Een alternatief voor jeugdige hackers? Plan- en procesevaluatie van Hack_Right (2021)
J.A.M. Schiks, M.S. van 't Hoff-de Goede, E.R. Leukfeldt (NSCR i.s.m. Haagse Hogeschool)
Politiewetenschap 121

Thema: 1.2 Cybercrime

Doelstelling
Het onderzoek heeft tot doel om de interventie Hack_Right en de tot nu toe uitgevoerde trajecten te evalueren. Omdat Hack_Right pas relatief kort loopt en aan het einde van de dataverzamelingsperiode van dit onderzoek veertien casussen waren afgerond, was het nog te vroeg voor een effectevaluatie. Wel is er een plan- en procesevaluatie worden uitgevoerd.

Onderzoeksvragen:
1. Wat is Hack_Right en hoe is Hack_Right theoretisch onderbouwd?
2. Hoe zijn de tot nu toe uitgevoerde Hack_Right trajecten verlopen?
3. Hoe hebben alle betrokkenen de tot nu toe uitgevoerde Hack_Right-trajecten ervaren?

Methoden van onderzoek
- Document analyse
- Interviews

Samenvatting
Waarom en hoe is Hack_Right ontstaan?
Uit de interviews en de analyse van beleidsdocumenten blijkt dat de aanleiding voor Hack_Right de toename in het aantal verdachten van computercriminaliteit, het verschil in profiel tussen daders van computercriminaliteit en daders van traditionele delicten en het gebrek aan werkzame interventies voor deze doelgroep is. Een kritische kanttekening is hier op zijn plek. De wetenschappelijke basis voor deze aanleiding ontbreekt namelijk grotendeels. Het klopt dat er nog geen effectieve interventies zijn die specifiek gericht zijn op cybercriminelen, echter ontbreekt empirisch onderzoek naar kenmerken van cybercriminelen nagenoeg. We weten dus simpelweg niet of, als we het hebben over cybercriminelen, we het hebben over een groep daders met een afwijkend profiel ten opzichte van de daders van allerlei vormen van traditionele offline criminaliteit.

Dat er nog weinig empirisch onderzoek gedaan is naar de kenmerken van cybercriminelen valt de initiatiefnemers van Hack_Right natuurlijk niet aan te rekenen en hoeft ook niet te betekenen dat er geen nieuwe interventie nodig is. Duidelijk is dat Hack_Right grotendeels is ontstaan vanuit een praktijkvraag: politie, OM, reclassering en Halt signaleren dat er een grote instroom van verdachten van cybercrimes is en zoeken naar de beste interventie om recidive te voorkomen. Wel moet er rekening mee worden gehouden dat toekomstig wetenschappelijk onderzoek naar kenmerken van cybercriminelen kan uitwijzen dat de kenmerken van cybercriminelen niet of nauwelijks verschillen van daders van traditionele vormen van criminaliteit.

Wat is het doel en de theoretische onderbouwing van Hack_Right?
Hack_Right heeft twee hoofddoelen: (1) het voorkomen van recidive bij deelnemers en (2) het ICT-talent van deelnemers ontwikkelen binnen de kaders van de wet. De hoofddoelen probeert Hack_Right te bereiken door in te spelen op verschillende criminogene factoren voor cybercriminaliteit. Ook hier speelt eenzelfde probleem als bij de onderbouwing van het 'nieuwe' profiel van cybercriminelen (zie vorige deelvraag). Er zijn simpelweg nog bijna geen studies gedaan naar criminogene factoren bij dit type dader en er is dus nog veel onbekend. Er is zelfs discussie over of traditionele beschermende factoren – zoals het hebben van werk – nog wel een beschermende factor is; werk in de ICT-sector zou ook juist gelegenheden kunnen bieden om cyberdelicten te plegen. De interventieontwikkelaars erkennen dat de wetenschappelijke basis ontbreekt en geven aan dat er daarom een tweesporenbeleid is waarbij meteen is gestart

met de interventie, maar waarbij ook wetenschappelijk onderzoek wordt gedaan naar criminogene factoren van cybercriminelen. Meer onderzoek op basis van beschikbare data uit de systemen van de politie, het OM, Halt en reclassering kunnen helpen om het wetenschappelijke fundament van Hack_Right steviger te maken.

