let's change
YOU. US. THE WORLD.

# STAGE EN ONDERZOEK BIJ HET CENTRE OF EXPERTISE CYBER SECURITY

## JUNI 2024

DE HAAGSE HOGESCHOOL

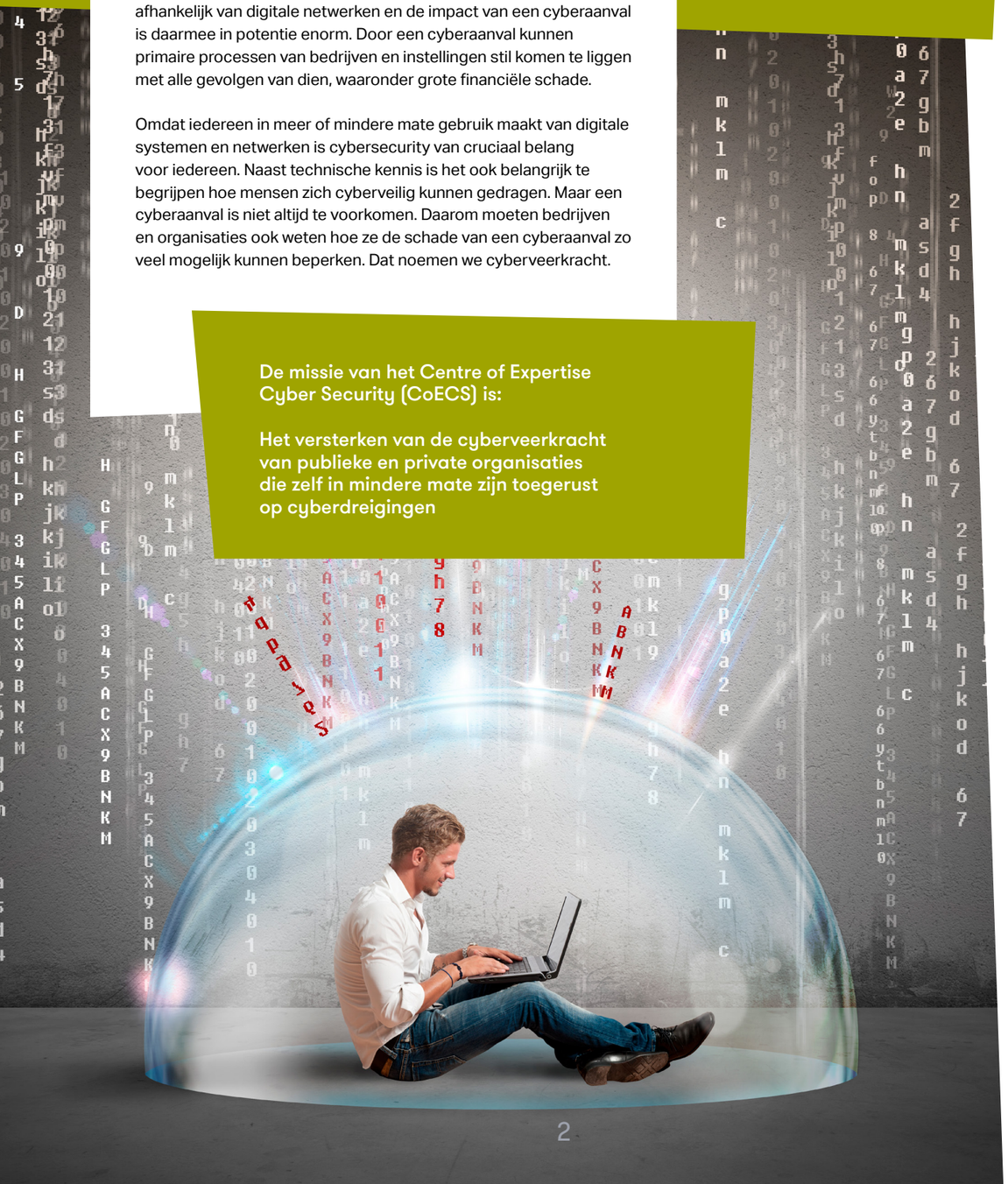
# Cybersecurity is belangrijk voor iedereen

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.

