Digitale en traditionele bedreiging vergeleken

Een studie naar risicofactoren van slachtofferschap

Johan van Wilsem

Computers en internet bieden nieuwe mogelijkheden om criminaliteit te plegen. In dit artikel wordt de routineactiviteitentheorie gebruikt om slachtofferschap van digitale bedreiging (bijv. via e-mail of sms) te bestuderen, aan de hand van gegevens uit een grootschalige slachtofferenquête (N=6.896). Risicofactoren voor digitale bedreiging worden vergeleken met risicofactoren voor traditionele bedreiging en het ontvangen van een mix van digitale en traditionele bedreigingen. De resultaten tonen aan dat jongeren en daders van digitale criminaliteit hogere risico's lopen op ieder van deze vormen van bedreiging. Verder blijkt dat activiteiten buitenshuis risicoverhogend zijn voor zowel traditionele als digitale bedreiging. Hetzelfde geldt voor bepaalde computeractiviteiten, zoals een profiel op Hyves. Dit duidt op verwevenheid van sociale interacties in de 'fysieke' en de digitale wereld. Tot sluit blijkt dat impulsieve mensen eerder met bedreiging in aanraking komen.

Ontwikkelingen op het gebied van informatisering hebben grote gevolgen gehad voor allerlei handelingen van mensen. Voor activiteiten die traditiegetrouw buitenshuis moesten worden uitgevoerd (zoals naar een winkel gaan om producten te kopen of bekijken), zijn digitale alternatieven ontstaan (surfen naar internetwinkels of vergelijkingssites). Naast de legale mogelijkheden die internet biedt voor communicatie, transacties en het verzamelen van informatie, zijn er echter ook illegale mogelijkheden opgekomen, zoals *e-mail scams* door fraudeurs die onder het mom van charitatieve doelstellingen opereren, vernieling van harde schijven door *hackers* die virussen verspreiden, en bedreigingen die via e-mail worden verzonden. Killias (2006) noemt zo'n ontwikkeling als informatisering een breuk met de oude (computerloze) maatschappij, die leidt tot nieuwe vormen van illegaal gedrag[1] en vervolgens reacties als nieuwe wetgeving en innovatie in preventievormen oproept. Ondanks de ernst van dergelijke criminaliteit – zowel financieel als emotioneel – is er over het algemeen echter nog weinig over bekend, zoals ook blijkt uit de recente overzichtsstudie van Van der Hulst en Neve (2008).

In dit artikel staat slachtofferschap van *bedreiging* centraal, een delict dat zowel op conventionele als digitale wijze kan worden gepleegd (bijvoorbeeld *face to face*, via telefoon of brief en via e-mail, sms of *chatroom*). Van der Hulst en Neve (2008) scharen een dergelijk type overtreding onder de zogenoemde *cybercriminaliteit*, omdat het een traditioneel delict is dat met behulp van ICT kan worden gepleegd,

1 Een voorbeeld is de recente rechtszaak in oktober 2008 tegen twee Friese jongeren die een leeftijdgenoot hadden bestolen van zijn punten in het internetspel *Runescape*.

net als bijvoorbeeld fraude. Dit is in tegenstelling tot de zogenoemde *computercriminaliteit*, die niet plaats kan vinden zonder computers, omdat die juist het doelwit vormen van het delict, zoals bij *hacking* het geval is.
De focus van dit artikel is de manier waarop de dagelijkse activiteiten van mensen van invloed zijn op hun kans om (digitaal) bedreigd te worden. Uit eerder onderzoek naar traditioneel, niet-digitaal geweld is gebleken dat men eerder slachtoffer wordt naarmate men zich vaker buitenshuis begeeft op plekken met weinig sociale controle, zoals in het uitgaansleven. Dergelijke resultaten vormen een duidelijke ondersteuning voor de routineactiviteitentheorie, die stelt dat buitenshuisactiviteiten gelegenheid creëren voor criminaliteit via blootstelling aan daders (Cohen & Felson, 1979; Mustaine & Tewksbury, 1998). Digitale media introduceren echter nieuwe omgevingen waar conflicten tussen mensen kunnen ontstaan en waar gedreigd kan worden met geweldpleging. Dat levert een aantal nieuwe verschijningsvormen op van bedreiging. Als eerste is er de puur digitale vorm, die zijn oorsprong vindt in digitale activiteiten (bijvoorbeeld door onenigheid in een e-mailwisseling) en ook digitaal 'afgehandeld' wordt (via een dreigmail). Het is echter ook mogelijk dat er bij een bedreiging sprake is van een verwevenheid tussen de digitale en 'fysieke' wereld. De voedingsbodem voor een conflict kan bijvoorbeeld tijdens het chatten op internet zijn ontstaan, maar – als de betrokkenen elkaar kennen – uiteindelijk resulteren in een 'traditionele' *face to face*-bedreiging. Andersom kan in de 'fysieke' wereld een conflict tussen mensen ontstaan, dat langs digitale weg met een bedreiging wordt afgehandeld. In dit artikel wordt slachtofferschap van digitale en traditionele bedreiging dan ook gerelateerd aan dagelijkse buitenshuis- én computeractiviteiten. Op deze manier kan worden nagegaan welke activiteiten welke vorm van bedreiging beïnvloeden; bijvoorbeeld of digitale bedreiging niet alleen afhankelijk is van computeractiviteiten, maar ook van *exposure* aan daders via activiteiten buitenshuis. Een dergelijke benadering houdt dan ook rekening met een duidelijke verbondenheid van interacties in de fysieke en virtuele wereld (zie ook De Haan, 2008). Door zowel traditionele als digitale bedreiging tegelijkertijd te bestuderen kan verder ook worden nagegaan in hoeverre de opkomst van digitale mogelijkheden om bedreigd te worden heeft geleid tot een nieuwe groep slachtoffers met specifieke kenmerken, of juist dat digitale en traditionele bedreiging gerelateerde fenomenen zijn, die uiteindelijk dezelfde groep mensen treffen (Grabosky, 2001).

