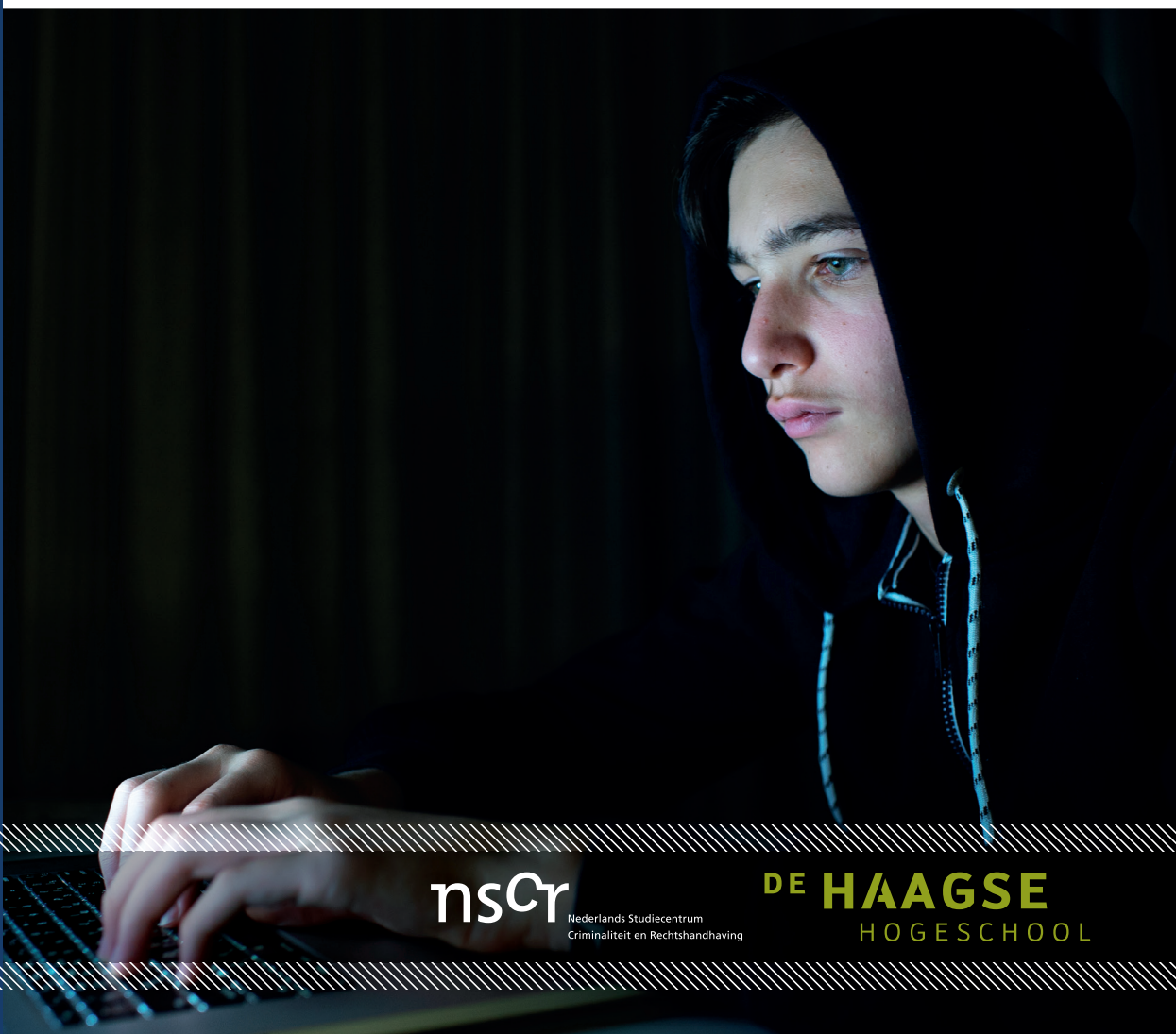
POLITIE & Wetenschap

Een alternatief voor jeugdige hackers?

Plan- en procesevaluatie van Hack_Right

J.A.M. Schiks, M.S. van 't Hoff-de Goede, E.R. Leukfeldt



nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

DE HAAGSE HOGESCHOOL

Een alternatief voor jeugdige hackers?

Een alternatief voor jeugdige hackers?

Plan- en procesevaluatie van Hack_Right

J.A.M. Schiks

M.S. van 't Hoff-de Goede

E.R. Leukfeldt

POLITIE & Wetenschap

DE HAAGSE HOGESCHOOL

nscr Nederlands Studiecentrum Criminaliteit en Rechtshandhaving

In opdracht van: het programma Politie en Wetenschap van de Politieonderwijsraad.

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:

Sdu Klantenservice

Postbus 20025

2500 EA Den Haag

tel.: (070) 378 98 80

website: www.sdu.nl

Omslagontwerp: Imago Media Builders

Afbeelding omslag: Shutterstock/Valua Studio, uitbeelding (door fotomodel) van hackende jongere

ISBN: 9789012406901

NUR: 600

Inhoudsopgave

Voorwoord

Voor u ligt een rapport over Hack_Right. Hack_Right is een recent ontwikkelde interventie gericht op een specifieke doelgroep: jongeren die hun eerste cyberdelict gepleegd hebben. Door de steeds verdergaande digitalisering van onze maatschappij is de verwachting dat we steeds vaker te maken krijgen met deze doelgroep. Jongeren zoeken ook online de grenzen op van wat mag en kan en gaan soms die grens bewust of onbewust over. Onbekend is hoe we deze groep jongeren 'de goede kant op' kunnen krijgen. Hack_Right speelt hier op in en het doel van Hack_Right is dan ook 'het resocialiseren van computercriminelen tussen 12 en 23 jaar en te voorkomen dat ze recidiveren door hun talent te ontwikkelen binnen de kaders van de wet'. (Projectplan 2.0, 2018).

In dit onderzoek kijken we kritisch naar Hack_Right: wat zijn de plannen, hoe zijn die plannen onderbouwd en hoe wordt Hack_Right in de praktijk uitgevoerd? Door als buitenstaanders kritisch mee te kijken met dit initiatief proberen wij bij te dragen aan de ontwikkeling van een effectieve interventie. Want alleen als een interventie daarwerkelijk effectief is en de doelen bereikt worden die de ontwikkelaars en uitvoerders voor ogen hadden, heeft het zin om door te gaan.

