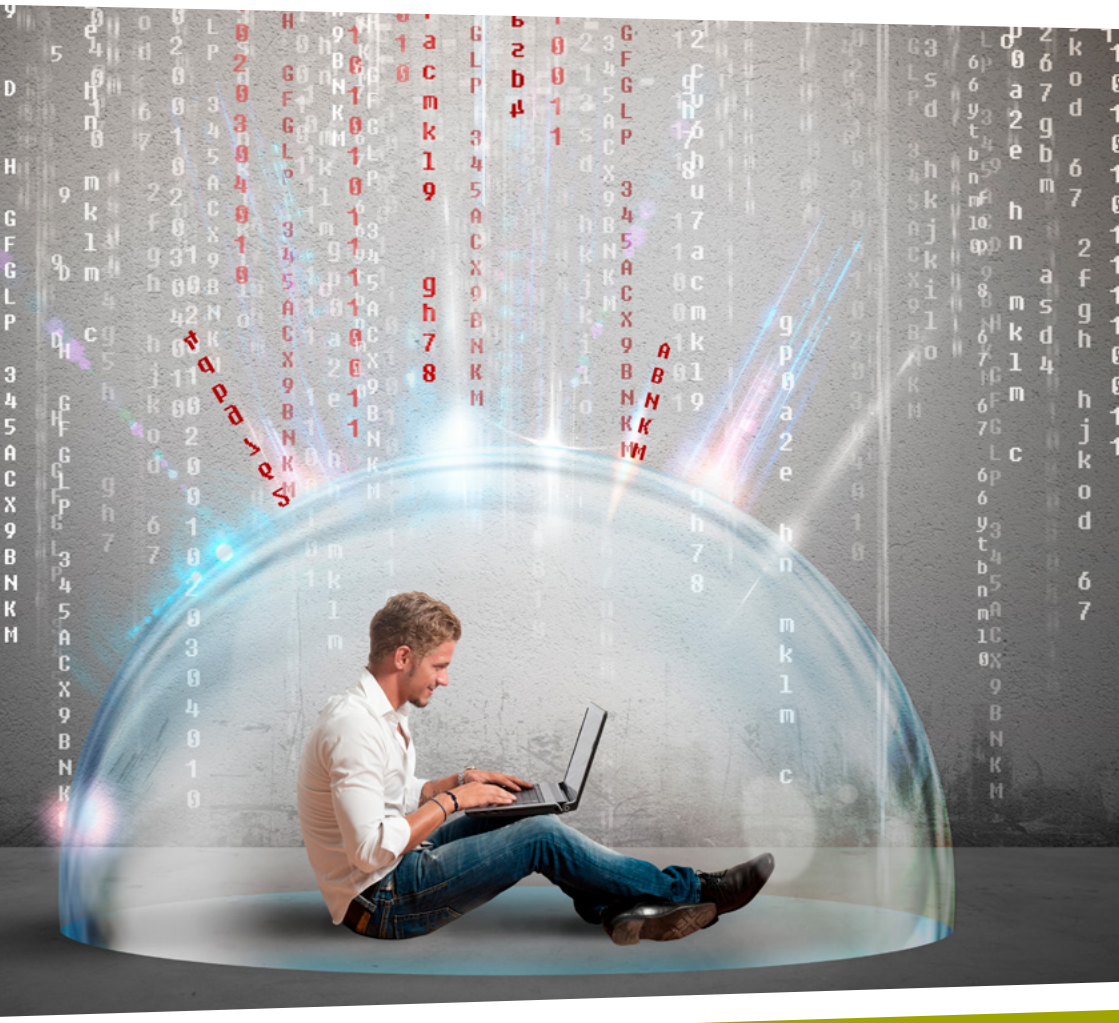
DE ‘HUMAN’ FACTOR IN CYBERSECURITY

Intreerede dr. Rutger Leukfeldt

Dinsdag 9 oktober 2018



let’s change
YOU. US. THE WORLD.

DE HAAGSE HOGESCHOOL

LECTORAAT CYBERSECURITY IN HET MKB

Dr. Rutger Leukfeldt is lector Cybersecurity in het mkb aan De Haagse Hogeschool. Daarnaast is hij senior onderzoeker cybercrime bij het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR).

Het lectoraat wil de kennispositie van het mkb op het gebied van cybercrime en cybersecurity vergroten en het slachtofferschap en de impact van cyberaanvallen onder mkb'ers verlagen. Dit wordt bereikt door het uitvoeren van praktijkgericht wetenschappelijk onderzoek langs vier onderzoekslijnen waarbij steeds het mkb centraal staat:

1. aard en omvang van slachtofferschap;
2. aard van cybercrime;
3. cyberweerbaarheid;
4. de aanpak van cybercrime.

1 Inleiding

Cybercrime – en daarmee cybersecurity – is een groot maatschappelijk probleem. De criminologische bestudering van cybercrime staat nog in de kinderschoenen. Het is echter niet alleen noodzakelijk om fundamenteel wetenschappelijk onderzoek uit te voeren ('de lange termijn'), maar ook om met de praktijk de acute problemen en uitdagingen van vandaag en morgen te onderzoeken. Het merendeel van het onderzoek op dit gebied – en dan heb ik het over zowel fundamenteel wetenschappelijk als praktijkgericht onderzoek – komt tot nu toe uit de hoek van de technische wetenschappen. Technologie speelt natuurlijk ook een belangrijke rol bij cyberincidenten, maar we hebben het over *mensen* die cyberaanvallen uitvoeren, *mensen* die – wetend of onwetend – meewerken aan die aanvallen, *mensen* die slachtoffer worden en *mensen* die zich bezighouden met het tegenhouden van cyberaanvallen.

Empirisch onderzoek naar de menselijke factor bij cybercrime en cybersecurity is schaars. De onder mijn redactie recent uitgebrachte onderzoeksagenda 'The human factor in cybercrime en cybersecurity' maakt dit helder.[1] In die onderzoeksagenda zijn tientallen onderwerpen geïdentificeerd waar de komende jaren onderzoek naar moet worden gedaan omdat basale kennis ontbreekt. Tegelijkertijd zit het werkveld te springen om bruikbare kennis over manieren om zich te beschermen tegen cyberaanvallen. Dat laatste is iets wat we zeker gemerkt hebben het afgelopen jaar. Al voor de officiële start van het lectoraat Cybersecurity in het midden- en kleinbedrijf (mkb) stroomden de verzoeken binnen van gemeenten, brancheorganisaties en bedrijven om gezamenlijk onderzoek te doen. Dit is dan ook de reden dat we, ondanks dat het lectoraat nog geen jaar geleden is ingesteld, al flink wat onderzoeken voor en met de praktijk uitvoeren.

De constatering dat onderzoek naar de menselijke factor binnen cybercrime en cybersecurity nog in de kinderschoenen staat terwijl er een grote vraag is naar evidence-based praktisch toepasbare kennis, is de reden dat De Haagse Hogeschool (HHs) en het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR) de handen ineengeslagen hebben voor de totstandkoming van dit lectoraat. Zowel De HHs als het NSCR hebben cybersecurity en cybercrime al enkele jaren geleden als prioriteit benoemd en hebben elk afzonderlijk onderzoeksprogramma's op dit gebied. Voor De HHs geldt dat onderzoeken toepassingsgericht moeten zijn en dat de nieuwste onderzoeksmethoden en -technieken moeten worden toegepast om hoogwaardige producten op te leveren. Voor het NSCR geldt dat onderzoeken ook fundamentele kennis moeten opleveren. Het is echter steeds duidelijker dat bij onderzoek naar cybercrime en cybersecurity het beste van beide werelden nodig is. Het lectoraat heeft dan ook de nadrukkelijke opdracht deze twee onderzoeksprogramma's te verbinden. Ik zal in deze inleiding een beknopte schets geven van de onderzoeksprogramma's van deze organisaties en van de toekomstige onderzoeken binnen het lectoraat.