In dit artikel wordt gebruikgemaakt van gegevens uit een grootschalige, representatieve steekproef van de Nederlandse bevolking. Deze hebben betrekking op ruim 6.500 respondenten uit de algemene bevolking van 16 jaar en ouder, uit het door CentERdata opgezette LISS panel (*Longterm Internet Studies in the Social Sciences*). Hierbij zijn in februari 2008 vragen aan het panel gesteld over onder andere slachtofferschap van criminaliteit. Samenvattend biedt dit artikel, door het vergelijken van risicofactoren voor digitale en traditionele bedreiging, via gebruik van directe metingen voor dagelijkse activiteiten – zowel buitenshuis als op internet – via een grootschalige survey, de mogelijkheid om een duidelijke stap voorwaarts te zetten in onderzoek naar de wijze waarop digitale media de aard en oorzaken van criminaliteit beïnvloeden.

Dagelijkse activiteiten en bedreiging

De routineactiviteitentheorie heeft zich inmiddels nuttig bewezen ter verklaring van de vraag wie slachtoffer wordt van traditionele delicten (Van Wilsem, 2003; Wittebrood, 2006), maar is echter nauwelijks getoetst voor *digitale* criminaliteit. Niettemin zijn er verschillende aanwijzingen dat de risicofactoren voor digitale en traditionele bedreiging overlappen. Voor het plaatsvinden van criminaliteit moet er een samenkomst in tijd en ruimte zijn van een gemotiveerde dader, een geschikt doelwit en gering toezicht (Cohen & Felson, 1979). In de virtuele wereld heeft met name de ruimtelijke samenkomst tussen dader en slachtoffer een andere lading: in plaats van een fysieke omgeving wordt het delict gepleegd en ondervonden via een digitaal kanaal. Niettemin zijn gelegenheidsfactoren wel degelijk van belang en kan de routine activiteitentheorie er op worden toegepast (Grabosky, 2001; Yar, 2005). In algemene zin wordt de VIVA-indeling (*Value, Inertia, Visibility, Accessibility*) veelal gehanteerd om te bepalen in hoeverre een doelwit geschikt is om als slachtoffer te worden geselecteerd (Felson & Clarke, 1998). Voor bedreiging – zowel digitaal als traditioneel – lijkt het met name om het laatste aspect te gaan: toegankelijkheid. Deze wordt bepaald door dagelijkse activiteiten die het doelwit blootstellen aan anderen onder omstandigheden waarbij sociale contacten snel conflictueus zijn, zoals *chatrooms* of het uitgaansleven. Naarmate mensen zich via dagelijkse activiteiten meer blootstellen aan daders, zijn zij toegankelijker en lopen zij een groter risico op slachtofferschap van bedreiging. Met de opkomst van digitale media is echter een belangrijke vraag welk soort activiteiten (digitaal/buitenshuis) risicoverhogend zijn voor welke vorm van bedreiging (digitaal/traditioneel).

Omdat sociale interacties zich namelijk zowel in de virtuele als in de fysieke wereld voordoen, geldt dat dus ook voor de plek waar mensen onenigheid met elkaar krijgen, en voor de plek waar deze onenigheid tot uitbarsting komt – via een bedreiging. Blootstelling aan daders vindt voor digitale bedreiging dan ook niet alleen plaats via computeractiviteiten, maar mogelijk ook via activiteiten buitenshuis. Dáár kan de voedingsbodem voor een conflict ontstaan, dat vervolgens digitaal wordt uitgevochten. Andersom kan slachtofferschap van traditionele bedreiging ook afhankelijk zijn van de mate van activiteit op internet.

Verder zou ook het aspect van zichtbaarheid (*visibility*) een rol kunnen spelen, omdat mensen die zich via een internetprofiel of webcam tonen aan anderen, om die reden grotere risico's op bedreiging kunnen lopen. Ook hiervoor geldt dat deze zichtbaarheid niet alleen het risico op digitale bedreiging kan verhogen, maar ook op traditionele bedreiging.

Een ander gelegenheidsaspect dat invloed heeft op het plaatsvinden van criminaliteit, is de mate van toezicht. Het gezin is hier een belangrijke bron; sociale controle in deze context blijkt niet alleen van invloed op daderschap, maar ook op slachtofferschap. Zo vinden Schreck en Fisher (2004) dat een warm gezinsklimaat leidt tot een kleinere kans op slachtofferschap van geweld bij jongeren, ook als gecorrigeerd wordt voor achtergrondkenmerken, routineactiviteiten en de invloed van vrienden. De aanname hierbij is dat gezinsleden controle kunnen uitoefenen over het gedrag van het doelwit en daarmee de kans verkleinen om in

aanraking te komen met een dader. Dit kan niet alleen plaatsvinden via directe controle, door veel tijd met het doelwit door te brengen, maar ook door leefregels op te leggen en het doelwit te leren gevaarlijke situaties te vermijden ('Direct uit school naar huis toe komen!'). De invloed van het gezin kan als zodanig niet alleen de aanraking met traditionele bedreiging beïnvloeden, maar ook met digitale bedreiging, via toezicht op computeractiviteiten en door digitale leefregels op te leggen. Verder is het mogelijk dat deze controle door gezinsleden niet alleen voor jongeren geldt, maar ook voor volwassenen, omdat relatiepartners eveneens toezicht op elkaar kunnen uitoefenen, en bijvoorbeeld in geval van een digitaal conflict met iemand anders elkaar kunnen adviseren wat adequate reactiestrategieën zijn die niet tot een escalatie leiden (bijvoorbeeld: over de levering van een product via marktplaats.nl). In huishoudens waarin géén twee partners aanwezig zijn – eenoudergezinnen en eenpersoonshuishoudens – wordt dan ook een groter risico op slachtofferschap van bedreiging verwacht, regulier én digitaal.
Een ander onderdeel van toezicht, het nemen van technische preventiemaatregelen (zoals *firewalls* en inbraakalarm), zijn weliswaar relevant voor het beperken van het risico voor allerlei vormen van digitale en traditionele criminaliteit (Giblin, 2008; CSI, 2007), maar lijken niet goed toepasbaar in de context van bedreiging. Er wordt dus geen risicobeperkende werking van verwacht voor slachtofferschap van dit delict. Tot slot bestaat er mogelijk ook iets als 'informeel' digitaal toezicht, dat bijvoorbeeld wordt uitgeoefend via chatvrienden die erop toezien dat iedereen zich aan bepaalde omgangsvormen houdt. Omdat ik bij dit aspect niet beschik over adequate gegevens, wordt daar echter verder niet op ingegaan.

