



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

**JUNI 2023**

**let's change**  
YOU. US. THE WORLD.

**DE HAAGSE**  
HOGESCHOOL

# Cybersecurity is belangrijk voor iedereen

We leven in een samenleving waarin niet alleen digitale ontwikkelingen, maar daarmee 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, inclusief grote financiële schade.

Omdat iedereen in meer of mindere mate gebruik maakt van digitale systemen en netwerken is cybersecurity relevant 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

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

Als stagiair word je onderdeel 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 kan gaan beantwoorden. Dit doe je niet alleen door literatuur te lezen, maar ook door het opzetten van een experiment of interviews af te nemen. In sommige projecten werk je ook aan een praktische oplossing of tool (bijvoorbeeld een app) die bedrijven en organisaties kunnen gaan 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.

**“ Tijdens mijn stage heb ik erg veel kennis opgedaan over cybercriminaliteit en over hoe je een compleet onderzoekstraject vormgeeft. ”**

**Mir Kurmandj**

Student Information Security Management  
Lectoraat Cybercrime & Cybersecurity



## Interesse?

Wil je bij ons stage komen lopen? Solliciteer dan op een van de projecten in deze brochure. Let op: de meeste projecten zijn geschikt voor studenten in het 3e of 4e jaar. Check zelf bij je opleiding wat de vereisten zijn voor een stage. Binnen onze stages ligt de nadruk op het uitvoeren van praktijkgericht onderzoek.

## Hoe solliciteer ik?

Je stuurt 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. Pas na dit kennismakingsgesprek wordt bepaald of je inderdaad kan starten als stagiair. Afspraken met je begeleider worden vervolgens vastgelegd in een stageovereenkomst.

## Andere vragen?

Is het onderwerp van je eerste keuze niet meer beschikbaar of heb je andere algemene vragen? Neem dan contact op via [cybersecurity@hhs.nl](mailto:cybersecurity@hhs.nl) met een toelichtende mail welke onderwerpen je interesseren. We kijken dan of er wellicht toch een match te maken 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. Per project staat een contactpersoon bij wie je kan solliciteren voor een stageplaats. In principe zijn dit projecten die in de periode september 2023 tot en met januari 2024 lopen. Mocht je voor een andere periode een stage zoeken, informeer dan via de contactpersoon bij 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 aankomend semester. In een aantal projecten zijn we afhankelijk van de planning en inzet van andere organisaties of bedrijven. Mocht tijdens je sollicitatie blijken dat de periode van het project niet meer goed past bij je stageperiode, dan word je hierover geïnformeerd en kijken we samen met je of er op een ander onderwerp alsnog mogelijkheden zijn.

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



# CYBER SECURITY & GEDRAG

## Experiment bouwen rondom veilig online gedrag (English/Nederlands)

In het Human Factor in Cybercrime Lab werken wij aan een online omgeving waarmee we online gedrag kunnen meten en veranderen. Hierdoor is het bijvoorbeeld mogelijk te observeren hoe mensen zich daadwerkelijk gedragen online. Ook gebruiken wij het Lab om interventies te ontwikkelen en testen, bijvoorbeeld door het bouwen van een app of andere software. Er zijn twee stage vacatures:

- Voor opdracht 1 zoeken we studenten die een applicatie of ander programma kunnen bouwen om veilig online gedrag te kunnen bevorderen. Eerder is bijvoorbeeld een applicatie gebouwd waarmee het updaten van telefoonsoftware werd 'verplicht'. Elke dag dat de gebruiker de software niet update werd een digitale 'barst' in het scherm groter tot de telefoon niet meer kon worden gebruikt. Let op: voor deze opdracht moet je beschikken over programmeervaardigheden en de skills om software te ontwikkelen.
- Voor opdracht 2 zoeken we studenten die met behulp van wetenschappelijk onderzoek een interventie willen bedenken, uitwerken en testen. Het gaat hier om een volledige beschrijving van de ontwikkelde interventie en welke wetenschappelijke grondslag deze heeft. Vervolgens wordt de interventie uitgewerkt en getest onder bijvoorbeeld mede-studenten. Hiervoor is het niet noodzakelijk om over programmeervaardigheden te beschikken.

Beide opdrachten zijn bedoeld als meeloopstage voor een 3e jaars student. Vermeld bij je sollicitatie voor welke opdracht je solliciteert en motiveer waarom je interesse hebt in een onderzoeksstage.