1 Leukfeldt (2017)

De HHs is sinds 2004 actief op het gebied van cybersecurity en heeft een Centre of Expertise Cyber Security (CoECS). Het CoECS heeft tot doel praktijkgericht onderzoek uit te voeren om zo organisaties te helpen die zelf niet voldoende middelen en/of expertise hebben om zich te beschermen tegen cyberaanvallen. Onder het CoECS ressorteren naast het lectoraat Cybersecurity in het mkb ook het lectoraat Cybersecurity & Safety van Marcel Spruit en het lectoraat Network & Systems Engineering Cyber Security van Thomas Quillinan. Deze twee lectoraten richten zich op respectievelijk cybersecurity bij individuen en in middelgrote overheidsorganisaties, en op de technische kant van de beveiliging van IT-systemen, met een bijzondere focus op het 'internet of things'. Het lectoraat Cybersecurity in het mkb focust op de menselijke kant van cybersecurity en sluit daarom aan op de bestaande lectoraten binnen het CoECS. Het NSCR doet sinds 2010 onderzoek naar cybercrime en cybersecurity en heeft cybercrime in 2015 tot een van de speerpunten voor toekomstig onderzoek benoemd.

Het cybercrime cluster binnen het NSCR bestudeert de menselijke factor in cybercrime en kent drie lijnen:

1 cybercriminelen;
2 cybercriminele ontmoetingsplaatsen;
3 de aanpak van cybercrime.

Binnen het lectoraat Cybersecurity in het mkb werken onderzoekers die verbonden zijn aan De HHs en het NSCR samen aan het onderzoek naar cybercrime en cybersecurity. De kennis en ervaring met het fundamentele onderzoek naar cybercrime van het NSCR wordt gekoppeld aan het toepassingsgerichte onderzoek aan De HHs. Hierdoor ontstaat een integraal onderzoeksprogramma dat het hele spectrum van relevant onderzoek naar cybercrime en cybersecurity beslaat: binnen het NSCR wordt het meer theoriegedreven fundamentele onderzoek uitgevoerd, vooral gericht op daders en dadersnetwerken, binnen De HHs wordt het meer slachtoffer- en aanpakgeoriënteerde onderzoek uitgevoerd, en dan specifiek gericht op het mkb.

Nu over naar de inhoud. In deze intreerede staat de menselijke factor binnen cybercrime en cybersecurity centraal. Wat is eigenlijk de menselijke factor en waarom is deze van groot belang? Om dat goed te kunnen uitleggen zal ik het eerst kort hebben over cybercrime en cybersecurity – twee veelgebruikte termen, waar lang niet iedereen eenzelfde beeld bij heeft. Daarbij behandel ik ook een aantal cybermythen. Vervolgens zal ik beargumenteren dat de sociale wetenschappen, en de criminologie in het bijzonder, een belangrijke bijdrage kunnen leveren aan het oplossen van cybersecurity vraagstukken. Ik eindig met een bespreking van het onderzoeksprogramma van het lectoraat, waarmee we niet alleen mooi onderzoek willen produceren maar ook, in samenwerking met de praktijk, slachtofferschap en de impact van cyberaanvallen daadwerkelijk verminderen.

2 De noodzaak van empirisch onderzoek naar de menselijke factor

2.1 Cybercrime en cybersecurity

De oplettende lezer – of in dit geval de oplettende toehoorder – was het misschien al opgevallen dat ik mijn intreerede begon met de woorden 'Cybercrime – en daarmee cybersecurity – is een groot maatschappelijk probleem (…)'. Dat ik eerst cybercrime noem en daarna pas cybersecurity is geen toeval. Uiteraard heeft dit te maken met mijn achtergrond als criminoloog. Ik vind de *crime* blijkbaar van nature interessanter dan de *security.* Nu lijkt dit misschien een academische discussie, maar er is verschil. Het belangrijkste verschil tussen de twee is dat cybercrime alleen gaat om criminele activiteiten die strafbaar zijn gesteld door de wetgever, terwijl cybersecurity betrekking heeft op de integriteit, beschikbaarheid en vertrouwelijkheid van informatie.[2, 3] Integriteit heeft te maken met de betrouwbaarheid van de informatie, beschikbaarheid gaat over de toegankelijkheid van de informatie en vertrouwelijkheid draait er om dat alleen personen die daartoe gerechtigd zijn daadwerkelijk bij de informatie kunnen. De integriteit, beschikbaarheid en vertrouwelijkheid van informatie kan in het gedrang komen door aanvallen van criminelen, die bijvoorbeeld met behulp van kwaadaardige software bestanden versleutelen en losgeld vragen om de bestanden weer toegankelijk te maken, maar ook door menselijk falen van bijvoorbeeld eigen medewerkers die per ongeluk een datalek veroorzaken.

2.2 Mens en techniek maken de crime

Als we het hebben over oplossingen voor cybercrime en cybersecurity problemen, dan wordt vaak gezocht in de technische hoek. Waarom dit is weet ik niet precies, maar het heeft vast te maken met het feit dat we onze cybermogelijkheden aan de techniek ontlenen. Daarvoor moeten we dankbaar zijn (ik zou niet weten hoe ik onderzoek zou moeten doen zonder allerlei digitale databases met wetenschappelijke artikelen of hoe ik samen zou moeten werken met collega's uit andere delen van de wereld zonder e-mail en Skype). Technologie heeft onze wereld veranderd. Maar diezelfde technologie heeft ons ook kwetsbaar gemaakt. Zo kan in software fouten zitten die misbruikt kunnen worden door criminelen. Ook schrijven criminelen zelf kwaadaardige software die gebruikt kan worden om computers van gebruikers over te nemen of om informatie

2 Zie met betrekking tot de strafbaarstelling van cybercrime het overzicht van Leukfeldt e.a. (2015). Verderop in deze intreerede zal ik dieper ingaan op het begrip cybercrime en de verschillende typen delicten die hieronder vallen.

3 Zie voor een overzicht van cybersecurity definities bijvoorbeeld: European Union Agency for Network and Information Security (2015).

te stelen. Om dat te voorkomen zijn beveiligingsmaatregelen nodig. Deze worden echter soms zo lastig gevonden door gebruikers, dat zij onveilige omwegen gebruiken, zoals overal hetzelfde wachtwoord gebruiken of niet op tijd software updaten.[4] Deze voorbeelden laten eigenlijk meteen zien wat het punt is dat ik wil maken. Ook al is de toegangspoort voor cyberaanvallen een technische onvolmaaktheid, de bron van de problemen zit bij de mens: de cybercrimineel probeert binnen te dringen en het potentiële slachtoffer laat na zich adequaat te beschermen. Dat betekent dat cybersecurity, en daarmee cybercrime, niet alleen het terrein is van de techniek, maar evengoed van criminologen, psychologen, bestuurskundigen, juristen en van vele andere disciplines.

Dat bescherming tegen cyberaanvallen nog steeds veelal gezien wordt als een technische aangelegenheid en cyberonderzoek als onderzoek dat binnen de techniek dient plaats te vinden, levert een levensgroot probleem op: we hebben te weinig inzicht in de factor mens – als aanvaller, zwakke link in de beveiliging, slachtoffer of als verdediger.

