PhD Projects 2025 - Centre of Expertise Cyber Security

Hacktivism: inspiring heroes or rogue villains? Ideological involvement, recruitment processes, and organizational dynamics
M. (Marco) Romagna, The Hague University of Applied Sciences – Leiden University

Hacktivism is described as the use of hacking techniques in order to promote a socio-political agenda to bring a change in society. Using diverse theoretical backgrounds rooted in social psychology and criminology, this project investigates:

a. the motivations for individuals to engage in hacktivism and the process they follow to become hacktivists;
b. the reasons that prompted them to use hacking as their main form of protest;
c. the organizational dynamics within different hacktivists' groups and networks.

Falling victim to ransomware: On the unfolding of attacks, victim-offender interactions and decision-making
S.R. (Sifra) Matthijsse, The Hague University of Applied Sciences

The aim of this dissertation is to examine how ransomware attacks unfold, considering the perspective of both offenders and victims. In addition, the decision-making processes and behaviour of victimised freelancers and SMEs are explored in more depth in relation to negotiation, payment of a ransom demand and reporting. In doing so, the aim is to gain a more comprehensive understanding of ransomware attacks and to identify measures to prevent attacks from occurring, mitigate the consequences of victimisation and support victims. This will be done using a combination of qualitative and quantitative research methods.

Money mules and cybercrime involvement mechanisms
L.M.J. (Luuk) Bekkers, the Hague University of Applied Sciences

Money mules are key in the execution of financially-motivated cybercrimes. By using both qualitative and quantitative research methods, this project aims to explain how money mules become involved in cybercriminal networks. Knowledge on this matter can be used to disrupt criminal activities and thus help prevent cybercrime victimization among civilians and businesses.

The Intersection Between Trust Signals and Cybercrime-as-a-Service
H. (Hannah) Kool, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

In this project, the decision-making process of cybercriminals who exploit trust signals as facilitators for engaging in illegal Cybercrime-as-a-Service (CaaS) activities is examined. The aim is to gain insight into how trust signals may lower barriers to entry and facilitate pathways into CaaS markets. To achieve this, expert interviews will be conducted and the characteristics of CaaS markets will be investigated, with particular attention to how trust-building mechanisms enable participation and operational success within these illicit ecosystems.

Secure Healthcare for All: Easing the Authentication Burden of eHealth used at Home
N.J. (Niek Jan) van den Hout, The Hague University of Applied Sciences – Radboud University

To alleviate the growing pressure on healthcare, eHealth solutions are increasingly being used in patients' home environments. This shift introduces new information security and privacy risks. To manage these risks, various authentication mechanisms are implemented. Research indicates that the security, usability and accessibility of these mechanisms is often inadequate, potentially leading to insecure situations and reduced access to (digital) healthcare. This research project studies and aims to reduce the influence of the 'authentication burden' on the security and accessibility of eHealth, ensuring that vulnerable user groups, such as the elderly, maintain access to secure healthcare.

The fraud game: factors and processes contributing to involvement in financial-economic cyber-enabled crime
J. (Joeri) Loggen, The Hague University of Applied Sciences – Leiden University

This research project investigates factors and processes that contribute to the involvement of individuals into financial cybercrime. Specifically, the project examines the role of preexisting ties, offender convergence settings, and online crime markets in facilitating financial cybercrime involvement.

Alternative interventions for online fraud: Future implications
M.A.G. (Merel) van Leuken, The Hague University of Applied Sciences

The criminal justice system at present seems insufficiently equipped to adequately address the needs of online fraud victims. In addition to reporting to the police, victims may seek financial compensation through private law by holding the beneficiary account holders liable. This study examines the (un)intended consequences of civil litigation for victims, offenders, and society, and identifies ways to mitigate potential risks to improve the handling of online fraud.

nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving
NWO
Universiteit Leiden
Tilburg University
Radboud University
De Haagse Hogeschool