Wat is de doelgroep van Hack_Right en wordt de doelgroep bereikt?
Hack_Right kent op papier een afgebakende doelgroep: jongeren tussen de 12 en 23 jaar, die een eerste delict computercriminaliteit plegen, de schadelijkheid van hun gedrag inzien en gemotiveerd zijn om aan Hack_Right deel te nemen. Verder geven de ontwikkelaars aan dat Hack_Right zich richt op jongeren die affiniteit hebben met – of kennis hebben van – ICT. Op een enkele uitzondering na bereikt Hack_Right ook de doelgroep zoals beschreven in de plannen. We hebben overigens geen zicht op welk deel van de jeugdige cybercriminelen juist geen Hack_Right opgelegd heeft gekregen terwijl ze wel vallen onder de doelgroep. Om hier wel zicht op te krijgen, kan een analyse gedaan worden van alle naar de projectgroep verwezen casussen en naar personen die als verdachte van een cybercrime geregistreerd staan in de politiesystemen.

Verloopt het programma van de tot nu toe uitgevoerde Hack_Right-trajecten volgens plan?
Hack_Right bestaat volgens de plannen uit vier verschillende modules: 'training', 'herstel', 'coaching' en 'positief alternatief '. De modules bestaan uit verschillende producten, zoals een training juridisch/ethisch hacken ('training'), een herstelconferentie ('herstel) en 'Capture-The-Flag-challenges' ('positief alternatief '). In de praktijk zijn volgens ontwikkelaars echter niet de hier omschreven modules gebruikt, maar zijn alleen elementen van de modules verwerkt in de trajecten. Het afwijken van de plannen zorgt ervoor dat het onduidelijk is welke beoogde criminogene factoren centraal staan in de trajecten. Dat individuele trajecten van deelnemers afwijken, komt deels doordat de trajecten bij reclassering sterk op het individu zijn afgestemd. Dit sluit aan bij het responsiviteitsprincipe van de 'what-works'-benadering, dat stelt dat een effectieve interventie zorgt voor een match tussen enerzijds de dader en anderzijds het programma en de uitvoerder. Echter wordt hiermee niet voldaan aan het principe van programma-integriteit: de uitvoering vindt niet plaats in de vorm van de module(s) en producten die van tevoren zijn beschreven. Een punt van zorg is daarbij begeleiding vanuit de bedrijven. Enerzijds zijn de deelnemende jongeren enthousiast – ze voelen zich begrepen door de begeleiders vanuit de ICT-bedrijven – anderzijds krijgen de bedrijven veel vrijheid in de invulling van het traject en hebben de begeleiders binnen de bedrijven niet per definitie de juiste opleiding of ervaring om de doelgroep te kunnen begeleiden. Juist dan is duidelijkheid omtrent de uit te voeren trajecten van belang.

Zijn de tot nu toe uitgevoerde Hack_Right-trajecten voldoende intensief en compleet uitgevoerd?
Of de tot nu toe uitgevoerde Hack_Right-trajecten voldoende intensief zijn uitgevoerd, is lastig te bepalen, aangezien er in de plannen geen concrete duur is gekoppeld aan de invulling van een Hack_Right-traject. De Hack_Right-trajecten bij Halt duurden 20 uur en trajecten bij de reclassering duurden 40 tot 144 uur. Van de tot nu toe uitgevoerde Hack_Right-trajecten die tijdens de interviews zijn besproken, is één deelnemer tijdens het traject uitgevallen. De rest van de trajecten is compleet uitgevoerd. Welke mogelijke positieve of negatieve gevolgen zijn er volgens betrokkenen voor deelnemers? Hoewel het niet het doel van dit onderzoek is geweest om effecten van Hack_Right vast te stellen, zijn er tijdens de uitvoering van dit onderzoek positieve en negatieve gevolgen van Hack_Right aan het licht gekomen die hier zullen worden besproken. Deze observaties kunnen gebruikt worden in toekomstig onderzoek naar het effect van Hack_Right. Mogelijke positieve gevolgen die naar voren komen, zijn dat deelnemers nog contact onderhouden met het bedrijf waar zij het Hack_Right programma hebben uitgevoerd of een stage/werk hebben bij het bedrijf. Andere mogelijke positieve gevolgen zijn volgens uitvoerders dat deelnemers zich bewust zijn geworden van de gevolgen van hun daden en handelingsperspectief hebben gekregen door de trajecten die ze hebben