**“Tijdens mijn stage heb ik ontzettend veel geleerd over de wereld van cyber security en heb ik mijn onderzoeksvaardigheden verbeterd”**

**Filipa Thoma**
Student Sociology - Universiteit Utrecht
Lectoraat Cybercrime & Cybersecurity
(januari-juli 2023)


## 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 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

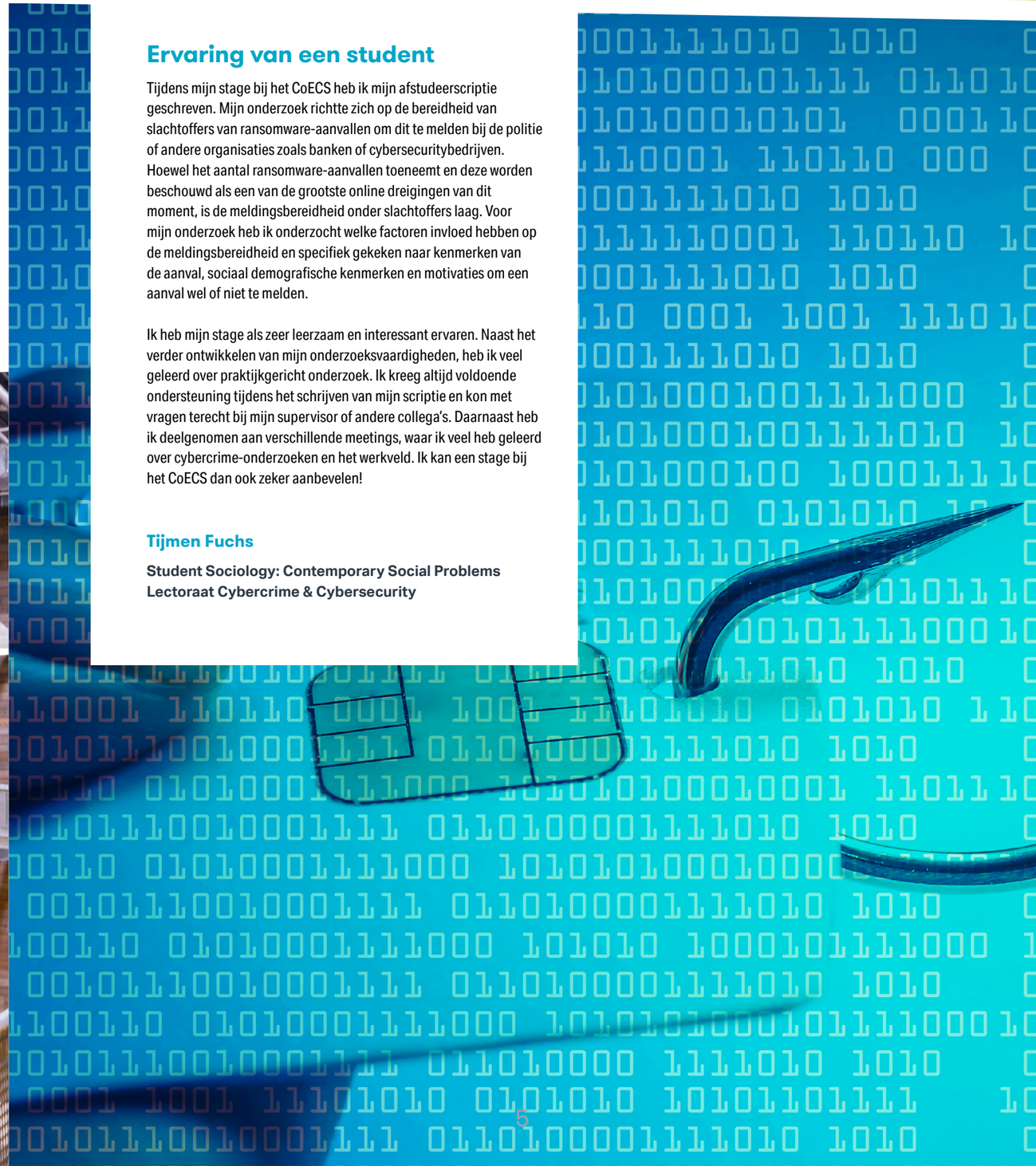
## Ervaring van een student

Tijdens mijn stage bij het CoECS heb ik mijn afstudeerscriptie geschreven. Mijn onderzoek richtte zich op de bereidheid van slachtoffers van ransomware-aanvallen om dit te melden bij de politie of andere organisaties zoals banken of cybersecuritybedrijven. Hoewel het aantal ransomware-aanvallen toeneemt en deze worden beschouwd als een van de grootste online dreigingen van dit moment, is de meldingsbereidheid onder slachtoffers laag. Voor mijn onderzoek heb ik onderzocht welke factoren invloed hebben op de meldingsbereidheid en specifiek gekeken naar kenmerken van de aanval, sociaal demografische kenmerken en motivaties om een aanval wel of niet te melden.

Ik heb mijn stage als zeer leerzaam en interessant ervaren. Naast het verder ontwikkelen van mijn onderzoeksvaardigheden, heb ik veel geleerd over praktijkgericht onderzoek. Ik kreeg altijd voldoende ondersteuning tijdens het schrijven van mijn scriptie en kon met vragen terecht bij mijn supervisor of andere collega's. Daarnaast heb ik deelgenomen aan verschillende meetings, waar ik veel heb geleerd over cybercrime-onderzoeken en het werkveld. Ik kan een stage bij het CoECS dan ook zeker aanbevelen!