Impulsiviteit, dagelijkse activiteiten en slachtofferschap
Impulsiviteit en gebrek aan zelfcontrole blijken niet alleen oorzaken van delinquentie, maar ook van slachtofferschap (bijv. Junger & Wittebrood, 1997; Schreck, 1999; Smith & Ecob, 2007). Deze kenmerken verhogen namelijk de kans dat iemand in riskante situaties verzeild zal raken, en daarmee ook de kans op slachtofferschap (Schreck, 1999). Ook heeft de concentratie van impulsieve mensen onder daders mogelijk tot gevolg dat zij meer worden geconfronteerd met vergelding van eerdere overtredingen (Wittebrood & Van Wilsem, 2000). Volgens deze redeneringen zou de invloed van impulsiviteit op slachtofferschap indirect zijn: impulsieve mensen ondernemen vaker activiteiten die hen aan risico's blootstellen (zoals veel *online* winkelen en daderschap van cybercriminaliteit), en dat verhoogt vervolgens hun kans op slachtofferschap. Daarnaast kan het echter ook zo zijn dat impulsieve mensen *binnen* die riskante situaties sneller bij conflicten betrokken raken en minder goed op hun eigen spullen passen, en daardoor nog een aanvullend verhoogd risico lopen. Er is in een dergelijk geval sprake van een zelfstandige invloed van impulsiviteit op slachtofferschap. In het huidige artikel wordt dit voor zowel traditionele als digitale bedreiging nagegaan.

Data

In deze paper wordt gebruikgemaakt van de data van het LISS panel van CentERdata. De steekproef voor dit panel is getrokken op adresniveau en is bij benadering representatief voor Nederlandse huishoudens. Als er geen computer aanwezig was in het huishouden, is er door CentERdata één toegekend voor de duur van het panelonderzoek (circa 5 procent van de steekproef).[2] Op elk adres mogen alle leden van het huishouden van 16 jaar en ouder de maandelijks wisselende vragenlijst invullen. De respondenten werd in februari 2008 gevraagd om vragen te beantwoorden over o.a. slachtofferschap, dagelijkse routine activiteiten en impulsiviteit. Voor deze vragenlijst gold een respons van 77 procent van het totale panel, resulterend in 6.896 respondenten die afkomstig zijn uit 4.353 huishoudens.

Operationaliseringen

Slachtofferschap van bedreiging

Om de prevalentie van slachtofferschap van bedreiging over de periode van het afgelopen jaar vast te stellen, werd respondenten eerst gevraagd of zij de volgende incidenten ooit hadden meegemaakt: (a) digitale bedreiging (bijvoorbeeld via e-mail of chatsite), of (b) andere vorm van bedreiging (bijv. via brief of *face to face*). Aan degenen die bevestigend antwoordden, werd vervolgens gevraagd hoe vaak zij dit het afgelopen jaar hadden meegemaakt. Aan de hand hiervan werden vier groepen onderscheiden: (a) niet-slachtoffers, (b) slachtoffers van alleen traditionele bedreiging, (c) slachtoffers van alleen digitale bedreiging, en (d) slachtoffers van zowel traditionele als digitale bedreiging. In totaal had ruim 7 procent van de respondenten ten minste één vorm van bedreiging meegemaakt gedurende het afgelopen jaar. Circa 5 procent was alleen op de traditionele manier bedreigd, 0,9 procent alleen digitaal bedreigd, en 1,3 procent had met zowel traditionele als digitale bedreiging te maken gehad.

Achtergrondkenmerken

Verschillende achtergrondkenmerken zijn verzameld onder de respondenten. Naast sekse en leeftijd weten we bijvoorbeeld het hoogst voltooide opleidingsniveau, dat zes categorieën heeft en varieert van 'basisschool' (1) tot 'universiteit' (6). Ook is een aantal huishoudenkenmerken bekend. Ten eerste is er een variabele die aangeeft of het huishouden twee (gehuwde of ongehuwde) partners heeft (1), of een eenpersoons- of eenouderhuishouden is (0). Ook is er informatie over het nettomaandinkomen van het huishouden (in duizend euro). Verder is geprobeerd om rekening te houden met omgevingsinvloeden, met name voor traditio-

2 Hoewel het op het eerste gezicht minder relevant lijkt deze groep mee te nemen voor dit onderzoek omdat zij geen slachtoffer van digitale bedreiging zou kunnen worden, is dat niet het geval. Vijfenzeventig procent van deze groep geeft namelijk aan wel een computer te gebruiken, maar op een andere plek dan thuis (werk, bibliotheek enz.). Om die reden bevat ook de groep niet-computerbezitters mensen die een digitale bedreiging hebben meegemaakt.

nele bedreiging, die zich op straat voor kan doen. Er is echter niet bekend in welke buurt het huishouden woont. Wel is er informatie over de stedelijkheid van de leefomgeving, zoals vastgesteld door het CBS. Deze variabele wordt bepaald door de adressendichtheid en bevat vijf categorieën, variërend van 'niet stedelijk/minder dan 500 adressen per km^2' (1) tot 'zeer stedelijk/2.500 adressen per km^2 of meer' (5). Uit eerder onderzoek is gebleken dat stedelijkheid en bevolkingsdichtheid positief gerelateerd zijn aan criminaliteit en slachtofferschap (bijv. Land e.a., 1990).

Routineactiviteiten buitenshuis
Vijf uiteenlopende dagelijkse activiteiten zijn de indicatoren voor de blootstelling van doelwitten buitenshuis aan daders van bedreiging. Hierbij is gevraagd hoe vaak de respondent (a) naar een restaurant gaat, (b) een café bezoekt, (c) met vrienden afspreekt, (d) gaat winkelen, en (e) sportactiviteiten onderneemt. Antwoordmogelijkheden variëren van 'nooit/niet vaker dan eens per jaar' (1) tot 'meer dan één keer per week' (5). Daarnaast is gevraagd naar de tijd die buitenshuis wordt doorgebracht vanwege verplichtingen voor werk of opleiding. Hierdoor is bekend hoeveel uur men per week doorbrengt op het werk of de plek voor scholing, en hoeveel uur per week men forenst (onderweg tussen huis en deze plek).