gevolgd. Een mogelijk negatief gevolg van Hack_Right kan volgens uitvoerders zijn dat deelnemers kennis hebben opgedaan die zij kunnen gebruiken voor criminele doeleinden. Voor enkele uitvoerders is het onduidelijk wat de gevolgen zijn voor deelnemers.

Hoe verloopt het contact tussen uitvoerders en deelnemers?
Zowel deelnemers als uitvoerders zijn over het algemeen tevreden over het contact dat zij hebben met elkaar. Uitvoerders van Halt en reclassering blijken over weinig tot geen technische kennis te beschikken. Enkele respondenten vinden dat enige mate van technische kennis nodig is om in contact te komen met de doelgroep en om in te schatten of een Hack_Right-traject daadwerkelijk goed verloopt, maar andere respondenten geven juist aan dat vooral de pedagogische kennis belangrijk is bij deze medewerkers. Een bijzondere groep binnen de Hack_Right-interventie vormen de bedrijven. Deelnemers voelen zich vooral gehoord en begrepen bij de (cybersecurity)organisaties. Maar in tegenstelling tot de andere organisaties die betrokken zijn bij Hack_Right is het voor personen binnen de ICT-bedrijven geen dagelijkse kost om jeugdige daders te begeleiden. Voor een effectieve interventie is het – volgens het professionaliteitsbeginsel – van belang dat een interventie wordt uitgevoerd door goed opgeleide en getrainde professionals. Een belangrijke vraag blijft dan ook of verwacht kan worden dat de begeleiders vanuit de bedrijven over de juiste capaciteiten beschikken om de jongeren te begeleiden.

Hoe tevreden zijn personen die betrokken zijn geweest bij de tot nu toe uitgevoerde trajecten en wat zijn bevorderende en belemmerende factoren voor een goed verloop?
De uitvoerders van de interventie zijn over het algemeen tevreden over het verloop van de Hack_Right trajecten omdat deelnemers de trajecten positief hebben afgerond en wat hebben geleerd. Deelnemers verschillen echter van mening over de mate waarin zij tevreden zijn over het Hack_Right programma. Minder tevreden deelnemers geven aan dat opdrachten (vooral bij Halt) te makkelijk waren of dat er geen duidelijk programma was. De belangrijkste belemmerende factoren voor een goed verloop van Hack_Right zijn volgens de uitvoerders de lange tijd tussen het plegen van het delict en de uitvoering van Hack_Right en de lage instroom van deelnemers bij Hack_Right. De lange tijd tussen het delict en Hack_Right zorgt ervoor dat het voor deelnemers moeilijk is om terug te blikken op het delict en dat het traject pedagogisch gezien wellicht minder zinvol is. De lage instroom zorgt ervoor dat de beoogde doelgroep niet wordt bereikt. Factoren die tot verbetering zouden kunnen leiden volgens respondenten zijn meer ondersteuning voor uitvoerders van bedrijven, een betere beoordeling van de geschiktheid van verdachten voor deelname aan Hack_Right, efficiënter contact tussen organisaties over de Hack_Right casussen en een opvolging of monitoring van deelnemers die Hack_Right hebben afgerond.