# 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. Mathias Björkqvist**
lector Network & Systems Engineering Cyber Security

**Dr. Jelle Groenendaal**
lector Risk Management & Cyber Security


Jaarupdate 2021

let's change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL


# Inhoud

# Terugblik 2021

Met gepaste trots kijken we terug naar een aantal hoogtepunten en succesvolle projecten die de onderzoekers van het Centre of Expertise Cyber Security in 2021 hebben gerealiseerd.

Onderzoekers van het lectoraat Cybercrime & Cybersecurity werkten in het meerjarig RAAK-project Cyberweerbaarheid samen met 12 gemeenten en 4 veiligheidsallianties aan de preventie van slachtofferschap van cybercrime. Het lectoraat Cyber Security & Safety voerde een verkenning uit naar de digitale veiligheid van glastuinbouw in de Greenport West-Holland. En samen met de Dutch Innovation Factory zijn twee innovatieve labs gelanceerd, waarin samen met bedrijven en studenten wordt gewerkt aan cybersecurity vraagstukken. Ook is de masteropleiding Cyber Security Engineering, waar wij als Centre of Expertise een bijdrage aan leverden, geaccrediteerd door de NVAO.

De onderzoeksgroep is gegroeid. We hebben niet alleen nieuw onderzoekstalent binnengehaald, maar zetten ook stevig in op de ontwikkeling en professionalisering van onze onderzoekers. Binnen het Centre of Expertise zijn meerdere promovendi bezig met verdiepend promotieonderzoek op het thema.

Ten slotte is de samenwerking met onze partners geïntensiveerd. De samenwerking met de gemeente Zoetermeer is in november 2021 met nog eens vier jaar verlengd. Door het succesvolle L.INT-programma (2017-2021) is de samenwerking met het NSCR verduurzaamd. En we werken binnen het consortium C-SIDE (2021-2026) nauw samen met Universiteit Leiden dat vanuit de Nationale Wetenschapsagenda van NWO financiering heeft gekregen om cyberveiligheidsproblemen op te lossen.

En dit is nog maar een greep uit onze activiteiten. In dit jaarverslag presenteren wij ons onderzoeksprogramma en geven we een overzicht van onze resultaten in 2021.

OVER HET CENTRE OF EXPERTISE

# Cyber Security

**Het Centre of Expertise Cyber Security richt zich op het versterken van de cyberveerkracht van publieke en private organisaties die zelf in mindere mate zijn toegerust op cyberdreigingen. Door de digitalisering van onze samenleving, neemt ook het plegen van criminaliteit in de online wereld toe. Het aantal cyberaanvallen op organisaties neemt toe en de maatschappelijke en financiële schade van cybercrime is enorm. Om ons daar tegen te wapenen is praktijkgerichte kennis en expertise nodig.**

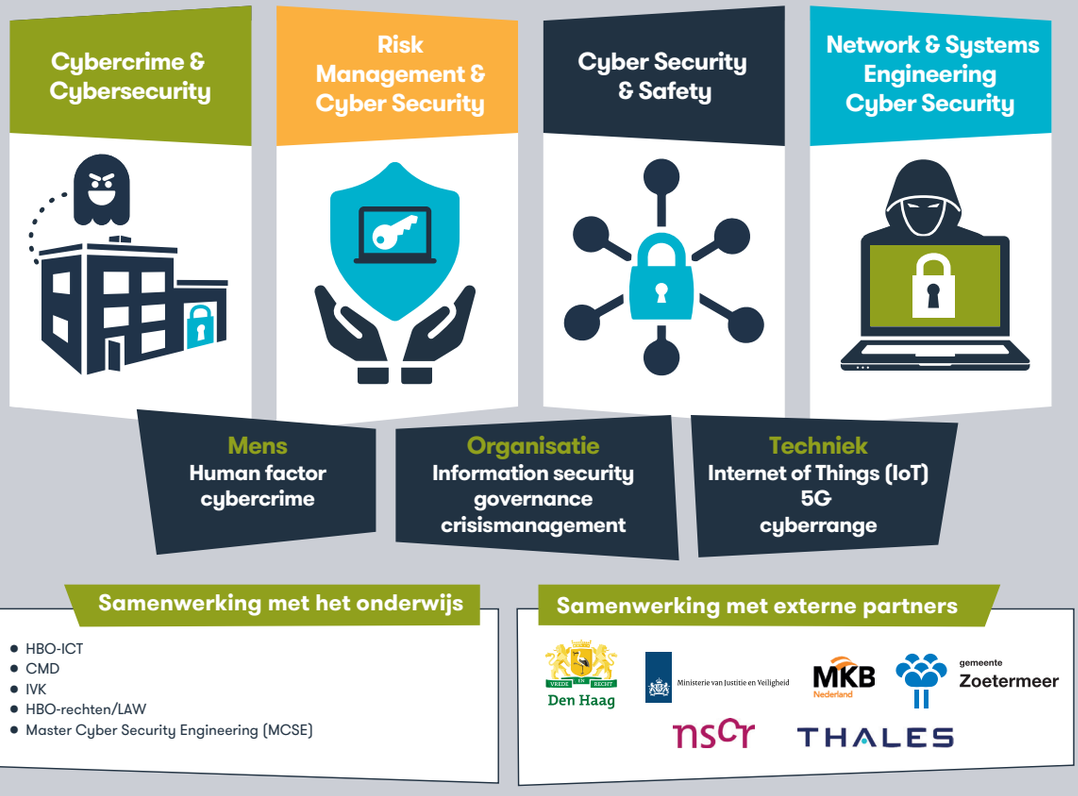
Cyberveerkracht of cyberweerbaarheid is een opkomend concept dat zowel binnen organisaties als de wetenschap steeds meer gebruikt wordt. Het concept staat voor het vermogen om cyberdreigingen te herkennen en hierop adequaat te reageren. Waar de nadruk van cybersecurity ligt op het voorkomen van cyberaanvallen, gaat het bredere concept van cyberveerkracht ervan uit dat aanvallen onvermijdelijk zijn. Het gaat dus niet meer alleen om het voorkomen van incidenten, maar ook om het beperken van de impact als onverhoopt een incident plaatsvindt. Dit vraagt om een multidisciplinaire benadering van cybersecurity.

Het onderzoek van het Centre of Expertise Cyber Security is onderverdeeld in drie thema's:

1. Mens: welke gedrag- en houdingsaspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten t.b.v. cyberveerkracht verbeteren?
2. Organisatie: welke organisatieaspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten t.b.v. cyberveerkracht verbeteren?
3. Techniek: welke technische aspecten beïnvloeden cyberveerkracht en hoe kunnen organisaties deze aspecten t.b.v. cyberveerkracht verbeteren?

Het Centre of Expertise heeft zich ontwikkeld tot multidisciplinair kenniscentrum bestaande uit vier lectoraten, namelijk Cybercrime & Cybersecurity, Cyber Security & Safety, Network & Systems Engineering Cyber Security en Cyber Security & Risk Management. Ieder lectoraat brengt specifieke expertise mee op de drie bovenstaande thema's. Door expertise van elkaar te benutten kunnen vraagstukken vanuit meerdere perspectieven worden bestudeerd. Dat maakt ons Centre of Expertise uniek ten opzichte van andere onderzoeksgroepen op het thema cybersecurity.

