Jeugdige daders van cybercrime in Nederland: Een empirische verkenning

Samenvatting

Sven Zebel[1]
Peter de Vries[1]
Ellen Giebels[1]
Margôt Kuttschreuter[1]
Wouter Stol[2]

[1] Universiteit Twente, vakgroep Psychologie van Conflict, Risico en Veiligheid (PCRV)
[2] Noordelijke Hogeschool Leeuwarden, Lectoraat Cybersafety / Politieacademie / Open Universiteit

Dit onderzoek is uitgevoerd in opdracht van het WODC, afdeling Extern Wetenschappelijke Betrekkingen, ministerie van Veiligheid en Justitie.

UNIVERSITEIT TWENTE.

NHL Hogeschool / Politieacademie / Open Universiteit

Het gebruik van Informatie- en Communicatie Technologie (ICT) heeft onder jongeren een grote vlucht genomen. Het wijdverbreide gebruik van ICT maakt echter dat ICT toepassingen ook in toenemende mate een rol kunnen spelen bij illegale en strafbare activiteiten waar jongeren mee te maken kunnen krijgen, hetzij als doelwit (slachtoffer), hetzij als daders van delicten.

Het is in verband met beleidskeuzes van de Directie Justitieel Jeugdbeleid van het Ministerie van Veiligheid en Justitie belangrijk om zo goed mogelijk zicht te krijgen op de rol van minderjarigen bij cybercriminaliteit in ruime zin (waarbij ICT als middel wordt gebruikt bij criminaliteit) en in enge zin (waarbij de ICT-structuur zelf het doel is van crimineel handelen), en hun onderlinge relatie. Wanneer blijkt dat cybercriminaliteit vooral gekarakteriseerd kan worden als traditionele jeugdcriminaliteit met nieuwe middelen, dan vergt dat andere beleidskeuzes dan wanneer blijkt dat cybercrime in enge zin in opkomst is met daders die qua kenmerken, motieven en werkwijze afwijken van “klassieke” jeugddaders (zie ook Yar, 2012).

Het doel van dit onderzoek is dan ook het in kaart brengen van de vormen en mate van cybercriminaliteit in Nederland waarbij jongeren tot 18 jaar betrokken zijn als daders, en het inzicht bieden in de achtergronden van deze criminaliteit.

Verschillende auteurs merken op dat er nog (zeer) weinig empirisch wetenschappelijk onderzoek naar daders van cybercriminaliteit is verricht (bijvoorbeeld Holt, Bossler & May, 2012; Van der Hulst & Neve, 2008; Leukfeldt, Veenstra & Stol, 2013). Om die reden zal in het onderhavige onderzoek de nadruk liggen op het formuleren van empirisch onderbouwde antwoorden op de onderzoeksvragen. De volgende onderzoeksvragen staan centraal:

1. In welke mate zijn jongeren tot 18 jaar als dader betrokken bij (verschillende vormen van) cybercriminaliteit in enge en ruime zin gepleegd in Nederland?
2. In welke mate en in welke zin doen zich combinaties voor van cybercriminaliteit in enge en ruime zin in Nederland door jeugdige daders tot 18 jaar?
3. Welk profiel hebben jongeren die cybercriminaliteit in enge en ruime zin plegen?
4. Welke modus operandi worden gehanteerd bij de verschillende vormen van cybercriminaliteit waar jongeren bij betrokken zijn als dader?
5. Op welke wijze raken jongeren betrokken bij cybercriminaliteit in enge en ruime zin?
6. Op welke wijze kijken jongeren zelf tegen cybercriminaliteit in enge en ruime zin aan?
7. Zijn er specifieke risico’s die volgen uit het digitale gedrag van jongeren en hun mogelijke betrokkenheid als daders van cybercriminaliteit?

Voor het beantwoorden van de onderzoeksvragen werd een brede mix van kwantitatieve en kwalitatieve methoden ingezet op verschillende informatiebronnen: de Monitor Zelfgerapporteerde Jeugdcriminaliteit van het WODC en het onderzoek “Jongeren en Cybersafety” van Kerstens en Stol (2012) – beiden zelfrapportagestudies-, de Onderzoek- en Beleidsdatabase Justitiële Documentatie (OBJD) van het WODC, de uitspraken die te vinden zijn op Rechtspraak.nl, en een serie interviews met deskundigen en betrokkenen. Tussen de bronnen is slechts in beperkte mate sprake van overlap. Zo geven ze niet allen antwoord op alle onderzoeksvragen, en ook is er variatie in de specifieke cyberdelicten die in de bronnen terug te vinden zijn.