**Tijmen Fuchs**

**Student Sociology: Contemporary Social Problems**
**Lectoraat Cybercrime & Cybersecurity**



# 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

### 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

### 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

### 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 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 meelopstage voor een 3e jaars student. Vermeld bij je sollicitatie voor welke opdracht je solliciteert en motiveer waarom je interesse hebt in een onderzoeksstage.

- **Contact:** Susanne van 't Hoff-de Goede (m.s.vanthoff-degoede@hhs.nl)
- **Lectoraat:** Cybercrime & Cybersecurity


### 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

### Prioritization of cybersecurity decisions within organizations (Nederlands/English)

This research focuses on categorizing key decisions regarding cybersecurity using different attributes such as impact, urgency, and costs. The main method chosen for this topic is rough set approach to multi attribute decision analysis, leveraging the mathematical representation of vague decision environments. This project will require understanding of different levels of cybersecurity responsibility within organization and risk management methods. The outcome of the research is aimed at mapping the most urgent, impactful and risky decisions.

- **Contact:** Natalia Zwarts (n.h.zwarts@hhs.nl)
- **Lectoraat:** Risk Management & Cyber Security

### Wat voor authenticatiemechanismen worden gebruikt bij eHealth in de thuisomgeving van de patiënt en wat zijn bijbehorende veiligheidsoverwegingen? (Nederlands/English)

Dit project richt zich op het begrijpen van de authenticatiemechanismen, zoals wachtwoorden, tokens, biometrie, en bijvoorbeeld DigiD, die worden toegepast in eHealth voor patiënten in hun thuisomgeving, en op de bijbehorende veiligheidsoverwegingen, inclusief veiligheidseisen. Het onderzoek omvat een literatuurstudie en interviews met experts.