Een kritische blik is alleen mogelijk als de belangrijkste stakeholders open en eerlijk meewerken aan het onderzoek. Dat gevoel hebben wij zeker. We danken dan ook alle respondenten die hun waardevolle inzichten met ons wilden delen. Zonder jullie zouden we dit onderzoek niet uit hebben kunnen voeren. Onze dank gaat uit naar de interventieontwikkelaars, medewerkers van het Openbaar Ministerie, Halt-medewerkers, reclasseringswerkers, begeleiders bij (IT-)bedrijven en deelnemers aan Hack_Right die ons te woord hebben gestaan. Ook de projectgroep Hack_Right bedanken wij voor de medewerking en het verstrekken van (contact)gegevens voor het onderzoek. Ten slotte bedanken wij de leescommissie voor hun kritische blik op de conceptversie van dit rapport.

Jim Schiks
Susanne van 't Hoff-de Goede

Rutger Leukfeldt

Samenvatting

Achtergrond

Online criminaliteit is een veelvoorkomende vorm van criminaliteit geworden. Bij online criminaliteit – en in het bijzonder bij vormen van cybercriminaliteit zoals hacken – wordt snel gedacht aan internationaal opererende dadersgroepen die hun aanvallen in Nederland uitvoeren vanuit verre landen met alle gevolgen van dien voor de opsporing en vervolging van daders. Een (aanzienlijk) deel van de daders van cybercriminaliteit bevindt zich echter ook in Nederland. De gevolgen van de door deze dadergroep gepleegde delicten kunnen groot zijn. Er zijn op dit moment geen bewezen effectieve interventies voor daders van online criminaliteit. Als reactie op de grote instroom van (jonge) cyberverdachten hebben het Openbaar Ministerie (OM) en de Nationale Politie de interventie Hack_Right ontwikkeld. Hack_Right is een alternatief of aanvullend straftraject voor jeugdige daders (12 tot 23 jaar) die hun eerste delict cybercriminaliteit plegen. Het is de eerste interventie in Nederland die zich richt op (jonge) cybercriminelen en is daarmee een unieke interventie.

Onderzoeksvragen en -methoden

Onderhavig 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, is het nog te vroeg voor een effectevaluatie. Wel kan er een plan- en procesevaluatie worden uitgevoerd. De volgende onderzoeksvragen staan in het onderzoek centraal: (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?

Voor de evaluatie van Hack_Right zijn kwalitatieve onderzoeksmethoden gebruikt. Kwalitatief onderzoek is een geschikte methode om de werkelijkheid van binnenuit te bestuderen en zodoende zicht te krijgen op de verschillende processen die een rol spelen bij een fenomeen. Daarnaast is er maar een klein aantal deelnemers dat Hack_Right tot op heden heeft gevolgd, waardoor kwantitatief onderzoek nog niet haalbaar is. De eerste onderzoeksmethode is documentanalyse. Het doel van de documentanalyse is om inzicht te krijgen in de plannen van Hack_Right, zoals die op papier staan. Zo kan worden onderzocht wat Hack_Right is, hoe Hack_Right theoretisch is onderbouwd en welke trajecten tot nu toe zijn uitgevoerd. Verschillende documenten zijn hiervoor geraadpleegd. De tweede onderzoeksmethode is het interviewen van bij de uitvoering

van Hack_Right betrokken personen. Het doel van de interviews was drieledig. Ten eerste was het doel om in aanvulling op de beleidsdocumenten een beter inzicht te krijgen in de plannen omtrent Hack_Right. Een tweede doel was om inzicht te krijgen in het verloop van de tot nu toe uitgevoerde Hack_Right-trajecten. Het derde doel van de interviews was om de ervaringen met Hack_Right van alle betrokkenen in kaart te brengen. In totaal zijn 28 interviews afgenomen met respondenten die op verschillende manieren betrokken zijn bij de Hack_Right interventie: twee interventieontwikkelaars, vijf toewijzers, elf uitvoerders en tien deelnemers.

Conclusies

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 ont-

breekt 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.

Aanbevelingen

Verbeter het fundament
Hack_Right is feitelijk ontstaan vanuit signalen uit de praktijk: een grote toestroom van verdachten met een 'nieuw' profiel waar nog geen effectieve interventie voor is ontwikkeld. Dat wetenschappelijke inzichten in enkele belangrijke aspecten van Hack_Right ontbreken, erkennen de ontwikkelaars maar tegelijk geven ze aan dat het belangrijk is om te starten en daarbij nieuwe inzichten uit de wetenschap in de gaten te blijven houden. Om te kunnen doorgroeien tot een volwaardige interventie is echter een stevigere basis nodig. Onderhavig onderzoek is daarbij een eerste stap, maar zeker niet de laatste. Inzichten in bijvoorbeeld kenmerken en criminogene factoren van de doelgroep zijn noodzakelijk om een effectieve interventie op te zetten. Enerzijds kan hierin inzicht worden verkregen door de uitgevoerde Hack_Right trajecten te (blijven) evalueren. Ten tijde van dit onderzoek was er immers slechts een beperkt aantal trajecten afgerond. Anderzijds kunnen andere bronnen gebruikt worden om meer inzicht te krijgen in kenmerken van de Hack_Right doelgroep. Data over verdachten die voorkomen in de politiesystemen kunnen bijvoorbeeld gebruikt worden om inzicht te krijgen in achtergrondkenmerken en criminele carrières.

Zorg dat de doelen duidelijk zijn
Ondanks dat het leerelement in Hack_Right centraal staat volgens alle uitvoerders van Hack_Right – deelnemers krijgen adviezen, begeleiding en ontwikkelen vaardigheden – leven er in de praktijk verschillende beelden bij wat de overige doelen van de interventie precies zijn. Verwachtingsmanagement richting interne en externe partijen omtrent het strafelement is daarom belangrijk. Communiceer daarom naar interne en externe partijen duidelijk over de doelen van Hack_Right en zorg indien noodzakelijk dat het strafelement in een andere maatregel of straf tot uiting komt.

Verbeter de programma-integriteit
Bij de invulling van de tot nu toe uitgevoerde Hack_Right-trajecten bestaat er een spanning tussen een op het individu afgestemde interventie (responsiviteit) en een programma dat wordt uitgevoerd zoals in de plannen beschreven (programma-integriteit). Door de vele verschillende invullingen die Hack_Right deelnemers hebben gehad, is niet duidelijk welke componenten van de interventie kunnen leiden tot bepaalde uitkomsten. Verder ontbreken op dit moment uitgewerkte producten en handleidingen voor de uitvoering van die producten. Voor de volgende stappen in evaluatieonderzoek is het belangrijk dat duidelijker wordt wat de invullingsmogelijkheden zijn voor een Hack_Right traject. Alleen dan kan – uiteindelijk met behulp van effectevaluaties – worden bepaald welke elementen van de interventie, onder welke omstandigheden, leiden tot bedoelde of onbedoelde gevolgen.