2.3 Onderzoek naar de cyberwerkelijkheid

Het ontbreken van onderzoek naar de menselijke factor binnen cybercrime en cybersecurity leidt ertoe dat er soms werkelijkheden worden gepresenteerd die voor de hand lijken te liggen en die veelvuldig worden herhaald maar nooit empirisch zijn onderzocht – en waarvan we dus niet weten of ze, ondanks dat ze zo logisch klinken, wel kloppen. Hiervan zal ik twee voorbeelden geven.

Het eerste voorbeeld: risicoprofielen van slachtoffers. Voor het tijdperk van ransomware aanvallen hadden we in Nederland het meeste last van phishing en malware aanvallen op onze online bankrekeningen.[5] Op menig expertbijeenkomst van bijvoorbeeld de politie en de bancaire sector wisten experts te vertellen dat slachtoffers vaak ouderen waren die niet bewust waren van de risico's die ze online lopen. Daar moesten dus ook campagnes op gericht worden. Toen we, nog niet eens zo heel lang geleden, het eerste landelijke onderzoek deden naar slachtofferschap van cybercrime[6] zag ik mijn kans schoon om wat aanvullende analyses te doen naar risicofactoren van mensen die slachtoffer waren geworden van phishing en malware.[7] Geheel tegen de verwachting in bleek dat op basis van deze representatieve steekproef geen duidelijke risicoprofielen konden worden vastgesteld. Phishers discrimineren dus helemaal niet tussen mensen met veel of weinig geld, veel of weinig kennis van computers, een hoge of lage mate van risicobewustzijn en ook specifieke online activiteiten werkten niet risicoverhogend.

4 Zelfs als mensen wel weten dat ze zich cyberveilig moeten gedragen doen ze dat vaak niet, zie bijvoorbeeld Spiekermann e.a. (2013), Hassenzahl e.a. (2010) en Van der Zee (2018).
5 Domenie e.a. (2012)
6 Domenie e.a. (2012)
7 Leukfeldt en Yar (2016)

Voor malware gold in grote mate hetzelfde, alleen bleek daar vooral dat het vaker uitvoeren van allerlei online activiteiten risicoverhogend werkte. Meer online zijn en meer online activiteiten uitvoeren werkt dus risicoverhogend.

Een tweede voorbeeld: cybercriminelen. De uitkomsten van de studies naar slachtofferschap en risicoprofielen waaraan ik meewerkte, waren voor mij aanleiding om me meer te gaan verdiepen in hoe cybercriminelen opereren. Immers, als we inzicht hebben in de werk- en denkwijze van deze criminelen kunnen we misschien gerichte drempels opwerpen om het die criminelen moeilijker te maken. Het heersende beeld van cybercriminele netwerken was dat het zou gaan om groepen die elkaar alleen in chatboxen en op cryptomarkten leren kennen en alleen in die virtuele wereld – relatief anoniem – samenwerken. In mijn promotieonderzoek keek ik naar de wijze waarop cybercriminele netwerken opereren, hoe samenwerking tot stand komt, en waar die cybercriminelen vandaan komen. Door grootschalige opsporingsonderzoeken te analyseren, interviews af te nemen met betrokken rechercheurs en officieren van justitie en fraudemanagementsystemen van grootbanken uit te pluizen, kantelde dit beeld. Bij het merendeel van de cybercriminele netwerken bleken de kernleden elkaar te kennen uit de echte – offline – wereld: ze groeiden op in dezelfde buurt, gingen naar dezelfde universiteit of kenden elkaar uit het uitgaansleven. Er waren ook netwerken waarbij de kernleden elkaar wel kenden via chatboxen of cryptomarkten, maar ook zij hadden contacten uit de offline wereld nodig om goed te kunnen functioneren. Vanuit criminologisch optiek eigenlijk – achteraf gezien – nogal logisch: waarom zou je niet blijven samenwerken met mensen die je persoonlijk kent, vertrouwt en waarvan je weet wat je er aan hebt? Het gaat immers om veel geld en potentieel hoge risico's. En het is ook logisch dat ze mensen nodig hebben in de offline wereld: hoe kan je anders die bitcoins witwassen en omzetten naar harde euro's? Dat gaat via bestaande offline netwerken die al jarenlang ervaring hebben met dergelijke praktijken.

Empirisch onderzoek naar de plegers, slachtoffers en aanpak van cybercrime is dus van groot belang. Tot voor kort wisten we niet eens hoeveel burgers en bedrijven eigenlijk slachtoffer werden van cyberaanvallen. Nog steeds is het onduidelijk hoe we mensen het beste kunnen beschermen tegen dergelijke aanvallen. Onlangs nog concludeerden de auteurs van het hoofdstuk over slachtofferschap in de eerder genoemde onderzoeksagenda dat de effectiviteit van maatregelen tegen cybercrime maar kort effectief zijn en na verloop van tijd weer afnemen.[8] In zijn algemeenheid is erg weinig zicht op de effectiviteit van interventies zoals trainingen en campagnes, of die nou gericht zijn op de mens als gebruiker die slachtoffer wordt, of de mens als crimineel, of de mens als verantwoordelijke om cybercrime aan te pakken.[9]

8 Jansen e.a. (2017) in Leukfeldt (2017).

9 Om over cyberdelicten nog maar te zwijgen. Onlangs concludeerden Oosterwijk en Fisher (2017) nog dat er geen bewezen effectieve interventies zijn gericht op jeugdige cybercriminelen.

2.4 (Cyber)criminologie

Criminologen hebben cybercrime pas recent ontdekt. In de beginjaren van mijn loopbaan als cybercrime onderzoeker hoorde ik vaak dat cybercrime (en daarmee cybersecurity) een onderwerp was dat nu even in de mode was, maar dat dit wel weer zou overwaaien omdat het simpelweg een van de vele verschijningsvormen van criminaliteit is. Zo'n tien jaar geleden was ik dan ook al blij als ik op congressen andere onderzoekers tegenkwam die ook iets met dit onderwerp wilden gaan doen. Maar ieder jaar volgden meer presentaties en soms zelfs hele sessies over cybercrime. De jaarcongressen in 2018 van zowel de Nederlandse Vereniging van Criminologie (NVC) als de European Society of Criminology (ESC) tonen aan dat criminologen cyber eindelijk omarmd hebben. Niet alleen was het centrale thema van het NVC congres criminaliteit in een gedigitaliseerde samenleving, ook werden binnen acht inhoudelijke cybergerelateerde sessies door tal van onderzoekers presentaties gegeven over hun laatste bevindingen over cybercriminelen, slachtoffers en de aanpak van cybercrime. Op de ESC was eenzelfde beeld te zien: zeven sessies gewijd aan cybercrimes en tal van cybergerelateerde presentaties in sessies over traditionele criminaliteit.