De resultaten van het onderzoek gaven aanleiding tot het formuleren van een aantal stellingen. Deze worden hieronder weergegeven en toegelicht. We sluiten af met een beschouwing van de risico’s die

voortvloeien uit het digitale gedrag van jongeren. Aanbevelingen op basis van dit onderzoek voor beleid, en de richting en methodologie van vervolgonderzoek bevinden zich in het slothoofdstuk van het rapport.

"Jongeren zijn in geringe mate betrokken bij cybercriminaliteit"

Het beeld dat in de media wordt geschetst van een groot, groeiend probleem van jongeren die cybercriminaliteit plegen, zagen wij niet bevestigd in het huidige onderzoek. Uit de zelfrapportagestudies en geregistreerde cybercriminaliteit onder jongeren komt naar voren dat het merendeel van de onderzochte cyberdelicten in de periode 2006-2011 in (zeer) geringe mate worden gerapporteerd (minder dan 5,5 % van alle ondervraagde jongeren in de steekproeven) of staan geregistreerd onder minderjarigen (0,3 % van alle geregistreerde jeugdcriminaliteit in Nederland). Het gaat dan om de cyberdelicten online veilingfraude, een virus verspreiden, hacken, het maken of verspreiden van seksueel beeldmateriaal, vervalsing van pinpas of waardekaart en online bedreiging.

De kwalificering 'in geringe mate' die wij verbinden aan deze percentages behoeft misschien enige uitleg. Als wij het percentage van 5,4 % dat hoort bij online bedreiging als uitgangspunt nemen, dan impliceert dat dat op een gemiddelde middelbare school van 800 leerlingen 43 leerlingen zullen aangeven dit cyberdelict gepleegd te hebben in het afgelopen jaar. Dat zijn bijna twee klassen vol van 25 leerlingen. Echter, het impliceert ook dat een overgrote meerderheid van 757 leerlingen op deze school zullen aangeven dit delict niet gepleegd te hebben. Met andere woorden, bijna 95 % geeft aan het voorgaande jaar niemand online te hebben bedreigd. Dit laatste is de reden dat wij deze bevindingen interpreteren als een 'geringe mate' van betrokkenheid van jongeren bij cybercrime. Overigens werden de andere cyberdelicten hierboven door 3,1 % of minder van de jongeren gerapporteerd, of maakten deze minder dan 0,3 % uit van de geregistreerde jeugdcriminaliteit in Nederland.

Drie andere strafbare cybergedragingen die vaker werden gerapporteerd door jongeren in het huidige onderzoek betroffen virtuele diefstal, het illegaal downloaden en/of delen van software en muziek, en cyberpesten. Er zijn echter duidelijke verklaringen voor deze hogere percentages. Niet alle acties die hieronder vallen zijn strafbaar in Nederland (bijvoorbeeld illegaal downloaden van muziek en roddelen als onderdeel van cyberpesten); jongeren zelf zien deze gedragingen dan ook niet als criminaliteit (zie Kerstens & Stol, 2012; Moon, McClusky, McClusky, & Lee, 2012). Dat virtuele diefstal strafbaar is blijkt onder jongeren nagenoeg onbekend (Jansen, 2012).

Kunnen we deze uitkomsten nu interpreteren als een betrouwbaar beeld van de geringe betrokkenheid van jongeren bij cybercriminaliteit in Nederland? Dat is een belangrijke en tegelijk lastige vraag. Enerzijds moet er in relatie tot het beeld van de geregistreerde cybercriminaliteit in de justitiële data in dit onderzoek worden opgemerkt dat deze data vrijwel zeker onvolledig zijn. Recent onderzoek van Leukfeldt, Veenstra, Domenie en Stol (2013) laat namelijk zien dat er zich belangrijke knelpunten voordoen in de doorstroom van cybercrime-zaken in de strafrechtketen in Nederland.