Zorg voor een goede opleiding van de uitvoerders
Vanuit het professionaliteitsbeginsel is het voor een effectieve interventie van belang dat begeleiders die een interventie uitvoeren voldoende zijn opgeleid en getraind. Enerzijds betekent dit dat het belangrijk is om zorgvuldig geschikte uitvoerders te selecteren. Anderzijds kunnen er trainingen of cursussen worden aangeboden aan de uitvoerders. Halt- en reclasseringswerkers kunnen bijvoorbeeld worden voorzien van basale kennis over cybercriminaliteit. Uitvoerders van ICT-bedrijven kunnen worden ondersteund door pedagogisch medewerkers of, indien zij gedurende lange termijn betrokken zijn bij Hack_Right trajecten, bijgeschoold worden in pedagogische kennis.

Verbeter de zichtbaarheid
Een belangrijke belemmerende factor volgens respondenten is de lage instroom van deelnemers bij Hack_Right. Het blijkt dat de selectie van deelnemers op dit moment afhankelijk is van individuen die op de hoogte zijn van Hack_Right als mogelijkheid en zelf beslissen om Hack_Right wel of niet aan te dragen aan de projectgroep Hack_Right. De overwegingen voor de selectie van deelnemers ligt niet alleen bij het OM, maar ook bij andere partners zoals de politie, Halt en reclassering. Het bereik van potentiële deelnemers is hierdoor afhankelijk van individuele kennis en keuzes. De zichtbaarheid van Hack_Right kan dan ook verhoogd worden, onder andere door het informeren van sleutelfiguren in het opleggen van Hack_Right over de mogelijkheden,

doelen en selectiecriteria van Hack_Right.

Onderzoek de schaalbaarheid
Hack_Right is eind 2017 ontwikkeld en heeft tot maart 2020 veertien afgeronde trajecten opgeleverd. Dit lijkt tegenstrijdig met de aanleiding van Hack_Right: een grote toename van daders computercriminaliteit. De verwachting is dan ook dat in de toekomst grotere stromen deelnemers Hack_Right zullen volgen. Op dit moment lijkt er echter sprake te zijn van een hoge mate van maatwerk: deelnemers worden aangereikt vanuit verschillende onderdelen van de strafrechtketen, de projectgroep beoordeelt de aanvragen en een beperkt aantal personen binnen Halt en reclassering voeren de trajecten vervolgens uit met ICT-bedrijven. Om Hack_Right op grotere schaal te kunnen uitvoeren, is het daarom enerzijds van belang om de programma-integriteit te verbeteren: er zullen immers meer uitvoerders nodig zijn die moeten weten wat het doel is van de interventie en hoe de interventie moet worden uitgevoerd. Anderzijds moet goed bekeken worden hoeveel geschikte ICT-bedrijven er zijn die zich voor langere tijd willen committeren aan Hack_Right. Zonder de bedrijven vervalt immers een belangrijk deel van de interventie.

Summary

Background

Online crime has become a common crime. Online crime, and in particular forms of cybercrime such as hacking, is often associated with international criminal groups that carry out their attacks in the Netherlands from distant countries, which has many implications for the investigation and prosecution of offenders. However, a (considerable) number of cybercrime offenders are also located in the Netherlands. The consequences of the crimes committed by this group of offenders can be major and there are currently no proven effective interventions for online crime offenders. As a response to the large increase of (young) cybercrime suspects, the Public Prosecution Service and the National Police in the Netherlands have developed the Hack_Right intervention program. Hack_Right is an alternative or additional criminal justice intervention for juvenile offenders (12 to 23 years old) who commit their first cybercrime offense. It is unique as it is the first intervention in the Netherlands that focuses on (young) cyber criminals.

Research questions and methods

The purpose of this study is to evaluate the Hack_Right intervention program and the pilot interventions that have been carried out so far. As Hack_Right has only been running for a relatively short time and only fourteen pilots had been completed by the end of the data collection period of the present study, an impact evaluation is not feasible. However, a plan and process evaluation can be carried out. The following research questions are central to the evaluation: (1) What is Hack_Right and what is the theoretical justification of Hack_Right? (2) How have the Hack_Right pilots been carried out so far? (3) How have the Hack_Right pilots carried out so far been experienced by all people involved?

Qualitative research methods were used for the evaluation of Hack_Right. Qualitative research is a suitable method to study reality from within in order to gain insight into the different processes that play a role in a particular phenomenon. In addition, there have only been a small number of Hack_Right participants to date, making quantitative research not yet feasible. The first research method that has been used is document analysis. The purpose of the document analysis was to gain insight into Hack_Right's plans as they are set out on paper. In this way, it is possible to examine what Hack_Right is, how Hack_Right is theoretically substantiated, and what pilots have been carried out so far. Various documents have been consulted for this purpose. The second research method was to interview people who were involved in the implementation of

Hack_Right. The purposes of the interviews were threefold. First, the goal was to gain a better understanding of the Hack_Right plans in addition to the policy documents. A second goal was to gain insight into the evolution of the Hack_Right pilots carried out so far. The third goal of the interviews was to map the experiences of the people involved in Hack_Right. A total of 28 interviews was conducted with respondents who are involved in the Hack_Right intervention program in different ways: two people who developed the intervention, five who imposed the program (working at the Public Prosecution Service), eleven people who implemented the program (supervisors and IT-employers) and ten participants.

Conclusions

Why and how was Hack_Right founded?
From the interviews and the analysis of policy documents, it appears that Hack_Right was established because of the increase in the number of computer crime suspects, the difference between the profile of perpetrators of computer crimes and perpetrators of traditional crimes and the lack of effective interventions for this target group. A critical comment has to be made here, because the scientific basis for this is largely lacking. It is true that there are no effective interventions specifically aimed at cyber criminals, but empirical research into the characteristics of cyber criminals is virtually non-existent. Therefore, we simply do not know whether, when we talk about cyber criminals, we are talking about a group of perpetrators with a different profile compared to the perpetrators of all kinds of traditional offline crimes. The fact that little empirical research has been done into the characteristics of cyber criminals is of course not the responsibility of the initiators of Hack_Right and does not necessarily mean that no new interventions are required. It is clear that Hack_Right largely arose from a practical demand: the police, Public Prosecution Service, probation service and Halt[1] have indicated that there has been a large influx of cybercrime suspects and they are looking for the best intervention to prevent recidivism. However, it must be taken into account that future scientific research into the characteristics of cyber criminals may show that they do not differ much, if at all, from perpetrators of traditional forms of crime.