Inmiddels begrijpen we dat het beeld dat cybercrime een zeer specifieke verschijningsvorm van criminaliteit is, net zo min klopt als de bewering dat het om een technisch probleem gaat. Er zijn inderdaad nieuwe cyberdelicten waarbij de techniek een grote rol speelt. Maar er zijn ook allerlei bestaande delicten die met behulp van technologische toepassingen beter uitgevoerd kunnen worden. Daarom onderscheiden we twee typen cyberdelicten.[10] Enerzijds is er sprake van nieuwe delicten, bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van websites of netwerken. Dit soort delicten valt onder de noemer cybercrime (ook wel cybercrime in enge zin of 'computer dependent crime' genoemd). Deze nieuwe delicten waren voor de komst van informatie- en communicatietechnologie (ICT) simpelweg niet mogelijk. Je kunt een database niet hacken als er geen databases zijn en je kunt een website niet platleggen als er geen websites zijn. Daarnaast zijn er traditionele vormen van criminaliteit waarbij ICT een steeds belangrijkere rol is gaan spelen. Voorbeelden zijn het plegen van fraude via internet en cyberstalking. Dergelijke delicten vallen onder de noemer gedigitaliseerde criminaliteit (ook wel cybercrime in brede zin of 'computer enabled crime' genoemd). Over of deze delicten nieuw zijn kunnen we lang discussiëren. Is het hacken van een database om daar creditkaartgegevens uit te stelen met als doel het verdienen van geld niet min of meer hetzelfde als het inbreken in een huis om daar geld te stelen? Echter, delen van het 'crime script' – alle stappen die nodig zijn om een delict te plegen – en de schaal waarop een en ander plaats vindt, zijn anders. Enfin, de discussie blijft lastig. In deze rede zal ik voor het gemak de term cybercrime hanteren voor zowel cybercrimes in enge zin als cybercrimes in brede zin.

10 Zie bijvoorbeeld de overzichtstudie van Bossler en Holt (2014).

Hoewel duidelijk is dat cybercrime niet iets is wat nu even in de mode is, is het denkbaar dat er trends zullen zijn in cyberdelicten. Zo kwam ransomware een aantal jaren geleden nog niet eens voor in de politiesystemen[11] en werd er niet naar gevraagd in het eerste landelijke slachtofferonderzoek naar cybercrime – het was nog geen maatschappelijk issue.[12] Dat is vandaag de dag ondenkbaar. Ransomware is op dit moment naast hacken en phishing een prominent cyberdelict. Of dat over een aantal jaar nog zo is, is de vraag. Het is goed mogelijk dat er dan een heel ander delict dominant is.

Los van dit soort kwesties is duidelijk dat digitalisering consequenties heeft voor het gehele spectrum van criminaliteit. En dat roept allerlei theoretische vragen op waar we op dit moment nog geen antwoord op hebben.[13] Hebben we bijvoorbeeld te maken met oude daders op een nieuw werkterrein, of gaat het om een nieuw type dader met dito kenmerken en motieven? Welke afwegingen maakt een crimineel voor het plegen van een cyberdelict? Zorgen online ontmoetingsplaatsen ervoor dat criminele samenwerkingsverbanden op een andere manier ontstaan en groeien? Worden door gebruik van ICT op een andere manier slachtoffers gemaakt en welke persoonlijke of situationele kenmerken zorgen voor een verhoogde of verlaagde kans op slachtofferschap? En welke actor is geschikt om de rol van 'capable guardian' op zich te nemen om potentiële slachtoffers te beschermen; is dat de politie, of zijn dat commerciële beveiligingsbedrijven of Internet Service Providers?

De onderzoeken die we doen binnen dit lectoraat passen binnen een stroming in de criminologie die focust op de situationele omstandigheden waaronder cyberdelicten worden gepleegd. De focus ligt niet op het achterhalen van de oorzaken van criminaliteit, maar op de wijze waarop cybercrime wordt gepleegd. Met meer kennis daarover ontstaat zicht op mogelijkheden om criminaliteit te voorkomen.[14] Daarbij vertrekken we vanuit bewezen principes: criminologen doen immers al decennialang onderzoek naar crimineel gedrag en daar kunnen we binnen cyberland van profiteren. Drie theoretische vertrekpunten lijken daarbij vooral van belang: de routine activiteitentheorie, 'resilience engineering' en situationele criminaliteitspreventie. Ik zal hier kort bij stil staan.

De routine activiteitentheorie veronderstelt dat gelegenheidsstructuren van invloed zijn op criminaliteit. Drie factoren zijn daarbij van belang:

1. de aanwezigheid van gemotiveerde daders;
2. de aanwezigheid van geschikte doelwitten;
3. de afwezigheid van toezicht (zogenaamde 'capable guardians').[15]

11 Leukfeldt e.a. (2010)
12 Domenie e.a. (2012)
13 Zoals we ook constateerden in de onderzoeksagenda the human factor in cybercrime and cybersecurity – Leukfeldt (2017). Onderstaande vragen zijn afkomstig uit die agenda.
14 Clarke (2004)
15 Cohen en Felson (1979)

Als deze drie elementen samenkomen in ruimte en tijd ontstaat criminaliteit. Deze theorie is al regelmatig gebruikt om slachtofferschap van cybercrime te verklaren.[16] Voorbeelden van online routine activiteiten die voor verschillende cybercrimes tot verhoogd risico leiden zijn: meer online zijn, bijlagen openen van e-mails van onbekende afzenders, op pop-ups klikken, internetbankieren, aankopen doen via webwinkels en niet up-to-date antivirussoftware hebben. Helaas is bij onderzoeken naar cybercrime de operationalisatie van deze theorie en/of de steekproef waarop onderzoeken worden uitgevoerd vaak nogal beperkt.[17] Daardoor weten we nog veel te weinig van kenmerken en gedrag van slachtoffers die aantrekkelijk zijn voor criminelen en welke beschermende factoren goed werken – om nog maar te zwijgen over inzicht in de specifieke doelgroep van dit lectoraat, het mkb. Meer daarover in het volgende deel van deze intreerede.

'Resilience engineering' is een denkkader over hoe om te gaan met risico's. De focus van 'resilience engineering' ligt op veerkrachtig functioneren. 'Resilience' is het vermogen van een organisatie om het functioneren aan te passen voorafgaand, tijdens of na veranderingen of verstoringen, zodat het functioneren op peil blijft onder verwachte en onverwachte condities.[18] Systemen die veerkrachtig zijn worden veelal omschreven aan de hand van vier stadia van een cyclus:

1 voorbereiden;
2 monitoren;
3 absorberen;
4 aanpassen aan bekende en onbekende dreigingen.[19]

In de eerste fase staat een goede voorbereiding centraal: het kunnen anticiperen op (on)voorziene dreigingen. In de tweede fase staat het vermogen om incidenten te herkennen voorop. In de derde fase draait het om snel en adequaat reageren op het incident, het continueren van de bedrijfsvoering tijdens een incident en het herstellen van verstoringen. In de vierde fase, ten slotte, staat het lerend vermogen voorop: kennis die is opgedaan tijdens het incident kan worden gebruikt om systemen, protocollen en mensen veerkrachtiger te maken.[20] Een digitaal veerkrachtige organisatie dient dan ook in voldoende mate de capaciteit te hebben om te anticiperen, monitoren, reageren en leren. In andere woorden: organisaties moeten weten hoe incidenten kunnen worden voorkomen, wat incidenten zijn en hoe deze te herkennen zijn, wat te doen tijdens een incident en, na afloop, weten wat er is gebeurd.[21]

16 Bijvoorbeeld Anderson (2006); Bossler en Holt (2009); Choi (2008); Hutchings en Hayes (2009); Leukfeldt (2014); Leukfeldt (2015); Jansen en Leukfeldt (2016); Ngo en Paternoster (2011); Pratt, Holtfreter en Reisig (2010); Van Wilsem (2013); Leukfeldt en Yar (2016).
17 Leukfeldt (2017)
18 Hollnagel e.a. (2010)
19 National Academy of Sciences (2012); Hollnagel (2011); Van der Kleij (2018)
20 Linkov e.a. (2013)
21 Van der Kleij (2018)

Onder situationele criminaliteitspreventie vallen verschillende strategieën om criminaliteit te voorkomen. Er zijn vijf strategieën met in totaal 25 technieken voor situationele criminaliteitspreventie[22]:

1 'increase the effort of crime' (bijvoorbeeld 'target hardening' door het aanbrengen van betere sloten);
2 'increase the risk of crime' (bijvoorbeeld 'extend guardianship' door een buurtwacht);
3 'reduce the rewards of crime' (bijvoorbeeld het moeilijker maken om gestolen waar te verhandelen);
4 'reduce provocations that invite criminal behaviour' (bijvoorbeeld groepsdruk om bepaalde handelingen uit te voeren proberen te voorkomen);
5 'remove excuses for criminal behaviour'(bijvoorbeeld het duidelijk stellen van regels).

