**Project descriptions vacancies 3 fulltime PhD research positions on Cyber Security & Law**

**Project description**

The PhD projects are initiated by [CLECS](https://www.eur.nl/esl/research/research-centers/clecs), Centre for the Law and Economics of Cyber Security, in collaboration with Ahold Delhaize, the Ministry of Infrastructure and Water Management and the LDE Cyber Security group. The PhD researchers will be employed at Erasmus School of Law and will be part of the Erasmus Graduate School of Law. Next to that, the PhD projects will be imbedded in the LDE cyber security PhD programme. LDE universities is a strategic alliance of Leiden University, TU Delft, and Erasmus University Rotterdam. LDE cyber security brings together the expertise of the three partners in and focuses on multidisciplinary research and education and partnerships with governments, businesses and knowledge institutions in Zuid-Holland.

We advertise for the following three 3 PhD projects.

1. **Stimulation of cybersecurity information diffusion on a sector level, with Ahold Delhaize**. This research project focuses on cyber security in the context of the dynamic business environment of Ahold Delhaize. The subject of the research is the increasing stimulation of cybersecurity information diffusion on a sector level. The goal in that respect is to increase the understanding of how the sector currently transforms information to all the actors along the supply chain (including subcontractors) to attain an optimal level of cybersecurity, taking into account the market dynamics in a multidisciplinary setting.
2. **Optimal cybersecurity at the system level, with the Ministry of Infrastructure and Water Management**
This research project is part of a collaboration with the Ministry of Infrastructure and Water Management. It focuses on fostering optimal cybersecurity at the system level and on the study of (the removal of) barriers that ensure that optimal cybersecurity is not yet achieved in the system as a whole. The focus of the PhD research is on the sectors covered by the following policy DGs: Aviation and Maritime Affairs, Mobility, Water and Soil and Environment and International
3. **Theoretical and empirical framework of the law and economics of cybersecurity**
 The third project will be in close cooperation with the two PhD projects together with Ahold Delhaize/The Ministry of infrastructure respectively and will further build upon the theoretical and empirical framework of the law and economics of cybersecurity. Hence the project description of the projects of together with Ahold-Delhaize and the Ministry of Infrastructure give a good indication of the starting point of the PhD research. Also, the role and responsibility of public and private actors will be taken into account.

The exact focus of these projects will be determined by the PhD researchers in cooperation with the supervisors.

The extended project description for project 1 and 2 can be find below:

1. **Stimulation of cybersecurity information diffusion on a sector level, with Ahold Delhaize**.

The CLECS/Ahold Delhaize research project, called “Instruments to Promote Cyber Security: what works?” focuses on cyber security in the context of the dynamic business environment of Ahold Delhaize and will result in recommendations about this theme.

**Background**

Economic and legal aspects of cyber security have attracted considerable academic, sector and government attention over the past 20 years (Anderson, 2001). In the early 2000s, computer scientists unravelled that economic incentives resulting from market failures to information asymmetry and externalities were the cause of failing attempts to gain an optimal level of cyber security. In the meantime, many legal instruments, both top down (such as the GDPR, NIS directive and the US data breach notification law) or bottom up (such as cyber insurance, cyber warranties, codes of conduct, certification and liability clauses) appeared in the cyber security theatre (see amongst many others: Anderson et al., 2008; Eling et al., 2016; Nieuwesteeg & Faure 2018).

To date, there is under- and overinvestment in cyber security. As the investments in cyber security will rise in the future through developments such as robotics, the ‘internet of things’ and blockchain, so will the need for a societal debate about the efficiency and effectiveness of those investments. Currently, there is a lack of theoretical and empirical knowledge on the return on investment of (legal, psychological, economic and technical) instruments, such as contracts, campaigns or technical measures (Nieuwesteeg, 2018). In other words: at various levels (through government regulation, but also through technical developments) a large and wide variety of different measures and instruments have been introduced to promote cybersecurity. However, little is known about the relative effectiveness of those instruments and measures, nor about their efficiency (more particularly whether the marginal benefits outweigh the marginal costs). As law and economics has more particularly focused on the efficiency of legal tools, a law and economics approach could provide an important added value compared to the current level of the debate. The law and economics approach could more particularly provide important insights regarding the efficiency and effectiveness of cybersecurity investments. That would be the specific goal of the research project below.

One of the biggest cyber security risks companies face is the human factor. It’s widely referenced that humans are often the weakest link as far as cyber security is concerned, while Ahold Delhaize considers humans, their associates, their biggest asset. Nevertheless, it cannot be denied that humans are the primary attack vector and therefore constantly investments on the upgrade of human “firewall” capabilities are needed, to meet the needs of today and tomorrow of these attacks. An important question is: “What works?”, specifically when it comes to something so dynamic as the associates’ maturity versus cyber security and their behavior regardless of their location - in or outside of the workplace.