What is the objective and theoretical foundation of Hack_Right?
Hack_Right has two main objectives: (1) to prevent recidivism among participants and (2) to develop participants' ICT talent in a legal manner. Hack_Right tries to achieve its main objectives by responding to various criminogenic needs regarding cybercrime. In this regard, we find the same problem as with the underpinning of the 'new' profile of cyber criminals (see previous sub-question): there are simply very few studies on the criminogenic needs of this type of offender, so much is still unknown. It is even debated whether traditional protective factors for offending – such as having a job – are still

1 Halt is a Dutch organization that provides an alternative sanction for juvenile offenders in order to prevent them being saddled with a criminal record.

protective factors. Working in the ICT sector could also provide opportunities to commit cybercrimes. The developers of the intervention acknowledge that the scientific basis is lacking and indicate that there is, therefore, a two-track policy which involves immediately starting the intervention, but also scientific research into the criminogenic needs of cyber criminals. More research – for example based on available data from the police, the Public Prosecution Service and Halt and probation services – can help to strengthen the scientific foundation of Hack_Right.

What is Hack_Right's target group and is the target group being reached?
Hack_Right has a defined target group on paper: young people between 12 and 23 years old who have committed their first computer crime offense, who understand the harmfulness of their behavior and who are motivated to participate in Hack_Right. The developers also indicate that Hack_Right is aimed at young people who have an affinity with – or have knowledge of – ICT. With a few exceptions, Hack_Right generally reaches the target audience as described in the plans. However, we have no insight into which proportion of juvenile cyber criminals has not participated in Hack_Right that could be categorized as part of the target group. To gain insight into this, analysis can be conducted of all cases referred to the project group and of all persons who are registered as being suspected of a cybercrime in the police systems.

Has the implementation of the Hack_Right pilots carried out so far been done in accordance with the plan?
According to the plans, Hack_Right consists of four different modules: 'training', 'recovery', 'coaching' and 'positive alternative'. The modules consist of various products, such as legal/ethical hacking training ('training'), a recovery conference ('recovery') and 'Capture-The-Flag-challenges' ('positive alternative'). In practice, however, according to those responsible for developing the intervention, the module (s) described here have not been used, but rather only certain elements of the modules have been incorporated into the pilots. Deviating from the plans means that it is unclear which targeted criminogenic needs are central to the pilots. The fact that the individual trajectories of participants differ is partly because the probation trajectories are strongly tailored to the individual. This is in line with the responsiveness principle of the 'what-works' approach, which states that an effective intervention ensures a match between, on the one hand, the offender and, on the other hand, the program and the person charged with its implementation. However, this is not in line with the principle of program integrity: implementation does not take place according to the terms of the modules and products that have been described in advance. In addition, there is a point of concern related to the guidance from the companies. On the one hand, the participating young people are enthusiastic and they feel understood by the supervisors from the ICT companies. But, on the other hand, the companies are given a lot of freedom in the implementation of the program and the supervisors within the companies do not necessarily have the right training or experience to guide young offenders. As such, clarity is especially needed with regard to the pilots to be carried out.

Have the Hack_Right pilots carried out so far been carried out in a sufficiently intensive and complete manner?
It is difficult to determine whether the Hack_Right pilots carried out so far have been carried out intensively enough, since the plans do not link a specific duration to the implementation of a Hack_Right trajectory. The Hack_Right trajectories at Halt took 20 hours and at the probation services they ran for 40 to 144 hours. Of the Hack_Right pilots carried out so far and discussed during the interviews, one participant dropped out during the pilot. All other pilots have been completed.

What possible positive or negative consequences are there for participants according to people involved in Hack_Right?
While it was not the purpose of this study to determine the effects of Hack_Right, the study revealed positive and negative consequences of Hack_Right that will be discussed here. These observations can be used in future research into the effects of Hack_Right. Possible positive consequences that emerged are that participants still maintain contact with the company where they carried out the Hack_Right program or have an internship/work at the company due to the Hack_Right program. According to those responsible for implementing the intervention, other possible positive consequences are that participants have become aware of the consequences of their actions and are focused on action as a result of the trajectories they followed. According to the implementers, a possible negative consequence of Hack_Right could be that participants have gained knowledge that they can use for criminal purposes. For other implementers, it is unclear what the consequences were for participants.

How is the contact between implementers and participants?
Both participants and implementers are generally satisfied with the contact they have had with each other. Halt and probation-workers appear to have little or no technical knowledge. Some respondents believe that some degree of technical knowledge is required to connect with the target group and to estimate whether a Hack_Right trajectory has actually gone well, but other respondents indicate that pedagogical knowledge is especially important for these employees.

The companies are a notable group of actors within the Hack_Right intervention program. Participants mainly feel that they are being heard and understood by the (cybersecurity) organizations. However, unlike for other organizations involved in Hack_Right, guiding juvenile offenders does not form part of the daily routine of persons within the ICT companies. For an intervention to be effective, it is important, according to the principle of professionalism, that it is carried out by well-educated and trained professionals. An important question therefore remains regarding whether the supervisors from the companies can be expected to have the right capabilities to guide the young people.

How satisfied are people who have been involved in the pilots carried out so far and what factors hinder or facilitate the implementation of Hack_Right?
The implementers of the intervention are generally satisfied with the evolution of the Hack_Right pilots because participants have completed the processes positively and have learned something. However, participants differ on how satisfied they are with the Hack_Right program. Less satisfied participants indicate that assignments (especially at Halt) were too easy or that there was no clear program.

According to the implementers, the main factors that hinder the proper implementation of Hack_Right are the long period of time between committing the crime and the execution of the program and the low influx of participants to Hack_Right. The long period of time between the offense and Hack_Right makes it difficult for participants to reflect on their offense and means that trajectories may be less useful from a pedagogical point of view. The low influx ensures that the intended target group is not reached.

According to respondents, factors that could lead to improvement are more support for the implementers at the companies, better assessment of the suitability of suspects to participate in Hack_Right, more efficient contact between organizations regarding the Hack_Right cases and follow-up or monitoring of participants who have completed Hack_Right.

Recommendations

Improve the foundation
Hack_Right has been developed because of several observations in practice: a large increase in suspects with a 'new' profile for which no effective intervention has yet been developed. The developers acknowledge that scientific insights into some important aspects of Hack_Right are lacking, but at the same time they indicate that it is important to start and to monitor new insights from science. However, in order to grow into a fully-fledged intervention, a stronger foundation is needed. The present research is a first step, but certainly not the last. Insights into, for example, the characteristics and criminogenic needs of the target group are necessary to design an effective intervention. On the one hand, insight can be gained here by (continuing to) evaluating the Hack_Right trajectories. After all, only a limited number of pilots had been completed at the time of this study. On the other hand, other sources can be used to gain more insight into the characteristics of the Hack_Right target group. Data about suspects that appear in the police systems can be used, for example, to gain insight into background characteristics and criminal careers.

