken aan het versterken van het internationale profiel van het lectoraat. Dat doen we via open science, peer reviewed publicaties en deelname aan internationale conferenties. Het Cyber Security Living Lab krijgt een stevigere positie als kennisplatform voor cyber risk management en cascade cyberrisico’s. Vanuit het lab organiseren we daarom ieder kwartaal wetenschappelijke congressen en workshops. Ook in 2025 blijft de focus onverminderd liggen op het versterken van de verbinding tussen onderwijs, onderzoek, samenleving en industrie. Op het Dutch Innovation Park bouwen we de co-creatie met partners verder uit. Zo rollen we het Shared SOC–SIEM testbed verder uit met studenten, en ontwikkelen we samen met partners een simulator voor cascade cyber risico’s.

PHD PROJECTEN

In 2024 werken zes promovendi binnen het Centre of Expertise Cyber Security aan hun proefschrift. Zij zijn verbonden aan verschillende universiteiten en doen onderzoek naar urgente thema's binnen cybersecurity, zoals hacktivisme, ransomware en geldezels. Hun werk draagt bij aan nieuwe inzichten én aan praktische oplossingen voor de cyberweerbaarheid van onze samenleving.

Hacktivism: honourable cause or serious threat?

Wat drijft mensen om zich aan te sluiten bij hacktivistische groepen? Waarom kiezen zij voor hacken als protestvorm? En hoe zijn deze groepen georganiseerd? Dit onderzoek combineert inzichten uit de sociale psychologie en criminologie om de dynamiek en motivatie van hacktivisten te doorgronden.

- **Promovendus:** Marco Romagna
- **Betrokken universiteit:** Universiteit Leiden

Recruiting money mules: The online and offline involvement mechanisms of cybercrime

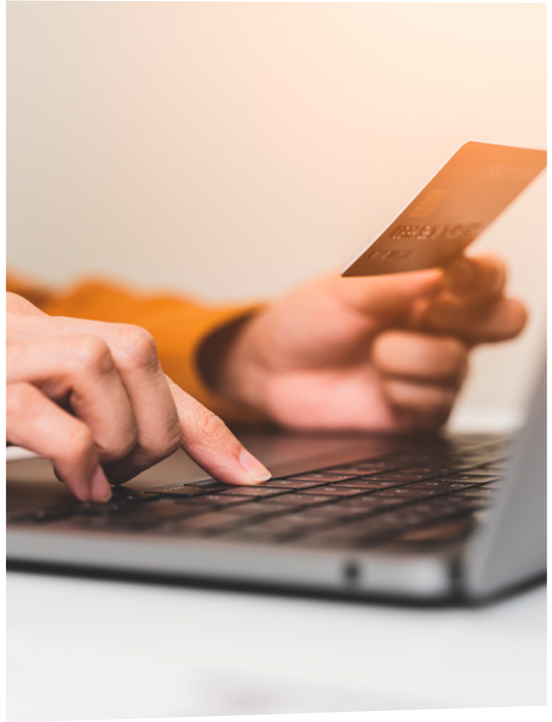
Geldezels spelen een belangrijke rol in financiële cybercriminaliteit. Ze helpen criminele netwerken door illegaal geld over te maken, vaak zonder precies te weten wat ze doen. Dit onderzoek brengt in kaart hoe criminelen hen werven – zowel online als offline – en welke mechanismen hierbij een rol spelen. Interviews en data-analyses geven inzicht in hoe betrokkenheid ontstaat, met als doel effectievere preventie en opsporing.

- **Promovendus:** Luuk Bekkers
- **Betrokken universiteit:** Vrije Universiteit Amsterdam

Nature and prevention of ransomware

Hoe ontstaan ransomware-aanvallen, welke factoren bepalen het succes ervan, en hoe reageren slachtoffers? Dit onderzoek biedt inzicht in het gedrag van daders en slachtoffers en vormt de basis voor interventies om ransomware effectiever tegen te gaan.

- **Promovenda:** Sifra Matthijsse
- **Betrokken universiteit:** Universiteit Leiden



Involvement mechanisms for financial-economic cyber-enabled crime, and prevention strategies against it

Waarom en hoe raken mensen betrokken bij financieel-economische cybercriminaliteit, zoals phishing? Dit project onderzoekt risicofactoren en betrokkenheidsmechanismen én ontwikkelt een interventie om deze processen te verstoren.

- **Promovendus:** Joeri Loggen
- **Betrokken universiteit:** Universiteit Leiden

Ethics of care as a corporate governance model

In dit project wordt een corporate governance-model ontwikkeld dat de implementatie van security by design bevordert. Het model biedt een bredere kijk op cybersecurity, waarbij sociale aspecten centraal staan. Door zorgethiek te combineren met de stakeholdertheorie, legt het model de nadruk op het belang van relaties, empowerment en de zorgplicht.

- **Promovenda:** Jasmijn Boeken
- **Betrokken universiteit:** Universiteit Leiden

Alternative interventions for online fraud: Future implications

Dit onderzoek bekijkt een alternatieve benadering voor het afhandelen van online fraude. Centraal staat de mogelijkheid voor slachtoffers om schade te verhalen op begunstigde rekeninghouders via civiel recht. Het project onderzoekt de impact van deze aanpak op slachtoffers, daders en de maatschappij.

- **Promovenda:** Merel van Leuken

In december 2024 is een nieuwe PhD-aanvraag gehonoreerd met een NWO-subsidie. Dankzij deze toekenning kan de promovendus in 2025 starten met zijn promotietraject:

Safe care for everyone: easing the authentication burden in the home use of eHealth solutions

Voor kwetsbare gebruikers, zoals ouderen, kan digitale zorg lastig toegankelijk zijn door ingewikkelde authenticatie-procedures. Dit project onderzoekt hoe deze processen gebruiksvriendelijker én veiliger kunnen worden ingericht, met oog voor privacy én inclusie.

- Promovendus: Niek Jan van den Hout
- Betrokken universiteit: Radboud Universiteit

PhD-Day 2024

Op 25 maart vond de jaarlijkse Cyber PhD-dag plaats in de Dutch Innovation Factory (DIF) in Zoetermeer. Voor het eerst werd dit evenement georganiseerd door Cyberweerbaar NL, een landelijk consortium van De Haagse Hogeschool, Hogeschool Saxion en NHL Stenden Hogeschool. Tijdens de dag presenteerden promovendi van de drie hogescholen hun onderzoek. Ze gingen in gesprek met collega-onderzoekers en experts op het gebied van cybersecurity en cybercrime. Het evenement bood volop gelegenheid voor kennisuitwisseling, netwerkvorming en het versterken van de samenwerking binnen het groeiende onderzoeksveld van digitale weerbaarheid.

ONS TEAM

De onderzoekers en het programmateam vormen samen de kern van het Centre of Expertise Cyber Security. Op onze website lees je meer over hun werk en drijfveren.

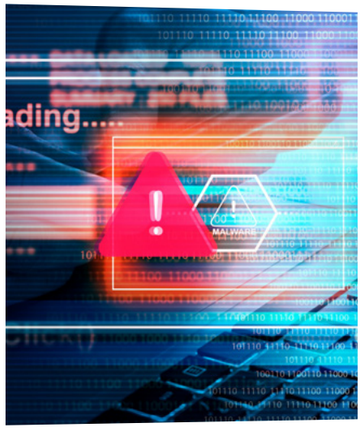
Expertisenetwerk Cyberweerbaar NL

Het aantal cyberaanvallen blijft toenemen, terwijl de digitale weerbaarheid van organisaties achterblijft. Cyberweerbaar NL streeft ernaar publieke en private organisaties beter te wapenen tegen cyberdreigingen, met een directe impact op de dagelijkse praktijk. Cyberweerbaar NL ging in 2023 van start als consortium van drie hogescholen: De Haagse Hogeschool (penvoerder vanuit het Centre of Expertise Cyber Security), Hogeschool Saxion en NHL Stenden Hogeschool. In 2024 sloot ook Avans Hogeschool zich aan. Samen met studenten, docenten, cyberprofessionals, onderzoekers en een groot aantal netwerkpartners werkt Cyberweerbaar NL aan nieuwe kennis over cybersecurity binnen organisaties. De nadruk ligt op het menselijk aspect: gedrag en houding als sleutels tot effectieve cyberweerbaarheid. Het consortium onderzoekt welke gedrags- en houdingsaspecten cyberweerbaarheid beïnvloeden en hoe organisaties deze kunnen verbeteren.

Met de vier betrokken hogescholen is landelijke dekking gerealiseerd. Tijdens evenementen en in gesprekken tussen lectoren en regionale en landelijke organisaties ontstaan waardevolle onderzoeksvragen. Deze ideeën worden vervolgens empirisch onderzocht, zodat hun effectiviteit in de praktijk kan worden vastgesteld. Elke hogeschool brengt daarbij eigen expertise en unieke onderzoeksperspectieven in.

In september 2024 organiseerde Cyberweerbaar NL, samen met het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV), het jaarlijkse event onder de titel Krachten bundelen voor cyberweerbaarheid. Tijdens deze bijeenkomst, die in het teken stond van de lokale aanpak van online criminaliteit, werd de gezamenlijke onderzoeksagenda gepresenteerd: Naar een cyberweerbaar Nederland. In deze agenda staan vier thema's centraal die de komende jaren prioriteit krijgen binnen het netwerk: mensgerichte cyberweerbaarheid, digitaal vakmanschap, slachtofferschap en online criminaliteit en daderschap.

