Centre of Expertise Cyber Security

Praktijkgericht onderzoek naar de cyberveerkracht van organisaties

Lectoren

Dr. Rutger Leukfeldt
lector Cybercrime & Cybersecurity
directeur van het CoECS

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 2023

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

Inhoud

Voorwoord

Voor u ligt de jaarupdate 2023 van het Centre of Expertise Cyber Security. We blikken terug op een jaar waarin we een mooie ontwikkeling hebben doorgemaakt. De uitdagingen die we hebben aangepakt en waar we ons in 2024 onverminderd voor blijven inzetten, liggen op het gebied van de ontwikkeling van het kenniscentrum, de koppeling met het onderwijs en de samenwerking met de markt. Op alle drie de terreinen zijn mooie stappen gezet.

We voerden meer onderzoeken uit en trokken meer onderzoekers aan. Daarnaast zijn er twee nieuwe lectoren aangesteld en zijn er stappen gezet in de verdere professionalisering van de onderzoeksinfrastructuur in de vorm van labs. Het aantal (docent)onderzoekers dat promotieonderzoek doet binnen ons kenniscentrum is ook gegroeid.

In 2023 is de samenwerking met het onderwijs verder versterkt. Er lopen veel projecten en de meeste onderzoekers dragen bij aan kennisoverdracht via het onderwijs.

Op het gebied van samenwerking met onze externe omgeving is Cyberweerbaar NL gestart, waarvoor we een belangrijke SPRONG-subsidie van NWO/SIA hebben ontvangen. Daarnaast zijn er veel nieuwe opdrachten en samenwerkingen gestart, wat heeft geleid tot een flinke toename van externe financiering.

De ontwikkeling van de hogeschoolbrede kennisagenda heeft ook de interne samenwerking versterkt. Er is meer samenwerking ontstaan met andere kenniscentra en faculteiten binnen het thema Digitale Toekomst, en deze samenwerking zal in 2024 verder worden uitgebreid.

In deze jaarupdate belichten we een aantal van onze successen en gaan we dieper in op onze onderzoeken. Gezien de ontwikkelingen in de wereld zal ons vakgebied in de toekomst een steeds belangrijkere rol spelen.

Wij wensen u veel leesplezier en kijken ernaar uit om met u in gesprek te gaan over mogelijke samenwerkingen.

Namens het Centre of Expertise Cyber Security
Rutger Leukfeldt

Over ons

Het kenniscentrum Cyber Security richt zich op het versterken van de cyberveerkracht van publieke en private organisaties die minder goed zijn uitgerust om cyberdreigingen het hoofd te bieden. Want in een tijdperk waarin digitale dreigingen toenemen en cyberaanvallen steeds geavanceerder worden, is het van cruciaal belang dat organisaties beschikken over de juiste kennis en middelen om zich te verdedigen.

Met praktijkgericht onderzoek werkt het kenniscentrum Cyber Security aan vraagstukken op het gebied van digitale veiligheid. We werken intensief samen met het onderwijs en de praktijk. Onze multidisciplinaire aanpak leidt tot nieuwe kennis, producten of diensten die direct toepasbaar zijn en impact hebben.

Onderzoeksthema's

In ons onderzoek ligt de focus op drie thema's:

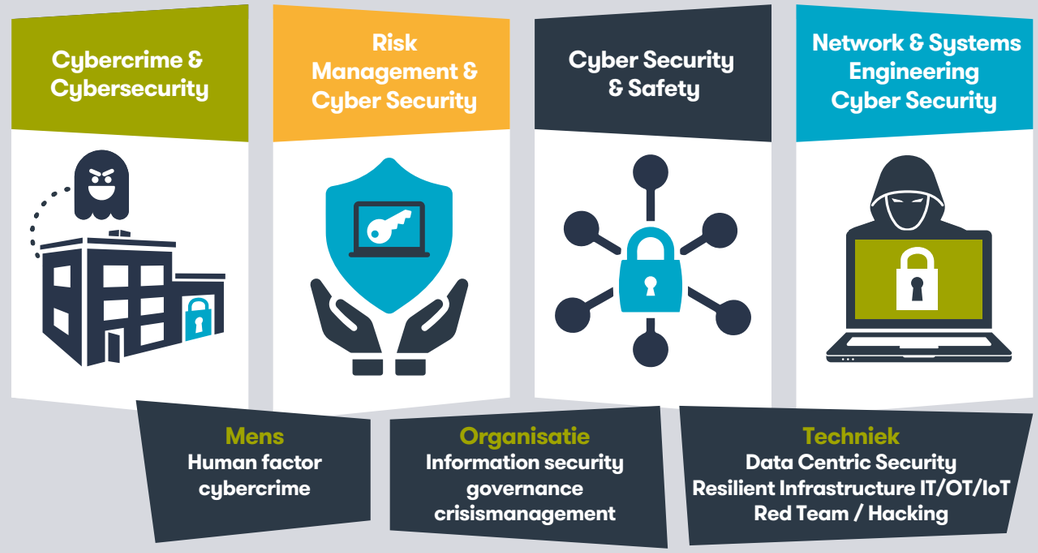
- **Mens:** welke gedrag- en houdingsaspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten verbeteren?
- **Organisatie:** welke organisatieaspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten verbeteren?
- **Techniek:** welke technische aspecten beïnvloeden cyberveerkracht en hoe kunnen technische maatregelen mensen en organisaties helpen om hun cyberveerkracht te verbeteren?

Samenwerking

In het kenniscentrum Cyber Security bundelen we de expertise van vier lectoraten: Cyber Security & Safety, Cybercrime & Cybersecurity, Risk Management & Cybersecurity en Network and Systems Engineering Cybersecurity. Elk lectoraat heeft zijn eigen expertise en perspectief. Door deze perspectieven samen te brengen kunnen we op een unieke manier bijdragen aan praktijkgericht onderzoek naar cybersecurity.

Binnen deze onderzoeksgroepen werken lectoren, onderzoekers, docent-onderzoekers, projectmanagers en studenten aan diverse projecten. We doen dit zoveel mogelijk in samenwerking met bedrijven, organisaties en andere instellingen. Het kenniscentrum is nauw verbonden met de faculteiten en opleidingen van De Haagse Hogeschool. Samenwerking met ons kenniscentrum biedt organisaties en bedrijven de kans om samen te werken met onderzoekers, docenten en studenten, waarbij zij bijdragen aan de ontwikkeling en praktische toepassing van nieuwe kennis.