Digitale routineactiviteiten
Ook de manier waarop computers en internet worden gebruikt, is voor de respondenten vastgesteld. Hierbij is gevraagd naar de hoeveelheid uren die men gemiddeld per week doorbrengt met (a) e-mail, (b) informatie zoeken op internet, (c) producten kopen via internet, (d) chatten, en (e) internetfora en *communities* bezoeken. Ook is gevraagd of men een profiel heeft op Hyves, een populaire netwerksite; dat bleek voor een kwart van de respondenten het geval te zijn. Tot slot werd vastgesteld of de respondent een webcam gebruikt; circa 15 procent in de steekproef gaf aan dat te doen.

Impulsiviteit
In dit onderzoek is informatie beschikbaar omtrent zogenoemde disfunctionele impulsiviteit. Om dit kenmerk vast te stellen, zijn de twaalf items hierover uit de Dickman Impulsivity Inventory gebruikt (Dickman, 1990). Elk item verwijst naar een gedraging waarvoor de respondent moet aangeven of hij/zij het ermee eens is (ja/nee) dat dit gedrag bij hem/haar past. Bijvoorbeeld: 'Ik maak geregeld afspraken zonder na te denken of ik ze ook daadwerkelijk kan nakomen.' Voor de schaalconstructie werd het gemiddelde berekend op deze twaalf items (α = 0,74). Hieruit blijkt dat ongeveer 40 procent van de steekproef geen enkele vorm van disfunctionele impulsiviteit bij zichzelf vindt passen. Circa 5 procent rapporteert impulsief gedrag op ten minste de helft van deze items. Ruim 2 procent van de respondenten gaf op onvoldoende items antwoord om een schaalwaarde te kunnen berekenen. Aan hen is de gemiddelde waarde toegekend; daarnaast is een dummyvariabele aan het voorspellingsmodel toegevoegd die aangeeft of de waarneming een *missing value* had voor impulsiviteit. Zodoende kan worden nagegaan

of het risico op bedreiging voor deze respondenten afwijkt van degene die daadwerkelijk gemiddeld impulsief zijn.

Daderschap digitale criminaliteit
Om vast te stellen in hoeverre respondenten zelf digitale overtredingen hebben begaan, zijn hun twee vragen gesteld: 'Hebt u de afgelopen 12 maanden zelf met opzet een virus verspreid naar andere computers?' (ja/nee), en 'Hebt u de afgelopen 12 maanden een bericht naar iemand verstuurd via e-mail, chatbox of sms om die persoon bang te maken?' (ja/nee). Aan de hand daarvan is een dichotome maat samengesteld die aangeeft of de respondent één of beide van deze activiteiten heeft ondernomen. Een kleine procent gaf aan het afgelopen jaar een digitale overtreding te hebben begaan. Bijna 8 procent van de respondenten gaf geen antwoord op deze vragen. Om hen niet te verliezen voor de uiteindelijke analyses zijn zij geclassificeerd als niet-daders en is ook hier een dummyvariabele aan het model toegevoegd die aangeeft of de waarneming oorspronkelijk een *missing value* op daderschap had.

Tabel 1 biedt een overzicht van de *descriptives* van de besproken variabelen.

Methode
Om te voorspellen aan welke aspecten slachtofferschap van bedreiging gerelateerd is, gebruik ik multinomiale logit modellen. Hierbij worden drie typen slachtoffers onderscheiden: (a) slachtoffers van *alleen* traditionele bedreiging, (b) slachtoffers van *alleen* digitale bedreiging, en (c) slachtoffers van *zowel* digitale als traditionele bedreiging. Iedere afzonderlijke vorm van bedreiging wordt telkens vergeleken met de niet-slachtoffers, en van daaruit worden risicofactoren afgeleid.[3] De multinomiale modellen worden geschat via multilevel analyse omdat de data een geneste structuur hebben – individuen binnen huishoudens (Goldstein, 1995, 104-106).[4]

3 Vooral voor digitaal slachtofferschap is het aan te raden om de 'zuiver' digitale slachtoffers te onderscheiden van de slachtoffers die digitaal én traditioneel zijn bedreigd. Relatief veel slachtoffers van digitale bedreiging (circa 60 procent) vallen namelijk in deze tweede categorie. Indien dit onderscheid niet wordt aangebracht en er een algemene maat voor digitaal slachtofferschap zou worden aangemaakt, dan brengt dat het risico met zich mee dat bepaalde kenmerken als risicofactoren voor digitale bedreiging worden gezien, terwijl het in werkelijkheid vooral het risico op traditionele bedreiging beïnvloedt, of juist de mix van bedreigingen.

4 Zoals aangeraden door Rasbash e.a. (2004) zijn de multinomiale modellen geschat aan de hand van de *second order PQL*-variant.

Tabel 1: Descriptives van de afhankelijke en onafhankelijke variabelen

	Gemiddelde	Std. deviatie	Min.	Max.	N
Slachtofferschap bedreiging: totaal	0.07	0.26	0	1	6.835
Slachtofferschap bedreiging: alleen traditioneel	0.05	0.22	0	1	6.835
Slachtofferschap bedreiging: alleen digitaal	0.01	0.09	0	1	6.835
Slachtofferschap bedreiging: zowel trad. als dig.	0.01	0.12	0	1	6.835
Vrouw	0.54	0.50	0	1	6.896
Leeftijd	45.79	15.74	15	94	6.895
Opleidingsniveau	3.44	1.52	1	6	6.896
Partner aanwezig in huishouden	0.80	0.40	0	1	6.896
Huishoudensgrootte	2.79	1.31	1	9	6.896
Huishoudensinkomen (per maand, in € 1.000)	3.53	1.31	0	347	6.896
Stedelijkheid van woonomgeving	3.01	1.28	1	5	6.894
Restaurantbezoek	2.26	0.80	1	5	6.858
Cafébezoek	2.07	0.99	1	5	6.834
Vrienden bezoeken	3.03	1.06	1	5	6.814
Winkelen	3.12	1.10	1	5	6.820
Sportactiviteiten	3.13	1.73	1	5	6.693
# uur per week: werk/school	23.43	18.36	0	61	6.759
# uur per week: forenzen	3.24	4.10	0	21	6.759
# uur per week: e-mail	3.41	5.17	0	30	6.896
# uur per week: informatie opzoeken op internet	2.10	2.97	0	20	6.896
# uur per week: producten kopen via internet	0.38	0.65	0	4	6.896
# uur per week: chatten op internet	0.94	2.70	0	18	6.896
# uur per week: internetfora bezoeken	0.33	1.03	0	7	6.896
Profiel op Hyves	0.25	0.43	0	1	6.890
Gebruik van webcam	0.15	0.36	0	1	6.855
Disfunctionele impulsiviteit	1.18	0.16	0	10	6.735
Missing value impulsiviteit	0.02	0.27	0	1	6.896
Dader digitale criminaliteit	0.01	0.09	0	1	6.358
Missing value dader digitale criminaliteit	0.08	0.15	0	1	6.896

