

let's change
YOU. US. THE WORLD.

STAGE EN ONDERZOEK BIJ HET CENTRE OF EXPERTISE CYBER SECURITY

FEBRUARI 2026

DE HAAGSE HOGESCHOOL

Cybersecurity is belangrijk voor iedereen

We leven in een tijd waarin niet alleen digitale ontwikkelingen, maar ook digitale bedreigingen zich in een razendsnel tempo opvolgen. Bedrijven, organisaties en overheidsinstellingen zijn inmiddels sterk afhankelijk van digitale netwerken en de impact van een cyberaanval is daarmee in potentie enorm. Door een cyberaanval kunnen primaire processen van bedrijven en instellingen stil komen te liggen met alle gevolgen van dien, waaronder grote financiële schade.

Omdat iedereen in meer of mindere mate gebruik maakt van digitale systemen en netwerken is cybersecurity van cruciaal belang voor iedereen. Naast technische kennis is het ook belangrijk te begrijpen hoe mensen zich cyberveilig kunnen gedragen. Maar een cyberaanval is niet altijd te voorkomen. Daarom moeten bedrijven en organisaties ook weten hoe ze de schade van een cyberaanval zo veel mogelijk kunnen beperken. Dat noemen we cyberveerkracht.

De missie van het Centre of Expertise Cyber Security (CoECS) is:

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



ONDERZOEK DOEN BIJ ONS CENTRE OF EXPERTISE

In ons kenniscentrum (Centre of Expertise) doen wij onderzoek naar cybersecurity, waarbij we ons richten op 1) menselijk gedrag, 2) organisatiefactoren en 3) technische aspecten. Hierdoor is onderzoek doen bij ons kenniscentrum interessant voor studenten van veel verschillende opleidingen. Afhankelijk van jouw interesse en studierichting kijken we naar de mogelijkheden.

Als stagiair maak je deel uit van ons onderzoeksteam. Onder begeleiding van een ervaren onderzoeker en expert ga je aan de slag met je onderzoeksvraag. Je leert hoe je een vraag op een systematische manier kunt beantwoorden. Dit doe je niet alleen door literatuur te bestuderen, maar ook door het opzetten van een experiment of het afnemen van interviews. In sommige projecten werk je ook aan een praktische oplossing of tool, zoals bijvoorbeeld een app, die bedrijven en organisaties kunnen toepassen.

De meeste onderzoekers bij ons kenniscentrum werken ook als docent bij een van de opleidingen van De Haagse Hogeschool, zoals HBO-ICT of IVK. Zij begeleiden bijvoorbeeld (groepen) studenten tijdens projectweken of challenges.

“ Dankzij de steun van mijn collega’s en de inspirerende bijeenkomsten waar ik aan mocht deelnemen, heb ik in korte tijd veel geleerd over onderzoek doen in de praktijk. ”

Romee Los
MSc Student Sociology, Stagiaire Lectoraat Cybercrime & Cybersecurity



Interesse?

Wil je bij ons stage komen lopen? Solliciteer dan op een van de projecten in deze brochure. Houd er rekening mee dat de meeste projecten geschikt zijn voor studenten in hun derde of vierde jaar. Controleer zelf bij jouw opleiding wat de vereisten zijn voor een stage. Bij onze stages ligt de nadruk op het uitvoeren van praktijkgericht onderzoek.

Hoe solliciteer ik?

Stuur je CV en motivatiebrief naar de contactpersoon die bij het project wordt genoemd. Geef in je motivatiebrief altijd aan: waarom je geïnteresseerd bent in cybersecurity, of je al onderzoekservaring hebt en hoe het project aansluit bij je opleiding.

De docent-onderzoeker neemt vervolgens contact met je op en nodigt je eventueel uit voor een kennismakingsgesprek. Na dit gesprek wordt bepaald of je kunt starten als stagiair. Afspraken met je begeleider worden vervolgens vastgelegd in een stageovereenkomst.

Andere vragen?

Als het onderwerp van je eerste keuze niet meer beschikbaar is of als je andere algemene vragen hebt, neem dan contact met ons op via cybersecurity@hhs.nl. Stuur een e-mail met toelichting op welke onderwerpen je interesseren. We kijken dan of er toch een match mogelijk is met een van onze onderzoekers.

STUDENTPROJECTEN

Op de volgende pagina's vind je een aantal projecten waarbinnen je als stagiair bij het Centre of Expertise Cyber Security onderzoek kan doen. Bij elk project staat een contactpersoon vermeld bij wie je kunt solliciteren voor een stageplaats. In principe zijn dit projecten die in de periode februari t/m juni 2026 lopen. Als je op zoek bent naar een stage voor een andere periode, informeer dan bij de contactpersoon van het project naar de mogelijkheden.