Multidisciplinair onderzoek kenniscentrum Cyber Security



Samenwerking met het onderwijs

- HBO-ICT
- CMD
- IVK/SSMS
- LAW
- Master Cyber Security Engineering (MCSE)

Samenwerking met externe partners

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

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 onderzoek en ontwikkelt hij onderwijs op dit gebied. Daarnaast geeft hij les in masteropleidingen aan De Haagse en enkele universiteiten. Voor en naast zijn aanstelling als lector werkte hij bij Fokker Space in kwaliteitsborging, als universiteit hoofddocent bij de TU Delft en als senior consultant voor cybersecurity bij PBLQ (voorheen Het Expertise Centrum). Het onderzoek van Marcel richt zich vooral op het meten en verbeteren van gedrag, het analyseren en optimaliseren van de organisatie van cybersecurity in publieke en dienstverlenende organisaties en de kwalificatie van cybersecurity-professionals.

“Simulaties en serious games kunnen de sleutel zijn tot effectieve cyberbeveiliging. Ze bieden een realistische en interactieve omgeving waarin gebruikers hun vaardigheden kunnen testen en verbeteren, wat essentieel is in de voortdurende strijd tegen cyberdreigingen.”

Wat doet het lectoraat Cyber Security & Safety?

Het lectoraat Cyber Security & Safety streeft ernaar het bewustzijn over cybersecurity bij mensen te vergroten, de cybersecurity binnen organisaties te optimaliseren, de rol van kunstmatige intelligentie met betrekking tot cybersecurity te onderzoeken en de kwalificaties van cybersecurity-professionals te verbeteren. Daarvoor doet het lectoraat onderzoek naar methoden en technieken voor het meten en verbeteren van cybersecurity-gedrag van mensen, het meten en verbeteren van de organisatie van cybersecurity in organisaties en de rol die kunstmatige intelligentie daarin kan spelen, evenals het verbeteren van het cybersecurity-onderwijs voor professionals. Het onderzoek van het lectoraat Cyber Security & Safety richt zich met name op dienstverlenende sectoren zoals overheden, onderwijs en zorg. Het doel is te ontdekken hoe mensen, individueel en in organisaties, en organisaties weerbaarder kunnen worden tegen cyberdreigingen.

Het onderzoek binnen het lectoraat richt zich op vier onderzoekslijnen:

1. Het verhogen van het cybersecurity-bewustzijn van mensen.
2. Het verbeteren van de cybersecurity in organisaties.
3. De rol van kunstmatige intelligentie in het cybersecurity-domein.
4. de kwalificatie van cybersecurity-professionals.

Samenwerking met onderwijs

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

WAT WE DOEN

Uitgelichte projecten

Digitale veiligheid in life sciences & health

Dit onderzoek had als doel om de huidige stand van digitale veiligheid binnen de life sciences & health (LSH)-sector te analyseren en aanbevelingen te formuleren ter verbetering ervan. De onderzoekers verkenden de belangrijkste dreigingen voor de digitale veiligheid van organisaties in de LSH-sector, ze onderzochten de potentiële impact van digitale veiligheidsincidenten op deze organisaties, ze stelden het niveau van digitale veiligheid van organisaties in de LSH-sector op dat moment vast en ze identificeerden de behoefte aan ondersteuning voor verbetering van digitale veiligheid.
Het resultaat van het onderzoek is een rapport met aanbevelingen ter bevordering van de digitale veiligheid in de LSH-sector. Het Leiden Bio Science Park, een belangrijk cluster binnen deze sector in Nederland, vervulde een centrale rol in dit onderzoek.

- **In opdracht van:** Security Delta, Stichting Leiden Bio Science Park
- **Gefinancierd door:** Metropoolregio Rotterdam Den Haag (MRDH)
- **In samenwerking met:** Hogeschool Leiden, REQON

Het (on)veilige gedrag met digitale mobiele media

In dit onderzoek naar het meten en verklaren van menselijk gedrag met betrekking tot cybersecurity is een nieuw gedragsverklarend model afgeleid. Dit model is uitgebreider en preciezer dan de gangbare modellen in het cybersecurity-domein. Het model is toegepast in een enquête over hoe mensen omgaan met hun mobiele digitale media, zoals smartphones en laptops, op het gebied van digitale veiligheid. Voor de enquête is gebruikgemaakt van een nieuw ontwikkelde vragenlijst.
De resultaten van de enquête laten zien dat het ontbreken van relevante kennis een oorzaak kan zijn van onveilig gedrag, maar dat ook andere factoren zoals bias, cognitieve attitude en affectieve attitude een belangrijke rol spelen. Dit heeft consequenties voor de interventies die worden opgesteld om het gedrag met betrekking tot cybersecurity te verbeteren.

The Detectable Vegetable

De Haagse Hogeschool leidt het brede praktijkgerichte onderzoeksproject The Detectable Vegetable om met de (door) ontwikkeling van contactloze sensortechnologie en data-intelligentie ziekte en bederf van tuinbouwgroenten vroegtijdig op te sporen.
In The Detectable Vegetable werken 2 hogescholen, 2 andere kennisinstellingen, 6 mkb-bedrijven, 5 glastuinbouwbedrijven en overkoepelende organisaties aan het verder ontwikkelen en optimaliseren van optische sensoren om ze geschikt te maken voor het monitoren van gewassen in de glastuinbouw. Voor de analyse van de verzamelde data en het verkrijgen van inzichten over ziekte en bederf maken ze gebruik van deep learning modellen en artifical intelligence. Het project omvat ook onderzoek naar het waarborgen van digitale veiligheid en de integratie van de sensoren in de digitale infrastructuur.
Het lectoraat Cybersecurity & Safety draagt bij aan verschillende onderdelen van het project, gericht op het waarborgen van de digitale veiligheid. Hierbij worden verschillende onderzoeksmethoden toegepast, variërend van het interviewen van tuinders om een beter inzicht te krijgen in mogelijke dreigingen, tot het ontwikkelen en testen van een proof-of-concept in een kas.

- **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 West-Holland, CombiVliet, Reijm&Zn, Tomatoworld en Innovation Quarter

Plannen voor 2024

In 2024 zullen de onderzoekslijnen van het lectoraat worden voortgezet. De onderzoekslijn over cybersecurity-bewustzijn leverde in 2023 veel data op. In 2024 zullen op basis daarvan artikelen worden ingediend bij wetenschappelijke journals en vaktijdschriften. Op dit moment zijn er meerdere lopende projecten binnen de onderzoekslijn over de organisatie van cybersecurity. Daarnaast diende het lectoraat subsidieaanvragen in en verwachten de onderzoekers externe aanvragen voor ondersteuning voor deze onderzoekslijn. De in 2023 gestarte onderzoekslijn over kunstmatige intelligentie en cybersecurity zal meer aandacht krijgen en naar verwachting gaat het eerste gesubsidieerde project in 2024 van start. Voor de onderzoekslijn over de kwalificatie van cybersecurity-professionals is voor 2024 een subsidie aangevraagd gericht op het mkb-domein.