# Multidisciplinair onderzoek kenniscentrum Cyber Security




Ons praktijkgericht onderzoek levert kennis en inzicht op die publieke en private organisaties kunnen gebruiken om hun cyberweerbaarheid te verhogen. We richten ons op organisaties zoals lokale overheden, politie en justitie, ziekenhuizen, scholen en het midden-en kleinbedrijf. Het mkb is de backbone van de Nederlandse economie, maar wordt echter relatief vaak slachtoffer van cyberaanvallen omdat ondernemers niet de capaciteit hebben om zich hier tegen te weren. Als sector is het mkb groot, maar de omvang van individuele bedrijven is beperkt. Dat brengt kwetsbaarheid met zich mee. Ook lokale overheden (gemeenten) staan voor de uitdaging om digitale veiligheid en privacy te waarborgen bij de implementatie van nieuwe technologie en worstelen met het vertalen van beleidsprioriteiten naar concrete acties tegen cybercrime.

Voor het realiseren van impact is samenwerking en integratie met het onderwijs en samenwerking met externe partners essentieel. Het Centre of Expertise Cyber Security kent een nauwe samenwerking met de faculteit IT & Design, de faculteit Bestuur Recht & Veiligheid en de Masteropleiding Cyber Security Engineering van De Haagse Hogeschool. Het onderwerp cybersecurity is niet meer weg te denken uit relevante opleiding zoals HBO-ICT en IVK. Andersom is de praktijkervaring van docenten en het innovatieve vermogen van studenten van onmisbare waarde voor de kennisontwikkeling op het gebied van cybersecurity.

Externe partners hebben een belangrijke rol in het identificeren van de kennisbehoefte in de praktijk en zijn van belang voor de doorwerking (valorisatie en implementatie) van resultaten in de beroepspraktijk. Strategische kernpartners waar wij mee samenwerken zijn: gemeente Den Haag, gemeente Zoetermeer, ministerie van Justitie en Veiligheid, Thales, MKB-Nederland en NSCR.

Het Centre of Expertise heeft de ambitie om (verder) uit te groeien tot hét toonaangevende instituut voor praktijkgericht onderzoek op het brede terrein van cybersecurity binnen publieke en private organisaties, dat hoogwaardige, relevante en praktische toepasbare kennis ontwikkelt op het gebied van cyberveerkracht. Daarmee dragen wij bij aan het cyberweerbaarder maken van Nederland.

# WAT DOEN WIJ

Het onderzoek vindt voornamelijk plaats binnen een van de vier lectoraten (zie bijlagen voor de focus en onderzoekslijnen per lectoraat). Binnen ieder project werken we nauw samen met interne of externe partijen. Het onderwerp cybersecurity staat hoog op de landelijke en regionale agenda's en dat merken we ook aan de investeringen op kennisontwikkeling op het thema. De meeste onderzoeksprojecten die wij uitvoeren zijn daarom extern gefinancierd. We dragen bij aan de kennisontwikkeling binnen het vakgebied en maken impact in het onderwijs en het werkveld op het gebied van cybersecurity.

Studenten van onze hogeschool zijn de toekomstige professionals die na hun studie zullen bijdragen aan de cyberveerkracht van organisaties en bedrijven waar zij terecht komen. Onze onderzoekers leveren daarom op verschillende manieren een bijdrage aan het bestaand curriculum, begeleiden stageopdrachten en afstudeerders en werken aan inspirerende studentinitiatieven binnen innovatieve labs.

In 2021 hebben 13 studenten bij het Centre of Expertise stage gelopen en zijn twee nieuwe labs gelanceerd. Ook is een bijdrage geleverd aan de Masteropleiding Cyber Security Engineering, die dit jaar door de NVAO geaccrediteerd is.

Zie voor een recent overzicht van onze publicaties en media-uitingen:

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


Op de volgende pagina's volgt een overzicht van de uitgevoerde en lopende projecten in 2021.

# Subsidieprojecten

## RAAK-publiek project: Cyberweerbaarheid. Een gemeentelijk offensief ter preventie van slachtofferschap van cybercrime

Met welke interventies kunnen ambtenaren openbare orde en veiligheid de cyberweerbaarheid van burgers en bedrijven binnen hun gemeente vergroten? Middels actieonderzoek gaan professionals van gemeenten en regio's samen met onderzoekers op zoek naar effectieve interventies.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: Saxion (projectleider), NSCR, gemeenten Capelle a/d IJssel, Rotterdam, Dordrecht, Utrecht, Almere, Amersfoort, Ede, Apeldoorn, Enschede, Haarlem, Den Helder en Zoetermeer, vier regionale samenwerkingsverbanden tussen gemeente (met vertegenwoordiging vanuit 167 gemeenten), Veiligheidsalliantie Regio Rotterdam, Veiligheidscoalitie Midden-Nederland, Veiligheidsnetwerk Oost-Nederland en Noord-Holland Samen Veilig.

## RAAK-PRO project: Durable CASE

In dit project werkt een groot aantal partijen samen om oplossingen te ontwikkelen voor samenwerkende robotvoertuigen in de agrarische sector. Binnen dit project heeft het lectoraat een risicobeoordeling voor de projectpartners uitgevoerd, en daarnaast ondersteuning geboden bij het opstellen van de eisen en het architectuurontwerp en bij de validatie van de beveiliging.

- Lectoraat Network & Systems Engineering
- Projectpartners: Hogeschool Arnhem Nijmegen (projectleider), LTO Noord, Lely, Maatschap Boon, ERF, Multi Tool Trac, TU Delft, Wageningen UR, Universiteit Twente, Distribute, Fontys, Verum, TNO, Track, Almende, Rexroth, Siemens, Altramotive, Weber-Hydraulik, H2Consultancy, Holland Robotics, Robo Vally, RDW

## KIEM-project: Digitale smart cities

Smart city-toepassingen bij gemeenten zijn in opmars. De veiligheid van deze toepassingen is echter nog onderbelicht. Doel van het onderzoek is om vast te stellen hoe digitaal veilig smart city-toepassingen zijn en om concrete oplossingen aan te reiken om die veiligheid te verbeteren. Moderne verkeersregelinstallaties en camera's ten behoeve van de openbare orde en veiligheid zijn de eerste casussen.

- Lectoraat Cyber Security & Safety
- Projectpartners: NHL Stenden, gemeenten Den Haag, Zoetermeer, Apeldoorn en Eindhoven.

## HBO-postdoc: Verbeteren van veilig digitaal gedrag van leerlingen

De sterke toename van interactieve en mobiele media in thuis-, straat- en werkomgeving en de vlucht die de sociale netwerken genomen hebben, vraagt bij leerlingen om een toenemende awareness op het gebied van cybersecurity. In de praktijk blijkt deze awareness in hoge mate te ontbreken. Dit onderzoek richt zich op het achterhalen van de factoren die het veilig digitaal gedrag van jongeren beïnvloeden, alsmede de wijze waarop deze factoren met interventies beïnvloed kunnen worden.

- Lectoraat Cyber Security & Safety
- Projectpartners: Koninklijke Bibliotheek, Kennisnet, SLO, Curriculum.nu

# Subsidieprojecten (vervolg)

## C-SIDE: Cyber Security by Integrated Design

Binnen dit consortium (Nationale Wetenschapsagenda) wordt gewerkt aan de ontwikkeling van een methodologie voor het softwareontwerpproces, waarin technische en niet-technische aspecten van cybersecurity zijn geïntegreerd. Wetenschappelijke disciplines worden gebundeld om inzichten in bestaand curriculum van de betrokken kennisinstellingen uit te breiden. Binnen het project worden meerdere promovendi aangesteld, waaronder 1 promovendus deels onder begeleiding van De Haagse Hogeschool.