The topic is multidimensional having in mind, that both Ahold Delhaizes’ users and the business environment (omni-channel) they work in, are dynamic. The business model is constantly evolving, users are mobile, the network perimeter is no longer there, and the employees are spread in different continents with substantial cultural differences, in different work locations (offices, warehouses, stores, home) depending on their job description.

**Subject**

The subject of the research is the increasing stimulation of cybersecurity information diffusion on a sector level. The goal in that respect is to increase the understanding of how the sector currently transforms information to all the actors along the supply chain (including subcontractors) to attain an optimal level of cybersecurity, taking into account the market dynamics in a multidisciplinary setting. The question will more particularly be addressed whether it is possible to analyse the relative effectiveness and efficiency of the various measures. Finally, the project will equally analyse whether particular improvements in the cybersecurity strategy at sector level could be proposed. Relevant topics are: understanding risks associated with human cyber security; promoting awareness & behavioral change; defining and implementing targeted awareness measures; calculating the Return on Investment (ROI) of the cyber security awareness program.

**Approach**

The project will start with a descriptive analysis of instruments focusing on prevention, detection and response for the internal and external stakeholders of a company. The scientific basis of these instruments will be subject of academic scrutiny. Second, the project will look into the possibilities to enhance data collection and the quantification of progress of a selection of these instruments in order to empirically observe their effectiveness. For instance: which type of instruments works for which segment? Would it be possible to target different groups with different instruments? This empirical observation could be used to foster the theory building and the development of better instruments.

**Organisation**

The project is initiated by [CLECS](https://www.eur.nl/esl/research/research-centers/clecs), Centre for the Law and Economics of Cyber Security, in collaboration with Ahold Delhaize. It will also be imbedded in the LDE cyber security PhD programme. LDE universities is a strategic alliance of Leiden University, TU Delft, and Erasmus University Rotterdam. LDE cyber security brings together the expertise of the three partners in and focuses on multidisciplinary research and education and partnerships with governments, businesses and knowledge institutions in Zuid-Holland.

**Cooperation CLECS/LDE/Ahold Delhaize**

The PhD researcher in this project will closely participate with the cybersecurity team at Ahold Delhaize, potentially even spending time at their offices. This on the one hand guarantees a full integration of the research project within the day-to-day cybersecurity business of Ahold Delhaize, but also a sharp awareness of the PhD researcher of the challenges concerning cybersecurity rising in daily practice.

1. **Optimal cybersecurity at the system level, with the Ministry of Infrastructure and Water Management**

Er gaat tegenwoordig geen dag voorbij zonder cyberincidenten in het nieuws. Cybersecurity wordt steeds meer ‘chefsache’. Het maatschappelijk belang is van optimale cybersecurity staat buiten kijf. Dit onderzoeksproject richt zich op het stimuleren van optimale cybersecurity op stelselniveau. Het stelsel behelst de publieke en private actoren op het gebied van infrastructuur en waterstaat. De focus van het PhD-onderzoek ligt op de sectoren die onder de volgende beleids-DGs vallen:

- DG Luchtvaart en Maritieme Zaken

- DG Mobiliteit

- DG Water en Bodem

- DG Milieu en Internationaal

Het ministerie heeft stelselverantwoordelijkheid over die sectoren die vallen onder de vier voornoemde beleids-DG’s. Dit betekent dat het ministerie een optimaal niveau van cybersecurity voor het geheel van publieke en private actoren in het stelsel kan faciliteren. De onderzoeksvraag ziet toe op het analyseren en verdiepen van de specifieke toegevoegde waarde van het ministerie voor het stimuleren van optimale cybersecurity op stelselniveau binnen de beleidsverantwoordelijheid van IenW.

Het onderzoeksproject richt zich op het bestuderen van (het wegnemen van) barrières die ervoor zorgen dat optimale cybersecurity in het stelsel als geheel nog niet bereikt wordt. Men kan bijvoorbeeld denken aan interventies op het vlak van kennisdeling en gegevensuitwisseling. In de literatuur worden op het gebied van cybersecurity in het stelsel collectieve actieproblemen beschreven en andere voorbeelden van verkeerde prikkels. Er kan dan toegevoegde waarde ontstaan voor een publieke actor. Men kan ook denken aan het stimuleren van positieve ‘spill-over’ effecten naar het stelsel als geheel en het wegnemen van negatieve spill-over’ effecten. Een voorbeeld: in de literatuur wordt gesproken over ‘liability dumping’, waarbij grote partijen verantwoordelijkheid en aansprakelijkheid voor cybersecurity afschuiven op kleine partijen. Zo kan een private overeenkomst negatieve effecten hebben voor het stelsel. Beleid dat toeziet op het verminderen van ‘liability dumping’ kan dan toegevoegde waarde hebben.