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 Rutger senior onderzoeker bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) en bekleedt hij de bijzondere leerstoel Governing Cybercrime bij de Universiteit Leiden. Zijn onderwijs en onderzoek richten zich op de human factor in cybercrime: wie zijn de daders, wat zijn hun werkwijzen, wat zijn de risicoprofielen van slachtoffers en hoe kunnen we de aanpak van cybercrime het beste inrichten? Rutger heeft meer dan 130 publicaties over cybercrime op zijn naam staan, waaronder meer dan 70 peer reviewed artikelen, 6 boeken en tal van vakpublicaties en rapporten. Hij is voorzitter van de Cybercrime Working Group van de European Society of Criminology (ESC) en een van de oprichters van de jaarlijkse Human Factors in Cybercrime Conference.

“Veel onderzoek is nu of heel fundamenteel of juist praktijkgericht. Ik geloof in het samenbrengen van die twee perspectieven en het kijken over de grenzen heen. Onderzoek op cybergebied is complex en vraagt om het beoordelen van vraagstukken vanuit verschillende perspectieven.”

Wat doet het lectoraat Cybercrime & Cybersecurity?

Het doel van het lectoraat Cybercrime & Cybersecurity is om het mkb, overheden en publieke instanties in Nederland op praktische wijze te helpen meer digitaal veilig en bewust te worden. We richten ons op het versterken van hun kennispositie, om uiteindelijk het aantal slachtoffers van cyberaanvallen te verminderen en de impact ervan te beperken.

Het onderzoek binnen het lectoraat richt zich op vier onderzoekslijnen:
- De aard en omvang van slachtofferschap.
- De aard van cybercriminaliteit.
- Het vergroten van cyberweerbaarheid.
- 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

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

Om ondernemers aan te sporen hun cyberweerbaarheid te verhogen, is in dit project een interventie ontwikkeld. De interventie analyseert de cybersecurity van bijna 2.000 ondernemers en richt zich op drie basisprincipes van veilig digitaal ondernemen: het inventariseren van kwetsbaarheden, het uitvoeren van updates en het voorkomen van malware. Onderdeel van deze interventie is het bieden van een handelingsperspectief voor deze drie maatregelen. De effectiviteit van de maatregelen is gemeten met een geautomatiseerde kwetsbaarhedenscan op de openbaar toegankelijke digitale infrastructuur van de ondernemers.

Tijdens de eerste meting werden 1.975 geautomatiseerde kwetsbaarhedenscans uitgevoerd. Vervolgens zijn op maat gemaakte adviesrapporten verstuurd naar 1.399 van deze bedrijven. Hierbij is gevarieerd met drie vormen van risicocommunicatie: sociale norm, geanticipeerde spijt en geen risicocommunicatie. Een controlegroep van 576 gescande bedrijven ontving geen adviesrapport. Met een nameting werd de effectiviteit van de verschillende vormen van communicatie bij alle 1.975 ondernemingen getest. Bedrijven die de risicocommunicatie geanticipeerde spijt ontvingen, bleken significant meer maatregelen te hebben genomen om hun cyberweerbaarheid te verhogen. Een kanttekening hierbij is dat deze groep bij de voormeting minder maatregelen nam dan de andere groepen. Op basis van deze resultaten en de geleerde lessen zal de interventie worden doorontwikkeld.

- **In samenwerking met:** Threadstone (ontwikkelaar van de scan) en PVO Den Haag

Criminele jeugdnetwerken in een digitaliserende samenleving

Een integrale aanpak is noodzakelijk voor zowel het verkrijgen van zicht op als de aanpak van cybercriminaliteit. Dit onderzoek biedt lokale veiligheidspartners handvatten om gezamenlijk zicht te krijgen op cybercriminele jeugdnetwerken en mogelijkheden voor de integrale aanpak daarvan. De beoogde resultaten van het onderzoek zijn een methodiekontwikkeling voor lokale veiligheidscoalities en handreikingen voor een integrale aanpak.

Deelconclusie: uit interviews met praktijkprofessionals blijkt dat lokale veiligheidspartners nauwelijks zicht hebben op cybercriminele jeugdnetwerken. Dit lijkt voornamelijk te komen doordat de informatievoorziening voor het in kaart brengen van dergelijke netwerken nog te veel leunt op straatinformatie, terwijl jongeren die betrokken zijn bij cybercrime niet op straat te vinden zijn.

Op basis van de netwerken die wel in beeld zijn, ontstaat het beeld dat deze netwerken ontstaan en groeien door offline sociale banden (bijvoorbeeld vrienden en familieleden), en door online ontmoetingen (bijvoorbeeld op Telegram). Verder lijkt er sprake te zijn van een verwevenheid tussen traditionele criminaliteit en cybercrime. Zo kan bijvoorbeeld het geld dat verkregen is via cybercrime worden geïnvesteerd in drugshandel,

en zijn sommige cyberdaders betrokken bij geweldsincidenten die ook lijken te kunnen worden gelinkt aan cybercrime.

- **Gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR, RIEC Noord-Nederland, OM, politie en gemeenten

Human Factor in Cyber Security Lab

Hoe (on)veilig gedragen medewerkers van bedrijven zich nu echt, 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 waar we exploratief praktijkgericht onderzoek doen, met een sterke connectie met zowel het onderwijs als de praktijk. Onderzoekers, professionals en studenten werken in het lab samen om werkbare oplossingen voor onveilig online gedrag te vinden. De kracht van het lab ligt in de sterke verbinding tussen onderzoek, onderwijs en praktijk. Ook in 2023 konden studenten er stage lopen en interventies ontwikkelen en testen. Studenten Information Security Management (ISM) voerden social engineering aanvallen uit bij verschillende bedrijven die zich daarvoor hadden opgegeven. Zij probeerden fysiek of digitaal bij de bedrijven binnen te komen om gevoelige informatie te achterhalen. Vervolgens gaven de studenten adviezen om de cyberweerbaarheid van de organisatie te verbeteren.

Plannen voor 2024

In 2024 zetten we ons verder in voor de ontwikkeling van de onderzoekslijn gericht op daders van cybercrime en de aanpak van cybercrime. Speciale aandacht daarbij gaat uit naar evidence-based interventies. We streven naar een betere kennisbasis over daders, slachtoffers en effectieve methoden in de aanpak van cybercriminaliteit. Daarnaast blijven we inzetten op de doorontwikkeling van labs, omdat dit een hele goede manier is om onderzoek, onderwijs en de praktijk aan elkaar te verbinden.

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 veiligheid bij Cyber Defence Solutions. Gerard werkte tien jaar in de telecommunicatie-industrie en vervulde daarna verschillende functies binnen Secure Communications & Information Systems van Thales Nederland. Hij deed promotieonderzoek bij het Centrum Wiskunde en Informatica (CWI) en promoveerde aan de Vrije Universiteit. Tot 2015 bleef Gerard als deeltijd postdoc onderzoeker verbonden aan het CWI.

“ Wiskunde is een universele taal om problemen te beschrijven en oplossingen te vinden, om te abstraheren en vervolgens de oplossing te optimaliseren. Ook in de cybersecurity kunnen we veel uit de wiskunde toepassen. ”

Wat doet het lectoraat Network and Systems Engineering Cyber Security?