- **Gefinancierd door:** Regieorgaan SIA (SPRONG)
- **In samenwerking met:** Hogeschool Saxion, NHL Stenden, Avans Hogeschool en 25 praktijkpartners



Ontwikkeling van OT-malware in cyberresiliente infrastructuren voor onderwijs en onderzoek

Offensieve securityvaardigheden, zoals het ontwikkelen van malware, zijn essentieel om cyberweerbare infrastructuren beter te kunnen beveiligen. Deze systemen – vaak een combinatie van IT-, OT- en IoT-componenten – worden gebruikt in productieomgevingen en kritieke infrastructuren. Door het ontwerpen van offensieve tools ontstaat inzicht in kwetsbaarheden en mogelijke verdedigingsstrategieën. Binnen dit project is een vorm van OT-malware ontwikkeld die in een laboratoriumsetting wordt ingezet als gesimuleerde cyberdreiging. Studenten leren deze dreiging te herkennen en neutraliseren tijdens praktijkopdrachten, waarmee zij waardevolle ervaring opdoen in het beveiligen van complexe systemen.

- **Lectoraat:** Network & Systems Engineering Cyber Security

Hacking Impulse

Onze maatschappij is in hoge mate afhankelijk van digitale systemen. Offensieve securitymethoden maken het mogelijk om kwetsbaarheden vroegtijdig te identificeren en zo misbruik te voorkomen. Dit projectvoorstel is een eerste stap in de uitbreiding en verdieping van technische offensieve securityactiviteiten binnen het onderwijs, toegepast onderzoek en de praktijk. Doel is om binnen 4 tot 6 maanden de volgende resultaten te realiseren:

- Een eerste serie onderzoeken en toepassingen op het gebied van vulnerability analyses, innovatieve pentesten en OT-malware
- Inzet van resultaten in dienstverlening aan mkb en overheden
- Fundament leggen voor de ontwikkeling van een post-masteropleiding in offensieve security
- Verdieping van kennis voor toekomstige onderzoeksprogramma's

De uitvoering start met het aantrekken van een geschikte student-assistent die betrokken wordt bij de eerste projectfase. Door studenten en professionals op te leiden in vernieuwende offensieve securityvaardigheden, dragen we bij aan een verhoogde digitale weerbaarheid van systemen en het beperken van misbruik.

- **Lectoraat:** Network & Systems Engineering Cyber Security

Testen en oefenen van informatiebeveiliging bij decentrale overheden

Testen en oefenen zijn cruciaal voor het verbeteren van informatiebeveiliging. Ze helpen organisaties inzicht te krijgen in kwetsbaarheden binnen hun IT-systemen en processen. In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzochten ICTU en De Haagse Hogeschool hoe gemeenten, provincies en waterschappen hiermee omgaan, en waar zij tegenaan lopen. Op basis van de bevindingen zijn aanbevelingen opgesteld om het testen en oefenen binnen deze overheden te stimuleren.

- **Lectoraat:** Cyber Security & Safety
- **Gefinancierd door:** Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
- **In samenwerking met:** ICTU

The Detectable Vegetable

In het project The Detectable Vegetable werken hogescholen, kennisinstellingen en bedrijven samen aan het ontwikkelen van sensortechnologie en data-analyse om ziektes en bederf in tuinbouwgewassen vroegtijdig te detecteren. Door gebruik te maken van optische sensoren en AI, worden ziekten en afwijkingen in een vroeg stadium zichtbaar. Het lectoraat Cybersecurity & Safety onderzoekt hoe deze technologie veilig kan worden geïntegreerd in digitale infrastructuren.

- **Lectoraat:** Cyber Security & Safety
- **Gefinancierd door:** Regieorgaan SIA vanuit het RAAK-PRO programma
- **In samenwerking met:** HAS Hogeschool, WUR, TU Delft, Mythronics, Gearbox, perClass, Hudson Cybertec, 2Harvest, Vertigo, Greenport WH, CombiVliet, Reijm&Zn, Tomatoworld en Innovation Quarter

(On)veilig gedrag met digitale mobiele media

In dit onderzoek is een nieuw gedragsmodel ontwikkeld om menselijk gedrag rondom cybersecurity beter te begrijpen en meten. De focus lag op het gebruik van mobiele apparaten zoals smartphones en laptops. Resultaten laten zien dat niet alleen kennisgebrek, maar ook denkfouten en houding bijdragen aan onveilig gedrag. Dit inzicht helpt bij het ontwerpen van effectievere interventies.

- **Lectoraat:** Cyber Security & Safety

Digitale veiligheid in de Greenport West-Holland

Bedrijven in de Greenport West-Holland maken steeds meer gebruik van digitale technologieën. Dat brengt nieuwe risico's met zich mee. Dit project onderzoekt hoe digitaal weerbaar deze bedrijven zijn en hoe dat kan worden versterkt.

- **Lectoraat:** Cyber Security & Safety
- **Gefinancierd door:** Provincie Zuid-Holland, SIA/RAAK PRO
- **In samenwerking met:** kenniscentrum Digital Operations & Finance, Provincie ZH, Greenport WH, HAS, TU Delft, WUR, Tomatoworld, Hudson Cybertec

Verbeteren van veilig digitaal gedrag

Om cybersecuritybewustzijn effectief te verbeteren, is eerst inzicht nodig in het huidige gedrag. In dit project is een meetinstrument ontwikkeld waarmee digitale veiligheid binnen verschillende doelgroepen kan worden gemeten.

- **Lectoraat:** Cyber Security & Safety

Cyberveiligheid in de medische zorg

Digitalisering van medische technologie brengt nieuwe cybersecurityrisico's met zich mee. Dit onderzoek brengt risico's in kaart en kijkt naar maatregelen voor veilige toepassing van medische technologie, zowel technisch als organisatorisch.

- **Lectoraat:** Cyber Security & Safety
- **In samenwerking met:** Hogeschool Leiden, TNO, LUMC, HMC

Qualification of Information Security

In de huidige informatiemaatschappij wordt het beschermen van informatie steeds belangrijker, maar ook moeilijker. Daarom zijn goed opgeleide en ervaren professionals essentieel. Er is een groeiende behoefte aan een uniform en internationaal erkend kwalificatiesysteem voor cybersecurityprofessionals. Dit project ontwikkelt zo'n systeem, op basis van bestaande behoeften en best practices.

- **Lectoraat:** Cyber Security & Safety
- **In samenwerking met:** PvIB, NCSC

Learning & Innovating Ahead of the Threat (LIAT)

Om een veilig land te blijven, moeten de toenemende dreigingen op het gebied van cyberveiligheid proactief worden aangepakt. Daarvoor zijn effectieve samenwerkingen binnen en tussen organisaties nodig – zogeheten leergemeenschappen – waarin publieke en private partijen én kennisinstellingen samenwerken. Tot nu toe lag de focus binnen deze leergemeenschappen vooral op kennisdeling, en minder op het daadwerkelijk ontwikkelen en implementeren van innovatieve veiligheidsoplossingen. In dit project helpen we leergemeenschappen om juist die volgende stap te zetten. We ontwikkelen ontwerprichtlijnen, strategieën, methoden én een ondersteuningsplatform om effectieve leergemeenschappen op het gebied van cybersecurity op te zetten en te versterken.

- **Lectoraat:** Risk Management & Cyber Security
- **Gefinancierd door:** NWO
- **In samenwerking met:** Saxion Hogeschool, Universiteit Twente, HSD

Cybersecurity in de keten

In dit project bundelen De Haagse Hogeschool en het platform Samen Digitaal Veilig (SDV) hun krachten om de digitale veiligheid van mkb-organisaties in Nederland te versterken. Er wordt in kaart gebracht hoe SDV kan bijdragen aan het verbeteren van de cyberweerbaarheid van bedrijfsketens. Onderzocht wordt hoe bedrijven gestimuleerd kunnen worden om cyberweerbaar gedrag te vertonen en welk effect het SDV-platform heeft op gedrag van ondernemers met betrekking tot cybersecurity.

- **Lectoraat:** Risk Management & Cyber Security
- **Gefinancierd door:** Samen Digitaal Veilig, een initiatief van MKB-Nederland en VNO-NCW
- **In samenwerking met:** Samen Digitaal Veilig

Cyber Security by Integrated Design (C-SIDE)

C-SIDE ontwikkelt een methodologie voor veilige softwareontwikkeling waarin zowel technische als niet-technische factoren worden meegenomen. Denk aan menselijk gedrag, teamstructuren, veiligheidscultuur en governance. Doel is een integrale benadering van Security-by-Design.