Echter, de zelfrapportagestudies in dit onderzoek kennen deze doorstroom problemen niet; jongeren wordt immers direct gevraagd welke strafbare gedragingen zij hebben gepleegd in de afgelopen periode. De anonimiteit van de gegeven antwoorden wordt daarbij gegarandeerd. Deze studies kennen uiteraard weer andere beperkingen (zie hoofdstuk methoden van onderzoek in dit rapport). De belangrijkste beperking van het zelfrapportage- onderzoek van Kerstens en Stol (2012) is dat de

steekproef van jongeren niet representatief is voor de populatie van Nederlandse jongeren. De bevindingen in het zelfrapportage-onderzoek van Van der Broek, Weijters en van der Laan (2013) kunnen echter wel representatief genoemd worden voor Nederlandse jongeren; en ook in deze studie waren de percentages zelfgerapporteerde cybercriminaliteit laag. Kortom, de beperkingen van de zelf-rapportagestudies in ogenschouw genomen, kunnen we daarom meer vertrouwen hebben in het beeld dat deze opleveren over de betrokkenheid van jongeren bij cybercriminaliteit in Nederland. En die is, zoals hierboven uiteengezet, gering.

"Als jongeren cybercriminaliteit plegen, betreft dat vaak één specifiek type cyberdelict"

Combinaties van verschillende vormen van cybercriminaliteit (in enge en ruime zin) onder jongeren doen zich volgens dit onderzoek zelden voor. Zo kwam uit het zelfrapportage onderzoek naar voren dat online bedreigen door jongeren (cybercrime in ruime zin: ICT als ondersteuning voor het plegen van criminaliteit) en virussen verspreiden (cybercrime in enge zin: de ICT structuur zelf is het doel van het strafbare gedrag) grotendeels door verschillende jongeren worden gepleegd; in de geregistreerde cybercriminaliteit bleek dat er in een grote meerderheid van alle cyberstrafzaken met jeugdige verdachten slechts één vorm van cybercriminaliteit werd aangetroffen (i.e. 1 wetsartikel). Ook de uitspraken op Rechtspraak.nl en de interviews geven geen aanleiding voor concrete conclusies over jongeren die combinaties van cybercrime in enge en in ruime zin plegen.

"Jeugdige cyberdaders vertonen voor een groot deel alledaagse kenmerken"

Voor een groot deel vertoonden (het geringe aantal) jongeren die cybercriminaliteit pleegden kenmerken die niet afwijken van alledaagse jeugdige delinquenten. De kenmerken sekse en leeftijd speelden hun gebruikelijke rol: jongens plegen vaker online bedreiging, veilingfraude, en virtuele diefstal, en produceren en verspreiden vaker seksueel beeldmateriaal dan meisjes, en de mate waarin cybercriminaliteit wordt gepleegd neemt toe tussen het 12^{e} en 17^{e} levensjaar. Het enige onderzochte cyberdelict dat hierop een uitzondering vormde was cyberpesten: dat rapporteren meisjes even vaak als jongens (zie Kerstens & Stol, 2012; p. 95). Het plegen van cyberdelicten werd ook voorspeld door slachtofferschap: jongeren die eerder het doelwit waren van cyberpesten, veilingfraude, virtuele diefstal en vervelende seksuele vragen en/of verzoeken, rapporteerden ook vaker dader te zijn van dergelijk cybercrimineel gedrag. Bij offline criminaliteit onder jongeren wordt deze relatie ook geconstateerd (zie Wittebrood & Van Wilsem, 2000). Jongeren hebben ook bekende motieven om over te gaan tot cybercriminaliteit: virtuele diefstal en cyberpesten worden gepleegd voor de lol, om terug te pesten (in het geval van cyberpesten), of wraak te nemen, of vanuit financieel motief (in het geval van virtuele diefstal) (Kerstens & Stol, 2012).

Is er dan niets wat jeugdige cyberdaders onderscheidt? Toch wel. In de inleiding wordt de psychologische "ontremming" besproken die plaats kan vinden als jongeren zich in cyberspace begeven (Suler, 2004). Deze online disinhibitie blijkt van grote betekenis voor het plegen van cybercriminaliteit: jongeren die zich online ongeremder voelen, en gemakkelijk persoonlijke informatie durven vrij te geven op internet rapporteren ook vaker daders te zijn van veilingfraude, virtuele diefstal, cyberpesten en het maken en verspreiden van seksueel beeldmateriaal. De invloed van deze disinhibitie blijft van kracht zelfs wanneer voor de invloed van allerlei andere, traditionele factoren is gecontroleerd (zie Kerstens & Stol, 2012).