- Lectoraat Risk Management & Cybersecurity (a.i. begeleiding door lector Cybercrime & Cybersecurity)
- Projectpartners: Universiteit Leiden (projectleider), NCSC, Ministerie J&V, SURFSara, LUMC

## Digitale veiligheid Greenport

Doel van deze verkenning is om de digitale veiligheid te inventariseren van de bedrijven in de keten Greenport West-Holland. In deze verkenning is gewerkt aan een roadmap en uitvoeringsagenda voor het verbeteren van de cyberweerbaarheid van de tuinbouwsector.

- Lectoraat Cyber Security & Safety
- Projectpartners: Greenport West-Holland, HSD, InnovationQuarter, TNO, mkb'ers in de glastuinbouw Westland.

## Politie & Wetenschap: Evaluatie interventie Hack_right

In Nederland hebben de politie en het OM de unieke interventie Hack_Right ontwikkeld als alternatief of aanvullend straftraject voor jeugdige daders die een cybercrime delict plegen. Hack_Right heeft tot doel om recidive onder deelnemers te voorkomen en kaders te bieden waarbinnen deelnemers hun ICT-talent op legale wijze kunnen ontwikkelen. In dit project is deze interventie geëvalueerd.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: NSCR, politie, OM, reclassering en Halt.

## Politie & Wetenschap: Parels van de lokale aanpak van cybercrime

Het lectoraat heeft gewerkt aan een overzicht van lokale projecten waarbij de politie samenwerkt met andere stake-holders om cybercrime te bestrijden. Dit levert inzicht in de doelen van de projecten en inzicht in of lokale projecten landelijk uit te rollen zijn.

- Lectoraat Cybercrime & Cybersecurity

# PhD projecten

In 2021 werkten 3 promovendi aan hun proefschrift. Daarnaast werden 5 nieuwe promotievoorstellen goedgekeurd die begin 2022 van start zijn gegaan.

## Hacktivism, honorable cause or serious threat?

Dit promotieonderzoek richt zich op het beschrijven en duiden van het fenomeen hacktivisme, alsook het ontwerpen van oplossingen voor geconstateerde problemen.

- Promovendus: Marco Romagna
- Betrokken universiteit: Universiteit Leiden

## Slachtofferschap in een gedigitaliseerde samenleving

Het onderzoek kijkt naar het maatschappelijk perspectief versus individueel perspectief van online slachtofferschap.

- Promovendus: Raoul Notté
- Betrokken universiteit: Universiteit van Tilburg

## Automated security analysis in graphs and state machines

Using machine learning algorithms for pattern recognition, this research project will investigate how to automate the process of analyzing graphs for patterns of software vulnerabilities and compose a list of secure and insecure patterns.

- Promovendus: Daniel Meinsma
- Betrokken universiteit: TU Delft

# Lab-activiteiten

## Human behavior of cyber security lab

Cyberveiligheid begint bij mensen. Maar we kunnen het cybergedrag van mensen nog niet goed meten om te onderzoeken wat de meest effectieve maatregelen zijn om mensen cyberweerbaar te maken. In dit lab hebben we een innovatieve manier ontwikkeld om dit gedrag objectief te kunnen meten. Door een virtueel en fysiek lab, worden experimenten uitgevoerd binnen of samen met organisaties. Met als uiteindelijke doel dat de mens van zwakke schakel een first line of defense wordt.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: Dutch Innovation Factory, Tellick

## IoT & Technical Security lab

Samen met studenten van de opleiding HBO-ICT is een miniatuurstad met smart city elementen gebouwd. Hierin kunnen security OT/IT vraagstukken worden aangepakt.

- Lectoraat Network & Systems Engineering
- Projectpartners: Dutch Innovation Factory, MBO Rijnland

## Joint Cyber Range NL

In Nederland is nog geen nationaal platform voor het hoger onderwijs op het gebied van cybersecurity. Cyber- en cloudsecurity vaardigheden worden vooral binnen de eigen instelling aangeleerd. Via het Joint Cyber Range NL Initiatief worden krachten gebundeld en wordt gewerkt aan een landelijke faciliteit waarin verschillende deelomgevingen worden gebouwd. De opzet is een cloud-voorziening die dient als Cyberrange-as-a-Service.

- Lectoraat Network & Systems Engineering
- Projectpartners: Hogeschool Utrecht, Fontys, Windesheim, Hanzehogeschool, UTwente, SURFnet

# Overige projecten

## City Deal Den Haag: Digitale buurtambassadeurs

Het lectoraat heeft een plan- en procesevaluatie uitgevoerd van het project Digitale buurtambassadeurs in Den Haag. Digitale buurtambassadeurs zijn in dit project ingezet om de cyberveerkracht van inwoners en ondernemers te vergroten. De resultaten en inzichten van deze pilot zijn ter beschikking gesteld aan andere gemeenten in Nederland.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: Gemeente Den Haag, Centrum voor Criminaliteit en Veiligheid (CCV)

## City Deal: Hackshield

HackShield is een cybersecurity spel voor kinderen tussen de 8 en 12 jaar en heeft tot doel om een cyberveilige generatie kinderen te creëren. Hackshield wordt toegepast in verschillende gemeenten in Noord Holland om jongeren de cyberveerkracht van ouders en omgeving (school, sportclubs, gemeente) te laten vergroten. In opdracht van Regionaal Samenwerkingsverband Noord Holland Samen Veilig is een plan- en procesevaluatie uitgevoerd. De beleidstheorie, uitvoering en ervaringen van het project zijn hiervoor in kaart gebracht aan de hand van 30 interviews met ontwikkelaars, uitvoerders en deelnemers.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: CCV en 27 Noord-Hollandse gemeenten


## Cybercrisismanagement bij gemeenten

Dilemma's inzichtelijk maken die spelen bij de omgang van gemeenten met grotere cyberincidenten en crises. Deze incidenten en crises kunnen gericht zijn op de gemeentelijke organisatie of een organisatie die gevestigd is in de gemeente.

- Lectoraten Risk Management & Cyber Security en Cybercrime & Cybersecurity
- Projectpartners: NHL Stenden en 18 verschillende gemeenten, waaronder Den Haag, Zoetermeer en Haarlem

## Ontwikkelen lokale interventies gericht op geldezels

Geldezels vormen een hele interessante groep om interventies voor te ontwikkelen: ze vervullen een cruciale positie binnen de modus operandi en ze zorgen voor de lokale inbedding van cybercriminelen. Lokale overheden hebben een rol in de aanpak van dit fenomeen. Om hen te ondersteunen is een verkenning uitgevoerd om kenmerken van geldezels en bestaande interventies gericht op geldezels in kaart te brengen.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartner: Saxion

## Cybersecurity in ketens: wat werkt?

In dit project is in kaart gebracht welke factoren leiden tot succesvolle samenwerking op het gebied van cybersecurity binnen ketens van bedrijven.

- Lectoraat Cybercrime & Cybersecurity
- Projectpartners: Ministerie J&V en MKB-Nederland

## Cybersecurity situational awareness en informatievisualisatie

Samen met het NCSC wordt gekeken hoe kennis over informatieverwerking en informatievisualisatie kan worden ingezet in een cybersecurity control room. Welke invloed heeft de manier waarop informatie wordt gevisualiseerd op de informatieverwerkingscapaciteit? En hoe draagt dit bij aan de algehele kwaliteit van situational awareness?

- Lectoraat Cyber Security & Safety
- Projectpartners: NCSC

# Overige projecten (vervolg)

## Cyberveiligheid in de medische zorg

Dit onderzoek richt zich op het verkrijgen van een beter inzicht in de cybersecurityrisico's die ziekenhuizen en patiënten lopen door de vergaande digitalisering van de medische technologie, alsmede in de maatregelen die nodig en mogelijk zijn om veilig met deze technologie om te gaan. Het betreft zowel de veiligheid van de digitale medische technologie, als het risicobewustzijn van de betrokken interne en externe actoren.