**Doelen van een onderzoeksprogramma met het Ministerie van Infrastructuur en**

**Waterstaat**

Het project start met een beschrijvende analyse van instrumenten die toegevoegde waarde leveren op stelselniveau. Vervolgens zal het project de mogelijkheden voor de dataverzameling van een selectie van deze instrumenten inventariseren om empirische observatie mogelijk te maken. Deze empirische observatie bevordert de theorievorming en de ontwikkeling van betere instrumenten.

De inhoudelijke analyse kan zich onder andere uitstrekken tot:

* Beleid met betrekking tot het wegnemen van barrières op stelselniveau (onder andere kennisdeling over actuele cyberdreigingen).
* Beleid met betrekking tot het verbeteren van juridische zorgplichten bij afsluiten van cybersecuritycontracten met leveranciers op stelselniveau.
* De wijze waarop informatie en data gedeeld worden met verschillende actoren, bijvoorbeeld over de effectiviteit van cybersecuritycampagnes.
* De wijze waarop in het stelsel risico-inschattingen worden gedaan en waarop risico inschattingen over het functioneren van het stelsel worden gedaan.

Na de beschrijvende en empirische analyse zal de ideale situatie vanuit rechtseconomisch perspectief worden geschetst. Vervolgens worden barrières op stelselniveau geïdentificeerd die ervoor zorgen dat de ideale situatie nog niet bereikt wordt. Een van de leidende principes bij de studie van deze barrières is het ‘least cost avoider’ principe: schade ten gevolge van cyberincidenten wordt idealiter beperkt door die partij die dat tegen de laagst mogelijke kosten kan doen. Vaak heeft deze partij tegen de laagst mogelijke kosten toegang tot de noodzakelijke informatie om schade kan beperken. Ook worden informatie-asymetriën en externe effecten op stelselniveau bestudeerd. Deze fenomenen kunnen ervoor zorgen dat op stelselniveau optimale cybersecurity nog niet wordt bereikt, zelfs als organisaties op individueel niveau hiernaar streven. Tenslotte wordt er in dit project verbeterpotentieel geïdentificeerd. Verbeterpotentieel betekent in dit opzicht de identificatie van de toegevoegde waarde van I&W als publieke organisatie ten opzichte van de individuele actoren in het stelsel. Dit mondt uit in beleidsopties op stelselniveau. Hierbij worden expliciet innovatieve instrumenten uit de rechtseconomische literatuur benut, zoals bijvoorbeeld (maar niet uitsluitend) innovatieve contracten, verzekeringsmechanismen en andere hybride systemen die de toegevoegde waarde van I&W op stelselniveau verder kunnen versterken. Ook wordt hier aandacht besteed aan de wijze waarop academische inzichten structureel naar beleid vertaald kunnen worden.

**Samenvattend**

Samenvattend kan het onderzoeksproject de volgende bouwstenen bevatten, waarbij in overleg de focus gelegd wordt op een of meerdere thema’s. Het is van belang om bewust te zijn van de

verschillende sectoren die onder de verschillende beleids-DGs vallen. Deze sectoren verschillen in dynamiek en grootte en governance. Tevens is het van belang om qua scope de bewegingsvrijheid van I&W in acht te nemen in het opstellen van beleid, daar waar ook het NCTV (Ministerie van J&V) op regelgevend gebied een leidende rol heeft. De rechtseconomische analyse van dit onderzoek beperkt zich echter niet alleen tot ‘top-down’ regelgeving, maar gaat ook over ‘soft-law’, het introduceren van innovatieve privaatrechtelijke juridische instrumenten en andere vormen van nudging, waardoor er in de formulering van beleidsopties niet alleen aan door J&V te initiëren kaders gedacht hoeft te worden.

|  |  |  |  |
| --- | --- | --- | --- |
| Onderzoeksopzet →Toegepast in de contextvan ↓ | Status quocybersecurity opstelselniveau(beschrijvende enempirische analyse) | Identificatiebelemmeringenrichting optimalecybersecurity opstelselniveau | Analyse toegevoegdewaarde I&W opstelselniveau enidentificatiebeleidsopties (met inachtneming van debewegingsvrijheid vanI&W) |
| Luchtvaart en maritiemezaken |  |  |  |
| Mobiliteit |  |  |  |
| Water en bodem |  |  |  |
| Milieu en internationaal |  |  |  |

1. The third project will be in close cooperation and interaction with the two PhD projects together with Ahold Delhaize/The Ministry of infrastructure and LDE universities. It will build upon the theoretical and empirical framework of the law and economics of cybersecurity. Hence the project description of the projects of together with Ahold-Delhaize and the Ministry of Infrastructure give a good indication of the starting point and context of the PhD research.

Also, the role and responsibility of public and private actors will be taken into account.

The exact focus of these projects will be determined by the PhD researchers in cooperation with the supervisors.