- **Lectoraat:** Risk Management & Cyber Security
- **Gefinancierd door:** NWA Cybersecurity
- **In samenwerking met:** Universiteit Leiden

Cyber Security simulatielab

In het Cyber Security simulatielab werken studenten, docenten en onderzoekers aan het ontwikkelen van geavanceerde AI-modellen die worden ingezet om alledaagse cyber security scenario's na te bootsen. Deze simulaties ondersteunen organisaties bij het nemen van weloverwogen beslissingen over cyber security en risicobeheer. Het lab is een samenwerking tussen het lectoraat Risk Management & Cyber Security en de faculteit Bestuur, Recht & Veiligheid van De Haagse Hogeschool, waarbij studenten van de opleidingen Integrale Veiligheidskunde en SSMS betrokken zijn. Daarnaast werken we in het lab samen met studenten en onderzoekers van de Vrije Universiteit Amsterdam. In 2023 bereidden we een minor voor waarin studenten leren hoe scenario's gemodelleerd kunnen worden in een speciale software-omgeving, waarbij ze kennismaken met het vakgebied van cybersecurity en het werken met complexe AI-modellen. De minor startte in februari 2024.

- **Lectoraat:** Risk Management & Cyber Security
- **In samenwerking met:** Vrije Universiteit Amsterdam

MKB Cyberproject 'Versterken cyberweerbaarheid van ketens'

Bedrijven maken deel uit van ketens van leveranciers, afnemers en dienstverleners, die steeds afhankelijker worden van ICT. Hierdoor nemen de cyberrisico's binnen die ketens toe. Eerder onderzoek naar ketenweerbaarheid liet zien dat een concrete blauwdruk essentieel is bij het aangaan van nieuwe samenwerkingen. Dit project bouwt daarop voort. We onderzoeken eerst bestaande, al geïdentificeerde risico's binnen ketens, en breiden de opgedane kennis uit eerdere sectorstudies (agrarisch, sierteelt en handel) uit naar andere sectoren. Het doel is om via verdiepend fenomeenonderzoek beter inzicht te krijgen in ketenweerbaarheid. Daarnaast ontwikkelen we een sectoroverstijgende blauwdruk, met speciale aandacht voor de rol van het mkb in het versterken van die weerbaarheid.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** MKB-Nederland
- **In samenwerking met:** Cyberweerbaar NL, een samenwerking van De Haagse Hogeschool, Hogeschool Saxion, NHL Stenden Hogeschool

Ontwikkelen van een evidence-based interventie om slachtoffers van online fraude en ransomware te ondersteunen in hun online zoektocht naar hulp

Slachtoffers van cybercriminaliteit schamen zich vaak voor wat hen is overkomen en zijn bang voor reacties van de omgeving. Dit weerhoudt hen er vaak van aangifte te doen of melding te maken. Wel zoeken veel slachtoffers anoniem online naar hulp en advies. Zoekmachines zijn een laagdrempelige en veilige omgeving waar ze zonder oordeel antwoorden vinden op vragen als: 'Hoe krijg ik mijn geld terug na oplichting?' of 'Hoe verwijder ik ransomware?'. Dit onderzoek is gericht op slachtoffers van online fraude en ransomware, met tweeledig doel: het vroegtijdig signaleren van slachtofferschap en het ontwikkelen van een interventie die hen ondersteunt bij het vinden van hulp.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Stichting Achmea Slachtoffer en Samenleving (SASS)
- **In samenwerking met:** Slachtofferhulp Nederland, Politie Nederland, Cyberweerbaar NL

What (s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenscan als evidence based gedragsinterventie

Om ondernemers te stimuleren hun cyberweerbaarheid te vergroten, is in dit project een interventie ontwikkeld waarbij bijna 2.000 bedrijven zijn geanalyseerd op drie basisprincipes van veilig digitaal ondernemen: het in kaart brengen van kwetsbaarheden, het uitvoeren van updates en het voorkomen van malware. Na een eerste kwetsbaarhedenscan ontvingen de deelnemende bedrijven een op maat gemaakt adviesrapport. Daarbij werd gevarieerd in de vorm van risicocommunicatie: sociale norm, geanticipeerde spijt of geen risicocommunicatie. Bedrijven die de boodschap met geanticipeerde spijt ontvingen, bleken significant vaker maatregelen te hebben genomen om hun cyberweerbaarheid te verbeteren. Op basis van deze resultaten en de geleerde lessen wordt de interventie doorontwikkeld.

- **Lectoraat:** Cybercrime & Cybersecurity
- **Gefinancierd door:** CCV (Versterken lokale cyberweerbaarheid)
- **In samenwerking met:** Threadstone en PVO Den Haag

Criminele jeugdnetwerken in een digitaliserende samenleving

Dit onderzoek biedt lokale veiligheidspartners concrete handvatten om gezamenlijk zicht te krijgen op cybercriminele jeugdnetwerken en om deze integraal aan te pakken. Een belangrijke deelconclusie is dat professionals in de praktijk momenteel nauwelijks zicht hebben op deze netwerken. Dit komt vooral doordat de informatievoorziening sterk leunt op straatinformatie, terwijl jongeren die betrokken zijn bij cybercrime zich juist buiten het straatbeeld bevinden. De netwerken ontstaan en groeien veelal via offline sociale relaties (zoals vrienden en familie) én via online contacten, bijvoorbeeld op platforms als Telegram. Bovendien is er vaak sprake van verwevenheid tussen traditionele criminaliteit en cybercriminaliteit, wat de aanpak complexer maakt.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van/gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR, RIEC Noord-Nederland, Vereniging COIN, de Nederlandse Vereniging van Banken, OM, Politie en gemeenten Leeuwarden, Groningen en Smallingerland

Jong ICT-talent op het rechte pad houden: effectevaluatie

Jongeren verkennen online vaak grenzen van wat toegestaan is. Met de toenemende digitalisering is het belangrijk hen positieve alternatieven te bieden. Dit project is een preventieve interventie gericht op jongeren met affiniteit voor IT die geneigd zijn grenzen online op te zoeken. Het doel is om hen te motiveren hun IT-talenten binnen wettelijke grenzen te benutten. De interventie bestaat uit één dag waarop jongeren sessies bijwonen met professionals van de politie, de cybersecurity- en game-industrie. Er is een apart programma voor ouders en docenten om meer inzicht te krijgen in de online leefwereld van de jongeren. In 2024 is gestart met de effectevaluatie van deze interventie.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Politie Nederland

Criminele netwerken achter geldezels

Dit onderzoek brengt de aard van de criminele netwerken achter geldezeldelicten in kaart, om zo concrete aangrijpingspunten te identificeren voor preventie, verstoring en opsporing van deze criminele netwerken. Hiermee kan worden voorzien in de behoefte aan een effectieve, integrale aanpak van zowel cybercrime als gedigitaliseerde criminaliteit.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Politie

Factoren die bijdragen aan onderhandelen, betalen en melden door slachtoffers van ransomware

Ransomware is momenteel een van de grootste online dreigingen. Toch is er nog weinig bekend over de omvang van slachtofferschap onder burgers en ondernemers, en over hoe zij reageren op een aanval. Dit project onderzoekt hoe vaak Nederlandse burgers en bedrijven slachtoffer worden van ransomware, hoe zij omgaan met de situatie—onder meer door te onderhandelen, losgeld te betalen of het incident te melden—en in hoeverre hun gedrag aansluit bij de adviezen van politie en IT-/cybersecuritybedrijven.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van/gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR

Jonge aanwas van cybercriminaliteit voorkomen: het verstoren van cybercrime-as-a-service (CaaS) markten

Dit onderzoek richt zich op het vergroten van kennis over de instroom van jonge daders in de wereld van cybercrime. Centraal staat de rol van Cybercrime-as-a-Service (CaaS) als mechanisme dat online betrokkenheid faciliteert. Daarnaast onderzoekt het project hoe CaaS-structuren benut kunnen worden om gerichte interventies te ontwikkelen voor potentiële of beginnende cybercriminelen.

- **Lectoraat:** Cybercrime & Cybersecurity
- **Gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR, TU Eindhoven, Politie COPS, Nationale Politie

Hybridisering van criminaliteit

Dit onderzoek brengt de verwevenheid tussen online en offline criminaliteit in kaart. Centraal staat de analyse van dadernetwerken die zowel digitale als fysieke componenten kennen, en van delicten waarbij beide werelden samenkomen in de modus operandi. Op basis van literatuuronderzoek en een media-analyse van relevante casussen wordt een typologie ontwikkeld van hybride criminaliteit. Daarnaast biedt het onderzoek inzicht in de wijze waarop hybride criminaliteit wordt aangepakt in Nederland en andere Europese landen. Interviews met politiefunctionarissen en experts maken het mogelijk om benaderingen, best practices en knelpunten in kaart te brengen. Het doel is om lessen en effectieve aanpakken te identificeren en te delen met de Nederlandse (politie)praktijk.

