nscr

Nederlandse samenvatting van Understanding cybercriminal behaviour among young people

Results from a longitudinal network study among a relatively high-risk sample

Marleen Weulen Kranenbarg
Yaloe van der Toolen
Frank Weerman

Amsterdam, 2022

Nederlands Studiecentrum
Criminaliteit en Rechtshandhaving

VU VRIJE UNIVERSITEIT AMSTERDAM

Nederlandse samenvatting van

Understanding cybercriminal behaviour among young people

Results from a longitudinal network study among a relatively high-risk sample

Marleen Weulen Kranenbarg
Yaloe van der Toolen
Frank Weerman

January, 2022

Deze studie is gefinancierd door het Home Office van het Verenigd Koninkrijk met een onderzoekssubsidie van het National Cyber Security program

VU UNIVERSITY AMSTERDAM
nscr Netherlands Institute for the Study of Crime and Law Enforcement

Dit rapport kan worden geciteerd als:
Weulen Kranenbarg, M., Van der Toolen, Y., & Weerman, F. (2022). *Understanding cybercriminal behaviour among young people: Results from a longitudinal network study among a relatively high-risk sample.* Amsterdam: VU University Amsterdam/Netherlands Institute for the Study of Crime and Law Enforcement.

Het volledige Engelstalige rapport is te vinden via deze link.

Cybercrimineel gedrag onder jongeren nader bekeken: resultaten van een longitudinaal netwerkonderzoek onder een (relatief) hoog-risicogroep

Dit rapport heeft als doel om meer inzicht te krijgen in de verklaringen voor cyber-delinquent gedrag onder jongeren. We hebben onderzocht welke individuele- en omgevingsfactoren samenhangen met verschillende typen cybercrime. Hierbij focussen we specifiek op de rol van leeftijdsgenoten. Dit longitudinale onderzoek (3 meetmomenten) is uitgevoerd onder een grote steekproef van Nederlandse jongeren in het voortgezet onderwijs en mbo (leeftijd 12-25 jaar), die allen ICT onderwijs volgen (in de vorm van één of meerdere vakken of een heel programma/opleiding). Van deze leerlingen werd verwacht dat zij een hoger risico hadden op het plegen van cybercrime. Wij gebruikten vragenlijsten om informatie te verzamelen over zelf gerapporteerd daderschap en karakteristieken van zowel offline als online vrienden. We maakten hierbij onderscheid tussen cybercriminaliteit (delicten waarbij het gebruik van ICT noodzakelijk is) en gedigitaliseerde criminaliteit (delicten die zowel online als offline kunnen worden gepleegd) en vroegen ook naar traditioneel daderschap. Daarnaast zijn respondenten bevraagd over allerlei individuele- en omgevingsfactoren en verzamelden we gedetailleerde informatie over het sociale netwerk van schoolvrienden van de respondenten. Deze methoden (zie voor details Hoofdstuk 3) speelden in op diverse tekortkomingen van eerder onderzoek naar cyberdelinquentie (zie Hoofdstuk 2).

Een substantieel deel van de respondenten maakte zich schuldig aan ten minste één van de verschillende typen cyber- en gedigitaliseerde criminaliteit. De jongeren in ons onderzoek rapporteerden zelfs vaker cyberdelinquentie dan traditionele delinquentie (zie voor details Hoofdstuk 4). Van alle deelnemende jongeren gaf 45% (meetmoment 1) tot 51% (meetmoment 2) aan dat zij cybercriminaliteit hadden gepleegd en 35-39% dat zij gedigitaliseerde criminaliteit hadden gepleegd (in de 3 maanden voorafgaand aan het onderzoek). De meest voorkomende vormen van cybercriminaliteit waren hacken d.m.v. het raden van een wachtwoord (24-25%), het stelen/illegaal kopiëren van gegevens (22-23%), en het aanpassen of verwijderen van gegevens (17-19%). De meer technische vormen zoals hacken met technische middelen (11-12%) of exploits (12-16%), kwamen ook relatief veel voor in deze hoog-risico groep. De meest voorkomende vormen van gedigitaliseerde criminaliteit waren het online uitvechten van conflicten (22-33%) en online fraude (6-15%).

Cybercriminaliteit was vooral gerelateerd aan individuele factoren, terwijl gedigitaliseerde- en traditionele criminaliteit ook samenhingen met de omgevingsfactoren. De tabel geeft een overzicht van de factoren die statistisch significant samenhangen met de onderzochte typen criminaliteit (zie voor details over de betekenis van de factoren Hoofdstuk 3). Groene factoren hangen significant positief samen met een specifiek type criminaliteit, terwijl rode factoren significant negatief samenhangen. Oftewel, groene factoren zorgen voor een toename van de kans op criminaliteit, terwijl rode factoren zorgen voor een afname van die kans. De meeste resultaten waren in lijn met eerder onderzoek onder cybercriminelen. De bevinding dat lage zelfcontrole gerelateerd is aan zowel cyber- als gedigitaliseerde criminaliteit is niet in lijn met een aantal onderzoeken die suggereren dat hoge zelfcontrole nodig is voor de meer technisch geavanceerde vormen van cybercrime. Dit zou kunnen worden verklaard doordat onze groep respondenten al een relatief hoog niveau van ICT kennis hadden.