Make sure that the objectives are clear
According to all executors of Hack_Right, the learning element is central to the intervention: participants receive advice, guidance and develop skills. However, in practice,

there are different opinions about Hack_Right's other objectives. Expectation management towards internal and external parties regarding the (lack of a) punitive element is therefore important. Therefore, the objectives of Hack_Right should be communicated clearly to internal and external parties and, if necessary, it should be ensured that the punitive element is expressed in another measure or punishment.

Improve program integrity
Within the implementation of the Hack_Right pilots that have been carried out so far, there is a tension between a program tailored to the individual (responsiveness) and a program that is carried out as described in the plans (program integrity). Due to the many different programs that Hack_Right participants have completed, it is not clear which components of the intervention can lead to certain outcomes. Furthermore, detailed products and manuals for the implementation of those products are currently lacking. For the next steps in evaluation research, it is important that it becomes clear what options there are for a Hack_Right trajectory. Only then can it be determined – ultimately with the help of impact evaluations – which elements of the intervention, under which circumstances, lead to intended or unintended consequences.

Provide proper training for the implementers
According to the principle of professionalism, for an intervention to be effective it is important that the supervisors who carry out an intervention have sufficient education and training. On the one hand, this means that it is important to carefully select appropriate supervisors. On the other hand, training or courses can be offered to the implementers. For example, Halt and probation workers can be provided with basic knowledge about cybercrime. Supervisors at ICT companies can be supported by pedagogical workers or, if they are involved in long-term Hack_Right trajectories, receive additional training regarding pedagogical knowledge.

Improve visibility
According to respondents, an important factor that hinders the proper implementation of Hack_Right is the low influx of participants. It turns out that selection of participants currently depends on individuals who are aware of Hack_Right as a possibility and who decide themselves whether to bring suspects to the Hack_Right project group. Suggesting participants is not only done by the Public Prosecution Service, but also by other partners such as the police, Halt and the probation service. The quantity of potential participants therefore depends on individual knowledge and choices. The visibility of Hack_Right can therefore be increased by, for example, better informing key figures in the imposition of Hack_Right interventions about the possibilities, objectives and selection criteria of Hack_Right. In addition, it must be explicitly communicated that Hack_Right does not fulfill a punitive function.

Explore scalability

Hack_Right was developed at the end of 2017 and had delivered 14 completed pilots up until March 2020. This seems to conflict with the reason why Hack_Right was developed: because of a large increase in computer crime offenders. It is therefore expected that larger flows of cybercrime offenders will participate in Hack_Right in the future. At the moment, however, there appears to be a high degree of customization: participants have been put forward by various sections of the criminal justice chain, the project group assesses the applications and a limited number of people within Halt and probation then carry out the trajectories with ICT companies. In order to be able to implement Hack_Right on a larger scale, it is therefore important, on the one hand, to improve the program integrity: after all, more implementers will be required who need to know what the purpose of the intervention is and how the intervention must be carried out. On the other hand, it is important to look carefully at how many suitable ICT companies want to commit to Hack_Right for a longer period. After all, without the companies, an important part of the intervention will disappear.

1. Inleiding

Online criminaliteit[2] is een veelvoorkomende vorm van criminaliteit geworden. Het Centraal Bureau voor de Statistiek (CBS) meet sinds 2012 het slachtofferschap van een aantal vormen van online criminaliteit, waaronder hacken en fraude via internet, en de CBS-rapporten laten steevast zien dat allerlei vormen van online criminaliteit niet meer weg te denken zijn uit onze maatschappij. In 2018 werd bijvoorbeeld 8,5 procent van de 14,5 miljoen internetgebruikers in Nederland slachtoffer van een vorm van online criminaliteit (CBS, 2019). Eenzelfde beeld zien we terug bij bedrijven. Grofweg een op de vijf bedrijven werd slachtoffer van een cyberaanval met financiële schade tot gevolg (Leukfeldt et al. (2020).

Bij online criminaliteit – en in het bijzonder bij vormen van cybercriminaliteit zoals hacken – wordt snel gedacht aan internationaal opererende dadersgroepen die hun aanvallen in Nederland uitvoeren vanuit verre landen met alle gevolgen van dien voor de opsporing en vervolging van daders. Daarmee zou dus de rol van de Nederlandse politie en zeker die van de regionale eenheden beperkt zijn. Deels klopt dat beeld. Er worden immers daadwerkelijk aanvallen uitgevoerd door groepen die opereren vanuit Oost-Europese landen die in Nederland en andere West-Europese landen slachtoffers maken (zie bijvoorbeeld Lusthaus & Varese, 2019; Leukfeldt et al., 2017). Maar dat is niet het hele verhaal.

Al in 2010 lieten Leukfeldt en collega's zien op basis van een analyse van 665 aangiftes cybercriminaliteit in Nederland dat veel van de hacks waarvan aangifte was gedaan werden uitgevoerd door bekenden van het slachtoffer. Veel delicten bleken in de relationele sfeer te liggen: een ex-medewerker of een ex-vriend die om allerlei verschillende redenen de hack pleegden. De auteurs concluderen dat cybercriminaliteit waarschijnlijk, net als traditionele criminaliteit, bestaat uit grote aantallen individuele daders die kleinere delicten plegen en enkele grote (inter)nationale netwerken. Recente Nederlandse voorbeelden – zoals een DDoS-aanval op overheidssites (NOS, 2020) en een

2 Onder online criminaliteit verstaan we in dit onderzoek twee categorieën delicten: cybercriminaliteit en gedigitaliseerde criminaliteit, in de internationale literatuur ook wel aangeduid als respectievelijk cyber dependent crime en cyber enabled crime (zie McGuire & Dowling, 2013). Onder de eerste categorie vallen delicten waarbij de informatie- en communicatie (ICT-)structuur zelf doelwit is én waarbij voor het plegen van dat delict ICT van wezenlijk belang is voor de uitvoering. Bijvoorbeeld het hacken van een database met persoonsgegevens of het platleggen van een website van een school met een zogenaamde DDoS-aanval. Binnen de tweede categorie vallen de digitale varianten van traditionele offline delicten, zoals het plegen van fraude via internet.

hack-aanval op schoolsystemen (Rechtspraak, 2020) – laten zien dat er inderdaad ook sprake is van Nederlandse daders die in Nederland actief zijn. Er is dus ook een belangrijke rol weggelegd voor nationale en lokale autoriteiten bij de aanpak van online criminaliteit. In Nederland wordt dit overigens ook gezien en heeft de politie bijvoorbeeld naast het landelijke Team High Tech Crime ook cybercrimeteams in alle eenheden die zich bezighouden met de opsporing van online criminaliteit (Boekhoorn, 2019).