Resultaten

Tabel 2 geeft de ongestandaardiseerde coëfficiënten en odds ratio's weer van de multinomiale logit modellen voor de verschillende vormen van bedreiging – alleen traditioneel, alleen digitaal en zowel digitaal als traditioneel. De eerste groep slachtoffers is de grootste, circa 5 procent; de digitale groep is de kleinste,

circa 0,8 procent; en de 'mix'-groep zit daartussenin met 1,2 procent. In algemene zin kan worden vastgesteld dat de verschillende groepen deels verschillen in hun risicofactoren, maar toch ook voor een flink deel overlappen; dat verklaart ook waarom relatief veel slachtoffers van digitale bedreiging ook een traditionele bedreiging hebben meegemaakt.

Tabel 2: Multilevel multinomiale regressie van slachtofferschap bedreiging, op individuele en huishoudenskenmerken (ongestandaardiseerde coëfficiënten en odds ratio's), N=6.373

	Alleen traditioneel vs. geen slachtoffer		Alleen digitaal vs. geen slachtoffer		Mix traditioneel én digititaal vs. geen slachtoffer	
	B	**(OR)**	**B**	**(OR)**	**B**	**(OR)**
Constante	-3.11**		-5.87**		-4.86**	
Achtergrondkenmerken						
Vrouw	-0.11	(0.90)	-0.18	(0.84)	-0.07	(0.94)
Leeftijd	-0.02**	(0.98)	-0.06**	(0.94)	-0.04**	(0.96)
Opleidingsniveau	-0.04	(0.96)	-0.14	(0.87)	-0.13	(0.88)
Partner aanwezig in huishouden	-0.85**	(0.43)	-0.50	(0.60)	-1.17**	(0.31)
Huishoudensgrootte	0.15**	(1.17)	0.06	(1.06)	-0.06	(0.95)
Huishoudensinkomen (per maand, in € 1.000)	0.005	(1.01)	-0.007	(0.99)	0.004	(1.00)
Stedelijkheid van woonomgeving	0.12*	(0.89)	-0.06	(1.06)	-0.04	(1.04)
Buitenshuis routine activiteiten						
Restaurantbezoek	0.20**	(1.22)	-0.06	(0.94)	-0.00	(1.00)
Cafébezoek	0.04	(1.04)	0.06	(1.06)	-0.04	(0.96)
Vrienden bezoeken	-0.10	(0.90)	-0.25	(0.78)	0.15	(1.16)
Winkelen	0.01	(1.01)	0.33*	(1.40)	0.16	(1.18)
Sportactiviteiten	0.13**	(1.14)	0.15	(1.16)	0.05	(1.05)
# uur per week: werk/school	-0.004	(1.00)	0.004	(1.00)	-0.005	(1.00)
# uur per week: forenzen	0.03*	(1.03)	0.07*	(1.07)	0.02	(1.02)
Digitale routine activiteiten						
# uur per week: e-mail	-0.01	(0.99)	-0.05	(0.95)	0.01	(1.01)
# uur per week: informatie opzoeken op internet	0.05**	(1.05)	0.05	(1.05)	0.01	(1.01)
# uur per week: producten kopen via internet	0.06	(1.06)	0.28*	(1.33)	0.31**	(1.37)
# uur per week: chatten op internet	-0.11**[a]	(0.90)	0.03	(1.04)	0.02	(1.02)
# uur per week: internetfora bezoeken	0.03	(1.03)	0.09	(1.09)	0.20**	(1.22)
Profiel op Hyves	0.27*	(1.31)	1.06**	(2.90)	-0.42	(0.66)
Gebruik van webcam	0.22	(1.24)	0.64*	(1.90)	0.76**	(2.14)

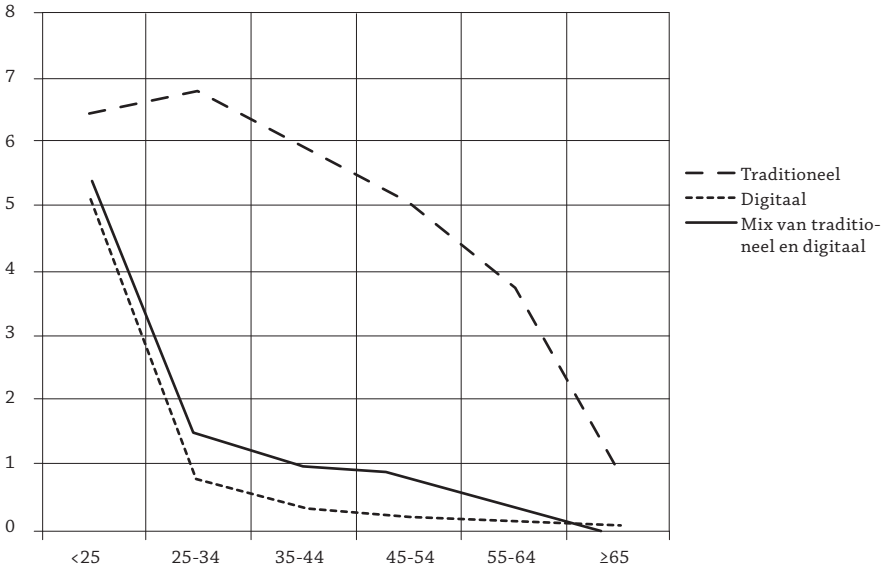
Tabel 2: (Vervolg)

	Alleen traditioneel vs. geen slachtoffer		Alleen digitaal vs. geen slachtoffer		Mix traditioneel én digititaal vs. geen slachtoffer	
	B	**(OR)**	**B**	**(OR)**	**B**	**(OR)**
Overig						
Disfunctionele impulsiviteit	0.13**	(1.14)	0.04	(1.04)	0.32**	(1.38)
Missing value impulsiviteit	-0.13	(0.88)	0.57	(1.76)	-0.62	(0.54)
Dader digitale criminaliteit	1.45**	(4.26)	2.44**	(11.43)	2.37**	(10.69)
Missing value dader digitale criminaliteit	0.10	(1.10)	1.10	(3.01)	-0.79	(0.46)