Om de digitalisering te versnellen, moeten netwerken en systemen efficiënte samenwerking tussen mensen en organisaties bevorderen en tegelijkertijd cyberweerbaarheid waarborgen. Dit vormt het onderzoeksgebied van het lectoraat Network and Systems Engineering Cyber Security. Om zowel nieuwe als bestaande netwerken en systemen veilig te houden, is het noodzakelijk dat de technologie helpt toekomstige dreigingen tijdig te detecteren en maatregelen te treffen om een zo hoog mogelijke weerbaarheid te bereiken. Door vanuit het perspectief van een aanvaller te denken, kunnen we de beste verdediging ontwikkelen.

Het onderzoek binnen het lectoraat richt zich op drie onderzoekslijnen:
- Data centric security.
- Cyberweerbare infrastructuren.
- Aanvalstechniek om beter te verdedigen.

Samenwerking met onderwijs

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

WAT WE DOEN

Uitgelichte projecten

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

De vaardigheden van offensieve beveiliging, zoals reverse engineering en software-exploitatie, zijn cruciaal in softwarebeveiliging. Om deze vaardigheden te ontwikkelen, oefenen studenten met kwetsbare programma’s. Een uitdaging hierbij is dat zodra zo’n programma bekend wordt, volledige oplossingen snel online beschikbaar zijn. Dit project richt zich op het gebruik van taalmodellen om een reeks van zulke kwetsbare programma’s te creëren. Deze programma’s zijn zodanig verschillend van een basisprogramma, dat elke student in een opleiding over software-exploitatie een unieke uitdaging krijgt. Het uiteindelijke doel van dit project is een werkend systeem te ontwikkelen dat opdrachten genereert volgens vooraf bepaalde criteria, speciaal voor gebruik in het onderwijs.

Het ontwikkelen van OT-malware in cyberweerbare infrastructuren, geschikt voor onderwijs en onderzoek

De vaardigheden van offensieve beveiliging, zoals het ontwikkelen van malware, zijn belangrijk in de beveiliging van cyberweerbare systemen. Deze systemen worden toegepast in productie-en kritische infrastructuur en bestaan uit een combinatie van IT-,OT- en IoT-middelen. Het ontwikkelen van offensieve beveiligingsprogramma’s biedt inzicht in hoe deze cyberweerbare systemen verdedigd moeten worden. Als onderdeel van dit project is malware ontwikkeld die in een laboratoriumopstelling kan worden ingezet als cyberdreiging. Deze dreiging moet door studenten in praktische opdrachten worden gedetecteerd.

Plannen voor 2024

In 2024 zal het lectoraat het onderzoek naar aanvalstechnieken intensiveren en deze ook toepassen binnen de onderzoekslijn cyberweerbare systemen. ‘Verdedigen vanuit de aanval’ is hierbij het motto. Door studenten en onderzoekers een beter begrip van aanvalstechnieken bij te brengen, kunnen nieuwe verdedigingstechnieken worden onderzocht en onderwezen. Hierdoor wordt waardevolle praktijkkennis uitgebreid en overgedragen aan studenten. Bij het verdedigen tegen nieuwe dreigingen is het essentieel om relevante informatie over cyberdreigingen te delen. Binnen de onderzoekslijn data centric security worden bestaande en nieuwe informatiebeveiligingstechnieken onderzocht om informatie sneller en effectiever te kunnen delen. Het beveiligen van de informatie zelf, in plaats van de systemen die informatie transporteren en opslaan, zal naar verwachting steeds relevanter worden. Ook dit veranderende concept heeft implicaties voor het opsporen van cyberdreigingen. Onderzoek op dit gebied zal later in het onderwijs worden toegepast.

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. Daarvoor werkte Peter bij de Technische Universiteit Delft. Zijn onderzoek was daar gericht op Safety en Security Science in het Centrum voor Veiligheid in de Zorg en hij was module manager van het vak Health System Management. Zijn expertise op het gebied van risicomanagement en cybersecurity strekt zich uit over diverse domeinen, waaronder gezondheidszorg en ziekenhuizen, smart cities, luchtverkeersleiding, marine en risicobeheer in verkeerstunnels. Peter behaalde zijn doctoraat in cognitieve psychologie en ergonomie aan de Vrije Universiteit Amsterdam. Hij heeft uitgebreide onderwijs- en onderzoekservaring op verschillende gebieden, zoals psychologie, sociale en culturele wetenschappen en informatica. Hij publiceerde o.a. over organisatieleren, Shared Mental Models, Safe by Design, het gebruik van AI-coaching/robotica en besluitvorming in commando- en controlecentra.

“ De samenwerking tussen cyber risk managers in Nederland en daarbuiten moet beter, om voldoende weerbaar te zijn tegen toekomstige bedreigingen in cyberspace. ”

Wat doet het lectoraat Risk Management & Cyber Security?

Het lectoraat Risk Management & Cyber Security onderzoekt hoe effectief cyberrisicomanagement eruitziet en welke risicomodellen en hulpmiddelen daarvoor nodig zijn. De focus ligt op besluitvormingsprocessen en de governance van cyberrisicomanagement, en op hoe organisaties cyberrisico’s kunnen voorkomen en beperken. Daarnaast analyseren de onderzoekers hoe organisaties effectief kunnen reageren op cyberrisico’s, waarbij ze zich richten op de benodigde voorbereiding. Hierbij hoort ook onderzoek naar effectieve manieren om schade en uitval van diensten door een cyberaanval te beperken. Het lectoraat kijkt ook naar de rol en betekenis van publiek/private samenwerkingsverbanden op het gebied van cybersecurity, de effecten van cyberaanvallen op organisaties en de rol die overheden en toezichthouders (kunnen) spelen om de cyberweerbaarheid van organisaties te versterken.

Het onderzoek binnen het lectoraat richt zich op drie onderzoekslijnen:
- 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

Cyber Security Living Lab

Het Cyber Security Living Lab, gevestigd in de Dutch Innovation Factory, is een nieuw project dat vanaf 2024 het cybersecurityonderwijs en -praktijk wil vernieuwen. Het lab richt zich op het opzetten van een eigen Security Operations Center (SOC) voor dreigingsmonitoring, incidentrespons en shared risk management, gericht op het mkb en bedrijven in de Dutch Innovation Community. Studenten doen praktijkervaring op en bedrijven worden ondersteund in het omgaan met cybersecurityrisico’s. Het lab bevordert kennisuitwisseling tussen academisch onderzoek en de industriële praktijk, wat innovatieve oplossingen voor cyberbeveiliging moet opleveren. Daarnaast streeft het lab naar een levendige gemeenschap van studenten, docenten en professionals die samenwerken aan verbetering van cyberbeveiligingsrisicobeheer. In het lab bundelt De Haagse Hogeschool krachten met verschillende partijen, waaronder mboRijnland, Pinewood, SURF en andere partners in de Dutch Innovation Community.