De 25 technieken voor situationele criminaliteitspreventie zijn ontwikkeld voor offline delicten. Verschillende onderzoeken laten echter zien dat deze technieken in principe net zo goed toepasbaar zijn voor cybercrimes als voor traditionele delicten.[23] Bijvoorbeeld een gerichte aanpak van de zogenaamde 'money mules' zodat het voor cybercriminelen moeilijker is om gestolen geld afkomstig van online bankrekeningen te cashen, door gebruikers aan te leren om back-ups te maken om het effect van een ransomware aanval te beperken, maar ook het verstoren van online criminele markten door die te voorzien van desinformatie of geheel offline te halen.

22 Cornish en Clarke (2004)
23 Hartel e.a. (2011); Leukfeldt (2016); Leukfeldt en Jansen (2018)

3 Cybercrime, cybersecurity en mkb

Het mag inmiddels duidelijk zijn dat dit lectoraat zich richt op de menselijke kant van cybercrime en cybersecurity. Zoals eerder al is opgemerkt, zit de praktijk te springen om evidence-based kennis over manieren om zich te beschermen tegen cyberaanvallen. Dit lectoraat richt zich op een specifieke doelgroep: het mkb.[24] Het mkb is de ruggengraat van de Nederlandse economie. Zo zijn er meer dan een miljoen mkb-bedrijven in Nederland die gezamenlijk zorgen voor meer dan drie miljoen banen en een totale omzet van 858 miljard euro.[25] Mkb'ers worden echter relatief vaak slachtoffer van cyberaanvallen en hebben niet de capaciteit om zich te weren tegen dergelijke aanvallen. Een vooronderzoek van het CoECS van De HHs laat dan ook zien dat een op de vijf mkb-ondernemers slachtoffer is geworden van een cyberaanval[26]. Die cijfers zijn vergelijkbaar met veelvoorkomende delicten waar ondernemers last van hebben, zoals inbraken en fraude.[27]

De bevinding dat het mkb van groot belang is voor de Nederlandse economie én dat datzelfde mkb vaak slachtoffer is van cyberaanvallen, staat in schril contrast met het onderzoek dat wordt uitgevoerd op dit gebied. Onderzoek naar deze doelgroep ontbreekt nagenoeg volledig.[28]

Het doel van het lectoraat is dan ook om de kennispositie van het mkb op het gebied van cybercrime en cybersecurity te vergroten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen. Omdat er nagenoeg geen studies zijn gedaan naar cybersecurity in het mkb zullen eerst basale vragen beantwoord moeten worden. Zo is inzicht nodig in slachtofferschap onder mkb'ers. Hoe vaak komen aanvallen op mkb- bedrijven voor? Welke mkb-bedrijven worden slachtoffer van cyberaanvallen en zijn er factoren die risicoverhogend of risicoverlagend werken? Wat is de werkwijze van criminelen? Selecteren ze specifieke mkb-bedrijven of voeren ze gewoon zoveel mogelijk aanvallen uit? En van welke zwakke plekken maken criminelen gebruik om hun aanvallen uit te voeren? Tegelijkertijd moet worden onderzocht hoe mkb'ers zichzelf weerbaarder kunnen maken. Weten mkb'ers welke risico's ze lopen, hoe ze aanvallen kunnen detecteren en afslaan? Welke factoren beïnvloeden de weerbaarheid? Welke interventiemogelijkheden zijn er om de weerbaarheid te verhogen? De bescherming van het mkb tegen cyberaanvallen ligt echter niet alleen bij het mkb zelf. Ook andere partijen hebben een rol bij het beschermen tegen cyberaanvallen.

24 Onder mkb verstaan we bedrijven met minder dan 250 werknemers en waarvan de jaaromzet niet hoger is dan 50 miljoen euro en het jaarlijkse balanstotaal niet hoger is dan 43 miljoen euro.
25 Zie voor de meest actuele cijfers van het CBS: https://www.staatvanhetmkb.nl/factsfigures (laatst geraadpleegd 23 augustus 2018).
26 https://www.dehaagsehogeschool.nl/docs/default-source/documenten-onderzoek/lectoraten/cybersecurity-in-het-mkb/infographic-nulmeting-cybersecurity-mkb.pdf
27 WODC (2011)
28 Op een enkele studie na zoals die van Veenstra e.a. (2015).

Daarom moet onderzocht worden welke rol politie en justitie nog hebben bij de aanpak van cybercrime gericht op het mkb.

Het doel van dit lectoraat is de kennispositie van het mkb op het gebied van cybercrime en cybersecurity vergoten om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen. Dit wordt bereikt door het uitvoeren van praktijkgericht wetenschappelijk onderzoek. Zoals hierboven beschreven staat, zijn verschillende thema's van belang.

Het lectoraat kent dan ook vier onderzoekslijnen, waarbinnen steeds het mkb centraal staat:

1. aard en omvang van slachtofferschap;
2. aard van cybercrime;
3. cyberweerbaarheid;
4. de aanpak van cybercrime.

3.1 De (potentiële) slachtoffers

Het is nog moeilijk om aan te geven hoeveel geslaagde cyberaanvallen er precies plaatsvinden en hoe groot de economische impact is. Enerzijds komt dat omdat het aantal delicten dat we kunnen scharen onder cybercrime groot is: van het hacken van een systeem en het platleggen van websites met zogenoemde 'Distributed Denail of Service' aanvallen (DDoS-aanvallen) tot het sturen van phishing e-mails om online bankrekeningen te plunderen en het gebruik van ransomware om losgeld te krijgen voor het ontsleutelen van bestanden. Anderzijds komt het gebrek aan inzicht omdat we simpelweg pas sinds een paar jaar slachtofferschap van cybercrime meten en dat dit soort slachtofferonderzoek ook nog eens beperkt is tot enkele vormen van cybercrime.

De beperkte cijfers die er zijn laten echter duidelijk zien dat cybercrime serieus genomen moet worden. Het Centraal Bureau voor de Statistiek (CBS) meet sinds een paar jaar slachtofferschap van hacken, online fraude en identiteitsdiefstal. De meest recente cijfers laten zien dat in een jaar tijd 5 procent van de Nederlanders slachtoffers werd van hacken, 4 procent slachtoffer werd van online fraude en 0,5 procent slachtoffer was van identiteitsdiefstal.[29] Helaas meet het CBS onder burgers geen andere vormen van slachtofferschap van cybercrime. Een iets ouder onderzoek leert ons echter dat ook andere vormen van cybercrime vaak voorkomen. Domenie en collega's lieten in 2012 bijvoorbeeld zien dat van de internetters in Nederland 16,7 procent slachtoffer werd van malware[30] (met financiële schade tot gevolg), 1,1 procent slachtoffer werd van cyberstalking en 0,4 procent slachtoffer werd van cyberbedreiging.

