



**STAGE EN ONDERZOEK BIJ
HET CENTRE OF EXPERTISE
CYBER SECURITY
DECEMBER 2024**

let's change
YOU. US. THE WORLD.

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.



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.

“Mijn stage was een leerzame ervaring die mij heeft geholpen mijn interesse in digitale oplossingen en inclusieve technologie verder te verdiepen”

Mutlu Dervisev

Student HBO-ICT

Stagiair lectoraat Risk Management & Cyber Security

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 september 2024 tot en met januari 2025 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

Tijdens mijn stage bij het kenniscentrum Cyber Security heb ik de gebruiksvriendelijkheid van Europese digitale identiteitsoplossingen onderzocht, met een focus op eHealth-platforms. In mijn onderzoek keek ik naar de uitdagingen die kwetsbare groepen, zoals ouderen en mensen met beperkte digitale vaardigheden, ervaren bij het gebruik van authenticatiemethoden zoals wachtwoorden, biometrie en tokens. Door deze systemen te analyseren, heb ik geprobeerd bij te dragen aan veiligere en beter toegankelijke digitale oplossingen voor iedereen. Daarnaast bood het onderzoek inzicht in hoe technologische ontwikkelingen in de digitale gezondheidszorg inclusiever kunnen worden ingezet.

Ik heb mijn stage als zeer waardevol ervaren. Naast dat ik veel heb geleerd over praktijkgericht onderzoek en authenticatiemechanismen, heb ik mijn onderzoeks- en analysevaardigheden verder kunnen ontwikkelen. Ook de begeleiding was erg prettig; ik kon altijd terecht bij mijn begeleider of collega's voor vragen of feedback. Door het bijwonen van verschillende overleggen en brainstormsessies heb ik daarnaast een goed beeld gekregen van het onderzoeksveld. Het was een leerzame ervaring die mij heeft geholpen om mijn interesse in digitale oplossingen en inclusieve technologie verder te verdiepen.

Mutlu Dervisev

Student HBO-ICT/ISM
Stagiair lectoraat Risk Management & Cyber Security

CYBER SECURITY & GEDRAG

Exploring pathways to cybercrime through web searches (English)

Internet users interested in cybercrime use search engines such as Google and platforms such as YouTube to search for related information. Some of this information is stored by Internet service providers and can be accessed by researchers through web scrapers, application programming interfaces (APIs), and observation. The information retrieved can be linked to real-world events and the interests of internet users, providing valuable insight into their pathways to cybercrime.

- **Contact:** Asier Moneva (a.monevapardo@hhs.nl)
- **Lectoraat:** Cybercrime & Cybersecurity

Serious Games for cyber-awareness: app development Supervision (Nederlands/English)

Municipalities have many responsibilities that intersect with cyber security. Often, a clear overview of who is exactly responsible for what is lacking, a potential security risk. To foster more awareness of this problem, we aim to develop a serious game tackling this problem. A skeleton ruleset stands but needs to be developed further. Especially the development of a supporting app is a priority, though we will also create more scenarios and sharpen the rules. This internship is especially suited to someone interested in game development, or someone with gaming experience interested in app development.

- **Contact:** Sam van Buuren (psvbuuren@hhs.nl)
- **Lectoraat:** Cybersecurity & Safety

Testing tracking software to detect cybercriminal behavior (English)

Accurately capturing illicit behavior of Internet users is a challenging task. What users say they do usually does not align well with what they actually do. Tracking software can collect objective measures of online behavior with high accuracy to help better understand cybercriminal activities. There are multiple tools that can serve this purpose, such as keyloggers or network traffic monitors. Case studies can be used to unveil the potential of these tools to detect cybercrime.

- **Contact:** Asier Moneva (a.monevapardo@hhs.nl)
- **Lectoraat:** Cybercrime & Cybersecurity

Building an experiment on safe online behavior (English/Nederlands)

At the Human Factor in Cybercrime Lab, we are working on an online environment that allows us to measure and change online behavior. This makes it possible, for example, to observe how people actually behave online. We also use the Lab to develop and test interventions, such as by building an app or other software. There are two internship positions available:

For Assignment 1, we are looking for students who can build an application or other program to promote safe online behavior. Previously, for example, an application was built that 'required' users to update their phone software. Every day the user didn't update the software, a digital 'crack' on the screen grew larger until the phone could no longer be used. Note: For this assignment, you must have programming skills and the ability to develop software.

For Assignment 2, we are looking for students who want to design, develop, and test an intervention using scientific research. This involves a complete description of the developed intervention and its scientific basis. The intervention is then developed further and tested, for instance, among fellow students. Programming skills are not required for this assignment.

Both assignments are intended as internships for third-year students. Please specify which assignment you are applying for in your application and explain why you are interested in a research internship.

- **Contact:** Madelief Akkerman (m.akkerman@hhs.nl)
- **Lectoraat:** Cybercrime & Cybersecurity

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:** Marcel Spruit (m.e.m.spruit@hhs.nl)
- **Lectoraat:** Cybersecurity & Safety

Ervaring van een student

Met de groeiende integratie van het internet in ons dagelijks leven zijn online criminele activiteiten, zoals oplichting, hacking en ransomware, niet langer beperkt tot experts. Fraude treft nu zowel individuen als bedrijven, in verschillende vormen zoals online winkelfraude, identiteitsdiefstal en phishing. In Nederland wordt dan ook één op de zes personen slachtoffer van dergelijke misdaden.