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 SSSM 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 officiële start van de minor staat gepland in februari 2024.

Plannen voor 2024

In 2024 wil het lectoraat voortbouwen op wat in 2023 is begonnen. In het Cyber Security Living Lab werken we aan het Security Operations Center van de toekomst. We ronden het Samen Digitaal Veilig-project af en starten het vervolg.

We beginnen met het NWO LIAT-project: Learning in Advance of the Threat. We werven fondsen voor onder andere PhD-projecten voor onze onderzoekers en richten ons op teamuitbreiding. Op 14 november 2024 vindt de intreerede van lector Peter Roelofsma plaats, gevolgd door het symposium Cyber Security Living Lab op 15 november 2024.

In 2023 werkten 6 promovendi binnen het kenniscentrum aan hun proefschrift. Deze promovendi zijn verbonden aan verschillende universiteiten. Een zevende PhD-kandidate start per 1 januari 2024.

Hacktivism: honourable cause or serious threat?

Using diverse theoretical backgrounds rooted in social psychology and criminology, this project investigates: the motivations for individuals to engage in hacktivism and the process they follow to become hacktivists; the reasons that prompted them to use hacking as their main form of protest; the organizational dynamics within different hacktivists' groups and networks.

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

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

Money mules are key in the execution of financial-economic cybercrimes. By using both qualitative and quantitative methods, the aim of the current dissertation is to explain how money mules are recruited by criminal networks. More knowledge on the involvement mechanisms of cybercrime has important implications for research and practice.

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

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

This PhD project aims to get a better understanding of the different involvement mechanisms and risk factors that play a role in the initiation process for financial-economic cyber-enabled crime (e.g. phishing). Furthermore, we aim to develop and evaluate an intervention aimed at disrupting this process.

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

Nature and prevention of ransomware

This research project will investigate the crime-commission process of ransomware attacks to gain insight into how cybercriminals and victims act and the aspects that are essential for criminals to successfully carry out the crime. Moreover, it will provide a starting point for the development of interventions to counter ransomware.

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

Ethics of care as a corporate governance model

In this PhD project, a corporate governance model that facilitates the implementation of security by design is suggested. It broadens our view on cybersecurity, highlighting social aspects. Integrating care ethics with stakeholder theory, the novel model will emphasize relationships, empowerment, and the obligation of care.

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

Victimisation in a digitised Society: Perception and Impact

Research into the impact of Image Based Sexual Abuse and Romance Scams, the public discourse on victimization and the relationship between these two to gain further insight into the depth of impact, victim- and self-blaming.

- **Promovendus:** Raoul Notté
- **Betrokken Universiteit:** Tilburg University

PhD-Day 2023

In maart was de Dutch Innovation Factory (DIF) het toneel voor PhD-Day, een jaarlijks terugkerend evenement georganiseerd 'door onderzoekers, voor onderzoekers'. Tijdens PhD-Day kregen promovendi van het kenniscentrum Cyber Security een kans om hun onderzoek te presenteren en feedback te ontvangen van collega-onderzoekers en andere experts op het gebied van cybercriminaliteit en cybersecurity. De PhD-kandidaten deden nieuwe ideeën op over hun theorie, onderzoeksmethoden en de implicaties van hun onderzoek.

Onze onderzoekers vormen samen met ons programmateam het hart van het kenniscentrum Cyber Security. Wil je meer over hen weten, kijk dan op onze website.


Asier Moneva


Merel van Leuken


Herman de Bruine


Marco Romagna


Pieter Burghouwt


Susanne van 't Hoff-de Goede


Assia Kraan


Emiel Kerpershoek


Jasmijn Boeken


Luuk Bekkers


Bernard van der Helm


Eric ten Bos


Daniel Meinsma


Henk van Ee


Joeri Loggen


Maaike van der Wal


Maaike Vergeer


Céline Kreffer


Mike Gilhespy


Niek Jan van den Hout


Marinus Maris


Milou Andriessen

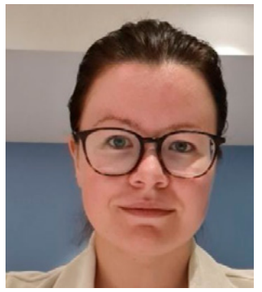

Luca de Boer

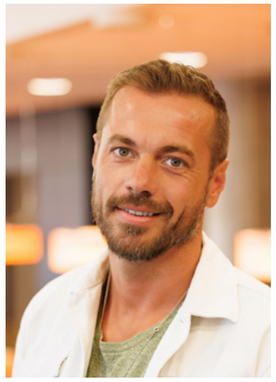

Pei-Hui Lin


Sifra Matthijsse


Matej Dolinsek


Jan Treur


Natalia Zwarts


Raoul Notté


Ligaya Butalid


Michelle Ancher


Nick Barelds


Saman Tamo


Yolanda van Setten

Expertisenetwerk Cyberweerbaar NL

In 2023 ging het expertisenetwerk Cyberweerbaar NL van start. Cyberweerbaar NL is een consortium van drie hogescholen: De Haagse Hogeschool (penvoerder vanuit het kenniscentrum Cyber Security), Hogeschool Saxion en NHL Stenden Hogeschool. Samen met studenten, docenten, cyberprofessionals, onderzoekers en een groot aantal partners, ontwikkelen we hoogwaardige kennis op het gebied van cybersecurity binnen organisaties. Onze focus ligt op het gedrag en de houding van mensen. Wij brengen in kaart welke gedrags- en houdingsaspecten cyberweerbaarheid beïnvloeden en hoe organisaties deze aspecten kunnen verbeteren.

Op 22 september 2023 vond het eerste evenement van Cyberweerbaar NL plaats. Tijdens een besloten symposium op De Haagse Hogeschool ontvingen we ruim 90 deelnemers, waaronder (cyber)burgemeesters, politie, het Openbaar Ministerie, onderzoekers en partners van Cyberweerbaar NL. Tijdens deze inspirerende middag gingen de deelnemers met elkaar in gesprek over de governance van cybercrime. Het programma bestond uit keynotes, posterpresentaties, workshops en een rondetafelgesprek, waarin burgemeesters, politie en het Openbaar Ministerie de aanpak van cybercriminaliteit vanuit verschillende invalshoeken bespraken.

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

Literatuurstudie: Testen en oefenen ter bevordering van informatiebeveiliging door decentrale overheden

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. Op basis van het onderzoek zijn aanbevelingen gedaan om het testen en oefenen bij medeoverheden te stimuleren.

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

PROJECTENOVERZICHT LECTORATEN

Digitale veiligheid van smart cities

Het doel van dit project is om te bepalen hoe digitaal veilig smart city-toepassingen (zoals slimme verkeersregelinstallaties en slimme camera's) zijn, en concrete oplossingen te bieden om die veiligheid te verbeteren. De beoogde resultaten zijn richtlijnen voor governance, risicoanalyse en digitale veiligheid met betrekking tot smart cities en oplossingen voor deelnemende gemeenten om smart-city toepassingen veiliger te maken.