29 CBS (2017)
30 Kwaadaardige software, zoals een computervirus.

Vooral hacken en malware zijn dus veelvoorkomende delicten. Om deze cijfers in perspectief te plaatsen: slachtofferschap van fietsendiefstal, toch een delict waar Nederland om bekend is en waarvan iedereen weet dat het vroeg of laat een keer gaat gebeuren, is 4 procent. Voor de goede orde: het gaat bij zowel hacken als fietsendiefstal om aan onderzoekers zelf gerapporteerd slachtofferschap. Of mensen wel of niet aangifte doen bij de politie speelt hier dus geen rol. Nederland is daarmee nu dus niet langer het land van fietsendiefstal, maar het land van hacken én fietsendiefstal.

Cijfers over slachtofferschap onder burgers zijn schaars, maar cijfers over slachtofferschap van cybercrime onder bedrijven ontbreken bijna volledig. Er is nagenoeg geen methodologisch verantwoord onderzoek verricht is naar bedrijfsspecifieke cyberrisico's en daartegen te treffen maatregelen.[31] Veel inschattingen blijken gemaakt te zijn op basis van geïsoleerde datastromen en case studies die worden geëxtrapoleerd naar de gehele samenleving, waardoor schattingen ver uiteen lopen en er zowel onder- als over gerapporteerd wordt.[32] Daardoor lopen getallen en percentages in verschillende cybercrime rapportages nogal uiteen.

Recent empirisch onderzoek laat zien dat zowel mkb-bedrijven als zzp'ers actieve internetters zijn die voor hun bedrijfsvoering in grote mate afhankelijk zijn van ICT.[33] Het gros van de ondernemers treft uiteenlopende technische maatregelen tegen cybercrime (bijvoorbeeld virusscanners of het beveiligingen van wifi-netwerken). De Haagse Hogeschool voerde in 2017 een nulmeting uit naar slachtofferschap onder mkb'ers waaruit bleek dat een op de vijf deelnemende mkb'ers slachtoffer is geworden van een cyberaanval waardoor zij schade opliepen. De slachtoffers rapporteerden verschillende vormen van criminaliteit: malware (30 procent), phishing (10 procent) en hacken (7 procent) werden het vaakst gemeld. Zoals eerder al vermeld: de omvang van cybercrime is daarmee vergelijkbaar met de omvang van traditionele criminaliteit onder organisaties zoals inbraken en fraudes.[34]

Op dit moment bestudeert ons lectoraat welke factoren samenhangen met slachtofferschap onder het mkb.[35] Eerste analyses laten zien dat slachtofferschap samenhangt met het aantal medewerkers dat een bedrijf in dienst heeft. Hoe meer mensen in dienst, hoe groter de kans op slachtofferschap. Verder is te zien dat bedrijven die medewerkers meer vrijheden geven op het bedrijfsnetwerk vaker slachtoffer zijn van een cyberaanval. Deze eerste resultaten laten zien dat de menselijke factor binnen cyberaanvallen van wezenlijk belang is. Verder lijkt de aandacht voor menselijk gedrag als risicofactor nog onderbelicht in de veiligheidsmaatregelen die het mkb neemt: de meeste mkb'ers nemen wel technische maatregelen, zoals een virusscanner of het maken van back-ups, maar beleid omtrent wachtwoorden of hoe om te gaan met incidenten

31 Afkomstig uit Leukfeldt (2017)
32 Bijvoorbeeld Anderson e.a. (2013)
33 Veenstra e.a. (2015)
34 WODC (2011)
35 Notté, Van 't Hoff-de Goede, Slot & Leukfeldt (te verwachten)

ontbreekt vaak. Eenzelfde beeld is te zien binnen lopend kwalitatief onderzoek waarbij we binnen elf metaalbedrijven onderzoeken hoe bestaande complexe risicomodellen bruikbaar kunnen worden gemaakt voor kleinere bedrijven.[36] Eerste resultaten laten zien dat doordat de verantwoordelijkheid voor de uitvoering en het beheer van de veiligheid van ICT wordt uitbesteed, er binnen de bedrijven geen goed beeld bestaat over de risico's die er zijn en de wijze waarop deze risico's kunnen worden verkleind. De uitkomsten van deze pilotstudie zullen worden gebruikt om binnen een grotere groep bedrijven op maat gemaakte risicomodellen te ontwikkelen.

3.2 Cyberweerbaarheid

Het mkb heeft onvoldoende middelen en (toegang tot) kennis om dreigingen te onderkennen en zich vervolgens weerbaar te maken.[37] Basale beveiligingsmaatregelen, zoals het updaten van software, het gebruik van sterke wachtwoorden of het maken van back-ups van belangrijke bestanden, worden vaak niet genomen.[38] Mkb-ondernemers achten zichzelf veelal niet interessant voor cyberaanvallen en zien cybercrime niet als een van de belangrijkste risico's. Het zijn vooral de sociaal-economische ontwikkelingen waar de ondernemer van wakker ligt.[39] Risico's blijven daardoor ongrijpbaar en het belang van cybersecurity krijgt onvoldoende prioriteit totdat het een keer echt misgaat. Daarmee vormt een gebrek aan weerbaarheid een serieus probleem.[40] Verder kan gesteld worden dat onveilig gedrag vaak aan de basis staat van geslaagde cyberaanvallen: iemand trapt in een phishing e-mail, heeft de verplichte software-update te lang uitgesteld of een standaardwachtwoord nooit aangepast. Daarom is het van belang dat er zicht komt in waarom mkb'ers zich onveilig gedragen. Tevens is inzicht vereist in manieren waarop mensen kunnen worden gestimuleerd om zich wél veilig te gedragen zonder al te veel impact op de dagelijkse routine.

Om hier meer zicht op te krijgen, voeren we op dit moment samen met de Gemeente Den Haag een cyberweerbaarheidsscan uit in twee winkelgebieden in Den Haag. De cyberweerbaarheidsscan is een vragenlijst die inzicht biedt in het vermogen van ondernemers om weerstand te bieden aan bekende en onbekende vormen van cybercrime. Ook maakt dit instrument inzichtelijk in welke mate organisaties het vermogen bezitten om veerkrachtig te zijn en snel te kunnen herstellen van een crisis als gevolg van een aanval. Inzicht in deze vermogens kan helpen om de juiste voorzieningen te treffen en meer digitaal weerbaar te zijn, zodat medewerkers cyberveilig kunnen werken. Eerste resultaten laten zien dat het met de digitale weerbaarheid van het mkb matig is gesteld. Vooral het vermogen om te leren van cyberincidenten is beperkt aanwezig bij het mkb. Kansen om kennis die is opgedaan tijdens het incident te gebruiken om systemen, protocollen

36 Notté, Van 't Hoff-de Goede, Slot & Leukfeldt (te verwachten)
37 Verhagen (2016)
38 Munnichs e.a. (2017)
39 Van den Berg en Reijmer (2015)
40 Munnichs e.a. (2017)

en mensen veerkrachtiger te maken, worden nog onvoldoende benut. Ten slotte zijn we onlangs gestart met een experimenteel onderzoek in opdracht van het Ministerie van Jusitie en Veiligheid waarvoor we in kaart brengen hoe het gesteld is met het cyberbewustzijn van internetters in Nederland, of ze daadwerkelijk cyberbewust handelen en om een eerste aanzet te geven om interventies te ontwikkelen om het cyberbewustzijn op een hoger niveau te tillen. De resultaten van dit onderzoek worden naar verwachting medio 2019 gepubliceerd.

3.3 De criminelen

Naast inzicht in slachtofferkenmerken is het van belang om inzicht te krijgen in de werkwijzen en verdienmodellen van cybercriminelen. Selecteren aanvallers specifieke mkb-bedrijven of vallen ze alles aan wat los en vast zit? En van welke zwakke plekken maken criminelen gebruik om hun aanvallen uit te voeren?