- **Contact:** Maaike van der Wal (m.l.vanderwal@hhs.nl)
- **Lectoraat:** Cybercrime & Cybersecurity

## Online seksueel misbruik / Romance scams; perceptie en impact op slachtoffers

Als stagiair neem je deel aan een onderzoeksproject naar de impact van slachtofferschap van online criminaliteit en doe je individueel onderzoek naar perceptie, attitude en gedrag ten aanzien van online seksueel misbruik.

- Contact:** Raoul Notté (r.j.notte@hhs.nl)
- Lectoraat:** Cybercrime & Cybersecurity

## Ervaring van een student

Tijdens mijn afstudeerstage deed ik onderzoek naar de impact van cybercrime op slachtoffers volgens mondiale experts en welke behoeftes slachtoffers van cybercrime hebben. Dit heb ik zo goed mogelijk in kaart gebracht met behulp van een vragenlijst, die ik zelf heb opgesteld. Hieruit kwam naar voren dat de impact van cybercriminaliteit in alle landen wel groot is. In deze stageperiode heb ik geleerd om vooral zelfstandig om te gaan met moeilijkheden binnen mijn eigen onderzoek. Hierbij heb ik alle benodigde hulp om mij heen gekregen om mijn onderzoek succesvol af te ronden. Iedereen in het CoECS staat ervoor open om je te helpen en je feedback te geven bij je onderzoek. Mijn stage vond plaats in het lectoraat Cybercrime & Cybersecurity. Door wekelijkse meetings en discussiesessies werd ik indirect geholpen met mijn eigen onderzoek. Ik leerde daar ook veel over onderzoeken van de andere onderzoekers van het CoECS. Als stagiair word je echt met open armen ontvangen binnen het kenniscentrum, waarbij je super veel kan leren van mede-onderzoekers. Zo is iedereen ook altijd bereid om je vragen te beantwoorden. Tijdens mijn stage heb ik erg veel kennis opgedaan over cybercriminaliteit en over hoe je een compleet onderzoekstraject vormgeeft.

### Mir Kurmandj

**Student HBO-ICT, Information Security Management, De Haagse Hogeschool**  
**Stagiair lectoraat Cybercrime & Cybersecurity**  
(februari - juli 2023).



# 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](mailto:a.monevapardo@hhs.nl))
- **Lectoraat:** Cybercrime & Cybersecurity

## 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](mailto:a.monevapardo@hhs.nl))
- **Lectoraat:** Cybercrime & Cybersecurity

## Ontwikkeling awareness game

Mensen (inclusief werknemers van een organisatie of bedrijf) zijn sterk afhankelijk geworden van digitale systemen, maar niet iedereen is zich daar voldoende van bewust. Een game kan een goed hulpmiddel zijn om mensen meer bewust te maken van de digitale risico's die ze lopen en de maatregelen die daarvoor nodig zijn. Binnen dit project ontwikkel je een cybersecurity awareness game, bijvoorbeeld als rollenspel of in de vorm van een app.

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



## Ervaring van een student

Ransomware aanvallen vormen een groot probleem voor het MKB in Nederland en brengen veel negatieve consequenties met zich mee. Als stagiaire voor het CoECS onderzocht ik middels kwalitatieve interviews hoe het besluitvormingsproces er voor het MKB uit zou zien als zij slachtoffer zouden worden van een ransomware aanval, en welke factoren hierin een beslissende rol zouden kunnen spelen. Op basis van deze resultaten, werd de hulpbehoefte van het MKB in kaart gebracht en werd er beleidsadvies gegeven.

Tijdens mijn stage bij het CoECS heb ik ontzettend veel geleerd over hoe de wereld van cyber security eruit ziet. Ook kreeg ik veel ruimte om mijn onderzoeksvaardigheden te verbeteren en kon ik altijd bij iemand terecht voor vragen. Ik werkte nauw samen met mijn supervisor en kreeg tegelijkertijd ruimte om zelfstandig te werk te gaan. Er worden regelmatig meetings georganiseerd waarin ik veel over de lopende onderzoeken van mijn collega's leerde en waarin ik ook ruimte kreeg om mijn visie te delen. Al met al ervaarde ik mijn stage als erg leerzaam en zinvol en kijk ik er positief op terug.

### Filipa Thoma

**Student Sociology: Contemporary Social Problems**  
Universiteit Utrecht  
Stagiaire lectoraat Cybercrime & Cybersecurity  
(februari – juli 2023).