- Lectoraat Cyber Security & Safety
- Projectpartners: Hogeschool Leiden, TNO, LUMC, HMC

## Verbeteren van veilig digitaal gedrag bij ouderen

Door de vergrijzing krijgen meer ouderen te maken met een steeds verder digitaliserende maatschappij. Ouderen handelen niet altijd even veilig online, maar het is onbekend welke factoren hieraan ten grondslag liggen, welke invloed ze hebben en hoe ze beïnvloed kunnen worden. Door dit te achterhalen kunnen passende interventies ontwikkeld worden om de cyberveiligheid bij ouderen te vergroten.

- Lectoraat Cyber Security & Safety

## Verkenning risico management: what works?

In deze verkenning is in kaart gebracht welke bestaande risico modellen beschikbaar zijn en wat de empirische bestudering van deze modellen is. De systematic review legt de basis voor de verdere ontwikkeling van evidence based risico modellen.

- Lectoraat Risk Management & Cybersecurity (a.i. begeleiding door lector Cybercrime & Cybersecurity)

## Impact van cyberincidenten op patiëntvertrouwen en patiëntveiligheid binnen de zorgsector

Doel van dit project is het in kaart brengen van de impact van cyberincidenten binnen de zorgsector. Ook is gekeken naar een algemeen theoretisch model waarmee de impact van cyberincidenten kan worden voorspeld en onderzocht voor (publieke) hybride organisaties.

- Lectoraat Risk Management & Cybersecurity

## Grip op cyberrisico's: cyber incident response decision making

In een verkenning is gekeken naar wat kan worden geleerd van ervaren cyber incident response consultants binnen organisaties. Organisaties die te maken krijgen met een grote cyberaanval schakelen vaak de hulp in van externe incident response dienstverleners. Deze dienstverleners nemen onder grote druk beslissingen en adviseren hun klanten. Op basis van interviews is inzicht verkregen in hoe incident responders in de praktijk deze beslissingen nemen.

- Lectoraat Risk Management & Cybersecurity

WIE ZIJN WIJ

# Lectoraat Cybercrime & Cybersecurity

## dr. Rutger Leukfeldt, lector Cybercrime & Cybersecurity

Dr. Rutger Leukfeldt is naast lector Cybercrime & Cybersecurity en directeur van het CoECS ook senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). Leukfeldt heeft ruim 10 jaar ervaring met wetenschappelijk onderzoek naar cybersecurity en cybercrime voor zowel publieke als private opdrachtgevers. Enkele voorbeelden zijn onderzoek naar de werkwijzen en daderkenmerken van cybercriminelen, onderzoek naar slachtofferschap van cybercrime onder burgers en onderzoek naar de doorstroom van cybercrimezaken binnen de strafrechtketen. Leukfeldt promoveerde op een onderzoek waarbij hij naar de ontstaans- en groeiprocessen en criminele mogelijkheden van cybercriminele netwerken keek en ontwikkelde een model voor de politie en banken dat gebruikt kan worden om cyberaanvallen effectiever te bestrijden. Verder kreeg Rutger twee prestigieuze onderzoeksbeurzen om onderzoek naar cybercrime te doen. In 2015 een Marie Curie Individual Fellowship (EU-subsidie voor veelbelovende onderzoekers) en in 2017 een Veni-subsidie (NWO-subsidie voor onderzoekstalent). Ten slotte is Rutger voorzitter van de Cybercrime Working Group van de European Society of Criminology.

### Dr. Rick van der Kleij, senior onderzoeker

Dr. Rick van der Kleij is psycholoog, gepromoveerd in de arbeid- en organisatiepsychologie, senior onderzoeker bij het lectoraat en de Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). Hij heeft meer dan 20 jaar ervaring in het doen van kwalitatief hoogwaardig toegepast onderzoek op maatschappelijk relevante vraagstukken binnen het veiligheidsdomein. Zijn onderzoek naar cybersecurity richt zich op manieren om de veerkracht van bedrijven tegen cyberaanvallen te verhogen. Een veerkrachtige organisatie heeft de capaciteit om adequaat te reageren op cyberincidenten en kan bovendien in veel gevallen voorkomen dat er problemen ontstaan.

### Dr. Susanne van ‘t Hoff – de Goede, onderzoeker

Dr. Susanne van ‘t Hoff-de Goede is criminoloog en onderzoeker bij het lectoraat. Na haar master Rechtshandhaving en Veiligheidsbeleid aan de Universiteit Leiden promoveerde zij aan de Universiteit Utrecht op de gevolgen van gevangenisstraf voor partners van gedetineerden. Haar onderzoeksinteresse gaat uit naar de verklaring, preventie, gevolgen en integrale aanpak van crimineel gedrag. Als onderzoeker bij het lectoraat houdt zij zich bezig met de menselijke kant van cybercrime en cybersecurity in het mkb. Haar onderzoek richt zich op inzicht krijgen in cybercriminaliteit en de aanpak van cybercriminaliteit gericht op mkb’ers.

### Dr. Asier Moneva Pardo, onderzoeker

Asier Moneva Pardo is postdoctoraal onderzoeker op het gebied van de menselijke factor in cybercrime aan De Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving. Met een achtergrond in criminologie behaalde hij zijn PhD over de toepasbaarheid van het kader voor omgevingscriminologie en criminaliteitsanalyse op cybercriminaliteit aan de Miguel Hernandez-universiteit in Elche (Spanje). Zijn onderzoek richt zich op de analyse en preventie van cybercriminaliteit vanuit een situationeel perspectief, waarbij hij gebruikmaakt van kwantitatieve methoden.

# WIE ZIJN WIJ

**Marco Romagna LLM MA,**
**docent-onderzoeker en promovendus**

Marco Romagna LLM MA is docent 'Juridische en criminologische aspecten van cybersecurity' en onderzoeker bij het kenniscentrum. Hij promoveert aan de Universiteit Leiden met een project over 'hacktivisme: eervolle zaak en/of ernstige bedreiging?' ("Hacktivism: honorable cause and/or serious threat?"). Eerder was Marco stagiair bij eCrime (Universiteit van Trento), de Cyber Security Academy (Den Haag) en Eurojust en werkte hij als fraude-analist voor de digitale handelsactiviteiten bij Nike. Marco heeft een master in de Rechten (Universiteit van Trento) en een MA in Global Criminology (Universiteit Utrecht). Naast hacktivisme en cybersecurity behoren cybercriminaliteit, criminologie en het daaraan gerelateerde strafrecht tot zijn belangrijkste onderzoeksinteresses. Marco volgt in het bijzonder nieuwe ontwikkelingen in de technologie op de voet, met name wanneer deze verband houden met juridische vraagstukken.

**Raoul Notté MA MSc,**
**docent-onderzoeker en promovendus**

Raoul Notté MA MSc heeft een achtergrond in de bestuurs- en organisatiewetenschap. Hij is als docent-onderzoeker verbonden aan het lectoraat cybercrime & cybersecurity. De afgelopen jaren publiceerde hij meerdere onderzoeken naar het slachtofferschap van cybercriminaliteit in het midden-kleinbedrijf en de wijze waarop bedrijven zich hiertoe beveiligen, alsmede de impact van cybercrimeslachtofferschap op burgers. Momenteel is Raoul promovendus (gefinancierd door de NWO promotiebeurs voor leraren) en doet onderzoek naar 'Slachtofferschap in een gedigitaliseerde samenleving' in samenwerking met de Universiteit Tilburg.