Een (aanzienlijk) deel van de daders van cybercriminaliteit bevindt zich dus gewoon in Nederland. De gevolgen van de door deze dadergroep gepleegde delicten kunnen groot zijn. Zowel voor slachtoffers (emotionele en economische schade) en de maatschappij in brede zin (de schaarse digitale capaciteit wordt op deze manier voor verkeerde zaken aangewend) als de daders zelf (strafblad, doorontwikkeling criminele carrière). Het is dan ook wenselijk om effectieve interventies in te zetten die deze groep op het goede pad kan brengen. Het is echter nog maar de vraag of bestaande interventies zoals een gevangenisstraf of taakstraf helpen bij deze doelgroep om recidive te voorkomen. Om een goede interventie te ontwikkelen, is het immers van belang om zicht te krijgen op het probleem dat de interventie probeert te verhelpen. Er zijn namelijk aanwijzingen dat daders van online criminaliteit andere kenmerken hebben dan daders van traditionele offline criminaliteit, al is er op dit moment nog (te) weinig empirisch onderzoek om de precieze verschillen en overeenkomsten die zij vertonen met daders van traditionele offline criminaliteit vast te stellen (zie bijvoorbeeld Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019).

Het is wenselijk om effectieve interventies in te zetten die cybercriminelen op het goede pad brengen. Er zijn op dit moment geen bewezen effectieve interventies voor daders van online criminaliteit (Oosterwijk & Fischer, 2017). Wel hebben in Nederland het Openbaar Ministerie (OM) en de Nationale Politie als reactie op de instroom van (jonge) cyberverdachten de interventie Hack_Right ontwikkeld. Hack_Right is een alternatief of aanvullend straftraject voor jeugdige daders (12 tot 23 jaar) die hun eerste delict cybercriminaliteit plegen (Bruijne, 2018). Het is de eerste interventie in Nederland die zich richt op (jonge) cybercriminelen en is daarmee een unieke interventie. De interventie beoogt recidive bij de jongeren te voorkomen en hen kaders te geven waarin zij hun ICT-talent op legale wijze kunnen ontwikkelen. Om dit doel te bereiken, worden de jongeren bijvoorbeeld aan cybersecuritybedrijven gekoppeld. Hier dienen zij te reflecteren op het delict, leren zij ethisch hacken en krijgen zij technische opdrachten. Op het moment van schrijven van dit rapport zijn er tussen de veertien en achttien Hack_Right trajecten uitgevoerd.[3]

Onderhavig 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 de

3 Op 10 maart 2020 waren er veertien casussen afgerond en vier casussen lopend volgens de projectgroep Hack_Right.

eerste casussen in 2018 en 2019 zijn afgerond, is het nog te vroeg voor een effectevaluatie. Wel kan er een plan- en procesevaluatie worden gedaan. De volgende onderzoeksvragen staan in het onderzoek centraal: (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?

Leeswijzer

Om deze onderzoeksvragen te beantwoorden, wordt eerst een theoretisch kader uiteengezet. In hoofdstuk 2 wordt inzicht gegeven in evaluatieonderzoek en de verschillende typen evaluatieonderzoek. Hoofdstuk 3 bespreekt wat er in de wetenschappelijke literatuur bekend is over factoren die bijdragen aan effectieve gedragsinterventies ten behoeve van recidivevermindering. In hoofdstuk 4 worden de methoden van het huidige onderzoek besproken. De resultaten en antwoorden op de onderzoeksvragen worden in de hoofdstukken 5, 6 en 7 gegeven. Ten slotte bevat hoofdstuk 8 de belangrijkste conclusies en aanbevelingen van dit onderzoek.

2. Evaluatieonderzoek

2.1 Inleiding

In dit hoofdstuk gaan we in op wat evaluatieonderzoek eigenlijk is. In de sociale wetenschappen richt evaluatieonderzoek zich op programma's of interventies[4] die bedoeld zijn om een maatschappelijk probleem te verminderen of op te lossen (Harte, 2019). Veel van deze programma's zijn gedragsinterventies, die een verandering in het gedrag van de deelnemers proberen te bewerkstelligen. Een interventie kan op verschillende manieren worden geëvalueerd. Idealiter verloopt evaluatieonderzoek volgens een bepaalde hiërarchie (Rossi, Lipsey & Freeman, 2004).

Aan een interventie ligt een theorie ten grondslag, die beargumenteert dat als bepaalde middelen aan personen worden aangereikt, dit hun gedrag kan veranderen. De theorie laat zien waarom het programma zou *kunnen* werken. Het is daarom van belang om de theorie die ten grondslag ligt aan het programma in kaart te brengen (planevaluatie). Vervolgens wordt gekeken of het programma volgens het plan wordt uitgevoerd (procesevaluatie) en ten slotte volgt een onderzoek naar het effect van het programma en een kosten-batenanalyse waarin dit effect wordt meegenomen (effect-evaluatie) (Pawson & Klein Haarhuis, 2005).

In dit hoofdstuk zal eerst dieper worden ingegaan op deze drie manieren van evalueren: de planevaluatie, procesevaluatie en effectevaluatie. Vervolgens gaan we kort in op een invloedrijke benadering uit de literatuur over evaluatieonderzoek: de realistische-benadering van Pawson en Tilley (2004). Het hoofdstuk sluit af met een kort resumé.

2.2 Planevaluatie, procesevaluatie en effectevaluatie

Een eerste vorm van evaluatieonderzoek betreft een planevaluatie, ook wel ex ante evaluatie genoemd. Van tevoren kan al op basis van de plannen worden bepaald of de beoogde doelen van een interventie duidelijk zijn, of de interventie aansluit bij de doelgroep en of de interventie ingrijpt op het probleem (Harte, 2019). Bij een planevaluatie staat de vraag waarom een interventie zou *kunnen* werken centraal. Met een planevaluatie wordt nagegaan of met het beoogde programma de gewenste uitkomsten zouden

4 De begrippen 'programma' en 'interventie' worden in dit hoofdstuk als synoniemen gebruikt.

kunnen worden bereikt op basis van de theorie die aan het programma ten grondslag ligt (Ooyen-Houben & Leeuw, 2010). Hierbij worden plannen ontrafeld en veronderstelde mechanismen blootgelegd. Daarnaast wordt onderzocht of de plannen consistent zijn en worden zij getoetst aan wetenschappelijke kennis.