Inzicht in de werkwijzen van cybercriminelen die zich richten op het mkb kan direct gebruikt worden voor het verhogen van de weerbaarheid van mkb-bedrijven. Zonder zicht op hoe de aanvallers te werk gaan is het immers moeilijk om mkb'ers weerbaarder te maken tegen die aanvallen. Daarnaast kan inzicht in werkwijzen en verdienmodellen gebruikt worden om criminele activiteiten te verstoren of zelfs te voorkomen. 'Crime script' analyses kunnen bijvoorbeeld worden gebruikt om alle stappen binnen een crimineel proces – van voorbereiding tot het wegsluizen van criminele verdiensten – in kaart te brengen.[41] Iedere stap brengt weer een mogelijkheid tot interventie met zich mee. De kosten voor het uitvoeren van cyberaanvallen moeten hoger gemaakt worden, terwijl de baten lager moeten worden.

41 Bijvoorbeeld Cornish (1994) en Somer e.a. (2016).

3.4 De aanpak

Cybercrimes zijn lucratief omdat de pakkans laag is en de potentiële opbrengsten hoog. Het verhogen van de pakkans of het bemoeilijken van het plegen van een delict zorgt voor minder criminaliteit. Verschillende partijen zijn betrokken bij de aanpak van cybercrime.[42] Ten eerste zijn er organisaties die cyberveiligheid niet als 'core business' hebben, maar wel een belangrijke rol kunnen hebben bij het verminderen van slachtofferschap. Internet Service Providers, verzekeringsmaatschappijen en hosting bedrijven zijn hier voorbeelden van. Dit soort partijen kunnen zelf maatregelen nemen om de kans op incidenten voor hun klanten te verkleinen. Door bijvoorbeeld 'contractual governance' kunnen zij het gedrag van hun klanten beïnvloeden. Een andere belangrijke vraag, als het gaat om de bescherming van mkb'ers, is welke rol brancheverenigingen en andere belangenverenigingen hierbij kunnen spelen.[43]

Daarnaast zijn er partijen die als primaire taak hebben om cybercrime te bestrijden. Dat zijn politie en justitie, maar wellicht nog meer dan bij andere vormen van criminaliteit, ook particuliere beveiligingsbedrijven en publiek-private samenwerkingen (zoals het in 2018 opgerichte Digital Trust Center[44]). De rol van traditionele partijen zoals politie en justitie lijkt kleiner te worden als het gaat om het tegengaan van cyberaanvallen – in ieder geval in de ogen van slachtoffers. Zo blijkt bijvoorbeeld dat de aangiftebereidheid na slachtofferschap van cybercrime onder mkb'ers laag is; nog lager dan bij traditionele delicten.[45] Het is overigens nog maar de vraag of redenen om wel of geen aangifte te doen gelijk zijn voor traditionele delicten en cyberdelicten. Daar weten we nog vrij weinig van af. In een door het NSCR uitgevoerde pilotstudie blijkt dat determinanten van aangiftebereidheid na traditionele delicten niet altijd ook aangiftebereidheid na cybercrime voorspellen.[46] Wat echter duidelijk is, is dat politie en justitie dus niet meer automatisch worden gezien als verantwoordelijke of enige partij om cybercrime aan te pakken.[47] Opgemerkt moet worden dat een onderzoek naar publiek-private samenwerking bij de aanpak van cyberaanvallen op het mkb laat zien dat respondenten vinden dat er te veel initiatieven zijn waardoor mkb'ers door de bomen het bos niet meer zien.[48] Het is daarom van belang om inzicht te krijgen in hoe effectief de huidige aanpak van cybercrime is en wat de verwachtingen en behoeften zijn van slachtoffers van cybercrime wat betreft de aanpak van politie en justitie en andere partijen.

42 Zie voor een uitgebreide analyse Boes en Leukfeldt (2017).
43 Notté, Van 't Hoff-de Goede, Slot & Leukfeldt (te verwachten) – respondenten in dit onderzoek geven aan dat ze ondersteuning willen bij het verbeteren van hun cybersecurity én dat bijvoorbeeld een branchevereniging daarbij een rol kan spelen.
44 https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2017/09/23/kamerbrief-oprichting-van-een-digital-trust-centre/kamerbrief+over+oprichting+van+een+digital+trust+centre.pdf
45 Veenstra e.a. (2015)
46 Jong, Leukfeldt en van de Weijer (2018)
47 Leukfeldt e.a. (2013), Domenie e.a. (2012), Jansen en Leukfeldt (2018).
48 Van den Oever (2018)

4 The proof of the pudding is in the eating: praktijkgericht onderzoek voor en met de praktijk

In deze intreerede heb ik uiteen gezet dat cyberaanvallen veelvoorkomend zijn, dat cybersecurity meer is dan een palet aan technische maatregelen alleen en dat een integrale aanpak nodig is waarbij wordt gekeken naar de (potentiële) slachtoffers en hun kenmerken en gedragingen, de criminelen en hun werkwijzen en verdienmodellen en de publieke en private 'capable guardians' en hun strategieën om cyberaanvallen te verminderen en de pakkans en daarmee de kosten te verhogen.

Het lectoraat beoogt bij te dragen aan het verlagen van slachtofferschap onder mkb'ers en de impact van cyberaanvallen door de kennispositie van dat mkb en andere relevante partijen op het gebied van cybercrime en cybersecurity te vergroten. Nadrukkelijk doel is om niet alleen nieuwe kennis op te doen en te delen, maar juist om experimenten op te zetten met interventies die slachtofferschap kunnen voorkomen of de impact van cyberaanvallen kan verminderen. Daarom is essentieel bij het uitvoeren van onderzoeken, die we binnen dit lectoraat de komende jaren gaan doen, het in stand houden en verder uitbouwen van de (regionale) community van mkb'ers, overheidsinstellingen, politie en justitie en cybersecurity bedrijven die De HHs nu heeft. Nadrukkelijk zeg ik hier – verder uitbouwen – omdat we al hard bezig zijn om precies dit te doen: met de Koninklijke Metaalunie ontwikkelen we bijvoorbeeld op kleine organisatie toegespitste risicomodellen, met de gemeente Den Haag voeren we cyberweerbaarheidsscans uit in een aantal winkelgebieden en voor de Nationale Politie zoeken we uit waarom ondernemers geen aangifte doen van cybercrimes. We doen dus niet alleen onderzoek vanuit onze studeerkamers, maar doen praktijkgericht onderzoek samen met de praktijk – in dit geval het mkb. Mijns inziens is dat ook de enige manier van onderzoek doen: op deze manier kunnen de ontwikkelingen in de grootste problemen die de samenleving ondervindt, geïdentificeerd worden. Daarnaast kunnen deze praktijkgerichte onderzoeken gebruikt worden om te inventariseren wat veelbelovende richtingen zijn voor theorievormend onderzoek. Wetenschappelijk onderzoek naar cybercrime en cybersecurity staat immers nog in de kinderschoenen. Er is daarom een grote behoefte aan theorievormend onderzoek: Is die routine activiteitentheorie nog wel van toepassing op cybercrimes? Welke methoden binnen het kader van situationele criminaliteitspreventie werken wel en welke niet? En kunnen we interventies ontwikkelen om mkb'ers weerbaarder te maken tegen cyberaanvallen? Met dit lectoraat verbinden we beide werelden: die van het doen van onderzoek voor de praktijk en met de praktijk en die van theorievormend onderzoek. Op deze manier leveren we een directe bijdrage aan empirische kennis over cybercrime en cybersecurity en vergroten we de kennispositie van het mkb op het gebied van cybercrime en cybersecurity om zo het slachtofferschap en de impact van cyberaanvallen onder mkb'ers te verlagen.