# 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 (bv. 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.

## Finding Smart Home Devices on the Web? Are they Vulnerable? (English/Nederlands)

Citizens in the Netherlands increasingly have smart home devices, such as smart vacuum cleaners, washing machines, microwaves, and, of course, a doorbell. Can these devices be found online and are they vulnerable to cyber-attacks? The objectives of this research are to (a) understand the protocols that are being used in smart home devices, (b) find smart home devices using the internet, (c) help identify most used smart home devices, (d) help identify the attack surface of smart home devices, (e) create awareness on this topic.

- **Contact:** Saman Tamo ([s.tamo@hhs.nl](mailto:s.tamo@hhs.nl))
- **Lectoraat:** Network & Systems Engineering Cyber Security

## Cyber Threat Intelligence on the IoT Honeypot (English/Nederlands)

Preliminary research on different kind of cyber threat intelligence processes and tools for the IoT-Honeypot. The objectives of this research are (a) to understand how IoT Honeypots are being used in a cyber threat intelligence process, (b) build an actual cyber threat intelligence process for the IoT Honeypot in a learning environment, (c) use the output from the IoT Honeypot in the cyber threat intelligence process, (d) share information about threats publicly.

- **Contact:** Saman Tamo ([s.tamo@hhs.nl](mailto:s.tamo@hhs.nl))
- **Lectoraat:** Network & Systems Engineering Cyber Security

## Hack Dutch Municipality Websites with Responsible Disclosure: Assessing Vulnerabilities (English/Nederlands)

This research aims to explore the vulnerabilities present in Dutch municipality websites and evaluate the effectiveness of responsible disclosure practices in mitigating security risks. The objectives of this research are to (a) identify common vulnerabilities present in municipality websites that could potentially be exploited by hackers, (b) investigate the challenges and benefits associated with implementing responsible disclosure practices in the context of municipality websites, (c) evaluate how municipalities handle reported vulnerabilities through responsible disclosure processes, including their responsiveness, timeliness, and effectiveness in addressing security issues.

- **Contact:** Saman Tamo ([s.tamo@hhs.nl](mailto:s.tamo@hhs.nl))
- **Lectoraat:** Network & Systems Engineering Cyber Security

## Using large language models to generate a corpus of binary exploitation challenges for use in education. (English)

The offensive security skills of reverse engineering and exploiting software play an important role in the field of software security. To facilitate the process of learning these skills, students are provided with vulnerable programs on which to practice. An issue can be that once such a program becomes known, full solutions are quickly to be found online. The purpose of this project is to leverage the capabilities of large language models to generate a corpus of such vulnerable programs which differ sufficiently from a provided "seed program" to provide a unique challenge for each student undergoing a course in software exploitation.

Students wishing to participate in this internship should have:

- Programming experience (windows and linux)
- Experience in software exploitation (or the desire and ability to learn very fast)
- Experience with or interest in the use of large language models to automate tasks

The end deliverables for this internship are:

- A working system to generate challenges according to a set of criteria
- A presentation and research paper

- **Contact:** Mike Gilhespy ([m.d.gilhespy@hhs.nl](mailto:m.d.gilhespy@hhs.nl))
- **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.





## How to create value from IIoT SOC monitoring in an OT environment (English/Nederlands)

**Niveau:** afstudeerder • **Locatie:** HHS, Delft

Samengestelde opdracht voor meerdere (>3) studenten

1. Design and build the environment
2. Design and realize attack vectors (offensive)
3. Design and realize IT, IIoT and OT monitoring (defensive)
4. Exercise purple team and improve attack techniques and monitoring

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

## Offensive attack surface reduction (English/Nederlands)

**Niveau:** afstudeerder • **Locatie:** Thales, Huizen

Op basis van externe threat en IOC kennis (internet) beschikbare informatie over een specifiek bedrijf geautomatiseerd vinden met focus op OT entry-points. Hieruit volgend een ontwerp maken over hoe OT aanvalsvectoren te reduceren.

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

## Operationele SOC-rapportages in detail automatiseren (English/Nederlands)

**Niveau:** derdejaars • **Locatie:** Thales, Huizen

Geautomatiseerd rapportages maken op basis van in datalake aanwezige data. Modulair opzetten.

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

## Ervaring van een student

Digitalisation is becoming a current hot issue in the EU and The Netherlands, for which at the EU level NIS and NIS2 Directives have arisen to reach a high common level of cybersecurity. However, there is often a misunderstanding of what these laws mean in practice as well as to what extent national entities are liable by them. In my internship project, I researched how cybersecurity risk-management measures are developed in practice by the Dutch governmental entities, public and private organisations; and, what is the process they follow to comply with these measures. The result was a qualitative study with interviews to both governmental institutions, public and private entities, after which I came up with policy recommendations that would be useful for them.