* p<.05, ** p<.01 (eenzijdig); [a] tweezijdig getoetst

Voor elke vorm van bedreiging geldt dat jongeren er vaker slachtoffer van worden. Wel wordt uit figuur 1 duidelijk dat de risico's het meest onder jongeren geconcentreerd zijn bij digitale bedreiging, zowel de 'zuiver' digitale variant als de mixvariant met traditionele bedreiging. Voor de groep jonger dan 25 jaar is het risico bij deze beide vormen ruim 5 procent; voor alle oudere leeftijdscategorieën is het risico daarentegen fors kleiner: 1 procent of minder. Bij traditionele bedreiging is de afname van het risico veel geleidelijker en zijn de risico's niet alleen relatief hoog voor jongeren, maar ook voor de groepen tussen 25 en 44 jaar: allen zo rond de 6 à 7 procent kans op slachtofferschap.

Figuur 1: Kans op verschillende vormen van slachtofferschap bedreiging (in %), naar leeftijdscategorie



Tabel 2 laat verder zien dat daders van *digitale* criminaliteit hogere risico's ondervinden op elk van de onderscheiden vormen van bedreiging. Voor zowel de digitale bedreiging als voor de mix van digitale en traditionele bedreiging lag dit wel in de lijn der verwachting, maar interessant is om te zien dat dit dus ook geldt voor traditionele bedreiging (hoewel dat effect wel significant minder sterk is). Deze bevindingen duiden er mogelijk op dat daders van digitale criminaliteit (van bedreiging en/of het verspreiden van virussen) met vergelding te maken kunnen krijgen en daardoor meer risico lopen om zelf bedreigd te worden – en dat kan digitaal, maar dus ook een traditionele bedreiging zijn.[5]

Wat betreft dagelijkse activiteiten blijkt dat zowel buitenshuis- als computeractiviteiten risicoverhogend zijn voor de drie verschillende vormen van bedreiging. Buitenshuisactiviteiten zijn met andere woorden niet alleen gerelateerd aan een grotere kans op traditionele bedreiging, maar interessant genoeg ook op digitale bedreiging. Zo zien we dat winkelen en forenzen gepaard gaan met een verhoogd risico op digitaal bedreigd worden. Andersom zien we ook dat computeractiviteiten niet alleen van belang zijn om te begrijpen wie digitaal (of gemengd) bedreigd wordt, maar ook wie traditioneel bedreigd wordt. Mensen die veel tijd besteden aan informatie zoeken op internet en die een Hyves-profiel hebben, worden eerder traditioneel bedreigd. Dit zijn indicaties dat sociale interacties die buitenshuis en via internet plaatsvinden, met elkaar verweven zijn. Verder verhoogt het gebruik van een webcam het risico op *zowel* digitale bedreiging als een mix van digitale en traditionele bedreiging, maar niet op een traditionele bedreiging. Ten slotte blijkt impulsiviteit het risico op traditionele bedreiging te verhogen, en met name op de kans om te maken te krijgen met een mix van digitale en traditionele bedreiging.

Tot slot biedt tabel 3 voor een aantal kenmerken inzicht in hoe zij samenhangen met concrete risico's op slachtofferschap van bedreiging, door de coëfficiënten uit tabel 2 door te rekenen.[6] Daaruit wordt bijvoorbeeld opnieuw duidelijk dat leden van eenpersoons- of eenouderhuishoudens meer risico lopen op traditionele bedreiging en de mix van digitale en traditionele bedreiging ten opzichte van mensen die deel uitmaken van een huishouden waarin twee partners samenleven. Ook blijken de risico's, afhankelijk van het concrete type bedreiging, hoger te zijn voor mensen met een Hyves-profiel en voor mensen die een webcam gebruiken. Forenzen beïnvloedt eveneens de risico's op bedreiging, gegeven de lagere kansen op bedreiging voor mensen die niet forenzen in vergelijking met degenen die in gemiddelde mate forenzen (3,2 uur per week). Daarnaast zien we dat mensen die niet (disfunctioneel) impulsief zijn, minder bedreigd worden dan degenen die dat

5 De dummyvariabele die aangeeft of de betreffende persoon ontbrekende informatie had op het gebied van daderschap, is in geen van de modellen significant. Dit duidt erop dat deze respondenten niet significant afwijken in hun risico op bedreiging van degenen die géén digitale dader zijn (en wiens waarde deze missing values toebedeeld kregen).

6 De overige kenmerken werden daarbij gecentreerd (voor ordinale, interval- en ratiovariabelen) of op de waarde 0 gehouden (voor dichotome variabelen). Dat betekent bijvoorbeeld dat bij het berekenen van de risico's voor het wel of niet hebben van een Hyves-profiel er onder andere uit wordt gegaan van een respondent van gemiddelde leeftijd, gemiddelde impulsiviteit, zonder gebruik van webcam, die geen dader van digitale criminaliteit is, enz.

Tabel 3: Voorspelde kansen op slachtofferschap van bedreiging voor uiteenlopende respondentkenmerken, uitgesplitst naar type bedreiging

	Traditioneel	Digitaal	Mix van traditioneel en digitaal
Partner in huishouden	2.6%	0.2%	0.2%
Geen partner	4.3%*	0.3%	0.8%*
Gemiddeld forenzen (3,2 u/week)	4.3%*	0.3%*	0.8%
Niet forenzen	3.9%	0.2%	0.7%
Hyves-profiel	5.5%*	0.8%*	0.5%
Geen Hyves-profiel	4.3%	0.3%	0.8%
Gebruik van webcam	5.3%	0.5%*	1.6%*
Geen gebruik van webcam	4.3%	0.3%	0.8%
Bovengemiddeld impulsief (80e per)	4.5%*	0.3%	0.9%*
Niet impulsief	3.7%	0.3%	0.5%
Dader digitale criminaliteit	16.0%*	3.1%*	7.7%*
Geen dader digitale criminaliteit	4.3%	0.3%	0.8%

* significant effect ($p<.05$)

in relatief hoge mate zijn. Tot slot zijn er duidelijke verschillen in risico's tussen daders en niet-daders van digitale criminaliteit. Voor elke vorm van bedreiging lopen daders een veelvoud van het risico in vergelijking met niet-daders. Wel gaat het hierbij om een relatief kleine groep in de steekproef (minder dan 1 procent).