De projecten richten zich op 1) gedrag, 2) organisaties en/of 3) techniek. Ze zijn ingedeeld op het aspect waar de meeste nadruk op ligt, maar in praktijk zal je in de meeste projecten het vraagstuk vanuit meerdere perspectieven (multidisciplinair) benaderen.

Deze lijst geeft een indruk van de mogelijkheden voor het komende semester. In sommige projecten zijn we afhankelijk van de planning en inzet van andere organisaties of bedrijven. Als tijdens je sollicitatie blijkt dat de projectperiode niet goed aansluit bij jouw stageperiode, word je hiervan op de hoogte gebracht. We kijken dan samen met jou naar alternatieve onderwerpen waar mogelijkheden zijn.

Let op: Bij een aantal projecten is de voertaal Engels. De beschrijvingen zijn in dat geval in het Engels weergegeven.



CYBER SECURITY & GEDRAG

Ervaring van een student

Steeds meer mensen worden slachtoffer van online fraude. Toch is het exacte aantal slachtoffers lastig vast te stellen, omdat lang niet iedereen melding maakt bij officiële instanties. Gevoelens van schaamte blijken vaak een belangrijke rol spelen in het besluit om geen aangifte te doen. Ook heerst er onder slachtoffers soms scepsis over het optreden van de politie en of hun melding wel serieus wordt genomen. De verwachting is dan ook dat mensen, in plaats van een officiële melding te maken of aangifte te doen, vaak zelf op het internet gaat zoeken naar een oplossing.

In mijn onderzoek kijk ik daarom naar zoekgedrag van slachtoffers van online fraude: gebruiken zij zoekmachines zoals Google of Yahoo? En zo ja, wat zoeken ze dan precies op? De uitkomsten van dit onderzoek kunnen helpen om veelvoorkomende zoektermen te identificeren. Deze termen zouden vervolgens gebruikt kunnen worden voor gerichte onlineadvertenties, zodat slachtoffers sneller de juiste hulp vinden op het moment dat ze daar behoefte aan hebben.

Vanuit de sociologische invalshoek kijk ik naar verschillen tussen mannen en vrouwen, leeftijden en opleidingsniveaus. Zo blijkt tot nu toe bijvoorbeeld dat oudere mensen minder snel online op zoek gaan naar hulp na een incident van online fraude dan jongere mensen.

Mijn stage bij het Centre of Expertise Cyber Security was een waardevolle leerervaring. Ik maakte deel uit van een warm en betrokken team waarin ik mij direct welkom voelde. Er was altijd ruimte voor vragen en begeleiding, terwijl ik tegelijkertijd de vrijheid kreeg om zelfstandig aan mijn onderzoek te werken. Deze stage gaf mij een interessante inkijk in de onderzoekswereld – een domein dat voor mij nog relatief nieuw was. Dankzij de steun van mijn collega's en de inspirerende bijeenkomsten waar ik aan mocht deelnemen, heb ik in korte tijd veel geleerd over onderzoek doen in de praktijk.

Romee Los
MSc student Sociology
Stagiaire Lectoraat Cybercrime & Cybersecurity

CYBER SECURITY & GEDRAG

Ervaring van een student

Tijdens mijn stage heb ik gewerkt aan de ontwikkeling van een serious game voor de gemeente, gericht op het vergroten van bewustwording rondom cybersecurity binnen OT-systemen.
Dit project heeft mij op een leerzame en interessante manier laten kennismaken met cybersecurity.

Wat mij opviel, is hoe bereid iedereen binnen het team is om te helpen. Wanneer ik ergens vastliep, was er altijd iemand beschikbaar om mee te denken of feedback te geven. De wekelijkse weekstart speelde daarbij een grote rol, deze bijeenkomsten zorgen voor een open en ondersteunende sfeer.

Mijn ervaring bij dit project was ontzettend waardevol, en ik kijk er met veel enthousiasme op terug.

Sacha Verduijn
Student CMD
Stagiair Lectoraat Cybersecurity & Safety

Ontwikkeling awareness game

Mensen, inclusief werknemers van organisaties en bedrijven, zijn in toenemende mate afhankelijk van digitale systemen, maar niet iedereen is zich daar voldoende van bewust.
Een game kan een effectief hulpmiddel zijn om mensen bewuster te maken van de digitale risico's die ze lopen en de noodzakelijke maatregelen om zich hiertegen te beschermen. In dit project ontwikkel je een cybersecurity awareness game, bijvoorbeeld in de vorm van een rollenspel of een app.