- **Lectoraat:** Cyber Security & Safety
- **In samenwerking met:** NHL Stenden, gemeenten, HSD, VNG

Cyberveiligheid in de medische zorg

Dit onderzoek richt zich op het verkrijgen van een beter inzicht in de cybersecurityrisico's waaraan ziekenhuizen en patiënten worden blootgesteld door de toenemende digitalisering van medische technologie. Het omvat ook het identificeren van noodzakelijke en mogelijke maatregelen om veilig gebruik van deze technologie te waarborgen, zowel wat betreft de veiligheid van de digitale medische systemen als het bewustzijn van risico's onder interne en externe betrokkenen.

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

Verbeteren van veilig digitaal gedrag

Bewustwording op het gebied van cybersecurity blijkt in alle lagen van de bevolking aanzienlijk tekort te schieten. De eerste stap naar verbetering van deze bewustwording is een effectieve meetmethode, wat een grote uitdaging blijkt te zijn. Het resultaat van dit onderzoek is een instrumentarium voor het meten van cybersecuritybewustzijn.

- **Lectoraat:** Cybersecurity & Safety

Verbeteren van veilig digitaal gedrag van leerlingen

In de praktijk blijkt dat leerlingen in het basisonderwijs een aanzienlijk gebrek aan bewustzijn hebben op het gebied van cybersecurity. Dit onderzoek richt zich op het identificeren van factoren die het veilige digitale gedrag van kinderen tussen 8 en 12 jaar beïnvloeden, evenals op mogelijke interventies om deze factoren te verbeteren.

- **Lectoraat:** Cybersecurity & Safety
- **In samenwerking met:** Koninklijke Bibliotheek, Kennisnet, SLO en Curriculum.nu

Qualification of Information Security

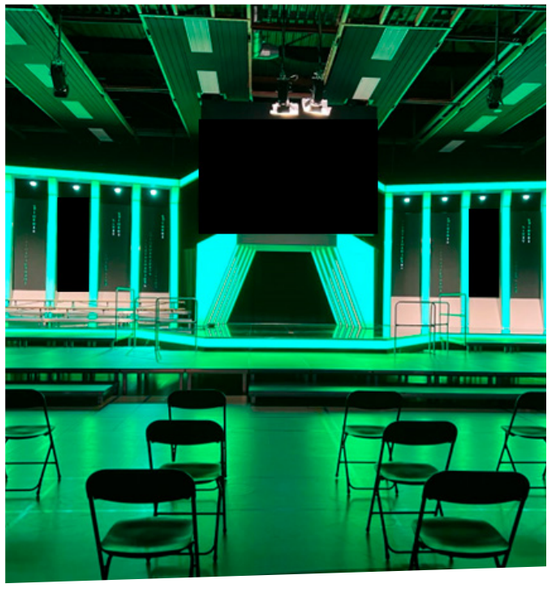
In de huidige informatiemaatschappij wordt het beschermen van informatie steeds belangrijker, maar ook moeilijker. Daarom zijn goed opgeleide en ervaren professionals essentieel. Uit eerder onderzoek blijkt dat binnen de cybersecuritybranche grote behoefte bestaat aan een breed gedragen, uniform en internationaal geaccepteerd kwalificatiesysteem. Dit onderzoek richt zich op het ontwikkelen van dit benodigde kwalificatiesysteem.

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

Re_B00TCMP

Re_B00TCMP is een preventieve interventie gericht op jongeren met affiniteit voor IT die geneigd zijn de grenzen online op te zoeken. Het doel van deze interventie 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. Daarnaast is er een apart programma voor ouders en docenten om meer inzicht te krijgen in de online leefwereld van jongeren. De planevaluatie en procesevaluatie van dit onderzoeksproject zijn afgerond. De effectevaluatie start in 2024.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Ministerie van Justitie & Veiligheid en het CCV
- **In samenwerking met:** Politie (COPS)



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

Gebruikersgerichte aanpak voor bruikbare cybersecurity

In dit project wordt onderzocht hoe mensen op de werkvloer geholpen kunnen worden om zich digitaal veiliger te gedragen door middel van gebruikersgericht ontwerp. Het doel is een gebruikersgerichte aanpak te ontwikkelen voor bruikbare cybersecurity, gebaseerd op wetenschappelijke inzichten over gedrag en design, toegepast in de praktijk. Het resultaat zal een handelingskader zijn dat een gebruikersgerichte aanpak beschrijft om bruikbare cybersecurity te realiseren.

- **Lectoraat:** Cybercrime & Cybersecurity
- **Gefinancierd door:** SIA KIEM GoCi
- **In samenwerking met:** Hogeschool Utrecht, Informaat, Infosequre en TO2/TNO

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

In dit project wordt onderzocht hoe vaak Nederlandse burgers en bedrijven slachtoffer worden van ransomware, hoe ze reageren met betrekking tot onderhandelen, betalen en melden en hoe zich dit verhoudt tot de adviezen van de politie en IT/cybersecuritybedrijven. Onderzoeksmethoden die hierbij worden gebruikt zijn vragenlijsten onder Nederlandse burgers en ondernemers die slachtoffer zijn geworden van ransomware, vragenlijsten met een hypothetisch scenario (vignet), interviews met politiemedewerkers, cybersecurityexperts en IT-dienstverleners en een expertbijeenkomst.

- **Lectoraat:** Cybercrime & Cybersecurity
- **Gefinancierd door:** Politie & Wetenschap
- **In samenwerking met:** NSCR

PROJECTENOVERZICHT LECTORATEN

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

Het doel van dit onderzoek is het vergroten van de kennis over de opkomst van jonge daders in cybercrime. We bestuderen specifiek de rol van CaaS als mechanisme voor online betrokkenheid en de mogelijkheden van CaaS om interventies te implementeren gericht op potentiële of beginnende cybercriminelen.

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

Hybridisering van criminaliteit

Dit onderzoek heeft als doel de verwevenheid van online- en offline criminaliteit in kaart te brengen. Het richt zich op het analyseren van de aard van de banden tussen daders, die vaak zowel online als offline dimensie vertonen, en op de verwevenheid van deze twee werelden in de modus operandi van verschillende delicten. Door gebruik te maken van bestaande literatuur en een media-analyse van relevante casussen wordt een typologie ontwikkeld van de hybride vorm van criminaliteit. Daarnaast beoogt het onderzoek inzicht te verschaffen in de aanpak van hybride criminaliteit in Nederland en omringende landen. Het hybride karakter van criminaliteit wordt in Europees perspectief geplaatst, aan de hand van interviews met politie en experts. Hierbij identificeren we verschillende benaderingen, good practices en uitdagingen in het bestrijden van deze vormen van criminaliteit, met als doel good practices en lessons learned te delen voor 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 heeft als doel een effectieve interventie te ontwikkelen voor een zelfverzekerde en lokale aanpak van gedigitaliseerde criminaliteit. Het 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 hoofdvraag van het onderzoek is hoe basisteams hun personeel kunnen voorbereiden op een effectieve en zelfverzekerde intensivering van de lokale aanpak van gedigitaliseerde criminaliteit. Met dit onderzoek willen we praktische handvatten bieden aan basisteams, zodat zij hun personeel kunnen voorbereiden op een succesvolle en zelfverzekerde aanpak van gedigitaliseerde criminaliteit op lokaal niveau.