Opvallend aan bovenstaande profielschets is dat deze uitsluitend betrekking heeft op jongeren die cybercrime in ruime zin pleegden. Het profileren van jongeren die cybercriminaliteit in enge zin pleegden bleek lastiger in dit onderzoek. Echter, de geregistreerde cybercriminaliteit in de justitiële data (OBJD van het WODC) bood, ondanks dat deze data onvolledig zijn, wel enig zicht op het profiel van jeugdige verdachten van cybercriminaliteit in enge zin (n = 106), alsmede van cybercriminaliteit in ruime zin (n = 166). Bovendien kon dat profiel vergeleken worden met het profiel van jeugdige verdachten in de algehele populatie in Nederland. Uit die bron kwam naar voren dat jeugdige verdachten van cybercriminaliteit in enge (en ruime) zin vaker in Nederland zijn geboren dan in de algehele populatie; bij cybercriminaliteit in enge zin was zelfs geen enkele verdachte elders geboren. Daarnaast onderscheiden jeugdige cyberverdachten zich qua criminele carrière: een groter deel is *first offender* en een veel groter deel blijft na de strafzaak op het rechte pad dan in de algehele populatie van jeugdige verdachten in Nederland. We moeten voorzichtig zijn met het trekken van harde conclusies op basis van deze data, maar bovenstaand profiel roept op zijn minst de vraag op of we bij jongeren die cybercriminaliteit in enge zin ten laste is gelegd in Nederland te maken hebben met een specifiekere, homogenere groep daders dan bij andere vormen van jeugdcriminaliteit?

"Weinig zicht op de modus operandi bij cybercriminaliteit in enge zin onder jongeren"

Opvallend is dat slechts bij een aantal vormen van cybercriminaliteit in ruime zin meer zicht komt op de modus operandi; de "MO" van jongeren die cybercriminaliteit in enge zin plegen blijft onbelicht. Cyberpesten wordt volgens Kerstens en Stol (2012) vaak samen met anderen gedaan, en in het merendeel zijn de slachtoffers bekenden van de dader. Bij virtuele diefstal geeft iets minder dan de helft aan het slachtoffer te kennen; vaak gaat het om bekenden, vrienden/vriendinnen uit de buurt of van school, en/of familieleden.

Een veel gebruikte techniek voor virtuele diefstal is social engineering: het overhalen van het slachtoffer om iets te doen dat hij normaal gesproken niet zou doen. Daders zetten "phishing" in, proberen een scam uit of vragen simpelweg het wachtwoord van slachtoffers om virtueel te kunnen stelen. Naast deze vormen van social engineering wordt ook getracht het wachtwoord af te kijken, of te hacken om te kunnen stelen.

Uit de uitspraken op Rechtspraak.nl komt naar voren hoe online bedreiging in zijn werk gaat: bedreigingen worden geuit via Twitter, Facebook, GSM of chat; er kan worden gedreigd richting het slachtoffer met mishandeling, de dood, zedenmisdrijven, of met het online zetten van kwetsend (beeld)materiaal over het slachtoffer.

Tot slot valt in de interviews enige steun te vinden voor het bestaan van twee typen jeugdige hackers zoals uiteengezet wordt in de inleiding. Er zijn jongeren die nog weinig kennis en vaardigheden bezitten, informatie krijgen van anderen over hoe te hacken, en daarmee gaan uitproberen, voor de kick (de "*novices"* of "*newbies"* uit het schema van Van der Hulst & Neve, 2008). Daarnaast zijn er de "nerds", die al behoorlijke kennis hebben en vanuit hun hobby gaan experimenteren op het internet; zij kunnen deze kennis later ook delen met andere jongeren, waardoor ze ook status verwerven in de offline wereld. Deze laatste groep lijken op de "*virus writers*" of "*coders*" die worden genoemd in de inleiding.

"Experimenteren, anonimiteit en het verwerven van aanzien als oorzaken?"

Over de ontstaanswijze van cybercriminaliteit onder jongeren kon alleen op basis van de interviews uitspraken gedaan worden; daarbij moet in ogenschouw worden genomen dat de geïnterviewden aangaven in beperkte mate ervaringen te hebben met jongeren die cybercriminaliteit plegen. Bij de vragen over de ontstaanswijze van cybercriminaliteit onder jongeren baseerden de geïnterviewden zich daardoor vooral op indirecte informatie, indrukken, en het algemene beeld van daders.