- **Lectoraat:** Cybercrime & Cybersecurity
- **Gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** Erasmus Universiteit Rotterdam

Expeditie Lokaal Digitaal: Intensivering lokale aanpak gedigitaliseerde criminaliteit

Dit project richt zich op het ontwikkelen van een effectieve interventie die basisteams van de politie in staat stelt om gedigitaliseerde criminaliteit op lokaal niveau zelfverzekerd en doeltreffend aan te pakken. Het onderzoek wordt uitgevoerd in samenwerking met basisteams van de politie-eenheden Noord- en Oost-Nederland, het Digitaal Platform Drenthe en het cybercrimeteam van de eenheid Oost-Nederland. De centrale onderzoeksvraag luidt: hoe kunnen basisteams hun personeel voorbereiden op een effectieve en zelfverzekerde intensivering van de lokale aanpak van gedigitaliseerde criminaliteit? Het project levert praktische handvatten op waarmee basisteams hun medewerkers beter kunnen toerusten om de digitale dimensie van criminaliteit lokaal het hoofd te bieden.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Politie & Wetenschap
- **In samenwerking met:** Hogeschool Saxion

Cybercriminaliteit: van wetenschappelijk onderzoek naar praktische aanpakken

Het doel van dit onderzoek is om bestaande wetenschappelijke kennis over daders, slachtoffers, crimescripts en effectieve aanpakken van cybercriminaliteit op een overzichtelijke en toegankelijke manier in kaart te brengen. Samen met ervaren politiemedewerkers vertalen we deze inzichten vervolgens naar praktische handvatten voor de bestrijding van zowel gedigitaliseerde criminaliteit (cyber-enabled crime) als cybercrime (cyber-dependent crime).

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Nationale Politie – project Centurion
- **In samenwerking met:** Hogeschool Saxion en NSCR

Cybercriminaliteit op Telegram

Telegram herbergt veel openbare groepen waarin illegale producten en diensten worden verhandeld. Het platform biedt daarmee toegang tot cruciale componenten voor cybercriminaliteit, zoals geldezels en kant-en-klare phishingkits. Het doel van dit project is om meer inzicht te krijgen in de cybercriminele activiteiten op Telegram. Hiervoor maken we gebruik van unieke data: gedurende een jaar hebben we alle content verzameld uit 25 Nederlandse Telegram-groepen die zich richten op de handel in illegale producten en diensten, wat resulteerde in meer dan 4 miljoen berichten.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In samenwerking met:** NSCR en TNO

Stolen Datamarkets on Telegram

Dit project onderzoekt hoe markten voor gestolen data op Telegram functioneren en hoe ze verstoord kunnen worden. In het eerste deel van het project beschrijven we de werking van deze markten aan de hand van een crime script-analyse en stellen we situationele maatregelen voor om criminaliteit te voorkomen. In het tweede deel richten we ons op het identificeren van de factoren die de populariteit van deze markten beïnvloeden, met als doel potentiële interventiepunten te bepalen.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In samenwerking met:** NSCR

Online Ads Against Cybercrime

Dit project onderzoekt hoe online advertenties kunnen worden ingezet om de toegang tot cybercriminaliteit op instapniveau te blokkeren. We richtten ons op het gebruik van advertenties om potentiële cybercriminelen af te schrikken en hen te begeleiden naar pro-sociale alternatieven binnen de cybersecurity.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van/gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR, Politie COPS en Nationale Politie

Procesevaluatie Citydeal 'Lokale Weerbaarheid Cybercrime' – deel 2

Sinds 2020 zijn er in het kader van de City Deal Lokale Weerbaarheid Cybercrime tientallen innovatieve cyberprojecten op lokaal niveau gestart, met als doel de cyberweerbaarheid van zowel inwoners als ondernemers te versterken. Het werken op basis van 'evidence-based' principes is essentieel voor het verkrijgen van draagvlak bij de implementatie en voor (vervolg)financiering. In dit project werd daarom de tweede tranche van de City Deal-projecten geëvalueerd, met focus op het proces en de potentiële werkzame elementen. De bevindingen uit deze evaluatie bieden waardevolle lessen voor toekomstige cyberprojecten.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** CCV (Citydeal Lokale Weerbaarheid Cybercrime)
- **In samenwerking met:** Hogeschool Saxion, NHL Stenden Hogeschool

Human Factor in Cyber Security Lab

Hoe gedragen medewerkers van bedrijven zich echt in termen van veiligheid, wat veroorzaakt onveilig gedrag en hoe kunnen we veilig online gedrag bevorderen? Deze vragen staan centraal in het Human Factor in Cyber Security Lab. Het lab is een plek voor exploratief, praktijkgericht onderzoek met een sterke verbinding tussen onderwijs en de praktijk. Onderzoekers, professionals en studenten werken samen om praktische oplossingen voor onveilig online gedrag te ontwikkelen. De kracht van het lab schuilt in de nauwe samenwerking tussen onderzoek, onderwijs en de praktijk. Ook in 2024 kregen studenten de mogelijkheid om stage te lopen, wetenschappelijk onderzoek te gebruiken om interventies te ontwikkelen en te testen, en applicaties of programma's te bouwen die veilig online gedrag bevorderen.

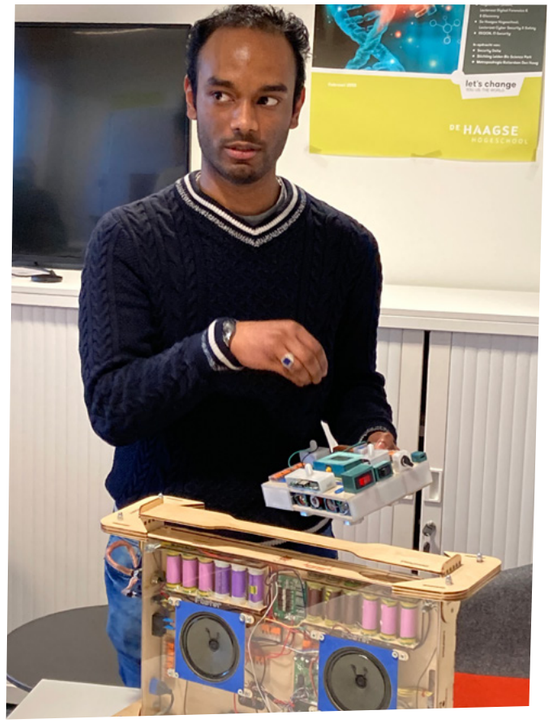
- **Lectoraat:** Cybercrime & Cybersecurity
- **In samenwerking met:** Tellick, Dutch Innovation Factory

Het onderzoek binnen het Centre of Expertise Cyber Security richt zich op drie kernthema's: mens, organisatie en techniek. Daardoor is een onderzoeksstage bij ons Centre of Expertise interessant voor studenten van uiteenlopende studierichtingen.

Elk semester bieden we via onze stagebrochure een actueel overzicht van beschikbare (afstudeer)stageplekken. Ook in 2024 vonden veel studenten via deze route een uitdagende stage bij een van onze lectoraten.

Tijdens hun stage zijn studenten volwaardig lid van een onderzoeksteam. Onder begeleiding van een ervaren onderzoeker werken zij aan een actuele onderzoeksvraag. Ze leren hoe ze die vraag systematisch kunnen beantwoorden – niet alleen door literatuuronderzoek, maar ook via bijvoorbeeld experimenten, interviews of praktijkonderzoek. In sommige projecten ontwikkelen studenten een concrete tool of oplossing, zoals een app of een bewustwordingscampagne, die organisaties kunnen inzetten om hun cyberweerbaarheid te versterken.

Ervaringen van studenten



Rachad Dhonre, *stagiair bij het lectoraat Network & Systems Engineering Cyber Security:*
"Tijdens mijn stage leerde ik hoe ik kwantitatieve (experimenten) en kwalitatieve (interviews) onderzoeksmethoden effectief kan combineren. Dankzij de wekelijkse feedbacksessies met mijn begeleider kreeg ik inzicht in de technische aspecten van mijn opdracht. Ook andere lectoraten van het Centre of Expertise Cyber Security hielpen me met inhoudelijke feedback op mijn paper. Mijn stage bij het Centre of Expertise was enorm leerzaam. Ik heb zowel binnen als buiten het Centre veel verschillende mensen leren kennen. Onderzoek doen wordt soms als eenzaam ervaren, maar dankzij het team van Cyber Security heb ik dat geen moment zo gevoeld."

Stefan Wigt, *stagiair bij het lectoraat Cyber Security & Safety:*
"Tijdens mijn stage heb ik veel geleerd over operationele technologie (OT) en de beveiliging daarvan. Deze ervaring heeft mijn bewustwording sterk vergroot en zal zeker van waarde zijn wanneer ik na mijn studie aan de slag ga in de informatiebeveiliging. "

Naomi Cairo, *stagiaire bij het lectoraat Cybercrime & Cyber Security*
"Door de toenemende integratie van het internet in ons dagelijks leven zijn online criminele activiteiten, zoals oplichting, hacking en ransomware, niet langer voorbehouden aan experts. Fraude treft inmiddels zowel particulieren als bedrijven, in uiteenlopende vormen zoals online winkelfraude, identiteitsdiefstal en phishing. In Nederland wordt maar liefst één op de zes mensen slachtoffer van dit soort cybercrime.
Mijn onderzoek richtte zich op de factoren die invloed hebben op de beslissing van slachtoffers om een civiele procedure te starten om schade te verhalen. Voorafgaand aan mijn stage was dit onderwerp voor mij grotendeels onbekend, maar dankzij mijn tijd bij het Centre of Expertise Cyber Security heb ik er veel over geleerd. Tijdens wekelijkse overleggen en discussiesessies kon ik kennis uitwisselen met andere onderzoekers binnen het Centre of Expertise. Ik kijk terug op een leerzame stage die mij heeft geholpen te ontdekken of een toekomst in onderzoek bij mij past."