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

### The risk of no decision in cybersecurity (Nederlands/English)

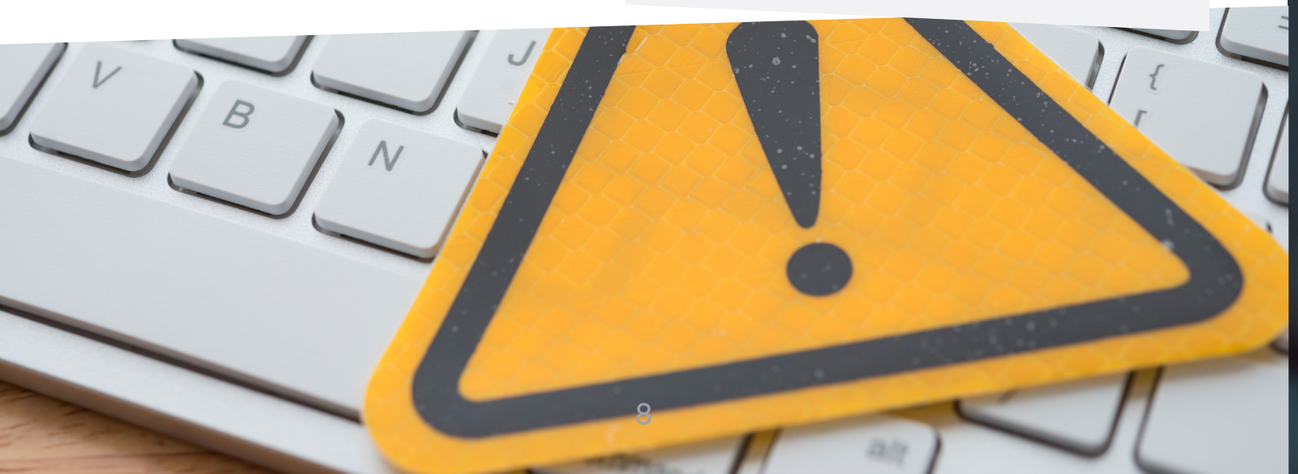
Most of the existing research focuses on the consequences of wrong decisions in times of cyber crisis. This project is aimed at exploring alternative setup, where the risk of not making any decision is described. This research requires multi-disciplinary approach to recognize the patterns of decision-making, as well as specific scenarios to explain the problem of not reaching a decision. The outcome of this research should present the risk of lack of decisions in a cybersecurity context.

- **Contact:** Natalia Zwarts (n.h.zwarts@hhs.nl)
- **Lectoraat:** Risk Management & Cyber Security

### 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

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)**

# 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.**

## OT Malware research & development for specific attack types (Nederlands/English)

This final assignment ('afstudeerder') is about extending generic malware towards more specific OT attacks on matching hardware. The first step in this assignment is to explore attack vectors beyond the current state of art. Subsequently the existing generic framework of attack malware needs to aim at specific hardware types. The necessary research and implementation of this is within the scope of the assignment.

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

## Segmented cyber resilient network architectures (Nederlands/English)

This internship is about investigating network infrastructures. Often existing infrastructures carry sensitive information, but also need external connectivity. Integrating untrusted network connectivity in segmented networks therefore requires measures to avoid compromises on the confidentiality, integrity and availability of the network infrastructure. Part of this assignment is to evaluate if the "Zones and Conduits"-model can be successfully applied.

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

## Automated playbooks for isolated Detection and Response (Nederlands/English)

The challenge in this assignment is formed by infrastructures that are not always well connected and may therefore not be helped with remote cyber expertise. For instance, infrastructures in remote areas may face cyber threats without having cyber expertise nearby. The goal of this assignment is to investigate and prototype automated playbooks for responding to cyber threats.

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

## IoT Malware investigation & development (Nederlands/English)

The goal of this assignment is to investigate and experiment with IoT malware techniques. IoT devices are virtually everywhere and often using popular protocols like MQTT. In this context MQTT command injection or automated reverse shell attacks need to be investigated on their usefulness. Based on the investigation, a feasible IoT Malware solution is implemented and evaluated.

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

## Challenges in Data-Centric Security solutions (Nederlands/English)

In general, parties that need to collaborate will need to share information. Data-centric security is a concept for protecting information rather than for instance the location where is it stored.
By doing so, information is encrypted and the next challenge is to control access to the encryption keys.
The goal of this assignment is to perform a survey on data centric security techniques to build trust relationships in untrusted networks and on efficient techniques to control the use of encryption keys.