- **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 de bestaande, wetenschappelijke kennis over daders, slachtoffers, crimescripts en praktische aanpakken van cybercriminaliteit overzichtelijk en toegankelijk in kaart te brengen. Vervolgens willen we deze kennis met ervaren politiemensen vertalen naar praktische handvatten voor de aanpak van gedigitaliseerde criminaliteit (cyber-enabled crime) en cybercrime (cyber-dependent crime).

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

Procesevaluatie 2023 in het kader van de City Deal Lokale Weerbaarheid Cybercrime

Sinds 2020 zijn er in het kader van de City Deal Lokale Weerbaarheid Cybercrime tientallen innovatieve cyberprojecten op lokaal niveau opgestart om de cyberweerbaarheid van inwoners en ondernemers te versterken. Met procesevaluaties worden de lessen die uit deze cyberprojecten zijn geleerd in kaart gebracht, met als doel toekomstige cyberprojecten succesvol op te starten en verder te ontwikkelen.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** CCV
- **In samenwerking met:** Hogeschool Saxion en NHL Stenden Hogeschool

Naar een toekomstbestendige civielrechtelijke afdoening van online fraude

Steeds meer mensen worden slachtoffer van online fraude en schakelen een civiele rechtsvertegenwoordiger in om de schade op de dader te verhalen. Deze groei benadrukt de noodzaak om inzicht te krijgen in de civielrechtelijke procedure en de gevolgen hiervan voor slachtoffers, daders en de maatschappij. In dit onderzoeksproject staat de volgende hoofdvraag centraal: 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 einddoel is om concrete handvatten te ontwikkelen voor slachtoffers en maatschappelijke organisaties om deze interventie succesvol in te zetten.

- **Lectoraat:** Cybercrime & Cybersecurity
- **In opdracht van:** Stichting Achmea Slachtoffer en Samenleving en Politie Nederland
- **In samenwerking met:** Slachtofferhulp Nederland, Ministerie van Justitie en Veiligheid, Fraudehelpdesk, CCV, LAVG Gerechtsdeurwaarders B.V., Stichting Achmea Rechtsbijstand, Brancheverenigingen Horus en Hogeschool Saxion

Stolen Datamarkets on Telegram

A project on how stolen data markets work on Telegram and how they can be disrupted. The first part of the project described how these markets functioned through a crime script analysis and proposed situational crime prevention measures to disrupt them. In the second part (ongoing), we want to identify the factors that influence the popularity of the markets in order to identify potential points of intervention.

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

Social Media as Online Offender Convergence Settings: Exploring the Cybercrime Landscape on Telegram

Op Telegram zijn er veel openbare groepen waar illegale producten en diensten worden verhandeld, soms met duizenden leden per groep. Dit platform biedt op deze manier toegang tot de componenten die nodig zijn voor cybercriminaliteit, zoals geldezels en kant-en-klare phishingkits. Toch is er nog vrijwel geen wetenschappelijk onderzoek gedaan naar Telegram als platform voor cybercriminaliteit. Het doel van dit project is om meer inzicht te krijgen in de cybercriminele activiteiten op Telegram. We maken hierbij gebruik van unieke longitudinale data: in een periode van een jaar hebben we alle content verzameld uit 25 Telegram groepen, wat resulteerde in meer dan 4 miljoen berichten.

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

Online Ads Against Cybercrime

A project on how online ads can be used to cut pathways into entry-level cybercrimes. In this project, we investigated the use of online ads to deter potential cybercriminals and divert them towards pro-social alternatives in cyber security in several phases: (1) exploring whether the ads reached the target population of potential cybercriminals; (2) determining which type of ad generates the most engagement among the target audience; and (3) examining whether online ad campaigns reduce DDoS attacks. The project was launched to investigate the use of text ads on Google, and is currently investigating the performance of video ad campaigns on YouTube.

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

PROJECTENOVERZICHT LECTORATEN

DurableCASE

In het project DurableCASE werken verschillende partijen, waaronder De Haagse Hogeschool, samen aan oplossingen voor samenwerkende robotvoertuigen in de agrarische sector. Het lectoraat Network & Systems Engineering Cyber Security voerde een risicobeoordeling uit voor de bouw van autonome robots voor de landbouwsector, en legde dit vast in een beknopte rapportage.

- **Lectoraat:** Network & Systems Engineering Cyber Security
- **Gefinancierd door:** SIA RAAK-PRO
- **In samenwerking met:** HAN Automotive Research en 24 andere partners

Cyber Security by Integrated Design (C-SIDE)

Het doel van het C-SIDE project is het ontwikkelen van een methodologie voor het ontwerpen van veilige softwaresystemen. Deze aanpak zal de niet-technische aspecten van cybersecurity integreren in de traditioneel technisch geleide benadering, om vanaf het begin van de ontwikkeling een grotere mate van beveiliging te waarborgen. Voorbeelden van deze niet-technische aspecten die van invloed zijn op softwareontwikkeling zijn menselijk gedrag, teamstructuren, personeelsbeheer, beveiligings- en betrouwbaarheidscultuur, en de financiële budgetten binnen organisaties.

- **Lectoraat:** Risk Management & Cyber Security
- **Gefinancierd door:** NWA Cybersecurity
- **In samenwerking met:** Universiteit Leiden, NCSC, Ministerie van Justitie & Veiligheid, SURFSara en LUMC

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. Het lectoraat Risk Management & Cybersecurity brengt in dit project in kaart hoe Samen Digitaal Veilig kan bijdragen aan het verbeteren van de cyberweerbaarheid van bedrijfsketens. We onderzoeken hoe bedrijven gestimuleerd kunnen worden om cyberweerbaar gedrag te vertonen en welk effect het SDV-platform heeft op het 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

Learning & Innovation Ahead of the Threat

Om ons land veilig te houden, is het essentieel om proactief om te gaan met toenemende (cyber)veiligheidsbedreigingen. Dit vraagt om effectieve samenwerking tussen publieke organisaties en kennisinstellingen. Huidige learning communities richten zich voornamelijk op kennisuitwisseling en minder op de daadwerkelijke ontwikkeling en implementatie van innovatieve veiligheidsoplossingen. Dit project heeft als doel om ontwerprichtlijnen, strategieën en methoden te ontwikkelen en een ondersteuningsplatform voor het opzetten van effectieve learning communities op het gebied van veiligheid. De Haagse Hogeschool is mede-aanvrager en wordt vertegenwoordigd door onder andere het lectoraat Risk Management & Cyber Security.