Quinten Ringenier, *student HBO-ICT en stagiair bij het lectoraat Cyber Security & Safety*
"Tijdens mijn stage deed ik onderzoek naar de cyberweerbaarheid van de operationele technologie (OT) binnen gemeenten en hoe deze versterkt kan worden met behulp van serious games en bewustwordingscampagnes. Ik analyseerde hoe awarenesscampagnes zijn opgebouwd en hoe houding en gedrag van mensen beïnvloed kunnen worden. Daarbij onderzocht ik welke gedragsfactoren van invloed zijn op de effectiviteit van scenario's. Om een goed beeld te krijgen van de huidige stand van zaken op het gebied van informatiebeveiliging, heb ik verschillende gemeenten geïnterviewd. Zo kon ik in kaart brengen waar nog verbeteringen mogelijk zijn. Het werd voor mij duidelijk hoe belangrijk het is om juist ook de beveiliging van OT-systemen serieus te nemen. Gedurende mijn stage heb ik mijn onderzoeksvaardigheden sterk ontwikkeld en meer inzicht gekregen in de werking en toepassingen van OT-systemen. Ik vond het interessant om te ontdekken dat er al veel initiatieven bestaan om bewustwording te vergroten, bijvoorbeeld via serious games en andere oefenscenario's. Mijn stage bij het CoECS was leerzaam en plezierig. Ik werd goed begeleid en had wekelijks overleg met mijn opdrachtgever, waarin we mijn voortgang bespraken en samen bepaalden wat de volgende stappen waren. Dat hielp mij om het overzicht te houden en zorgde voor een fijne werkstructuur."

HIGHLIGHTS 2024

JAN

Testen en oefenen ter bevordering van informatiebeveiliging

Testen en oefenen zijn belangrijke componenten van informatiebeveiliging. Ze zijn nodig om inzicht te krijgen in kwetsbaarheden in de ICT en de organisatie als geheel, en dragen bij aan het versterken van de effectiviteit van de informatiebeveiliging. In opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties onderzochten ICTU en De Haagse Hogeschool hoe gemeenten, provincies en waterschappen omgaan met het testen en oefenen van hun informatiebeveiliging en welke knelpunten zij daarbij ervaren.

FEB

Start Hague Hackers

Een doorlopende buitenschoolse activiteit voor studenten met interesse in offensive security. Deze activiteit staat open voor alle (oud-)studenten van De Haagse Hogeschool en partnerinstellingen.

MRT

Cyber PhD-dag

Op 25 maart vond de jaarlijkse Cyber PhD-dag plaats in het Dutch Innovation Park in Zoetermeer. Dit evenement bood PhD-kandidaten de kans om hun onderzoek te presenteren en te bespreken met collega-onderzoekers en andere experts op het gebied van cybercriminaliteit en cybersecurity. De dag bracht een diverse groep onderzoekers samen om hun bevindingen, uitdagingen en onderzoeksmethoden te delen en feedback te ontvangen.

APR

Bijeenkomst Cyberweerbaar NL en HSD over slachtofferschap

Op donderdag 18 april kwamen onderzoekers, kennispartners en professionals bijeen bij De Haagse Hogeschool voor een gezamenlijke bijeenkomst van Cyberweerbaar NL en Security Delta (HSD), waarbij het thema slachtofferschap centraal stond. Jildau Borwell deelde haar bevindingen uit een onderzoek naar de ervaringen van slachtoffers van cybercrime, terwijl Rutger Leukfeldt de laatste ontwikkelingen in praktijkgericht onderzoek naar cyberweerbaarheid presenteerde.

Start van het AI & Data Science Expert Team

In samenwerking met het Centre of ExpertiseDigital Operations & Finance ging vanuit het thema Digitale Toekomst het AI & Data Science Expert Team van start met vijf onderzoekers. Het Expert Team zet zich hogeschoolbreed in voor verantwoorde en effectieve implementatie van AI en Data Science in onderzoeks- en onderwijsprojecten.

JUN

Rutger Leukfeldt in PIT magazine

Hoe beschermen we ons beter tegen digitale criminelen? Cyberaanvallen op burgers, overheden en bedrijven nemen flink toe, maar onze weerbaarheid blijft achter. In plaats van te focussen op nieuwe technologie is het verstandig om aan de slag te gaan met ons eigen gedrag. Rutger Leukfeldt (lector Cybercrime & Cybersecurity bij De Haagse Hogeschool) en Remco Spithoven (lector Maatschappelijke Veiligheid bij Hogeschool Saxion) bespreken dit in een gezamenlijk interview in PIT magazine van Nationaal Regieorgaan Praktijkgericht Onderzoek SIA.

Digitale veiligheid van Nederlandse gemeenten

Van sluizen tot bruggen en verkeersinstallaties: Nederlandse gemeenten beheren een scala aan belangrijke technologieën die onze openbare ruimte draaiende houden. Maar hoe goed zijn deze systemen digitaal beveiligd? Een onderzoek, dat De Haagse Hogeschool uitvoerde in opdracht van de Vereniging van Nederlandse Gemeenten (VNG), werpt hier licht op.

JUL

Civielrechtelijke afdoening van online fraude

Online fraude treft veel Nederlanders: in 2023 werd meer dan 9 procent van de bevolking slachtoffer. De impact is groot, maar de kans op genoegdoening binnen het strafrecht is beperkt. Hierdoor overwegen steeds meer slachtoffers om via het civielrecht schade te verhalen. Om deze optie beter te begrijpen, is het lectoraat Cybercrime & Cybersecurity van De Haagse Hogeschool, samen met praktijkpartners, een onderzoeksproject gestart naar de civielrechtelijke afhandeling van online fraude. Onderzoekers Susanne van 't Hoff-de Goede en Merel van Leuken publiceerden twee deelrapporten van dit project.

Effectieve interventies ter versterking van de cyberweerbaarheid van ondernemers

Een groeiend aantal ondernemers in Nederland is zich bewust van de risico's van digitalisering en neemt maatregelen om hun cyberweerbaarheid te verbeteren. Desondanks loopt een aanzienlijk deel van de ondernemers nog achter op dit gebied, wat hen kwetsbaar maakt voor cybercriminaliteit. Om dit aan te pakken, voerde De Haagse Hogeschool onderzoek uit naar effectieve interventies om de cyberweerbaarheid van Nederlandse ondernemingen te vergroten. Centraal in dit onderzoek stond het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence based gedragsinterventie.

AUG

De Nationale Cybersecurity Summer School

De Nationale Cybersecurity Summer School (NCS3) is een intensieve cursus die bachelorstudenten en zij-instromers inzicht biedt in zowel de technische als de niet-technische aspecten van cybersecurity. Op de vierde dag van de Summer School verwelkomde De Haagse Hogeschool de deelnemers. Voor het eerst speelde een hogeschool een rol in de organisatie van dit evenement. Susanne van 't Hoff-de Goede, senior onderzoeker bij het Centre of Expertise Cyber Security sprak over slachtofferschap van cybercrime.

SEP

Bijeenkomst Krachten bundelen voor cyberweerbaarheid

Het jaarevent van Cyberweerbaar NL, dit jaar in samenwerking met het CCV georganiseerd, vond op 19 september plaats en richtte zich volledig op de nieuwste ontwikkelingen, onderzoeken en preventieve aanpakken van cybercrime en gedigitaliseerde criminaliteit. Tijdens dit event werd ook de onderzoeksagenda gepresenteerd.

Rutger Leukfeldt in EenVandaag

Steeds meer jongeren worden op social media geronseld voor criminele klussen. In een recente aflevering van EenVandaag bespreekt Rutger Leukfeldt de rol van geldezels. Een geldezel laat zijn bankrekening gebruiken om geld van criminelen naar iemand anders over te maken of wit te wassen.

OKT

ZeroDay Zoetermeer

Studenten van De Haagse Hogeschool en mboRijnland gingen in teams van maximaal vijf personen de uitdaging aan om kwetsbaarheden in de online systemen van de gemeente Zoetermeer op te sporen. Ze testten hun vaardigheden als ethical hackers en droegen bij aan een veiliger digitaal Zoetermeer. Het lectoraat Network & Systems Engineering Cyber Security was vertegenwoordigd in de organisatie en jury.

De impact van generatieve AI op cybersecurity in de financiële sector

In samenwerking met HCLTech voerde het lectoraat Cyber Security & Safety een kort onderzoek uit, waarin experts uit verschillende financiële organisaties zijn geïnterviewd. Het onderzoek biedt inzicht in hoe de financiële sector GenAI toepast en welke risico's hierbij komen kijken. Tijdens het HSD Café op 10 oktober presenteerde Pieter Burghouwt, senior onderzoeker bij Centre of Expertise Cyber Security van De Haagse Hogeschool, de resultaten van een onderzoek naar de impact van generatieve AI (GenAI) op cybersecurity in de financiële sector.

HIGHLIGHTS 2024

NOV

DEC

Intreerede Peter Roelofsma

Op 14 november gaf Peter Roelofsma zijn intreerede over cyberrisicomanagement en de complexiteit van cascade cyberrisico's. Hij besprak de kloof tussen theorie en praktijk, schetste zijn toekomstvisie voor het lectoraat, vertelde over de ontwikkeling van het Cyber Security Living Lab, en liet zien hoe hij samenwerkt met studenten, onderzoekers, docenten en het werkveld aan een veiligere digitale samenleving.