- **Contact:** Sam van Buuren (p.s.vanbuuren@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.**

DUTCH INNOVATION FACTORY



## Pentesting tools for cloud environments and risk levels related to data storage (Nederlands/English)

This research is aimed at collecting the state-of-the-art pentesting tools and practices for cloud environments. With the catalogue of existing tools, different risk levels for data storage can be described with insights on securing the relevant assets. The outcome of this project is both in the area of knowledge on pentesting tools, as well as improved risk management in the future.

- **Contact:** Natalia Zwarts (n.h.zwarts@hhs.nl)
- **Lectoraat:** Risk Management & Cyber Security

## Onderzoek gebruik Mitre Caldera voor Operational Technology (Nederlands/English)

Mitre Caldera is een platform waarmee complexe red team aanvallen uitgevoerd kunnen worden. Onlangs is een plug-in voor OT uitgebracht, deze willen we analyseren op bruikbaarheid. We willen dit koppelen aan een case waarin een waterbedrijf (zoals Dunea) aangevallen wordt. Ook willen we de incident response mogelijkheden van Mitre erbij betrekken. De student dient dus in staat te zijn om Mitre Caldera op bruikbaarheid te onderzoeken en vervolgens de case van deze hypothetische aanval hierin te implementeren. Voor deze opdracht zijn we op zoek naar een afstudeerder.

- **Contact:** Marinus Maris (m.g.maris@hhs.nl)
- **Lectoraat:** Cyber Security & Safety

## Het opzetten en inrichten van een Security Operations Center (SOC) op basis van verschillende probleem- en doelstellingen (Nederlands/English)

Op dit moment wordt er een Cyber Security Living Lab opgezet in de Dutch Innovation Factory. Dit lab fungeert als Security Operations Center (SOC) die monitoring en incident response diensten levert aan externe partijen en tegelijkertijd een leeromgeving is waar studenten (mbo, hbo, universiteit) ervaring kunnen opdoen met het werken in een SOC. De opdracht heeft als doel zowel de benodigde hardware (sensoren, netwerk apparatuur) als software (o.a. een SIEM oplossing) in te regelen om zo naar een functionerend SOC toe te werken.

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

## Ervaring van een student

Het Internet of Things (IoT) wordt groter naarmate er meer geïntegreerde systemen (embedded systems) verbinding maken met het internet. Het doel van IoT en OT (Operationele Technologie) apparaten is om specifieke taken uit te voeren. De beveiliging is echter een secundair aspect, waardoor hackers de apparaten gebruiken om ongezien netwerken binnen te komen. Een IoT-honeypot is een ideale tool om hackers te verleiden naar een fictief IoT-apparaat waar ze zolang mogelijk worden weggehouden van het echte netwerksysteem. Tijdens mijn stage ontwikkelde ik een uniek IoT-honeypot concept, waarbij gebruik werd gemaakt van een zelfgemaakte IoT-powerbank als proefmiddel, om aan te tonen dat het mogelijk is hackers naar de honeypot om te leiden. Uit het onderzoek is gebleken dat dit concept in een vroege ontwikkelingsfase is, omdat nog niet is bewezen dat het hackers effectief verleidt om in de honeypot te trappen. Het concept is een Low-Interaction IoT-honeypot, omdat het hackers kan detecteren tijdens gerichte scans of verbindingen met de powerbank. Uit de resultaten kunnen andere IoT-honeypot concepten worden ontwikkeld en het huidige concept in een vervolgstudie verder worden onderzocht.

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**

# 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
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

### 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**
Matej Dolinsek
Niek Jan van den Hout
Natalia Zwarts

## Adresgegevens

Johanna Westerdijkplein 75
2521 EN Den Haag

cybersecurity@hhs.nl

dehaagsehogeschool.nl