- **Lectoraat:** Risk Management & Cyber Security
- **Gefinancierd door:** NWO
- **In samenwerking met:** Saxion Hogeschool, Universiteit Twente, TNO, Politieacademie, CVD, HSD, Space53, Gemeente Den Haag, ICSS, Koninklijke Landmacht, SAAB Defensie, Achmea, NIPV, TechYourFuture, Dutch Innovation Cluster, Brandweer Amsterdam-Amstelland, Politie Nederland, AI-Maps en VNG

VOORUITBLIK 2024

Groei van het kenniscentrum

In 2024 zal het kenniscentrum Cyber Security zijn groeiambitie verder vormgeven. In samenwerking met de faculteiten IT & Design, Bestuur, Recht & Veiligheid en Technologie, Innovatie & Samenleving zullen twee nieuwe lectoraten worden opgericht. Een daarvan richt zich op de juridische aspecten van cybersecurity. Het andere nieuwe lectoraat versterkt het technische portfolio van het kenniscentrum. De ambitie is om in 2024 de basis hiervoor te leggen en de benodigde procedures te doorlopen. Tegelijkertijd zal het kenniscentrum onderzoek starten binnen deze thema's.

Daarnaast zal er in 2024 een stevige basis worden gelegd voor verdere professionalisering van de ondersteuning vanuit het kenniscentrum naar de lectoraten en lopende projecten. Ook worden de mogelijkheden voor internationale samenwerking verder onderzocht.

Bijdrage aan (vernieuwing) van minor-, bachelor- en masteronderwijs

De integratie met het onderwijs wordt in 2024 verder versterkt. De opleiding HBO-ICT biedt al een differentiatie Cyber Security Technology. Bij BRV wordt de minor Cyber Security aangeboden en dragen onze onderzoekers met hun inhoudelijke expertise en lopende projecten bij aan de nieuwe minor Cybercrime. Ons kenniscentrum levert kerndocenten voor de masteropleiding Cyber Security Engineering en blijft sparringpartner en gastdocent voor de masteropleiding Risk Management. Bij het Human Behaviour Research Semester van HBO-ICT/ISM fungeren onze onderzoekers als research coach. Bovendien zijn onze onderzoekers ieder semester opdrachtgever van stage- en afstudeeropdrachten. Verder zal de samenwerking met de Dutch Innovation Factory in Zoetermeer worden geïntensiveerd.

Onderwijs wordt direct gekoppeld aan praktijkgericht onderzoek in onze labs. Naast het bestaande Human Factor in Cybersecurity Lab worden er een nieuw Living Lab en Cyber Security simulatielab ontwikkeld.

Kennisagenda 'Samenwerken aan transities'

In 2024 zet De Haagse Hogeschool een volgende stap in het versterken van ons praktijkgericht onderzoek. In de nieuwe kennisagenda 'Samenwerken aan transities' staan drie thema's centraal: rechtvaardig samenleven, transitie naar duurzaamheid en digitale toekomst. Het kenniscentrum Cyber Security is samen met het kenniscentrum Digital Operations & Finance trekker van het thema digitale toekomst, dat een impact moet hebben op de hele Haagse Hogeschool.

Thema Digitale Toekomst

Hoe de digitale toekomst eruit gaat zien, bepalen we nú. We moeten keuzes maken over hoe mens, organisatie en techniek het beste kunnen samenwerken. De digitale toekomst moet volgens De Haagse Hogeschool een toekomst zijn waarin burgers en professionals digitale technologieën inzetten om een samenleving vorm te geven waarin mensen veilig, gezond en goed kunnen leven, gelijke kansen hebben en een positieve impact hebben op het natuurlijke systeem. Als kennisinstelling willen wij hieraan bijdragen door onze studenten en organisaties om ons heen de kennis en tools te geven om die toekomst vorm te geven.

Binnen het thema digitale toekomst ligt de focus op veiligheid en weerbaarheid en de toekomst van werk. We richten ons daarbij op het opzetten van een hogeschoolbrede onderzoeksinfrastructuur die hogeschoolbreed bijdraagt, zoals een expertbank voor data science. Daarnaast zien we het als onze taak om nieuwe onderzoeken te initiëren, zowel binnen als buiten het kenniscentrum. Op deze manier dragen we bij aan de algehele ontwikkeling van De Haagse Hogeschool op dit cruciale thema.

DE HAAGSE HOGESCHOOL

CENTRE OF EXPERTISE CYBER SECURITY 2023

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

LECTORATEN

Cybercrime & Cybersecurity
Rutger Leukfeldt

Cyber Security & Safety
Marcel Spruit

Network & Systems Engineering Cyber Security
Gerard Hoekstra

Risk Management & Cyber Security
Peter Roelofsma

IMPACT

KENNISDOMEIN

- **36** deelname aan conferenties
- **8** organisatie van conferenties
- **25** publicaties (20 peer-reviewed)
- **20** workshops / lezingen
- **15** commissies
- **5** boek(hoofdstukken) (2 peer-reviewed)
- **4** internationale netwerken

113

ONDERWIJS

- **67** studentbegeleiding (afstuderen, stage, projecten)
- **96** (gast)colleges / workshops
- **2** ontwikkeling onderzoekslijn curriculum
- **19** ontwikkelde/uitgevoerde minor of keuzemodule
- **7** ontwikkelde onderwijs-materialen
- **7** bijdrage curriculum-vernieuwing

198

WERKVELD/MAATSCHAPPIJ

- **30** projecten
- **3** rapporten
- **42** workshops / presentaties
- **4** adviestrajecten
- **2** tools
- **1** symposium

82

19 FTE

CAPACITEIT PERSONEN

40

waaronder **6** promovendi

HIGHLIGHTS

- Start SPRONG Expertisenetwerk Cyberweerbaar NL: een breed consortium met focus op gedrag en houding van de mens, voor een cyberweerbaar Nederland
- 'What (s)can we do?' evidence based gedragsinterventie: toename in cyberweerbaarheid na geautomatiseerde kwetsbaarhedenscan en op-maat adviesrapportages onder 1975 organisaties

BELANGRIJKSTE PARTNERS

nscr
MKB Nederland
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
- Communicatie Multimedia Design (CMD)
- Integrale Veiligheidskunde (IVK)
- LAW
- Master of Cyber Security Engineering (MCSE)

Wil jij op de hoogte blijven van ontwikkelingen in het kenniscentrum Cyber Security? Volg ons dan op **LinkedIn** of abonneer je op onze **nieuwsbrief.** Heb je vragen of opmerkingen, wil je samenwerken of meer weten over ons onderzoek? Kijk dan op onze **website** of neem contact met ons op via **cybersecurity@hhs.nl.**

Adres- en contactgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

cybersecurity@hhs.nl

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