LITERATUUR

Anderson, K.B. (2006). Who are the victims of identity theft? The effect of demographics. *Journal of Public Policy & Marketing*, *25*(2), 160–171.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In R. Böhme (ed.), *The Economics of Information Security and Privacy*. Springer-Verlag Berlin Heidelberg.

Boes, S., & Leukfeldt, E.R. (2017). Fighting Cybercrime: A Joint Effort. In M. R. Clark & S. Hakim (Eds.), *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level* (pp. 185-203). Cham: Springer International Publishing.

Bossler, A.M. & Holt, T.J. (2009). Online activities, guardianship, and malware infection: An examination of routine activities theory. *International Journal of Cyber Criminology*, 3(1), 400-420.

CBS (2017) Veiligheidsmonitor 2017. Den Haag/Heerlen: CBS.

Choi, K. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology*, 2(1), 308-333.

Clarke, R.V. (2004). Technology, crime and Crime Science. *European Journal on Criminal Policy and Research*, *1*(10), 55-63.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *4*(44), 588–608.

Cornish, D. B. (1994). The procedural analysis of offending and its relevance for situational prevention. Crime prevention studies, 3, 151-196.

Cornish, D. B., & Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, (16),* 41-96.

Domenie, M. M. L., Leukfeldt, E.R., Van Wilsem, J. A., Jansen, J., & Stol, W. P. (2012). *Slachtofferschap in een gedigitaliseerde samenleving.* Den Haag: Boom Lemma.

European Union Agency for Network and Information Security (ENISA) (2015). Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport Laatste geraadpleegd op 1 november 2017.

Hartel, P., Junger, M., & Wieringa, R. (2011). *Cyber-crime Science = Crime Science + Information Security*. Enschede: University of Twente.

Hassenzahl, M., Diefenbach, S., & Goritz, A. (2010). Needs, affect, and interactive products – Facets of user experience. Interacting with computers, *22*(5), 353-362.

Hollnagel, E., J. Pariès, D. Woods and J. Wreathall (Eds.) (2010). Resilience Engineering in Practice. A Guidebook, Ashgate Publishing Ltd., Farnham, Surrey, UK.

Hollnagel, E., Paries, J., Woods, D., & Wreathall, J. (2011). Resilience engineering in practice: a guidebook. Ashgate, United Kingdom.

Hutchings, A., & Hayes, H. (2008). Routine activity theory and phishing victimisation: Who gets caught in the 'net'. *Current Issues Criminal Justice*, *20*(3), 433–451.

Jansen, J. & Leukfeldt, R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

Jansen, J., & E.R. Leukfeldt (2018) Coping with cybercrime victimization: An exploratory study into impact and change. J*ournal of Qualitative Criminal Justice & Criminology.*

Jong, L., E.R. Leukfeldt & S. van de Weijer (2018) Aangiftebereidheid na slachtofferschap van cybercrime. Tijdschrift voor Veiligheid. 17(1-2) 66-78.

Kleij, R. van der (2018). Digitale weerbaarheid in het mkb: een serieus probleem? *Tijdschrift voor Human Factors, 43*(1), 19-21.

Leukfeldt, E.R. & Yar, M. (2016). Applying routine activity theory to cybercrime. A theoretical and empirical analysis. *Deviant Behavior.* DOI:10.1080/01639625.2015.1012409.

Leukfeldt, E.R. (2014). Phishing for suitable targets in the Netherlands. Routine activity theory and phishing victimization. *Cyberpsychology behavior and social networking* 17(8) 551-555.

Leukfeldt, E.R. (2015). Comparing victims of phishing and malware attacks. Unraveling risk factors and possibilities for situational crime prevention. *International Journal of advanced studies in Computer Science and Engineering* 4(5) 26-32.

Leukfeldt, E.R. (2016). Cybercriminal networks: Origin, growth and criminal capabilities. (Doctorate thesis) The Hague: Eleven International Publishers.

Leukfeldt, E.R. (ed) (2017). Research Agenda: The Human Factor in Cybercrime and Cybersecurity. The Hague: Eleven International Publishers.

Leukfeldt, E.R., Veenstra, S., & Stol, W.P. (2013) High Volume Cyber Crime and the Organization of the Police. The results of two empirical studies in the Netherlands. *International Journal of Cyber Criminology* 7(1) 1-17.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471-476.

Munnichs , G., Kouw, M., & Kool, L. (2017). Een nooit gelopen race: Over cyberdreigingen en versterking van weerbaarheid. Rathenau instituut, Den Haag.;

National Academy of Sciences (2012). Disaster resilience: a national imperative. Washington DC, United States.

Ngo, F. T., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology, 5 (1),* 773-793.

Notté, R., Slot, L., Van 't Hoff-de goede, S. & Leukfeldt, E.R. (te verwachten). Nulmeting cybersecurity in het mkb. Den Haag: Haagse Hogeschool.

Notté, R., Van 't Hoff-de goede, S. & Leukfeldt, E.R. (te verwachten). Cybersecurity binnen smart industry. Den Haag: Haagse Hogeschool.

Oosterwijk, K. & Fischer, T.F.C. (2017). Interventies jeugdige daders cybercrime. Den Haag: WODC.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, *47*(3), 267–296.

Somer, T., Hallaq, B., & Watson, T. (2016). Utilising journey mapping and crime scripting to combat cyber crime and cyber warfare attacks. Journal of Information Warfare, 14 (4). pp. 39-49.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy In 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior. *Proceedings of the ACM Conference on Electronic Commerce*, Tampa, Florida, USA — October 14 - 17, 2001.

Van den Berg, M. & Reijmer, T. (2015). Cybersecurity in het mkb. https://www.interpolis.nl/~/media/files/ebook_cybersecurity_in_het_mkb.pdf Laatst geraadpleegd 25 augustus 2018.

Van den Oever, A. (2018). De cyberweerbaarheid van het mkb: faalt de markt of de overheid? Een onderzoek naar de rol van de markt en de overheid bij de cyberweerbaarheid van het mkb. (master thesis) Den Haag/Rotterdam: Haagse Hogeschool / Erasmus Universiteit Rotterdam.

Van Der Zee, S. (2018). Cyber Security Paradox: When knowing what's right does not lead to doing what's right. Oral presentation at the Security & Human Behavior workshop 2018. Summary was last retrieved on 20-08-2018 from https://www.lightbluetouchpaper.org/2018/05/24/security-and-human-behavior-2018/

Veenstra, S., Zuurveen, R., & Stol, W.Ph. (2015). *Cybercrime onder bedrijven. Een onderzoek naar slachtofferschap van cybercrime onder het Midden- en Kleinbedrijf en Zelfstandigen zonder Personeel in Nederland.* Leeuwarden: Lectoraat Cybersafety.

Verhagen, H. (2016). De economische en maatschappelijk noodzaak van meer cybersecurity. Nederland digitaal droge voeten . Verkregen op 15.02.2018 van : https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf.

Wilsem, J. van (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. Journal of Contemporary Criminal Justice, 29, 437-453.

WODC (2011). *Monitor Criminaliteit Bedrijfsleven 2010: Feiten en trends inzake aard en omvang van criminaliteit in het bedrijfsleven*. Den Haag: WODC.

De Haagse Hogeschool
Johanna Westerdijkplein 75
2521 EN Den Haag

dehaagsehogeschool.nl