Meerdere geïnterviewden geven aan dat jongeren betrokken kunnen raken als dader bij vormen van cybercriminaliteit (hacken, identiteitsdiefstal en smaad of laster via het internet) door een combinatie van experimenteren en anonimiteit, vanuit de veilige thuisomgeving. Voor jongeren die in de offline wereld minder sociaal vaardig of populair zijn is cybercriminaliteit ook een manier om aanzien te verwerven. Omdat de pakkans relatief klein is, en de opsporingsdiensten alle nieuwe ontwikkelingen lastig kunnen bijbenen (iets wat de jongeren ook weten), kunnen ze daarbij steeds een stapje verder gaan.

Geïnterviewden uit de IT- en opsporingssector geven aan dat technische kennis geen grote rol hoeft te spelen binnen de cybercriminaliteit in enge zin, maar interesse wel. Een geïnterviewde uit de IT sector geeft aan dat cybercriminaliteit in enge zin wel begint bij de "nerds"; analoog daaraan stelt een geïnterviewde uit de wetenschap dat cybercriminaliteit in enge zin ontstaat door het uitproberen van de kennis die de dader al heeft. Dit is in lijn met een recente Chinese studie op basis van interviews met Chinese hackers met als conclusie dat het juist de getalenteerde studenten zijn die uiteindelijk gaan hacken. De onderzoekers schrijven dit enerzijds toe aan identificatie met gelijkgestemden in combinatie met beperkte controle en anderzijds aan een beperkte morele ontwikkeling (Xu, Hu & Zhang, 2013). Overigens suggereert dit onderzoek dat er ook een positief verband kan zijn tussen bepaalde vormen van cybercriminaliteit en opleidingsniveau.

Verder wordt door meerdere bronnen de rol van de media genoemd: Cybercriminaliteit wordt door de media soms ook nog positief belicht waardoor jongeren sneller geneigd zijn om mee te doen.

"Jongeren neutraliseren, bagatelliseren of vertonen kenmerken van disinhibitie als ze over het plegen van cybercriminaliteit spreken"

Op basis van twee van de vijf bronnen (de interviews en Kerstens & Stol, 2012) kwam informatie naar voren over de zienswijze van jongeren ten aanzien van cybercriminaliteit in ruime en enge zin. We observeerden drie terugkerende aspecten. Ten eerste maken jongeren gebruik van neutralisaties als ze over cybercriminaliteit praten: bijvoorbeeld "iedereen doet het" of "het hoort erbij" bij virtuele diefstal, of "misstanden aan het licht brengen" als motief om te hacken. Ten tweede bagatelliseren jongeren de criminele aspecten van cybercrime: ze denken of weten niet dat iets strafbaar is, of denken dat er geen opsporing plaats vindt (lage pakkans). Ten slotte vinden we in dit onderzoek aanwijzingen voor de rol van disinhibitie als jongeren online gaan: reacties van anderen op internet zijn vaak asynchroon en uitgesteld, waardoor jongeren het idee krijgen dat criminele acties geen schadelijke gevolgen hebben online. Daarnaast komt uit de interviews naar voren dat jongeren bijvoorbeeld online een andere naam aannemen, waardoor zij dissociatie gaan ervaren: de criminele acties die zij uitvoeren zijn niet die van henzelf, het is een spel (zie ook Suler, 2004).

"Risico's van het digitale gedrag van jongeren: Disinhibitie, seksueel gedrag en de opkomst van criminele dienstverlening op het internet"

Met de komst van internet lijkt het gemakkelijker te zijn geworden om criminaliteit te plegen. In de inleiding wordt melding gemaakt van een aantal aspecten waardoor daders hun gedrag en de consequenties daarvan gemakkelijker kunnen negeren of goedpraten: neutralisaties, bagatelliseren, disinhibitie, en dissociatie (zie ook Suler, 2004). In lijn hiermee is in de zelfrapportagestudies gevonden dat uitspraken als "iedereen doet het" of "het hoort erbij" vaak worden opgetekend als daders gevraagd wordt naar hun motieven, en geven de deskundigen in de interviews aan dat daders vaak verrast zijn als ze worden opgepakt en beweren geen kwaad in de zin te hebben gehad. Zoals eerder uiteengezet blijkt de mate waarin men zich ongeremder voelt online en daar makkelijker persoonlijke informatie vrijgeeft een robuuste voorspeller voor meerdere vormen van cybercriminaliteit. Het lijkt er daardoor sterk op dat antisociale en criminele acties en handelingen die online worden ondernomen vaak anders worden beleefd door jongeren dan vergelijkbare acties offline. Denk hierbij bijvoorbeeld aan het feit dat jongeren zich niet bewust zijn van de strafbaarheid van virtuele diefstal (Jansen, 2012). Dit alles in ogenschouw nemend, lijkt de grens tussen legaal en illegaal gedrag online voor jongeren minder scherp en duidelijk te zijn dan tussen legaal en illegaal gedrag offline. In deze zin kent het gedrag van jongeren online dus een duidelijk risico, ondanks het feit dat de betrokkenheid van jongeren bij cybercriminaliteit tot nu toe gering kan worden genoemd.