**Luuk Bekkers MSc,**
**onderzoeker**

Luuk Bekkers MSc heeft een achtergrond in de forensische psychologie en criminologie. De afgelopen jaren publiceerde hij als junior onderzoeker bij het lectoraat Cybercrime & Cybersecurity meerdere studies naar daders van cybercriminaliteit en cyberweerbaarheid in het midden- en kleinbedrijf. De komende jaren gaat Luuk zich bezig houden met zijn promotieonderzoek, gericht op het onderwerp geldezels.

**Drs. Michelle Ancher,**
**docent-onderzoeker**

Drs. Michelle Ancher is docent bij de opleiding HBO-ICT (richting Information Security Management) en onderzoeker bij het lectoraat Cybercrime & Cybersecurity. Ze is sociaal psycholoog en richt zich op de menselijke factor van de information security. Factoren die het menselijk (cyber)gedrag beïnvloeden en creatieve manieren waarop je gedrag kunt veranderen, hebben haar aandacht.

### Jim Schiks MSc, onderzoeker (t/m juni 2021)

Jim Schiks Msc is junior onderzoeker op het gebied van cybercriminaliteit bij De Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Hij heeft een achtergrond in bedrijfskunde en criminologie. Als criminoloog is Jim geïnteresseerd in de menselijke aspecten van cybersecurity. Zo verricht hij onder andere onderzoek naar de wijze waarop personen bij cybercriminaliteit betrokken raken en naar interventies waar deze personen aan worden onderworpen door politie en justitie. Hij gaat hierbij graag de verbinding aan met de praktijk, om zo een beter beeld te krijgen van de werkelijkheid.

### Joeri Loggen MSc, onderzoeker en promovendus

Joeri Loggen MSc heeft psychologie en criminologie gestudeerd aan de Vrije Universiteit Amsterdam en is sinds 1 oktober 2021 werkzaam als junior onderzoeker binnen het lectoraat. Hier doet hij promotieonderzoek naar de verschillende preventiemaatregelen die genomen kunnen worden om te voorkomen dat minderjarigen cybercriminaliteit gaan plegen. Hij is geïnteresseerd in het beschrijven, verklaren en beïnvloeden van cybercrimineel gedrag.

### Sifra Matthijsse MSc, onderzoeker en promovendus

Sifra Matthijsse Msc heeft een achtergrond in de criminologie en is als junior onderzoeker verbonden aan het lectoraat Cybercrime & Cybersecurity. Hier doet zij promotieonderzoek dat zich richt op crime scripts van cyberdelicten en mogelijke interventies gericht op daders en slachtoffers. In het verleden heeft ze bij de Erasmus Universiteit onderzoek gedaan naar kenmerken van en passende interventies voor daders van cybercriminaliteit.

### Dr. Juul Gooren, docent-onderzoeker (t/m mei 2021)

Sinds 2010 is dr. Juul Goren als docent aangesteld bij De Haagse Hogeschool voor de Faculteit Bestuur, Recht en Veiligheid bij de opleiding Integrale Veiligheidskunde/Safety & Security Management Studies. Eerder was hij lid van de kenniskring Filosofie en Beroepspraktijk. Van 2019 – 2021 maakte hij deel uit van de kenniskring van het lectoraat Cybercrime & Cybersecurity. Zijn onderzoek richt zich op ‘Resilience’ als theoretisch model voor zowel industriële als publieke veiligheid.

WIE ZIJN WIJ

# Lectoraat Cybersecurity & Safety

## Dr. Marcel Spruit, lector Cybersecurity & Safety

Dr. Marcel Spruit is lector Cybersecurity & Safety. Hij heeft een jarenlange ervaring in informatiebeveiliging en cyber security. Marcel Spruit is verantwoordelijk voor onderzoek op het gebied van cyber security en het ontwikkelen van onderwijs op dit gebied. Hij is zelf intensief betrokken bij zowel het onderzoek als de onderwijsontwikkeling. Daarnaast is hij als senior consultant verbonden aan de adviesorganisatie PBLQ. Hij geeft advies op organisatorisch terrein, met name op de onderwerpen informatiebeveiliging en cyber security. Tevens voert hij audits, second opinions en beveiligings-onderzoeken uit. Voor zijn aanstelling als lector werkte Marcel Spruit in de kwaliteitsborging bij Fokker Space en als Universitair Hoofddocent bij de vakgroep Informatiesystemen van de Technische Universiteit Delft. Hij specialiseerde zich in informatiebeveiliging, menselijk falen en het organiseren van beveiliging.

## Dr. Emiel Kerpershoek, senior onderzoeker

Sinds maart 2021 is dr. Emiel Kerpershoek als onderzoeker verbonden aan het lectoraat Cyber Security & Safety van het Kenniscentrum Cyber Security. Zijn onderzoek richt zich op governance-, cultuur- en gedragsaspecten van informatiebeveiliging en cyber security. Emiel promoveerde aan de TU-Delft - Technische Bestuurskunde op een onderzoek naar effecten van het DBC bekostigingssysteem onder medisch specialisten in Nederlandse ziekenhuizen. Ook werkte hij bij het NIVEL enkele jaren als onderzoeker aan diverse projecten op het gebied van zorgstelsel en sturing. De afgelopen zes jaar was hij actief als beleidsadviseur bij InEen, branche-vereniging voor eerstelijns huisartsen-organisaties, waar hij werkte aan dossiers op het gebied van strategisch informatiebeleid, governance, regionale samenwerking en onderzoek.

## Dr. ir. Marinus Maris, docent-onderzoeker

Dr. ir. Marinus Maris is als hoofddocent verbonden aan de opleiding HBO-ICT van De Haagse Hogeschool. Naast het ontwikkelen en verzorgen van onderwijs op het gebied van Computernetwerken en Mobiele Apps voert hij onderzoek uit als lid van de kenniskring van het Lectoraat Cyber Security & Safety bij De Haagse Hogeschool. Zijn onderzoek richt zich met name op de cybersecurity-awareness op basis- en middelbare scholen. Marinus is afgestudeerd in elektrotechniek aan de Technische Universiteit te Delft en gepromoveerd aan de Universiteit van Zürich op het gebied van kunstmatige intelligentie.

## Dr. ir. Pieter Burghouwt, docent-onderzoeker

Dr. ir. Pieter Burghouwt is als hogeschoolhoofddocent verbonden aan de opleiding HBO-ICT van De Haagse Hogeschool. Naast het ontwikkelen en verzorgen van onderwijs op het gebied van Cyber Security en Computernetwerken voert hij onderzoek uit als lid van de kenniskring van het Lectoraat Cyber Security & Safety bij De Haagse Hogeschool. Zijn onderzoek richt zich met name op de technische beveiligingsaspecten van computernetwerken. Pieter promoveerde in 2015 aan de TU-Delft op een onderzoek naar detectietechnieken van botnetverkeer in bedrijfsnetwerken. Sinds 2015 verzorgt hij ook onderwijs voor de Executive Master Cyber Security op de CSA (Cyber Security Academy), een samenwerkingsverband tussen de Universiteit Leiden, TU-Delft en De Haagse Hogeschool.

### Deborah Oosting MSc, onderzoeker

Deborah Oosting MSc heeft een achtergrond in psychologie en human factors. Ze is werkzaam als junior onderzoeker binnen het lectoraat Cyber Security & Safety'. Hier houdt ze zich voornamelijk bezig met het ontwikkelen van een meetmodel waarmee een (nul) meting van cyber security awareness kan worden gedaan en kan worden beoordeeld. Haar onderzoeksinteresses gaan uit naar het vinden en meten van factoren achter bepaald gedrag, maar ook om deze gevonden factoren te verklaren en te benutten om zo gedrag te kunnen veranderen.

