PhD Projecten 2025 - Centre of Expertise Cyber Security

Hacktivism: inspiring heroes or rogue villans? Ideologische betrokkenheid, rekruteringsprocessen en organisatorische dynamiek.

M. (Marco) Romagna, De Haagse Hogeschool - Universiteit Leiden

Hacktivisme wordt omschreven als het gebruik van hacktechnieken om een sociaal-politieke agenda te bevorderen en zo verandering in de samenleving te bewerkstelligen.

Met behulp van diverse theoretische kaders uit de sociale psychologie en criminologie, onderzoekt dit project:

a. de motivaties van individuen om zich bezig te houden met hacktivisme en het proces dat zij doorlopen om hacktivisten te worden;
b. hun redenen om hacking in te zetten als belangrijkste protestvorm;
c. de organisatorische dynamiek binnen verschillende hacktivistengroepen en -netwerken.

Slachtofferschap van ransomware: Het verloop van aanvallen, slachtoffer-dader interacties en besluitvorming

S.R. (Sifra) Matthijsse, De Haagse Hogeschool - Universiteit Leiden

Het doel van dit project is om te onderzoeken hoe ransomware-aanvallen verlopen, vanuit het perspectief van zowel daders als slachtoffers. Daarnaast worden de besluitvormingsprocessen en het gedrag van getroffen freelancers en midden-klein bedrijven met betrekking tot onderhandelen, het betalen van losgeld en melden nader onderzocht. Aan de hand hiervan wordt meer inzicht verkregen in ransomware-aanvallen en worden maatregelen geïdentificeerd die aanvallen kunnen voorkomen, de gevolgen van slachtofferschap kunnen beperken en slachtoffers kunnen ondersteunen. Daarbij zal een combinatie van zowel kwalitatieve als kwantitatieve onderzoeksmethoden worden gebruikt.

Geldezels en betrokkenheidsmechanismen van cybercriminaliteit

L.M.J. (Luuk) Bekkers, De Haagse Hogeschool

Geldezels spelen een sleutelrol bij de uitvoering van financieel gemotiveerde cybercriminaliteit. Door zowel kwalitatieve als kwantitatieve onderzoeksmethoden te gebruiken, is het doel van dit project om beter te begrijpen hoe geldezels betrokken raken bij cybercriminele netwerken. Kennis over dit onderwerp kan worden gebruikt om de uitvoering van financiële cybercriminaliteit te verstoren en zo bij te dragen aan de preventie van zowel slachtofferschap als daderschap.

Het snijvlak tussen vertrouwenssignalen en cybercrime-as-a-service

H. (Hannah) Kool, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Dit project onderzoekt het beslissingsproces van cyberdaders die vertrouwenssignalen misbruiken om illegale cybercrime-as-a-service (CaaS) activiteiten te faciliteren. Het doel is om inzicht te krijgen in hoe vertrouwenssignalen de toegang tot CaaS-markten kunnen vergemakkelijken en de drempel tot toetreding verlagen. Om dit te onderzoeken worden experts geïnterviewd en de kenmerken van CaaS-markten geanalyseerd, waarbij specifiek wordt gekeken naar hoe vertrouwensmechanismen deelname en operationeel succes binnen deze illegale ecosystemen mogelijk maken.

Veilige zorg voor iedereen: het verlichten van de authenticatielast bij thuisgebruik van eHealth oplossingen

N.J. (Niek Jan) van den Hout, De Haagse Hogeschool - Radboud Universiteit

Om toenemende druk op de gezondheidszorg te verlichten, wordt eHealth steeds vaker ingezet in de thuisomgeving van de patiënt. Dit brengt nieuwe risico's omtrent informatiebeveiliging en privacy met zich mee. Om deze risico's te beheersen, worden authenticatiemechanismen geïmplementeerd. Onderzoek toont aan dat de veiligheid, gebruiksvriendelijkheid en toegankelijkheid van deze mechanismen te wensen overlaat, met onveilige situaties en verminderde toegang tot (digitale) gezondheidszorg tot gevolg. Dit project onderzoekt en beoogt de invloed van de "authenticatielast" op de veiligheid en toegankelijkheid van eHealth te reduceren, zodat kwetsbare gebruikersgroepen, zoals ouderen, toegang blijven houden tot veilige gezondheidszorg.

De F-game: factoren en processen die bijdragen aan de betrokkenheid bij financieel-economische gedigitaliseerde criminaliteit

J. (Joeri) Loggen, De Haagse Hogeschool - Universiteit Leiden

Binnen dit project worden factoren en processen onderzocht die bijdragen aan de betrokkenheid bij financiële cybercriminaliteit. Het project richt zich specifiek op de rol van reeds bestaande relaties, criminele ontmoetingsplekken, en online criminele markten bij het faciliteren van betrokkenheid bij financiële cybercriminaliteit.

Een alternatieve afdoening van online fraude

M.A.G. (Merel) van Leuken, De Haagse Hogeschool

Het huidige strafrechtsysteem lijkt onvoldoende tegemoet te komen aan de behoeften van slachtoffers van online fraude. Naast het doen van aangifte bij de politie, kunnen slachtoffers financiële compensatie proberen te verkrijgen door de begunstigde rekeninghouders civielrechtelijk aansprakelijk te stellen. Deze studie onderzoekt de (on)bedoelde gevolgen van civielrechtelijke procedures voor slachtoffers, daders en de samenleving, en brengt mogelijkheden in kaart om potentiële risico's te beperken en de afhandeling van online fraude te verbeteren.

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