Conclusie

Computers en internet hebben de mogelijkheden veranderd voor het plegen van criminaliteit. Niet alleen kunnen computers zelf het doelwit zijn van criminaliteit, maar bestaande vormen van criminaliteit kunnen op nieuwe manieren worden gepleegd, zoals oplichting, diefstal en bedreiging. Dit artikel concentreert zich op dit laatste facet van cybercriminaliteit – bedreiging via digitale hulpmiddelen, zoals e-mail. In het algemeen is er weinig bekend over criminaliteit die met behulp van computers wordt gepleegd (Van der Hulst & Neve, 2008), en digitale bedreiging vormt daarop geen uitzondering. In dit artikel is slachtofferschap van digitale bedreiging vergeleken met traditionele bedreiging, die bijvoorbeeld *face to face* of via een brief plaatsvindt. Op deze manier is bekeken wat risicofactoren van digitale bedreiging zijn en zijn deze vergeleken met traditionele bedreiging.
Een opvallende bevinding is dat – in tegenstelling tot de publieke beleving van het fenomeen – digitale bedreiging relatief weinig voorkomt: ruim 2 procent van de steekproef ontving het afgelopen jaar een bedreiging via e-mail, sms of chatsite. In vergelijking hiermee komen 'traditionele' bedreigingen (bijv. via brief of *face to face*) vaker voor: ruim 6 procent maakte dit het afgelopen jaar mee. De twee groepen slachtoffers zijn overigens deels overlappend: 1,3 procent van alle respondenten gaf aan *beide* vormen van bedreiging te hebben meegemaakt het afgelopen

jaar. Digitale bedreiging lijkt in zoverre dus niet een volstrekt nieuw fenomeen, omdat het voor een flink deel de mensen treft die ook traditioneel bedreigd worden; als zodanig is het deels te bestempelen als 'oude wijn in nieuwe zakken' (Grabosky, 2001). Met name onder jongeren is digitale bedreiging relatief veelvoorkomend; ruim 10 procent maakt het op jaarbasis mee. De helft van deze groep is 'puur' digitaal slachtoffer van het delict, dus niet in combinatie met traditionele bedreiging. Bij mensen ouder dan 25 jaar komen digitale bedreigingen maar zeer weinig voor.

De resultaten geven verder aanleiding om te stellen dat in de routineactiviteitentheorie – waarin slachtofferschap van criminaliteit als een resultaat wordt gezien van blootstelling aan daders via dagelijkse activiteiten – voortaan ook rekening moet worden gehouden met *computer*activiteiten, zowel voor het verklaren van traditionele als digitale criminaliteit. Sommige van deze activiteiten, zoals een internetprofiel op Hyves, blijken namelijk niet alleen van invloed op slachtofferschap van digitale bedreiging, maar ook op *traditionele* bedreiging. Daarnaast zijn het kopen van producten via internet en het gebruik van een webcam niet alleen risicoverhogend voor digitale bedreiging, maar ook voor het ontvangen van een mix van digitale en traditionele bedreigingen. Andersom blijken buitenshuisactiviteiten niet alleen het risico op traditionele bedreiging te verhogen, maar in sommige gevallen ook het risico op *digitale bedreiging*, zoals veel winkelen en forenzen. Wellicht verhogen dergelijke activiteiten de blootstelling aan of zichtbaarheid voor daders van bedreiging, en worden deze bedreigingen ook digitaal geuit. Deze resultaten tonen de verwevenheid aan tussen activiteiten buitenshuis en op internet (De Haan, 2008). Conflicten tussen mensen kunnen zowel via internet ontstaan als via traditionele communicatiemiddelen; en dat geldt ook voor de bedreigingen waarmee deze conflicten een vervolg kunnen krijgen. Toetsingen van de routineactiviteitentheorie moeten hier in het huidige digitale tijdperk daarom voortaan bij stilstaan. Ook deze bevindingen tonen aan dat digitale en traditionele bedreiging niet wezenlijk verschillen van elkaar: beide worden door activiteiten op internet en in de buitenwereld beïnvloed. Wel verschillen de specifieke risicoverhogende activiteiten voor de uiteenlopende vormen van bedreiging (zoals informatie opzoeken op internet voor traditionele bedreiging en *online* winkelen voor digitale bedreiging). Interessant voor vervolgonderzoek is dan ook om na te gaan of de internetactiviteiten van het doelwit ook de risico's voor andere traditionele delicten verhogen, zoals inbraak en mishandeling. En andersom, of buitenshuisactiviteiten ook andere digitale delicten beïnvloeden, zoals identiteitsfraude.

In de routineactiviteitentheorie is niet alleen blootstelling aan daders, maar ook de aanwezigheid van bescherming tegen daders (*guardianship*) van invloed op slachtofferschap. Ook in dit onderzoek bleken daar aanwijzingen voor, zowel voor traditionele bedreiging als voor de mix met digitale bedreiging. De resultaten lieten namelijk zien dat leden van huishoudens met twee partners, zoals tweeoudergezinnen of stellen zonder kinderen, minder vaak slachtoffer worden. Deze bevinding duidt er voor digitale bedreiging mogelijk op dat gezinsleden kunnen dienen als bescherming tegen situaties op internet die tot conflicten en bedreigingen leiden, bijvoorbeeld door advies te geven over verstandig *surf*-gedrag of het daad-

werkelijk controleren van computeractiviteiten van gezinsleden. Een andere mogelijkheid is dat de gezinscontext een bron van digitale daders kan zijn: leden van eenpersoonshuishoudens en eenoudergezinnen hebben wellicht vaker te maken met digitale bedreiging door een ex-partner (Southworth e.a., 2007). Om dat te achterhalen is het voor vervolgonderzoek nodig dat aan slachtoffers van bedreiging wordt gevraagd *door wie* zij bedreigd zijn, en wat de ernst en duur ervan was. Informatie daarover ontbrak voor dit onderzoek – en is een lacune in veel risicoanalyses omtrent slachtofferschap (zie bijv. ook Mustaine & Tewksbury, 1998). Ook de precieze manier waarop bedreigingen voortvloeien uit sociale interacties die op internet en buitenshuis plaatsvinden, zou aan nader onderzoek moeten worden onderworpen, bijvoorbeeld aan de hand van kleinschaliger kwalitatief onderzoek.