### Dr. Nicole van Deursen, senior onderzoeker

Dr. Nicole van Deursen doet bij De Haagse Hogeschool onderzoek naar de bijdrage van informatievisualisatie aan een beter begrip van cybersecurity. Zij werkt als onderzoeker bij het Nationaal Cyber Security Centrum en is hoofdredacteur van Informatiebeveiliging Magazine. Naast een lange carrière als consultant informatiebeveiliging en risicomanagement promoveerde zij in 2014 aan Edinburgh Napier University op het analyseren en voorspellen van informatiebeveiligingsincidenten in de zorg. Nicole's onderzoeksinteresses omvatten naast informatievisualisatie ook security by design, data analyse en toekomstverkenning.

### Céline Kreffer MSc, onderzoeker

Céline Kreffer MSc heeft een achtergrond in de psychologie en criminologie. Ze is werkzaam als junior onderzoeker binnen het lectoraat Cyber Security & Safety van het Kenniscentrum Cyber Security. Hier houdt ze zich bezig met onderzoek naar de risicoperceptie en -attitude in ziekenhuizen, en naar gepaste maatregelen om de omgang met digitale middelen veiliger te maken.

### Herman de Bruine, docent-onderzoeker

Drs. Herman de Bruine is docent bij de opleiding Integrale Veiligheidskunde en kenniskringlid bij het lectoraat Cyber Security & Safety. Het onderzoek van Herman richt zich op het meten en verbeteren van situational awareness met betrekking tot cyberrisico's in organisaties in de vitale sector.

### Erik van den Brink MEd, docent-onderzoeker

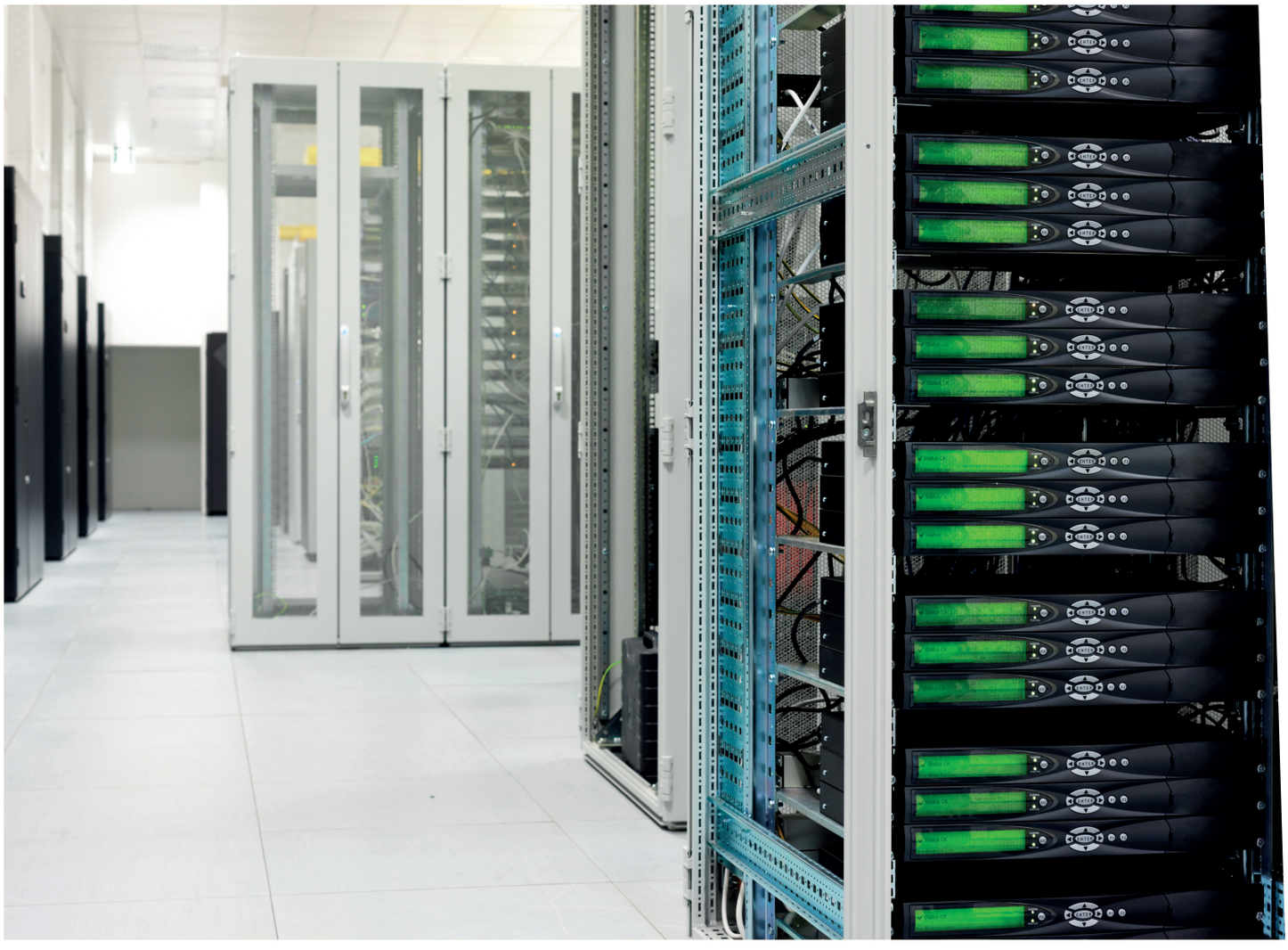
Erik van den Brink is docent bij de pabo-opleiding van De Haagse Hogeschool en kenniskringlid bij het lectoraat Cyber Security & Safety. Hij richt zich in zijn onderzoek specifiek op de cybersecurity awareness van scholieren. Daarnaast kijkt hij hoe de digitale component in het curriculum van de pabo kan worden verbeterd.

WIE ZIJN WIJ

# Lectoraat Network & Systems Engineering Cyber Security

## Dr. Mathias Björkqvist, lector Network and Systems Engineering Cyber Security

Dr. Mathias Björkqvist is sinds september 2020 lector Network & Systems Engineering Cyber Security aan De Haagse Hogeschool. Daarnaast vervult hij de functie van security researcher bij Thales Research and Technology Nederland. Voordat hij bij Thales kwam, werkte hij 12 jaar bij IBM Research - Zürich, met focus op storage security, encryption key management en blockchain. Mathias behaalde zijn MSc in computer networking aan de Technische Universiteit van Helsinki. Zijn PhD over 'Resource management of replicated service systems in the Cloud' behaalde hij aan de Università della Svizzera italiana, Italy. Mathias' onderzoeksinteresses omvatten key management, veiligheid van computernetwerken, veiligheid van gebruiksapparaten en IoT.



### Daniel Meinsma MSc, docent-onderzoeker en promovendus

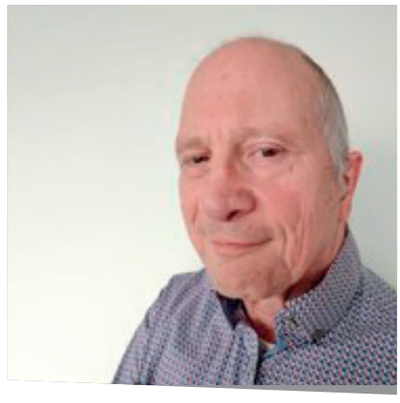
Daniel Meinsma MSc is als docent verbonden aan de opleiding HBO-ICT aan De Haagse Hogeschool. Naast het ontwikkelen en verzorgen van onderwijs op het gebied van technische informatiebeveiliging faciliteert Daniel studenten ook in een breed scala aan technische onderzoeksprojecten. Sinds 2021 is Daniel begonnen als deeltijd promovendus aan de Technische Universiteit van Delft op het gebied van Automated Vulnerability Research. Daarnaast is Daniel medeoprichter van de Dutch Joint Cyber Range en draagt hij actief bij aan Capture the Flag onderwijs.