- **Contact:** Emiel Kerpershoek (E.F.P.Kerpershoek@hhs.nl)
- **Lectoraat:** Cybersecurity & Safety





Ervaring van een student

GPS-systemen spelen een cruciale rol in de maritieme sector, bijvoorbeeld bij het navigeren, het positioneren van schepen of het uitvoeren van onderwaterwerkzaamheden. Tegelijkertijd zijn deze systemen kwetsbaar voor spoofingaanvallen, waarbij foutieve locatiegegevens worden doorgestuurd. Dit kan leiden tot ernstige incidenten, zoals verkeerde positionering of onverwachte koerswijzigingen.

Mijn onderzoek richt zich op het detecteren van GPS-spoofing door GPS-data te manipuleren. In een gecontroleerde opstelling onderzocht ik of afwijkingen zichtbaar zijn en of deze gebruikt kunnen worden voor detectie. De resultaten geven inzicht in hoe dergelijke aanvallen herkend kunnen worden in operationele omgevingen.

Tijdens mijn stage heb ik zelfstandig gewerkt aan een technisch complex vraagstuk. Ik heb geleerd hoe ik een onderzoek systematisch opzet, meetresultaten analyseer en deze vertaal naar toepasbare inzichten. Het werken aan dit project heeft me vooral het belang laten inzien van onderzoek als fundament voor effectieve beveiligingsmaatregelen.

Emirhan Baser
Stagiair lectoraat Network & Systems Engineering Cyber Security



CYBER SECURITY & ORGANISATIE

Authenticatie binnen eHealth: veiligheid- en gebruiksvriendelijkheidsoverwegingen
(Nederlands/English)

Dit project richt zich op het onderzoeken van de authenticatiemechanismen, zoals wachtwoorden, tokens, biometrie, en bijvoorbeeld DigiD, die worden toegepast in eHealth oplossingen. Hierbij ligt de nadruk op het bestuderen van de authenticatielast bij kwetsbare gebruikersgroepen, zoals ouderen.

Het onderzoek omvat een literatuurstudie en interviews met experts en/of gebruikers.

- **Contact:** Niek Jan van den Hout (**n.j.vandenhout@hhs.nl**))
- **Lectoraat:** Cyber Security & Risk Management

Ervaring van een student

Technologie evolueert steeds sneller, en dat geldt ook voor Operationele Technologie (OT). Informatietechnologie (IT) en OT groeien steeds meer naar elkaar toe, maar dit brengt ook een aantal risico's met zich mee. Mijn onderzoek richt zich op de OT-beveiliging van Nederlandse gemeenten. Het doel was hierbij een oefenscenario te ontwikkelen dat bijdraagt aan de bewustwording bij gemeenten.

Tijdens mijn stage heb ik veel geleerd over OT en de beveiliging hiervan. Dit heeft sterk bijgedragen aan mijn eigen bewustwording en zal zeker van waarde zijn wanneer ik na mijn studie aan de slag ga in de informatiebeveiliging.

Ik heb mijn stage als zeer positief ervaren. De collega's zijn gezellig en staan altijd klaar om te helpen. Ook is er ruimte om thuis te werken en de begeleiding is uitstekend.

Stefan Wigt
Student HBO-ICT/ISM
Stagiair lectoraat Cybersecurity & Safety





CYBER SECURITY & TECHNIEK

Voor de projecten in het technisch domein zijn soms specifieke vaardigheden nodig. Geef aan welke ervaring je hebt op het gebied van: toegepaste security, programmeertalen (bijvoorbeeld Java/Python/C++), Linux power user, machine learning (AI) en reverse engineering.

For the internships or student projects in the technical domain, please specify your skills and interests on: applied security, programming language (e.g. Java/Python/C++), Linux power user, machine learning, reverse engineering.

Improve the stealthiness of OT Malware and enhance detection mechanism
(Nederlands/English)

This project aims to enhance OT malware designed for Modbus and Siemens S7 protocols by improving its stealth and boosting OT SOC monitoring. The goal is to provide insights into increasing cyber resilience in OT environments. Using the existing conveyor belt setup at THUAS lab in Delft, the project will follow these steps:

1. Install and test three operational scenarios on the conveyor belt system.
2. Adapt malware for the system.
3. Install and test Nozomi monitoring technology.
4. Activate malware and monitoring, detect it, and repeat.
5. Refine malware stealth and detection rules.
6. Final report and conclusions.