Opening Cyber Security Living Lab

Op 15 november werd het Cyber Security Living Lab feestelijk geopend in de Dutch Innovation Factory. Dit initiatief van lector Peter Roelofsma biedt een innovatieve omgeving waar 24/7 real-time cybersecuritydreigingen worden gesimuleerd. Studenten van mbo, hbo en universiteiten werken er samen met bedrijven om praktische ervaring op te doen in het omgaan met deze dreigingen. Het doel: gezamenlijk bijdragen aan een weerbaardere digitale samenleving.

Oratie Rutger Leukfeldt

Rutger Leukfeldt is benoemd tot bijzonder hoogleraar Governing Cybercrime aan de Universiteit Leiden. Tijdens zijn oratie op 25 november benadrukte hij het belang van empirisch onderzoek naar cybercrime.

Brainstorm: onderzoek integreren in opleidingen

Onderzoekers en lectoren van het Centre of Expertise Cyber Security van De Haagse Hogeschool brainstormden samen met docenten van de opleiding HBO-ICT. Het doel was te verkennen hoe onderzoek al vanaf de propedeuse kan worden geïntegreerd in de opleiding. Dit resulteerde in creatieve ideeën, als basis voor volgende stappen. Zo leggen we het fundament voor een generatie studenten die niet alleen leert, maar ook onderzoekt en innoveert.

Rutger Leukfeldt in Libelle en Margriet

Hoe bescherm je jezelf tegen online fraude én de gevolgen ervan? In een artikel in Libelle en Margriet deelt Rutger Leukfeldt drie belangrijke lessen over cybercrime met de doelgroep van deze magazines: iedereen kan slachtoffer worden, de impact van digitale fraude is heel groot en wees gezond argwanend.

Honorering project 'Lokaal Cyberweerbaar Den Haag'

Om organisaties in de regio digitaal weerbaarder te maken, bundelen De Haagse Hogeschool, gemeente Den Haag en stichting Connect2Trust hun krachten. Doel van het project is lokale organisaties met elkaar te verbinden, zodat zij gezamenlijk kunnen werken aan het verbeteren van hun cyberweerbaarheid door middel van kennisdeling en praktische hulpmiddelen. In de eerste fase van het project zullen 1400 organisaties in de regio Den Haag worden benaderd. Dit initiatief wordt mogelijk gemaakt door de subsidieregeling Versterking Cyberweerbaarheid van het Digital Trust Center.

VOORUITBLIK 2025

Ontwikkeling lectoraten en versterking onderzoek

In samenwerking met de faculteiten IT & Design (IT&D) en Bestuur, Recht & Veiligheid (BRV) van De Haagse Hogeschool is de ambitie om in 2025 een lector te werven voor het vijfde lectoraat Legal Aspects of Cybersecurity. Tegelijkertijd wordt de aanvraagprocedure afgerond voor het zesde lectoraat Cybersecurity voor Smart Industry, waarna ook voor deze functie de werving start. Tijdens dit proces starten we al met het opbouwen van onderzoek binnen beide thema's. In augustus 2025 neemt de huidige lector van de onderzoeksgroep Cyber Security & Safety afscheid vanwege zijn welverdiende pensioen. Voor deze stevig verankerde kenniskring wordt tijdig een geschikte opvolger gezocht.

Daarnaast zetten we in 2025 in op verdere professionalisering van de ondersteuning vanuit het Centre of Expertise naar de lectoraten en lopende projecten. Het versterken van de kennisinfrastructuur binnen De Haagse Hogeschool blijft hierbij een belangrijk aandachtspunt. Proactieve betrokkenheid bij ontwikkelingen op het gebied van huisvesting, ICT en onderzoeksondersteuning blijft essentieel.

Strategische samenwerkingen

We continueren onze gezamenlijke onderzoeksprogramma's met bestaande strategische partners en zetten waar nodig in op verlenging. De samenwerking met NSCR en Universiteit Leiden wordt verder geïntensiveerd. Ook verkennen we mogelijkheden om internationale netwerken uit te breiden, onder andere door positionering binnen Europese subsidieprogramma's.

Bijdrage aan onderwijsvernieuwing

Binnen de faculteit BRV zijn we betrokken bij de minor Cyber Security. Onze onderzoekers leveren daarnaast een actieve bijdrage aan de ontwikkeling van de minor Cybercrime, op basis van hun inhoudelijke expertise en lopende projecten. De opleiding HBO-ICT (faculteit IT&D) biedt inmiddels de differentiatie Cyber Security Technology aan. Binnen het Human Behaviour Research Semester zijn onze onderzoekers actief als research coaches. Daarnaast treden zij op als opdrachtgevers voor stage- en afstudeeropdrachten en verzorgen zij op verzoek gastcolleges binnen hun vakgebieden.

Ons Centre of Expertise levert kerndocenten voor de masteropleiding Cyber Security Engineering en blijft als gastdocent en sparringpartner betrokken bij de masteropleiding Risk Management. De samenwerking met de Dutch Innovation Factory in Zoetermeer wordt verder versterkt. Onderwijs wordt daar direct gekoppeld aan praktijkgericht onderzoek in het Cyber Security Living Lab en het Human Factor Lab. In 2025 streven we ernaar om een technisch georiënteerd lab op te richten op de locatie Delft, gericht op de technische aspecten van cybersecurity en verbonden aan het lectoraat Network & Systems Engineering Cyber Security.

Thema Digitale Toekomst

Het Centre of Expertise Cyber Security is samen met het Centre of Expertise Digital Operations & Finance trekker van de 'Digitale Toekomst', een van de drie hoofdthema's van de kennisagenda van De Haagse Hogeschool. Binnen dit thema werken we aan een toekomst waarin burgers en professionals digitale technologieën inzetten voor een veilige, gezonde en inclusieve samenleving, met aandacht voor gelijke kansen en duurzaamheid.

Ook in 2025 betrekken we andere lectoraten, Centres of Expertise en opleidingen bij de planvorming. Concreet richten we ons op:

- Verdere ontwikkeling van het vijfde (juridische) en zesde (technische) lectoraat in samenwerking met onderwijs, met name de faculteiten BRV en ITD;
- Inzet van onderzoekscapaciteit binnen deze twee lectoraten;
- Versterking van de centrale expertbank van data scientists, zodat de hele hogeschool hiervan kan profiteren;
- Voortzetting van de Community of Practice Onderzoek Digitale Toekomst, waarin lectoren en docentonderzoekers kennis, ideeën en netwerken delen en ondersteund worden bij nieuwe onderzoeksaanvragen, die met seed money vanuit het thema worden ondersteund;
- Oprichting van een red team dat meedenkt over het portfolio rond het thema Cyberweerbaarheid, in nauwe samenwerking met bedrijfsleven, overheid en onderwijs;
- Realisatie van een Experience Centre, in samenwerking met andere Centres of Expertise, om de zichtbaarheid van onderzoek binnen De Haagse Hogeschool te vergroten.

DE HAAGSE HOGESCHOOL

CENTRE OF EXPERTISE CYBER SECURITY 2024

Missie: Het versterken van de cyberveerkracht van publieke en private organisaties die zelf in mindere mate zijn toegerust op cyberdreigingen

LECTORATEN

Cyber Security & Safety
Marcel Spruit

Cybercrime & Cybersecurity
Rutger Leukfeldt

Network & Systems Engineering Cyber Security
Gerard Hoekstra

Risk Management & Cyber Security
Peter Roelofsma

IMPACT

KENNISDOMEIN

- **46** Deelname aan conferenties
- **7** Organisatie van conferenties
- **38** Publicaties (26 peer-reviewed)
- **28** Workshops / lezingen
- **16** Commissies
- **46** Boek(hoofdstukk)en (34 peer-reviewed)
- **6** Internationale netwerken

187

ONDERWIJS

- **65** Studentbegeleiding (afstuderen, stage, projecten)
- **92** (Gast)colleges / workshops
- **1** Ontwikkeling onderzoekslijn curriculum
- **16** Ontwikkelde / uitgevoerde minor of keuzemodule
- **8** Ontwikkelde onderwijsmaterialen
- **9** Bijdrage curriculumvernieuwing

191

WERKVELD/MAATSCHAPPIJ

- **40** Projecten
- **13** Rapporten
- **67** Workshops / presentaties
- **1** Adviestraject
- **2** Tools
- **1** Symposium

124

19 FTE CAPACITEIT PERSONEN **42**

Waaronder **6** promovendi

HIGHLIGHTS

- **Opening Cyber Security Living Lab:** Studenten werken samen met bedrijven aan het versterken van de digitale weerbaarheid en doen praktijkervaring op in het bestrijden van cyberdreigingen.
- **Honorering project Lokaal Cyberweerbaar Den Haag:** De HHs, gemeente Den Haag en Connect2Trust bundelen krachten om organisaties in de regio digitaal weerbaarder te maken.
- **Empirisch onderbouwde aanpak van cybercrime:** Lector Rutger Leukfeldt is benoemd tot bijzonder hoogleraar Governing Cybercrime aan de Universiteit Leiden.
- **Cascade Cyber Risk Management - Between Rule and Reality:** In zijn intreerede pleitte lector Peter Roelofsma voor een gezamenlijke aanpak van cyberrisico's.