### Saman Barjas, docent-onderzoeker

Saman Barjas MSc is sinds 2016 als docent verbonden aan de differentiatie Information Security Management (ISM) van de opleiding HBO-ICT van De Haagse Hogeschool. Daarnaast ontwikkelt en verzorgt hij onderwijs op het gebied van Risk Management, Business Continuity Management, Social Engineering en Cyber Security. Tot augustus 2021 was hij kennis-kringlid bij het lectoraat Risk Management & Cyber Security, sinds september 2021 is hij onderzoeker bij het lectoraat Network & Systems Engineering Cyber Security. In zijn onderzoek is hij vooral geïnteresseerd in de relatie tussen risico management en techniek.

### Mike Gilhespy MSc, docent-onderzoeker

Sinds 2020 werkt Mike Gilhespy MSc bij De Haagse Hogeschool als docent bij de opleiding HBO-ICT. In zijn lessen behandelt hij technische veiligheidsonderwerpen met focus op het offensieve perspectief, tevens zijn primaire interesse op het gebied van onderzoek. Mike doceert aan bachelor studenten, maar is ook betrokken bij het Master Cybersecurity Engineering programma, waar hij kerndocent is voor de module “Hacking & Malware”.



### Bernard van der Helm, onderzoeker

Bernard is sinds september 2021 onderzoeker ‘Network and Systems Cyber Security’ aan De Haagse Hogeschool. Daarnaast is hij werkzaam binnen het ICT bedrijf van ING Nederland waarin hij ervaring heeft opgedaan op het gebied van: hardware architectuur; data center migraties; Inside Business Payments Performance management; Implementeren van Wholesale Banking Cyber Fraud Prevention applicaties. Zijn huidige functie is Product owner van Azure Yaml building pipelines. In zijn vrije tijd was Bernard 12 jaar een van de ontwikkelaars van zHercules mainframe emulator, met specifieke focus op crypto en compressie; en 10+ jaar voorzitter van de NL GSE werkgroep mainframe. De onderzoek interesses van Bernard omvatten alle aspecten van systeem security.

WIE ZIJN WIJ

# Lectoraat Risk Management & Cyber Security

## Jelle Groenendaal, lector Risk Management & Cyber Security (t/m juni 2021)

Met ingang van 1 mei 2020 gaf dr. Jelle Groenendaal zijn nieuwe onderzoeksgroep op het snijvlak van risk management en cybersecurity vorm. Jelle begon zijn carrière bij Crisislab en is gepromoveerd op een proefschrift naar frontlijnsturing en commandovoering binnen de brandweer en politie. Vervolgens werkte hij bij Deloitte waar hij multinationals adviseerde over het versterken van cyberveerkracht. Daarna stapte hij over naar ING Bank en werkte er binnen het Cybercrime Expertise & Response Team (CERT) als incident- en crisismanager. De laatste twee jaar bij ING was hij wereldwijd verantwoordelijk voor de bedrijfscontinuïteit en crisismanagement.


## Jetze Dalmeijer, docent-onderzoeker (t/m juni 2021)

Jetze Dalmeijer MSc is afgestudeerd aan de VU met een Master in Political Science, International Relations. Daarna is hij tien jaar werkzaam geweest in hoofdzakelijk het maatschappelijk middenveld, in veel verschillende organisaties als beleidsadviseur en secretaris. Binnen het maatschappelijk middenveld was Jetze actief bij de overheid (Gemeente Amsterdam), de zorg (GGZ Rivierduinen), het Hoger onderwijs (De V.U. en De Haagse Hogeschool). In 2019 maakte hij de overstap naar het lesgeven binnen De Haagse Hogeschool, waar hij sindsdien met veel plezier werkt binnen de opleiding Bedrijfskunde.

## Jasmijn Boeken, onderzoeker

Jasmijn Boeken MSc heeft een achtergrond in de politicologie. Ze is werkzaam als PhD kandidaat binnen de samenwerking voor het C-SIDe project met Universiteit Leiden. Zij zal zich bezighouden met governance vraagstukken betreffende de implementatie van security by design in organisaties. Als politicoloog is Jasmijn geïnteresseerd in de effecten van digitalisering op onze veiligheid. Ze wil in haar onderzoek verbinding maken met de praktijk om zo bedrijven concreet bij te staan bij het in kaart brengen en aanpakken van cyberrisico's.

# Coördinatie en ondersteuning

### Ligaya Butalid, programmacoördinator

Dr. Ligaya Butalid is de programmacoördinator van het Centre of Expertise Cyber Security. Met een achtergrond in de gezondheidspsychologie deed Ligaya onderzoek naar het belang van empathie en het menselijk contact in de medische zorg. Ze promoveerde bij het NIVEL / Universiteit Utrecht op een onderzoek naar arts-patiënt communicatie in de huisartsenzorg. Daarnaast heeft ze veel ervaring in programmamanagement. Ze werkte onder andere bij subsidiegevers ZonMw en Regieorgaan SIA (onderdeel van NWO) en bij de dienst Onderwijs, Kennis en Communicatie van De Haagse Hogeschool.

### Maaike Vergeer, senior managementassistent

Maaike zorgt voor de dagelijkse ondersteuning van het Centre of Expertise Cyber Security en de lectoraten Cybercrime & Cybersecurity, Cyber Security & Safety, Network & Systems Engineering Cyber Security en Risk Management & Cyber Security. Daarnaast draagt ze bij aan o.a. de interne en externe communicatie van het CoECS en de lectoraten.

BIJLAGEN

# Focus en onderzoekslijnen per lectoraat

## Lectoraat Cybercrime & Cybersecurity

Het doel van het lectoraat Cybercrime en Cybersecurity is om de kennispositie van midden- en kleinbedrijf (mkb) en de publieke instellingen op het gebied van cybercrime en cybersecurity te vergroten. Hiermee wordt het slachtofferschap en de impact van cyberaanvallen verlaagd.

De vraag naar evidence-based praktische toepasbare kennis is de reden dat de Haagse Hogeschool en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) de handen ineen hebben geslagen voor de duurzame samenwerking binnen dit lectoraat.

Het lectoraat kent vier onderzoekslijnen:

**1 Aard en omvang van slachtofferschap**
Projecten binnen deze onderzoekslijn richten zich op de volgende vragen: Welke mkb bedrijven worden slachtoffer van cyberaanvallen en zijn er factoren die risicoverhogend of risicoverlagend werken? Hoe vaak komt slachtofferschap van cybercrime (zoals whatsappfraude) voor? En wat is de impact op slachtoffers van online delicten?

**2 Aard van cybercriminaliteit**
Het lectoraat doet binnen deze onderzoekslijn o.a. onderzoek naar insider threats, social engineering, geldezels en cybercriminele netwerken.

**3 Cyberweerbaarheid**
Binnen deze onderzoekslijn wordt gekeken hoe je cyberweerbaarheid binnen organisatie kan meten en hoe (on) veilig mensen zich online gedragen.

**4 De aanpak**
Projecten binnen deze onderzoekslijn kijken o.a. naar de aangiftebereidheid na slachtofferschap, de effectiviteit van lokale interventies, en de rol van gemeenten in de bestrijding van cybercrises.