- **Contact:** Eric ten Bos (e.tenbos@hhs.nl)
- **Lectoraat:** Network & Systems Engineering Cyber Security

Detecting and Preventing GPS Spoofing on Ships
(Nederlands/English)

GPS and other GNSS systems (Global Navigation Satellite Systems) are essential for accurate navigation. GPS spoofing involves transmitting false signals, causing receivers to determine incorrect locations. This can have severe consequences, such as collisions or disruptions for ships maintaining a fixed position, for instance, during cable laying or underwater operations. Spoofing can also be used by state actors to create chaos and inflict damage. Detecting spoofing requires the implementation of a network monitoring tool to identify anomalous signals and patterns promptly, ensuring the integrity of GNSS usage.

- **Contact:** Eric ten Bos (e.tenbos@hhs.nl)
- **Lectoraat:** Network & Systems Engineering Cyber Security



Ervaring van een student

Tijdens mijn onderzoekstraject heb ik geleerd hoe zowel kwantitatieve benaderingen (het uitvoeren van experimenten) als kwalitatieve benaderingen (interviews afnemen) gecombineerd kunnen worden om een uitgebreid onderzoeksresultaat te krijgen uit een complex topic. Met mijn opdrachtgever had ik wekelijks informatieve meetings waarin ik feedback kreeg op de technische aspecten van de opdracht. Andere lectoraten van het kenniscentrum Cyber Security hielpen me bij de aanpak van deze benadering door gerichte feedback op mijn paper. Mijn ervaring bij het kenniscentrum was ontzettend leerzaam, en ik heb er zowel intern als extern veel verschillende mensen leren kennen. Er wordt gezegd dat dit werk eenzaam kan zijn, maar met de mensen van Cyber Security om me heen, heb ik mijn tijd als onderzoeker nooit echt als eenzaam ervaren.

Rachad Dhonre
Student HBO-ICT, Information Security Management
Stagiair Lectoraat Network & Systems Engineering Cyber Security



In de Dutch Innovation Factory (DIF) werken studenten samen met bedrijven en instellingen aan innovaties rond onder meer cybersecurity, smart mobility, eHealth en big data. In het gebouw zijn ruim 25 verschillende ICT-bedrijven en een internationaal georiënteerde start-up incubator gevestigd. Sommige projecten zullen (deels) plaatsvinden in onze locatie in Zoetermeer, die onderdeel is van de DIF.

DUTCH INNOVATION FACTORY



EXPERTISEGEBIEDEN

Ben je docent en/of coördinator van een vak, minor of module en zoek je gastdocenten voor specifieke onderwerpen gerelateerd aan cybersecurity en cybercrime? Bekijk hieronder welke expertise ons onderzoeksteam te bieden heeft. Neem contact met ons op om de mogelijkheden te bespreken!

Cybercrime

Cyberdelicten, online crimineel gedrag, online slachtofferschap (burgers en bedrijven), cybercriminele netwerken, georganiseerde criminaliteit, ondermijning, interventies en straf-trajecten, digitale recherche/ politie

Gastdocenten / experts
Susanne van 't Hoff – de Goede
Asier Moneva
Marco Romagna
Luuk Bekkers
Sifra Matthijsse

Wet- en regelgeving

Law in cybercrime, AVG, nationale cybersecurity, cybersecurity & globalisering

Gastdocenten / experts
Marco Romagna

Online gedrag

Attitudes en intenties, sociale psychologie, cyberveilig gedrag, gedragsbeïnvloeding, metingen & oplossingen, cyberweerbaarheid

Gastdocenten / experts
Emiel Kerpershoek
Marinus Maris
Michelle Ancher

Social engineering

Gedragsbeïnvloeding, nudging, security-by-design, phishing

Gastdocenten / experts
Michelle Ancher
Luuk Bekkers

Cybersecurity governance

Organiseren van cybersecurity, cyberveilig gedrag binnen organisaties

Gastdocenten / experts
Herman de Bruine
Emiel Kerpershoek
Niek Jan van den Hout

Hacktivism en ethisch hacken

Hacktivism, cyberrange, capture-the-flag

Gastdocenten / experts
Marco Romagna
Mike Gilhespy
Pieter Burghouwt

Internet of Things

(IoT), Trusted IoT, trusted computing (general)

Gastdocent / expert
Eric ten Bos

Onderzoeks-vaardigheden

Onderzoeksmethoden, statistiek, interviewvaardigheden, surveyontwikkeling

Gastdocenten / experts
Asier Moneva
Susanne van 't Hoff – de Goede
Emiel Kerpershoek

Cybersecurity risk management

Risk assessment & management, cyber threat and vulnerability analysis, effective counter measures

Gastdocent / expert
Peter Roelofsma
Niek Jan van den Hout

Mathematics

Gastdocent / expert
Sam van Buuren



Adresgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

cybersecurity@hhs.nl

dehaagsehogeschool.nl