BELANGRIJKSTE PARTNERS

nscr · MKB Nederland · THALES · Den Haag · Ministerie van Justitie en Veiligheid · gemeente Zoetermeer

THEMA'S

Mens
Human factor
Cybercrime

Organisatie
Information security
Governance
Crisismanagement

Techniek
Data Centric Security
Resilient Infrastructure IT/OT/IoT
Red Team / Hacking

OPLEIDINGEN

We werken nauw samen met

- HBO-ICT
- Integrale Veiligheidskunde (IVK)
- LAW
- Master of Cyber Security Engineering (MCSE)

Peer reviewed artikelen

- Bekkers, L., A. Moneva & E.R. Leukfeldt (2024) Understanding cybercrime involvement: a quasi experiment on engagement with money mule recruitment ads on Instagram. Journal of Experimental Criminology. https://doi.org/10.1007/s11292-022-09537-7.
- Bekkers, L., E.R. Leukfeldt & E.R. Kleemans (2024) Recruiting co-offenders for financial cybercrime: An analysis of police investigations into cybercriminal networks. Trends in Organized Crime. https://doi.org/10.1007/s12117-024-09556-y.
- Bouma, D., Hoffmans, C., Van den Hout, N.J., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Cyber Security in Hospitals: A Network-Oriented Model for Behavioral Learning of Employees during Phishing Simulations. In: Proc. of the 17th International Conference on Computational Intelligence in Security for Information Systems, CISIS'24. Lecture Notes in Networks and Systems, Springer Nature.
- Burghouwt, P., Kerpershoek, E., & Spruit, M. (2024). The impact of Generative AI on Cyber Security in the Financial sector. *ONE Magazine 2024*, NCTV. https://emagazine.one-conference.nl/2024/the-impact-of-generative-ai-on-cybersecurity-in-the-financial-sector/.
- Dupont, B., F. Fortin & E.R. Leukfeldt (2024) Broadening our understanding of cybercrime and its evolution. Journal of Crime and Justice. https://doi.org/10.1080/0735648X.2024.2323872.
- Garkava, T., A. Moneva & E.R. Leukfeldt (2024) Stolen Data Markets on Telegram: A Crime Script Analysis and Four Situational Crime Prevention Measures. Trends in Organized Crime. https://doi.org/10.1007/s12117-024-09532-6.
- Loggen, J., A. Moneva & E.R. Leukfeldt (2024) Pathways into, desistance from, and risk factors related to cyber-dependent crime: A systematic narrative review. Victims and offenders. 1–32. https://doi.org/10.1080/15564886.2024.2370295.
- Matthijsse, S.R., A. Moneva, M.S. van 't Hoff-de Goede & E.R. Leukfeldt (2024). Examining ransomware payment decision-making among small- and medium-sized enterprises. European Journal of Criminology, https://doi.org/10.1177/14773708241285671.
- Moneva, A., S. Ruiter & D. Meinsma (2024) Criminal expertise and hacking efficiency. Computers in Human Behavior, 155, 1-15. https://doi.org/10.1016/j.chb.2024.108180.
- Moneva, A. & E.R. Leukfeldt (2024). Interest in booter services and distributed denial of service attacks: Insight from Google search data. European Journal of Criminology https://doi.org/10.1177/14773708241275424.
- Romagna, M. & E.R. Leukfeldt (2024) Hacktivism: From Loners to Formal Organizations? Assessing the Social Organization of Hacktivist Networks. Deviant Behavior. https://doi.org/10.1080/01639625.2024.2431066.
- Romagna, M. & E.R. Leukfeldt (2024) Social Opportunity Structures in Hacktivism: Exploring Online and Offline Social Ties and the Role of Offender Convergence Settings in Hacktivist Networks. Victims and offenders. https://doi.org/10.1080/15564886.2024.2372054.
- Spruit, M., Oosting, D., & Kreffer, C. (2024). Factors that affect the motivation to use mobile digital devices securely. Information and Computer Security, 32 (5), 729-747.
- Stibbe, D., S. Ruiter, W. Steenbeek & A. Moneva (2024). Sweeter than honey: Are Gmail accounts associated with greater rewards at a higher risk of hijacking? Computers in Human Behavior Reports, 14. https://doi.org/10.1016/j.chbr.2024.100410.
- Van de Weijer, S., E.R. Leukfeldt & A. Moneva (2024) Cybercrime during the COVID-19 pandemic: Prevalence, nature and impact of cybercrime for citizens and SME owners in the Netherlands. Computers & Security. https://doi.org/10.1016/j.cose.2023.103693.

Artikelen in (vak)tijdschriften

- Burghouwt, P., Kerpershoek, E., & Spruit, M. (2024). Kansen en bedreigingen van AI in het onderwijs. IB Magazine, 24 (3), 10-13. https://www.pvib.nl/actueel/ib-magazines/ib-magazine-3-2024/downloaden
- Kerpershoek, E, Niemann, L., & Burghouwt, P. (2024). Cyberweerbaarheid in de openbare ruimte vaak niet op orde. iBestuur online, https://ibestuur.nl/artikel/cyberweerbaarheid-in-de-openbare-ruimte-vaak-niet-op-orde/.
- Pouw, R., Stokkel, M., van 't Hoff-de Goede, S., & van der Wal, M. (2024). Van twijfel naar enthousiasme. Innovatie in het meten van awareness en daadwerkelijk veilig gedrag. iB Informatiebeveiliging Magazine, p.4-7. https://www.pvib.nl/actueel/ib-magazines/ib-magazine-1-2024/downloaden.
- Ruiter, S., M. van Leuken, T. van Ruitenburg, J. Schiks & E.R. Leukfeldt (2024) In- en doorstroom van online criminaliteit in de strafrechtketen onderzocht. Tijdschrift voor de Politie.
- Spruit, M., & Kreffer, C. (2024). Informatie(on)veilig gedrag van medewerkers. IB Magazine, 24 (5), 8-13. https://www.marcelspruit.nl/papers/Spruit_Kreffer_Informatieonveilig_gedrag_van_medewerkers_2024.pdf
- Spruit, M., & Kreffer, C. (2024). Meten en verbeteren van informatieveilig gedrag. iBestuur online, https://ibestuur.nl/artikel/meten-en-verbeteren-van-informatieveilig-gedrag.
- Van Leuken, M.A.G. & Van 't Hoff-de Goede, M.S. (2024). De civielrechtelijke afdoening van online fraude. Secondant. https://ccv-secondant.nl/platform/article/de-civielrechtelijke-afdoening-van-online-fraude.
- Van 't Hoff-de Goede, S. & Janssen, J. (2024). De overlap tussen offline en online geweld in -afhankelijkheidsrelaties. PROCES, 102(1), 57-66.

Boek

- Leukfeldt, E.R. (2024). Meer dan alleen een goed idee. Naar een empirisch onderbouwde aanpak van cybercrime. Leiden: Universiteit Leiden.

Peer reviewed hoofdstukken in boek

- Akers, D., Blomquist, T., Niedziela, J., Šebok, S., Van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Organizational Response to APT attacks: Computational Analysis by Behavioral Network Modelling. In: Proc. of the Third International Conference on Information Systems for Business Management. Lecture Notes in Networks and Systems, Springer Nature.
- Börcsök, T., Bos, M., Buter, W., Van Der Hoeven, D., Velev, A., Van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Adaptive Defence Mechanisms: An Adaptive Network Model to Protect HiX Systems Against Cyber Attacks. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature.
- Bouma, D., Den Oudsten, T., Naffakh, A, Waliji, M., Treur, J., Roelofsma, P.H.M.P. (2024). Cyber Risk Management and Organisational Alignment Using Endley's Risk Management Model: Computational Analysis from an Adaptive Dynamical System Perspective. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature.
- Caneva, J., Oliver, S., Rietze, N.E., Šileris, L., Barelds, N., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). The Unforeseen Blackout and Cyber Risk Management for Business Continuity: Network-Oriented Computational Analysis. In: Proc. of the 8th International Conference on Computational Methods in Systems and Software, CoMeSySo'24. Lecture Notes in Networks and Systems, Springer Nature.
- Fischer, T. F. C., Matthijsse, S. R., van der Wagen, W., & Van 't Zand, E. G., (2024). De forensische aanpak van cybercriminaliteit. In J. Bosker & A. Menger (Eds). Werken in gedwongen kader: Methodiek voor het forensisch sociaal werk (pp. 426-437). SWP Uitgever.
- Jeffery, E., Malsagov, U., Tijssen, N., Zeisig, A., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of the Effectiveness of the Intelligence Cycle for Organizational Cyber Risk Management. Proc. of the Third International Conference on Information Systems for Business Management. Lecture Notes in Networks and Systems, Springer Nature.
- Keijzer, S., Lochtenbergh, D., Marsman, T., Voorhoeve, S., Zwarts, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Managing Classified Information by a Third-Party Contractor: A Computational Cybersecurity Analysis. In: Proc. of the Third International Conference on Information Systems for Business Management. Lecture Notes in Networks and Systems, Springer Nature.
- Matthijsse, S.R., Loggen, J., Leukfeldt, R., & Van 't Hoff-de Goede, S. (2024). De waarde van crime script analyse voor nieuwe vormen van criminaliteit: Geleerde lessen uit de ontwikkeling van drie (cyber)crime scripts. T. Snaphaan & P. Klerks (eds.) Crime Scripting: Theorie en praktijk. Den Haag: Boom Uitgevers.
- Van den Hout, N.J., Bouma, D., Hoffmans, C., Zwarts, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Addressing Organizational Cyber Security Challenges in Healthcare using Adaptive Network-Oriented Modeling Approach. Springer Nature.