### Naamswijziging van het lectoraat

Van 2017-2021 werd de naam ‘Cybersecurity in het mkb’ gehanteerd. Deze naam deed echter inmiddels onvoldoende recht aan het actuele onderzoeksprogramma, waarbij de kennisontwikkeling over cybercrime en cybersecurity door de praktijk alleen maar breder werd gevoeld en erkend. De kennisbehoefte leeft niet alleen bij het mkb, maar wordt ook door (lokale) overheden en publieke instellingen ervaren. Daarnaast is het lectoraat zich steeds verder gaan verdiepen in de groeiende cybercriminaliteit. Op basis van deze observaties en ontwikkelingen is gekozen om per januari 2022 een nieuwe naam te hanteren voor het lectoraat: ‘Cybercrime & Cybersecurity’.

**“Cybercrime is een groot maatschappelijk probleem. De criminologische bestudering van cybercrime staat nog in de kinderschoenen. Het is echter niet alleen noodzakelijk om goed wetenschappelijk onderzoek uit te voeren, maar ook om met de praktijk de acute problemen en uitdagingen van vandaag en morgen te onderzoeken.”**

## Lectoraat Cyber Security & Safety

Het primaire doel van het lectoraat is het doen van onderzoek ten behoeve van het uitbreiden en het praktisch toepasbaar maken van bestaande (wetenschappelijke) kennis en technieken op het gebied van cybersecurity van individuen en in organisaties. We streven ernaar dat de resultaten van het onderzoek toepasbaar zijn en toegepast worden in de beroepspraktijk.

Het onderzoek is geënt op de volgende onderzoeksvraag:
Hoe kunnen we de cybersecurity verbeteren bij individuen en bij publieke organisaties die niet of onvoldoende zijn toegerust om cyberdreigingen aan te pakken of zich onvoldoende van deze dreigingen bewust zijn?

De onderzoekslijnen binnen dit lectoraat richten zich op:

1 **het verhogen van de cybersecurity-awareness van mensen**

In de praktijk blijkt de awareness op het gebied van cybersecurity in hoge mate te ontbreken. Dit onderzoek richt zich met name op het meten van awareness en het formuleren van maatregelen en interventies (zoals serious games) waarmee awareness verbeterd kan worden.

2 **het verbeteren van de cybersecurity-governance in organisaties**

In organisaties raken de fysieke en digitale componenten steeds meer met elkaar vervlochten. Managers en cybersecurity-specialisten spelen hierbij een cruciale rol, maar zijn niet altijd in staat deze rol goed in te vullen. Onderzoek richt zich daarom op hoe cybersecurity binnen bijvoorbeeld gemeenten, waterschappen en ziekenhuizen beter ingericht kan worden.

3 **de kwalificatie van cybersecurity-professionals**

Activiteiten binnen deze onderzoekslijn richten zich op het ontwikkelen van beroepsprofielen voor het cybersecurity-domein, nieuw onderwijs en een kwalificatiestelsel.
Het secundaire doel is het verbeteren van het hoger onderwijs op het gebied van cybersecurity. Daartoe draagt het lectoraat bij aan het curriculum binnen HBO-ICT, de masteropleiding Cyber Security engineering en de professionalisering van hbo-docenten.

**“ In onze informatiemaatschappij zijn de veiligheid in de digitale wereld, ook wel de cyberwereld of cyberspace genoemd, en de veiligheid in de ‘gewone’ fysieke wereld onlosmakelijk met elkaar verbonden. Mensen en organisaties gebruiken steeds meer digitale systemen en netwerken, waardoor we ook afhankelijk zijn geworden van digitale systemen en netwerken. Veiligheidsproblemen in de digitale wereld kunnen ernstige gevolgen hebben in de fysieke wereld. ”**

# Focus en onderzoekslijnen per lectoraat (vervolg)

## Lectoraat Network & Systems Engineering Cyber Security

The research group Network and Systems Engineering focuses on three main research areas:

1 **Identity and Access Management;**
2 **Security of Systems and the Internet of Things;**
3 **Usable Security.**

These areas are interlinked and offer focus for meaningful results, while they also cover a research area that is wide enough to be of relevance to the educational programs of THUAS. Security research is never an activity performed on its own: it is vital to link security to real-world problems and other research activities.

As systems have become more interoperable and where different organizations must combine their solutions, the need to study systems security from a multidisciplinary approach is growing. Increasing numbers of devices that produce data are becoming connected, and companies often provide Cloud-based applications with respect to the IoT area. The primary question on which this research group focuses is: how can system security and usability be balanced where legal and privacy aspects are respected?

The research group Network and Systems Engineering is a close collaboration between THUAS and Thales. From the THUAS perspective, Thales provides real world application areas and the perspective from the practitioners in the field. From Thales's perspective, THUAS researchers and students can perform experiments that are not feasible in a corporate environment. Furthermore, Thales gains the ability to help guide the educational direction and can hopefully attract enthusiasm in relevant areas. Finally, the multidisciplinary nature of research performed in this research group will lead to novel results that will give students a more holistic view of solutions that are required in the future.

**"Access control is a very important area for systems security. Access control is concerned with providing control over security critical actions that take place in a system. Providing control over actions consists of explicitly determining either the actions that are, or are not, permitted by the system. In terms of cyber security, determining not only who is allowed access a system, but also when, and for how long, are vital towards building systems that are both sustainable, and secure."**

## Lectoraat Risk Management & Cyber Security

Hoe effectief cyber risk management eruit ziet, en welke risicomodellen en hulpmiddelen daarvoor nodig zijn, zijn de centrale vragen van de onderzoeksgroep Risk Management & Cyber Security. Het lectoraat kijkt daarbij naar de besturing van cyber risk management en de wijze waarop organisaties cyberrisico's kunnen voorkomen en beheersen. Daarnaast onderzoekt het lectoraat hoe organisaties effectief op cyberrisico's kunnen reageren (cyber incident respons en crisis management) en welke voorbereiding hiervoor noodzakelijk is. Hierbij hoort ook het doen van onderzoek naar effectieve manieren om schade en uitval van diensten door een cyberaanval te beperken (bedrijfscontinuïteitmanagement). Het doel van het lectoraat is om organisaties te ondersteunen bij het nemen van beslissingen over cyber risico's en (de organisatie van) cyberweerbaarheid. Dit met als doel om cyberincidenten te voorkomen, of, als dit niet lukt, de impact ervan te beperken.

Het onderzoek richt zich op de volgende thema's:

1. **Risicomanagement methoden, modellen en processen;**
2. **Werking en effectiviteit van 3 risciobeheersingsmaatregelen;**
3. **Impact van cyberincidenten- en crisis voor organisaties;**

Betekenis van cyber voor hulp- en veiligheidsdiensten.
Tot slot kijkt het lectoraat ook naar de rol en betekenis van publiek/private samenwerkingsverbanden op het gebied van cybersecurity, de effecten van cyberaanvallen voor organisaties en de rol die overheden en toezichthouders (kunnen) spelen om de cyberweerbaarheid van organisaties te vergroten.

**“ Risico is een centraal kenmerk geworden van de moderne, technologie gedreven, geglobaliseerde, genetwerkte en individualistische samenleving; door sommigen ook wel ‘de risicomaatschappij’ genoemd. Van oudsher spant de overheid zich in om deze risico’s zoveel mogelijk te voorkomen en te beheersen. Tegenwoordig zijn hier ook steeds meer private partijen bij betrokken en komen er steeds meer digitale risico’s. Elke organisatie moet moeilijke beslissingen nemen over hoeveel tijd en geld wordt gespendeerd aan het beschermen van haar klanten, technologie en diensten. Risicomanagement maakt het mogelijk om deze beslissingen te verbeteren, op basis van de best mogelijke informatie. ”**

## Adres- en contactgegevens

**Johanna Westerdijkplein 75**
**2521 EN  Den Haag**

**cybersecurity@hhs.nl**

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