Verder blijkt dat de impulsiviteit van het doelwit een rol speelt bij de kans om slachtoffer te worden van bedreiging. Impulsiviteit is tot nog toe vooral gerelateerd aan daderschap (White e.a., 1994), maar omdat het samengaat met onvermogen om vooruit te plannen en een oriëntatie op bevrediging van kortetermijndoelen, ligt een verband met slachtofferschap óók voor de hand (Smith & Ecob, 2007). Impulsieve mensen worden hierbij gezien als makkelijk toegankelijke doelwitten, die minder investeren in het vermijden van ongewenste gevolgen via preventie en ook sneller verzeild raken in conflicten. In het huidige onderzoek bleken zij vaker zowel traditionele bedreigingen als een mix van digitale en traditionele bedreigingen mee te maken. Deze samenhang blijft overigens ook duidelijk aanwezig als rekening wordt gehouden met de verhoogde kans op daderschap (van digitale bedreiging en het verspreiden van virussen) onder impulsieve mensen en hun hogere mate van activiteit buitenshuis en op internet.

Het is interessant om het hier gehanteerde verklaringsmodel ook te gebruiken voor andere vormen van cybercriminaliteit, zoals slachtofferschap van digitale oplichting. Ook op het gebied van digitale bedreiging blijven er vragen openstaan, bijvoorbeeld omtrent het bestaan van eventuele voorwaardelijke invloeden op slachtofferschap. Hebben dagelijkse computeractiviteiten bijvoorbeeld voor impulsieve mensen een andere uitwerking op de kans om bedreigd te worden dan voor anderen? Andere bestaande onderzoeksvragen die op het gebied van cybercriminaliteit verder kunnen worden uitgewerkt, hebben betrekking op herhaald slachtofferschap (Ousey e.a., 2008) en aanpassing van dagelijkse (computer)activiteiten na slachtofferschap of uit angst daarvoor (Keane, 1998). Er is, kortom, volop werk aan de winkel op dit terrein.

Literatuur

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

CSI – Computer Security Institute (2007). CSI Survey 2007. *The 12th annual computer crime and security survey*. Ontleend aan www.gocsi.com.

Dickman, S.J. (1990). Functional and dysfunctional impulsivity. Personality and cognitive correlates. *Journal of Personality and Social Psychology, 58*, 95-102.

Felson, M. & Clarke, R.V. (1998). *Opportunity makes the thief. Practical theory for crime prevention*. London: Home Office.

Giblin, M.J. (2008). Examining personal security and avoidance measures in a 12-city sample. *Journal of Research in Crime and Delinquency, 45*, 359-379.

Goldstein, H. (1995). *Multilevel statistical models*. Geraadpleegd op 16 februari 2009 via www.cmm.bristol.ac.uk/team/HG_Personal/multbook1995.pdf.

Grabosky, P. (2001). Virtual criminality. Old wine in new bottles? *Social & Legal Studies, 10*, 243-249.

Haan, J. de (2008). Sociale contacten via digitale kanalen. In: P. Schnabel, R. Bijl & J. de Hart (red.). *Betrekkelijke betrokkenheid. Studies in sociale cohesie. Sociaal en Cultureel Rapport 2008*. Den Haag: SCP.

Hulst, R. van der & Neve, R. (2008). *High-tech crime. Soorten criminaliteit en hun daders. Een literatuurinventarisatie*. Den Haag: Boom Juridische uitgevers.

Junger, M. & Wittebrood, K. (1997). Daderschap, slachtofferschap en ongevallen. In: K. Wittebrood, J. Michon & M. ter Voert (red.). *Nederlanders over criminaliteit en rechtshandhaving*. Deventer: Gouda Quint, 33-44.

Keane, C. (1998). Evaluating the influence of fear of crime as an environmental mobility restrictor on women's routine activities. *Environment and Behavior, 30*, 60-74.

Killias, M. (2006). The opening and closing of breaches. A theory on crime waves, law creation and crime prevention. *European Journal of Criminology, 3*, 11-31.

Land, K.C., McCall, P. & Cohen, L.E. (1990). Structural covariates of homicide rates. Are there any invariances across time and social space? *American Journal of Sociology, 95*, 922-963.

Mustaine, E.E. & Tewksbury, R. (1998). Predicting risks of larceny theft victimization. A routine activity analysis using refined lifestyle measures. *Criminology, 36*, 829-857.

Ousey, G.C., Wilcox, P. & Brummel, S. (2008). Déjà vu all over again. Investigating temporal continuity of adolescent victimization. *Journal of Quantitative Criminology, 24*, 307-335.

Rasbash, J., Steele, F., Browne, W. & Prosser, B. (2004). *A user's guide to MLwiN. Version 2.0*. Bristol: Centre for Multilevel Modeling.

Schreck, C.J. (1999). Criminal victimization and low self-control. An extension and test of a general theory of crime. *Justice Quarterly, 16*, 633-654.

Schreck, C.J. & Fisher, B.S. (2004). Specifying the influence of family and peers on violent victimization. *Journal of Interpersonal Violence, 19*, 1021-1041.

Smith, D.J. & Ecob, R. (2007). An investigation into causal links between victimization and offending in adolescents. *British Journal of Sociology, 58*, 633-659.

Southworth, C., Finn, J., Dawson, S., Fraser, C. & Tucker, S. (2007). Intimate partner violence, technology, and stalking. *Violence against Women, 13*, 842-856.

White, J.L., Moffit, T.E., Caspi, A., Jeglum Bartusch, D., Needles, D.J. & Stouthamer-Loeber, M. (1994). Measuring impulsivity and examining its relationship to delinquency. *Journal of Abnormal Psychology, 103*, 192-205.

Wilsem, J. van (2003). *Crime and context. The impact of individual, neighborhood, city, and country characteristics on victimization*. Amsterdam: Thela Thesis.

Wittebrood, K. (2006). *Slachtoffers van criminaliteit. Een inleiding in de victimologie*. Den Haag: Boom Juridische uitgevers.

Wittebrood, K. & Wilsem, J. van. (2000). Jongeren en geweld. De relatie tussen slachtofferschap, daderschap en leefstijl. *Sociale Wetenschappen, 43*, 59-71.

Yar, M. (2005). The novelty of 'cybercrime'. An assessment in light of routine activity theory. *European Journal of Criminology, 2*, 407-427.