Hoofdstukken in boeken

- Leukfeldt, E.R., R. Roks & T. Holt (2024) Cybercriminal networks. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.) Essentials in cybercrime. A criminological overview for education and practice. The Hague: Eleven.
- Roks, R., E.R. Leukfeldt & T. Holt (2024) Cybercriminele samenwerkingsverbanden. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.) Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk. Den Haag: Boom Uitgevers.
- Smith, T., E.R. Leukfeldt & S. van de Weijer (2024) Moving from risk factors to positive online behaviors: An integrated behavioral change approach. In: R. Graham, S. Humer, C. Lee, & V. Nagy (Eds.), Routledge International Handbook of Online Deviance. Routledge Taylor & Francis Group. https://doi.org/10.4324/9781003277675-13.
- Van 't Hoff-de Goede, S. & E.R. Leukfeldt (2024) Slachtofferschap van online criminaliteit. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.) Basisboek cybercriminaliteit. Een criminologisch overzicht voor studie en praktijk. Den Haag: Boom Uitgevers.
- Van 't Hoff-de Goede, S. & E.R. Leukfeldt (2024) Cybercrime Victimization. In: W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (eds.) Essentials in cybercrime. A criminological overview for education and practice. The Hague: Eleven.
- van 't Zand, E. G., Matthijsse, S. R., Fischer, T. F. C., & van der Wagen, W. (2024). Interventies voor cyberdaders. In W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Reds.). Basisboek cybercriminaliteit (2e druk). Boom Uitgevers.
- van 't Zand, E. G., Matthijsse, S. R., Fischer, T. F. C., & van der Wagen, W. (2024). Interventions for cyber offenders. In W. van der Wagen, J.J. Oerlemans & M. Weulen Kranenbarg (Eds.). Essentials in cybercrime: A criminological overview for education and practice (2nd ed.). The Hague: Eleven

Rapporten

- Andriessen, M., Van Leuken, M.A.G. & Van 't Hoff-de Goede, M.S. (2024). Jong ICT-talent op het rechte pad houden. Een plan- en procesevaluatie. Den Haag: Centre of Expertise Cybersecurity, THUAS. https://www.dehaagsehogeschool.nl/media/jong-ict-talent-op-het-rechte-pad-houden
- Bekkers, L., M. van Leuken & E.R. Leukfeldt (2024) Criminele netwerken achter geldezels. Rapportage deel 1: verkenning. Den Haag: Haagse Hogeschool.
- Burghouwt, P., E. Kerpershoek & M. Spruit (2024). The Impact of Generative AI on cybersecurity in financial services. Whitepaper. HCLTech.
- Kerpershoek, E. & L. Niemann (2024). Beveiliging van Operationele Technologie (OT) door gemeenten. Resultaten van een enquête onder CISO's ter voorbereiding op de NIS2 richtlijn. Den Haag: De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/media/beveiliging-van-operationele-technologie-gemeenten
- Uiterweerd, F., C. Geurts & E. Kerpershoek (2024). Adviesrapport Testen en oefenen van informatiebeveiliging door gemeenten, waterschappen en provincies. Overheidsbreed Cyberprogramma. https://www.digitaleoverheid.nl/document/adviesrapport-testen-en-oefenen-van-informatiebeveiliging/
- Van Leuken, M.A.G. & Van 't Hoff-de Goede, M.S. (2024). Ervaringen van slachtoffers met de civielrechtelijke afdoening van online fraude. Den Haag: Centre of Expertise Cybersecurity, THUAS.
- Van Leuken, M.A.G. & Van 't Hoff-de Goede, M.S. (2024). Praktische uitvoering en juridische grondslag van de civielrechtelijke afdoening van online fraude. Den Haag: Centre of Expertise Cybersecurity, De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/media/deelrapport-1-naar-een-toekomstbestendige-civielrechtelijke-afdoening-van-online-fraude
- Van 't Hoff-de Goede, S., M.L. van der Wal & E.R. Leukfeldt (2024) What (s)can we do? Onderzoek naar het gebruik van een geautomatiseerde kwetsbaarhedenmeting als evidence based gedragsinterventie. Den Haag: De Haagse Hogeschool. https://www.dehaagsehogeschool.nl/media/what-scan-we-do

Conferentiepapers

- Bezembinder, J., Cadoni, M., de Waal, A., Hoffmans, C., van Ommen, J., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of a Virtual Assistant Supporting the Use of Home Health Devices: an Adaptive Network Model. https://www.researchgate.net/publication/382975606.
- Jong, de R., Geerman, D., Oduber, A., Paterson, B., Popova, K., Zwarts, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Electromagnetic Signature Management on the Battlefield: Computational Analysis by Adaptive Network Modelling. https://www.researchgate.net/publication/382975651.
- Belkuyu, E., Bijl, T., Nobre Dos Santos, J.R., Sevdalakis, J.I., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Breaking through Escalation of Commitment and Groupthink in Cyber Risk Management by AI Coaching: a Network-Oriented Computational Analysis. https://www.researchgate.net/publication/382975602.
- Lepădatu, F., Mihăilescu, T., Spaan, Ţiţei, P., van der Vossen, M., van den Hout, N.J., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). Analysis of Management of Phishing Attack Risks Based on an Adaptive Network Model. https://www.researchgate.net/publication/382975599.
- Babayusuf, Y., Bouma, D., Feteasco, A., van Hekezen, L., Vasov, J., Zwarts, N., Treur, J., Roelofsma, P.H.M.P. (2024). Enhancing Cyber Resilience Securing Governmental Applications for Citizens: Computational Analysis. https://www.researchgate.net/publication/382975648.
- Erdogan, A., Hoffmans, C., Sbita, A., Wach, E., Zuijderduijn, K., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P (2024). Network-Oriented Computational Analysis of Cyber-Attacks. https://www.researchgate.net/publication/382975658
- Bart, J., Milani, S., Raïkkönen, Sultani, D., Van 't Hoff, F., Zwarts, N., Hoffmans, C., Treur, J., Roelofsma, P.H.M.P.(2024). Computational Analysis of Disruptions of Mobile Networks during Wartime: an Adaptive Network Modeling Approach. https://www.researchgate.net/publication/382544551.
- Bell, A., Flik, Y., Hotsma, N., Tande, P.J.L., Zwarts, N. Hoffmans, C., Treur, J., Roelofsma, P.H.M.P. (2024). CyberAttacks Triggering a Collective Response within NATO: A Network-Oriented Computational Analysis. https://www.researchgate.net/publication/382424047.
- Daza, M., Duivesteijn, D., Jouma, M., Reichardt, F., Barelds, N., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). The Delicate Balance of Ethics and Control for Smart Cities: A Network-Oriented Analysis Approach. https://www.researchgate.net/publication/382975762.
- Abromaitytė, M., Dubero, E., Kruger, Q., Lucassen, B., Vos, T., van den Hout, N.J., Bouma, D., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of User Experience of Password-Based Authentication Systems. https://www.researchgate.net/publication/382975936.
- Capră, A.M.C., Dekker, E., Hoffmann, L., Hoffmans, C., Hoogstad, M., Mueller, T., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P. (2024). Computational Analysis of Human Factors in Spear-Phishing Attacks: An Adaptive Network Model. https://www.researchgate.net/publication/382975864.
- Hoffmans, C., van der Does, L., van der Kolk, M., van Rooyen, T., Barelds, N., Treur, J., Roelofsma, P.H.M.P. (2024). Analysing the Rise of Biohacking in a Tech-Driven City: Assessing Risks through Adaptive Network Modeling. https://www.researchgate.net/publication/382975862.
- Mestour, W., van den Hout, N.J., Treur, J., Roelofsma, P.H.M.P. (2024). An Adaptive Network Model to Analyse Cybersecurity: Understanding Cyber Threats in Financial Institutions. https://www.researchgate.net/publication/382975671.
- Ivan, I., van den Hout, N.J., Hendrikse, S.C.F., Treur, J., Roelofsma, P.H.M.P. (2024). Understanding Insider Threats Behaviour: An Adaptive Network Model for the Evolution of an Insider Threat https://www.researchgate.net/publication/382975930.

Blijf op de hoogte van het laatste nieuws uit het Centre of Expertise Cyber Security!
Volg ons op **LinkedIn** voor updates over ons onderzoek, samenwerkingen en evenementen.
Heeft u een vraag, wilt u meedenken of samenwerken? Neem een kijkje op onze **website** of mail ons via **cybersecurity@hhs.nl** – we horen graag vanu!

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

cybersecurity@hhs.nl

dehaagsehogeschool.nl/onderzoek/kenniscentra/details/centre-of-expertise-cyber-security