Mijn onderzoek richt zich op de factoren die van invloed zijn op de beslissingen van slachtoffers om civiele procedures te starten om schade te verhalen. Uit de literatuur blijkt dat er aarzeling blijft bestaan om civiele procedures te starten, vanwege onder andere zorgen over de kans op succes, represailles en gebrek aan kennis over het proces. Deze mogelijke obstakels heb ik in kaart gebracht via een vragenlijst en bevindingen verkregen over de perceptie van respondenten over deze obstakels.

Tijdens mijn stage bij het CoECS heb ik veel geleerd over een onderwerp dat voorheen voor mij onbekend was. Door wekelijkse meetings en discussiesessies kreeg ik de kans om kennis op te doen van andere onderzoekers binnen het CoECS. Ik heb mijn stage als erg leerzaam ervaren en het heeft mij geholpen om te ontdekken of de onderzoekswereld bij mij past.

Naomi Cairo

Student Sociology: Contemporary Social Problems Universiteit Utrecht
Stagiaire lectoraat Cybercrime & Cybersecurity

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

Exploring implemented password lock-out strategies on websites (Nederlands/English)

This project will explore and review what kind of password lock-out strategies are implemented on websites. Password lock-out strategies can include a threshold for a maximum amount of incorrect password attempts before a user account is locked. Preliminary research suggests that the implemented threshold varies greatly, from three tries to no threshold at all. This project will dive into this topic deeper, by looking at current industry guidelines and review a large sample of websites to find out how they implement these guidelines.

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



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

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 [English/Nederlands]

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 [English/Dutch]

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:** Gert den Neijssel (g.c.h.denneijssel@hhs.nl) i.s.m. Eric ten Bos
- **Lectoraat:** Network & Systems Engineering Cyber Security

Ervaring van een student

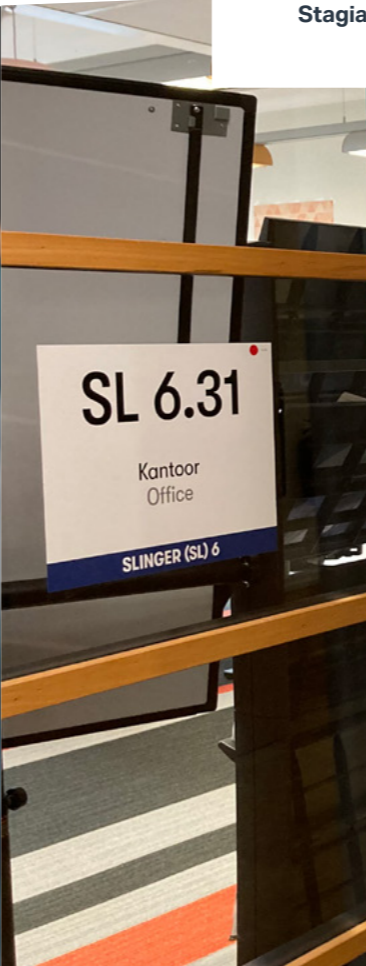
Voor mijn stage heb ik een onderzoek gedaan naar de cyberweerbaarheid van de operationele technologie (OT) van gemeenten en hoe we dit kunnen verbeteren via serious games en awareness. Zo heb ik tijdens mijn onderzoek gekeken naar hoe awareness campagnes in elkaar zitten en hoe ik houding en gedrag van een persoon kan veranderen. Tegelijkertijd heb ik gekeken naar wat voor factoren er zitten in het gedrag van een persoon en hoe je daarmee de effectiviteit van de scenario's kan verhogen. Ook heb ik hierbij gemeenten geïnterviewd om te weten te komen wat de huidige staat is van de informatiebeveiliging en wat er nog verbeterd kan worden bij de gemeenten in Nederland. Het is belangrijk dat er naar de beveiliging wordt gekeken van OT-systemen

Tijdens mijn stage bij het kenniscentrum Cyber Security heb ik mijn onderzoekvaardigheden verbeterd. Ik heb ook meer geleerd over wat OT-systemen zijn en hoe ze gebruikt worden. Wat ik hiervoor eigenlijk niet zo heel goed wist. Ik vond het ook leerzaam en leuk om erachter te komen dat er al veel geprobeerd wordt om awareness te verbeteren door gebruik te maken van serious games en andere oefen scenario's.

Ik heb een leuke ervaring gehad bij het kenniscentrum en word ook goed begeleid tijdens mijn onderzoek. Wekelijks heb ik samen met mijn begeleider gekeken naar het werk dat ik gedaan had de afgelopen week en hebben we samen gekeken naar wat er verbeterd kon worden en wat de volgende stappen zijn. Dit hielp mij goed het overzicht te houden en vond ik erg fijn.

Quinten Ringenier
Student HBO-ICT/ISM
Stagiair lectoraat Cybersecurity & Safety

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.



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 straftrajecten, 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
Marcel Spruit
Michelle Ancher

Social engineering

Gedragsbeïnvloeding, nudging, security-by-design, phishing

Gastdocenten / experts

Michelle Ancher
Luuk Bekkers
Natalia Zwarts

Cybersecurity governance

Organiseren van cybersecurity, cyberveilig gedrag binnen organisaties

Gastdocenten / experts

Marcel Spruit
Herman de Bruine
Emiel Kerpershoek
Niek Jan van den Hout
Natalia Zwarts

Hactivism en ethisch hacken

Hactivism, 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

Gastdocenten/experts

Peter Roelofsma
Niek Jan van den Hout
Natalia Zwarts

Mathematics

Gastdocent/expert

Sam van Buuren



Adresgegevens



Johanna Westerdijkplein 75
2521 EN Den Haag



cybersecurity@hhs.nl



dehaagsehogeschool.nl