Een tweede risico betreft de manier waarop seksuele handelingen van jongeren online gelabeld worden. Leukfeldt, Domenie en Stol (2010) constateerden dat bijna een tiende van de verdachten van kinderpornografie in hun onderzoek jonger was dan 18 jaar; zij stelden dat dit enerzijds een gevolg zou kunnen zijn van technische middelen die het gemakkelijker maken crimineel gedrag ten uitvoer te brengen, waardoor de prevalentie wordt verhoogd. Anderzijds echter, zou het volgens hen ook een nieuwe uiting kunnen zijn van een oud verschijnsel, dat jongeren de neiging hebben (en altijd hebben gehad) te experimenteren met hun seksualiteit. De vraag die dit laatste oproept is hoe politie en justitie hiermee om zouden moeten gaan. Indien het daadwerkelijk gaat om een nieuwe uiting van normaal gedrag, zou ze deze zaken vaak moeten negeren? Of moet dit als delict aangemerkt blijven en moeten de daders ervoor vervolgd worden?

Eén van de geïnterviewden bij het OM wees erop dat er op dit punt sprake is van een gewijzigde beleidslijn. Het verspreiden van seksueel beeldmateriaal door minderjarige daders en met dito slachtoffers werd aanvankelijk vervolgd als het "maken en verspreiden van kinderporno". Dat bleek echter erg zware gevolgen voor de minderjarige dader te hebben; deze werd na veroordeling namelijk aangemerkt als dader van een zedendelict. Daarom is men ertoe overgegaan onderscheid te maken tussen zware gevallen, waarbij sprake is van bijv. dwang, en gevallen waarbij sprake van vrijwilligheid. Deze laatste categorie wordt nu behandeld als smaad, een heel ander delict met veel minder zware gevolgen voor jeugdige betrokkenen.

De bevindingen met betrekking tot het produceren en verspreiden van seksueel beeldmateriaal in dit onderzoek wijken enigszins af van die van Leukfeldt en collega's (2010). Voor zover harde gegevens beschikbaar waren, leken ze te wijzen in een de richting van een veel kleiner aantal daders van deze vorm van cybercriminaliteit. Dit lijkt de mogelijkheid die Leukfeldt en collega's ter berde brengt, dat het wellicht om een vorm van experimenteergedrag gaat, enigszins te nuanceren. Anderzijds dient te worden aangemerkt dat bij de gegevens in dit onderzoek wellicht sprake is geweest van sociaal

wenselijke zelfrapportages (wellicht in versterkte zin bij dit onderwerp), en daardoor mogelijkerwijs tot onderrapportage van dit gedrag.

Tot slot geeft één van de OM-medewerkers in de interviews als derde risico aan te verwachten een toename te zullen zien in specifiek cybercriminaliteit in enge zin onder jongeren. De “criminele dienstverleningsindustrie” en het ICT-kennisniveau onder jongeren zal volgens hem blijven toenemen, terwijl er zeer veel geld mee te verdienen zal zijn; dit zal ertoe leiden dat “economisch gedreven” criminaliteit in enge zin zal stijgen. Verder geeft hij aan dat misdaadsyndicaten in de offline wereld zich steeds verder online aan het ontwikkelen zijn, zoals te zien is in de online handel in verdovende middelen en wapens. Voor deze activiteiten is er behoefte aan mensen met ICT-vaardigheden, en dus komen cybercriminelen wellicht ook bij jongeren terecht. Het verwerven van status en respect is voor veel jongeren een belangrijk motief om bijvoorbeeld te hacken, en zij zullen hun prestaties ook graag delen met anderen op webfora. Dat verschaft cybercriminelen de mogelijkheid om relatief gemakkelijk met hen in contact te treden.