During my internship, I met nice colleagues and professionals. Monthly, we have various Centre's meetings thanks to which I gained research, analytical, public speaking and time management skills. These meetings also gave me feedback on my on going work. I worked closely with my supervisor in the Centre, collaborated with researchers, lecturers, governmental institutions and legal practitioners in The Netherlands. By carrying out my interviews and having possibilities to attend different conferences in both Brussels and The Hague, I learnt how to combine both cybersecurity risk-management and EU studies, while coming up with recommendations that can have a practical impact. It has been a great experience both personally and professionally that I would cherish forever.

### Virginia González

Student European Governance, Universiteit Utrecht  
Stagiaire lectoraat Risk Management & Cybersecurity (Februari - juni 2023)

## THALES

Vanuit ons lectoraat Network & Systems Engineering Cyber Security werkt de Haagse Hogeschool (HHS) sinds 2016 samen met Thales Nederland. Thales richt zich binnen de samenwerking vooral op de technische kant van cybersecurity, zoals het leveren van systemen die cyberdreigingen detecteren. In 2023 werd deze samenwerking voor vier jaar verlengd en werden vanuit Thales een nieuwe lector en onderzoeker aangesteld binnen het lectoraat, waar zij samenwerken met docent-onderzoekers van de Haagse Hogeschool (HBO-ICT). Door het benutten van elkaars expertise, versterken Thales en de HHS elkaar in het doen van innovatief praktijkgericht onderzoek.



# EXPERTISEGEBIEDEN

Ben je docent en/of coördinator van een vak/minor/module en zoek je gastdocenten voor specifieke onderwerpen gerelateerd aan cybersecurity en cybercrime?

Zie hieronder welke expertise wij in ons onderzoeksteam hebben.

Neem contact met ons op voor de mogelijkheden!

## 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  
Raoul Notté  
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  
Deborah Oosting  
Marinus Maris  
Céline Kreffer  
Marcel Spruit  
Michelle Ancher

## Social engineering

Gedragsbeïnvloeding, nudging, security-by-design, phishing

### Gastdocenten / experts

Michelle Ancher  
Luuk Bekkers  
Saman Tamo

## Cybersecurity governance

Organiseren van cybersecurity, cyberveilig gedrag binnen organisaties

### Gastdocenten / experts

Marcel Spruit  
Herman de Bruine  
Emiel Kerpershoek

## Hactivism en ethisch hacken

Hactivism, cyberrange, capture-the-flag

### Gastdocenten / experts

Marco Romagna  
Mike Gilhespy  
Pieter Burghouwt  
Saman Tamo

## Internet of Things

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

### Gastdocent / expert

Eric ten Bos

## Onderzoeksvaardigheden

Onderzoeksmethoden, statistiek, interviewvaardigheden, surveyontwikkeling

### Gastdocenten / experts

Asier Moneva  
Susanne van 't Hoff – de Goede  
Deborah Oosting  
Emiel Kerpershoek

## Cybersecurity risk management

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

### Gastdocent / expert

Matej Dolinsek

## Ervaring van een student

As my internship project, I wrote a thesis on the causality between cybercrime victimisation and the fear of it, using longitudinal data with two waves. While both longitudinal research and cybercrime as a research subject were fairly new for me at the beginning of the internship, this project combined with the support and feedback from my supervisors helped me gain a lot of knowledge and experience on the subject, which is probably why my interest in cybercrime research grew more and more during the internship.

In addition to having supportive supervisors at the centre, other colleagues also welcomed us interns to the team and the atmosphere at the office was always great. Team meetings, where for instance research ethics and methods were discussed, provided technical knowledge that I can use in my future career, but also gave an opportunity to see what are some questions other researchers may struggle with and how these can be collectively answered. All in all, I feel lucky for having landed an internship at CoECS!

### **Pirkko Sarkki**

**Student Sociology: Contemporary Social Problems,  
Utrecht University (February 2023 – June 2023)**



## Adresgegevens



Johanna Westerdijkplein 75  
2521 EN Den Haag



[cybersecurity@hhs.nl](mailto:cybersecurity@hhs.nl)



[dehaagsehogeschool.nl](http://dehaagsehogeschool.nl)