Cybercriminaliteit	Gedigitaliseerde criminaliteit	Traditionele criminaliteit
INDIVIDUAL FACTORS		
- Leeftijd	- Leeftijd	- Leeftijd
+ Lage zelfcontrole	+ Lage zelfcontrole	+ Lage zelfcontrole
+ Goede sociale vaardigheden	+ Goede sociale vaardigheden	+ Goede sociale vaardigheden
+ Computer verslaving	+ Computer verslaving	+ Computer verslaving
+ ICT kennis		- ICT kennis
+ Positief cybergedrag	+ Positief cybergedrag	+ Positief cybergedrag
ENVIRONMENTAL FACTORS		
		- Offline regels van ouders
	+ Alleen thuis zijn	
		- Online regels van school
	- Tevredenheid school	- Tevredenheid school
	+ Tevredenheid ICT onderwijs	+ Tevredenheid ICT onderwijs

Rood (-) = negatief significant effect; green (+) = positief significant effect.

Samenvattend suggereren de resultaten dat factoren die samenhangen met gedigitaliseerde criminaliteit sterker lijken op traditionele criminaliteit dan factoren die samenhangen met cybercriminaliteit. ICT kennis lijkt sterker van belang bij cybercriminaliteit dan bij gedigitaliseerde criminaliteit en veel gamen hangt daar ook enigszins mee samen. Daarentegen zijn omgevingsfactoren zoals alleen thuis zijn en tevredenheid met school niet gerelateerd aan cybercriminaliteit maar wel aan gedigitaliseerde criminaliteit. Dit suggereert dat het lastiger is om cybercriminaliteit via ouders en school aan te pakken. Details over de interpretatie van de individuele resultaten uit de tabel staan in Hoofdstuk 4.

Er was een verrassende overlap tussen cyberdelinquent gedrag en positief cybergedrag. Dit suggereert dat het niet zo makkelijk is om onderscheid te maken tussen "goede" en "slechte" jongeren. Ook bleken zowel beide typen cyberdelinquent gedrag alsook traditionele delinquentie samen te hangen met sterkere sociale vaardigheden. Hoewel het op het eerste gezicht vreemd is dat deze positieve eigenschappen samenhingen met daderschap, kan dit ook laten zien dat regelovertreding niet zo zwart-wit is als het lijkt. Leerlingen met sterke sociale vaardigheden zouden een onderliggende neiging kunnen hebben om meer actief te zijn online. Dit kan zowel resulteren in cyberdelinquentie als in online activiteiten waarmee ze anderen op een positieve manier helpen. Zowel positief als negatief cybergedrag kan uitdagingen bieden voor leerlingen die ICT onderwijs volgen. Deze bevinding impliceert dat interventies kunnen helpen om jongeren te laten kiezen voor de positieve alternatieven voor delinquentie (zie Hoofdstuk 4).

Respondenten onderschatten vaak de mate waarin hun schoolvrienden zich schuldig maken aan cybercrime. In ongeveer de helft van de gevallen waren leerlingen niet op de hoogte van het daadwerkelijke cyber delinquente gedrag van hun schoolvrienden (zie Hoofdstuk 5 voor details).

Percepties over de mate van cyberdelinquentie van vrienden waren sterker gerelateerd aan het eigen gedrag dan de daadwerkelijk zelf gerapporteerde delinquentie van vrienden. Dit suggereert dat jongeren de neiging hebben om hun cybergedrag aan te passen aan hoe zij *denken* dat hun vrienden zich gedragen, niet aan hoe hun vrienden zich *daadwerkelijk* gedragen. Het kan ook betekenen dat jongeren denken dat hun vrienden meer op hen lijken dan daadwerkelijk het geval is (zie voor details Hoofdstuk 5).

Percepties over cyberdelinquentie van *online* vrienden waren even sterk gerelateerd aan het eigen gedrag als deze percepties over *offline* vrienden. Aan de andere kant was deze relatie bij traditionele delinquentie wel sterker voor offline vrienden dan voor online vrienden (zie Hoofdstuk 5). Dit suggereert dat percepties over het gedrag van online vrienden relatief belangrijker zijn voor cyberdelinquentie dan voor traditionele delinquentie.

Er zijn geen duidelijke oorzaken gevonden voor veranderingen in cyberdelinquentie van jongeren op de korte termijn (in 6 maanden). Specifiek voor de rol van vrienden is er geen duidelijke aanwijzingen gevonden voor beïnvloeding door het daadwerkelijke gedrag van schoolvrienden. De netwerkanalyse liet zien dat cyberdelinquentie ook geen belangrijke factor was bij het maken van nieuwe schoolvrienden. Respondenten kozen hun vrienden eerder op basis van hun geslacht en algemene netwerk mechanismen (zoals het kiezen van vrienden van vrienden, of het kiezen van populaire leerlingen). Traditionele delinquentie bleek wel een mogelijke selectie factor te zijn in dit proces, maar cyberdelinquentie was dat niet (in ieder geval niet binnen scholen; zie voor meer details Hoofdstuk 6).