De tweede vorm van evaluatieonderzoek is een procesevaluatie, die zich richt op de uitvoering van een programma in de praktijk en nagaat of het programma consistent en volgens het plan wordt geïmplementeerd (Ooyen-Houben & Leeuw, 2010). Een zorgvuldige implementatie van een gepland programma, vrij van serieuze implementatieproblemen, is gerelateerd aan betere uitkomsten (Durlak & DuPre, 2008). In de praktijk worden interventies echter niet altijd volgens het vooropgezette plan uitgevoerd. Uitvoerders hebben voldoende kennis, tijd en middelen nodig en moeten gemotiveerd zijn om de interventie volgens het plan uit te voeren (Nas et al., 2011; Harte, 2019). Het is daarom niet altijd haalbaar om een interventie perfect volgens protocol uit te voeren. Daarnaast kan enige mate van vrijheid tot aanpassing van de interventie de effectiviteit juist vergroten (Durlak & DuPre, 2008). In de literatuur wordt de spanning tussen integriteit en aanpassing van interventies uitvoerig besproken (zie bijvoorbeeld Castro et al., 2004; Durlak & DuPre, 2008; Anyon et al., 2019).

Ten slotte gaat een effectevaluatie na wat de resultaten en effecten van een programma zijn (Ooyen-Houben & Leeuw, 2010). Het laat met andere woorden zien wat het programma concreet heeft opgeleverd. Alleen de effectevaluatie kan causale relaties laten zien tussen de inzet van een programma en de positieve of negatieve gevolgen van de interventie. Als een interventie nog niet volledig en consistent wordt uitgevoerd, heeft dergelijk onderzoek geen nut omdat de invloed van het programma dan moeilijk is vast te stellen. Op basis van de 'Maryland Scientific Methods Scale' kunnen er verschillende niveaus worden onderscheiden waarop een effectevaluatie plaats kan vinden (Van der Laan, 2004; Farrington et al., 2003). Deze niveaus, die verwijzen naar de methodologische kwaliteit van een onderzoek, variëren van het laagste niveau (1) waar enkel achteraf naar de uitkomstvariabele wordt gekeken tot aan het hoogste niveau (5) waar een voor- en nameting en een experimentele en controlegroep nodig zijn. Alleen in de hoogste niveaus van het onderzoeksdesign kunnen causale effecten van een programma worden vastgesteld (Rovers, 2007).

2.3 De realistische-benadering

Voor het uitvoeren van evaluatieonderzoek is in de wetenschappelijke literatuur het werk van Pawson en Tilley (2004) invloedrijk. In de studie wordt een voorkeursbenadering omschreven voor het uitvoeren van evaluatieonderzoek. Deze voorkeursbenadering wordt de realistische-benadering genoemd. Volgens de benadering dienen interventies te worden gezien als ingewikkelde, verfijnde sociale interacties te midden van een complexe sociale realiteit (Pawson & Tilley, 2004). Om de werking van interventies te kunnen begrijpen, zijn er drie aan elkaar gekoppelde concepten van belang: mechanisme, context

en uitkomstpatronen. Ten eerste kan een interventie meerdere mechanismen activeren. Een mechanisme verwijst naar de manier waarop een van de componenten van de interventie, of een combinatie daarvan, zorgt voor verandering bij het onderwerp van de interventie. Mechanismen verklaren dus de logica van een interventie. Een tweede concept betreft de context waarin interventies plaatvinden. Er wordt verondersteld dat mechanismen van een interventie slechts actief zijn in bepaalde contexten. Een context beschrijft de omstandigheden waarin interventies plaatsvinden die relevant zijn voor de werking van de mechanismen van de interventie. Ten slotte zorgen verschillen in context en mechanismen ervoor dat een interventie verschillende uitkomstpatronen heeft. Uitkomstpatronen zijn de bedoelde en onbedoelde gevolgen van de interventie. Er dienen volgens Pawson en Tilley dan ook meerdere uitkomstmaten te worden onderzocht. Een goede evaluatie is in staat om het complexe karakter van de uitkomsten uit te leggen.

Een realistische evaluatie focust zich op de theorie die verklaart hoe een programma zou moeten werken en vraagt zich af of deze theorie goed, aannemelijk, duurzaam, praktisch en valide is. Een realistische evaluatie bestaat uit vier fasen (Pawson & Tilley, 2004). Tijdens de eerste fase wordt de theorie van het programma aan het licht gebracht over waarom, voor wie en onder welke omstandigheden het programma zou moeten werken. Deze theorie kan in kaart worden gebracht met behulp van verschillende bronnen, zoals documenten, programmaontwikkelaars, praktijkdeskundigen, eerder evaluatieonderzoek en wetenschappelijke literatuur. De tweede fase bestaat uit het verzamelen van data om de theorie of hypothesen te kunnen testen. Vervolgens dient tijdens de derde fase de theorie systematisch te worden getest met behulp van de verzamelde data. Tijdens de laatste fase worden de resultaten geïnterpreteerd en wordt beoordeeld of de theorieën over hoe het programma werkt ook daadwerkelijk worden ondersteund door de resultaten (Pawson & Tilley, 2004). Het expliciteren van de theoretische aannames die ten grondslag liggen aan een programma en het toetsen van deze aannames op basis van empirisch onderzoek is een belangrijke en noodzakelijke stap richting een effectieve interventie (Leeuw, 2005).

2.4 Resumé

Uit dit hoofdstuk is gebleken dat evaluatieonderzoek in de sociale wetenschappen een interventie evalueert die een maatschappelijk probleem probeert op te lossen. Een gedragsinterventie probeert daarbij het gedrag van deelnemers te veranderen. Evaluatieonderzoek verloopt idealiter volgens een bepaald aantal stappen. Eerst wordt in een planevaluatie gekeken of een interventie zou kunnen werken op basis van de plannen die ten grondslag liggen aan de interventie. Vervolgens kijkt een procesevaluatie hoe de interventie in de praktijk wordt uitgevoerd en of de uitvoering volgens plan verloopt. Ten slotte wordt met een effect-evaluatie bepaald welke resultaten het programma daadwerkelijk heeft opgeleverd.