Onze resultaten kunnen bruikbaar zijn in het verder ontwikkelen van manieren om cyberdelinquentie tegen te gaan. Dergelijke initiatieven kunnen zich richten op de algemene populatie (primaire preventie), specifieke hoog-risico groepen (secundaire preventie) of op het verminderen van recidive van jongeren die al cyberdelicten plegen (tertiaire preventie). Initiatieven hebben mogelijk de meeste potentie wanneer deze zich richten op relatief hoog-risico groepen, zoals ICT leerlingen die relatief veel cyberdelinquentie rapporteren. Wat betreft specifiek cybercriminaliteit kunnen deze interventies zich vooral richten op individuele factoren zoals computerverslaving, aangezien er geen omgevingsfactoren met dit type delinquentie samenhingen in dit onderzoek. Gedigitaliseerde criminaliteit kan ook worden aangepakt via school of ouders. Interventies moeten wel worden aangepast op de specifieke behoeften van het individu, aangezien er verschillende typen daders kunnen worden geïdentificeerd en hun motivaties en vaardigheden sterk kunnen verschillen (zie Hoofdstuk 7).

Scholen kunnen vroeg in de criminele carrière ingrijpen. Algemene maatregelen om tevredenheid met school te verbeteren kunnen gedigitaliseerde delinquentie laten afnemen. Meer specifiek kunnen scholen daarnaast vroege signalen van potentiële cyberdelinquentie oppikken en maatregelen ontwikkelen om hier snel op te reageren. Daarnaast zal enkel regels opstellen op dit gebied wellicht niet voldoende impact hebben, maar scholen hebben wel de mogelijkheid om positief cybergedrag extra te stimuleren. De gevonden overlap tussen positief en negatief cybergedrag suggereert dat scholen les kunnen geven in het onderscheid tussen “goed” en “slecht” cybergedrag en hun leerlingen stimuleren het positieve alternatief te kiezen (zie Hoofdstuk 7).

Ouders kunnen vooral een rol spelen in de preventie van gedigitaliseerde criminaliteit. Het stellen van meer regels over online gedrag en het verminderen van de tijd die jongeren alleen thuis zijn kunnen gedigitaliseerde delinquentie verminderen. Scholen kunnen het bewustzijn van ouders vergroten en hen helpen met preventieprogramma's en suggesties geven voor online toezicht op kinderen en het maken van regels over online gedrag (zie Hoofdstuk 7).

Preventie en interventie maatregelen moeten zich niet alleen richten op schoolvrienden (en percepties over hun gedrag), maar ook op andere typen vrienden (en percepties over hun gedrag). Anders dan voor traditionele delinquentie, blijken percepties over het gedrag van verschillende vrienden (offline én online) belangrijk (zie Hoofdstuk 7). Als jongeren denken of zien dat hun vrienden cyberdelinquent gedrag vertonen, is het belangrijk dat ze zich tegen groepsprocessen kunnen weren en cyber delinquente leeftijdsgenoten niet zien als rolmodel.

Ons onderzoek heeft beperkingen die van belang zijn bij de interpretatie van de resultaten. Ten eerste zijn de resultaten wellicht niet generaliseerbaar naar jongeren in deze leeftijdscategorie in het algemeen, aangezien ons onderzoek zich specifiek richt op Nederlandse jongeren met een relatief hoog risico op cybercrime. Ten tweede hebben we geen onderscheid gemaakt tussen ernstige en minder ernstige vormen van cybercrime; we hebben enkel onderscheid gemaakt tussen de twee algemene categorieën die vaker in onderzoek worden gebruikt (cyber en gedigitaliseerd). Ten derde konden wij slechts een selectie van de meest belangrijke individuele- en omgevingsfactoren meenemen in het onderzoek. Andere factoren die niet zijn onderzocht kunnen ook samenhangen met cybercrime. Ten vierde zijn de metingen over het daadwerkelijke gedrag van vrienden beperkt tot schoolvrienden, waardoor we verschillen tussen percepties en daadwerkelijk gedrag niet konden onderzoeken voor andere offline vrienden en online vrienden. Voor meer details en suggesties om hiermee om te gaan in toekomstig onderzoek zie Hoofdstuk 7.

In het kort suggereren onze resultaten dat preventiemaatregelen verschillende factoren moeten aanpakken en daarbij onderscheid moeten maken tussen specifieke groepen daders en hun behoeften. Scholen en ouders kunnen (naast formele interventies van bijvoorbeeld politie en reclassering) een belangrijke rol spelen in het voorkomen van negatief cybergedrag en het stimuleren van positief cybergedrag (zie Hoofdstuk 7).