Een interventie kan worden gezien als een verzameling van ingewikkelde, verfijnde sociale interacties die midden in een complexe sociale realiteit plaatsvinden. Een interventie kan daarom meerdere mechanismen activeren, die slechts in bepaalde contexten actief zijn. Verschillen in context en mechanismen zorgen er vervolgens voor dat een interventie verschillende (bedoelde of onbedoelde) gevolgen heeft. In het volgende hoofdstuk wordt op basis van eerder uitgevoerde evaluatieonderzoeken duidelijk hoe interventies mogelijk effectief kunnen zijn.

3. Effectieve interventies

3.1 Inleiding

In dit hoofdstuk wordt op basis van eerder evaluatieonderzoek inzicht gegeven in factoren die kunnen bijdragen aan een effectieve interventie. Deze inzichten komen uit een grote hoeveelheid effectevaluaties die zijn uitgevoerd op het gebied van criminaliteitspreventie en rehabilitatie van daders. Eerst gaan we in paragraaf 3.2 en 3.3 in op twee dominante rehabilitatietheorieën: het 'Risk-Need-Responsivity (RNR)'-model en het 'Good-Lives-Model' (GLM). Vervolgens schetsen we in paragraaf 3.4 de opkomst van evaluatieonderzoek en komen de belangrijkste inzichten uit grootschalige overzichtsstudies aan bod. Daarna zal in paragraaf 3.5 worden besproken wat er vanuit evaluatieonderzoek bekend is over effectieve interventies in Nederland. In paragraaf 3.6 volgt een overzicht van interventies gericht op daders van online criminaliteit. Ten slotte volgt in paragraaf 3.7 een kort resumé.

3.2 Het 'Risk-Need-Responsivity'-model en 'What Works'-beginselen

Het RNR-model voor criminaliteitspreventie en behandeling stelt dat een rehabilitatieprogramma om effectief te zijn, moet worden afgestemd op het risico dat de dader in herhaling valt ('Risk'), de criminogene behoeften van de dader ('Need') en de responsiviteit van de dader ('Responsivity') (Andrews et al., 1990). Aanvullend kunnen er drie andere principes aan het RNR-model worden toegevoegd waar een rehabilitatieprogramma aan dient te voldoen om effectief te zijn: het beginsel van behandelmodaliteit, het beginsel van programma-integriteit en het professionaliteitsbeginsel (Van der Laan, 2004). De beginselen tezamen worden ook wel de 'What Works'-beginselen genoemd (Van der Laan, 2004) en worden hier verder toegelicht.

Ten eerste wordt het risicobeginsel genoemd als voorwaarde voor een programma om resultaat te bereiken (Andrews et al., 1990; Van der Laan, 2004). Volgens het risicobeginsel dient de intensiteit van een programma te worden afgestemd op het risico dat de dader in herhaling valt. Een interventie met een intensief programma moet worden gebruikt voor personen die een hoog risico hebben om te recidiveren. Personen die een laag risico lopen om te recidiveren, kunnen het best worden toegewezen aan een minimaal programma. Een goede afstemming van de intensiteit en duur van de interventie op dit recidiverisico zorgt voor een grotere effectiviteit van de interventie. Een slechte

afstemming tussen het risico en de intensiteit van een interventie kan er zelfs toe leiden dat personen meer criminaliteit gaan plegen (Lowenkamp & Latessa, 2004). Dit kan het geval zijn wanneer personen met een laag risico op recidive worden onderworpen aan intensieve behandeling en begeleiding.

Een tweede beginsel is het *behoeftebeginsel,* dat stelt dat effectieve interventies gericht moeten zijn op de criminogene, dynamische behoeften van een dader (Andrews et al., 1990; Van der Laan, 2004). Criminogene behoeften zijn factoren of problemen van personen die rechtstreeks samenhangen met het delinquente gedrag van de persoon, zoals antisociaal gedrag of drugsgebruik. Dynamische risicofactoren zijn factoren die kunnen worden beïnvloed, zoals de sociale vaardigheden of kennis van de dader. Statische risicofactoren zijn daarentegen niet te beïnvloeden, zoals geslacht en leeftijd (Van der Laan, 2004). Een interventie dient zich dus te richten op veranderbare factoren die rechtstreeks samenhangen met het gepleegde delict.

Ten derde moet er volgens het *responsiviteitsbeginsel* een match zijn tussen de dader, de uitvoerder van het programma en het programma zelf (Andrews et al., 1990; Van der Laan, 2004). Zo moet het programma dat wordt aangeboden aansluiten bij de intellectuele en sociale vaardigheden van de dader (Van der Laan, 2004). Met betrekking tot de match tussen de dader en uitvoerder suggereert onderzoek uit de psychiatrie dat enkel de aandacht voor een patiënt, zonder dat die patiënt wordt behandeld, al een groot effect heeft (Harte, 2019). De persoonlijke behandelrelatie zou dan ook tot verbetering kunnen leiden. Rovers (2007) verwijst in dit kader naar het belief-effect, dat stelt dat wanneer iemand verwacht of gelooft in een specifieke toekomstige werkelijkheid, dit de kans vergroot dat deze werkelijkheid daadwerkelijk zal plaatsvinden. De professional die de interventie uitvoert, heeft hierin een belangrijke rol. Zijn of haar houding, gebruikte methodieken en ervaringen leiden namelijk tot belief-effecten die invloed hebben op de uitkomst van de interventie. Dat de persoon van de behandelaar belangrijk is voor de uitkomsten van een interventie kan ook 'who works' worden genoemd, verwijzend naar de what works beginselen (De Jong & Denkers, 2020).

Een vierde beginsel is die van *behandelmodaliteit,* en impliceert dat een programma zich bij voorkeur richt op meerdere criminogene factoren en daarbij ook verschillende methodieken gebruikt (Van der Laan, 2004). Cognitieve en gedragsgeoriënteerde methoden zijn volgens onderzoek het meest succesvol in het tot stand brengen van blijvende veranderingen in het gedrag (o.a. Lipsey et al., 2001; Van der Laan, 2004). Deze methoden laten personen inzien hoe hun gedrag tot stand komt en richten zich op de ontwikkeling of versterking van (sociale) vaardigheden van de personen. Daarnaast leidt beloning van gewenst gedrag tot betere resultaten dan bestraffing van ongewenst gedrag.

Het vijfde beginsel betreft het beginsel van *programma-integriteit* en heeft betrekking op de ontwikkeling, opzet en uitvoering van een interventie (Van der Laan, 2004). Ef-

fectieve programma's moeten zijn ontwikkeld op basis van theoretische verklaringen van crimineel gedrag die ook daadwerkelijk zijn getoetst. De uitvoering van een programma moet vervolgens verlopen zoals van tevoren is bepaald en daarbij dienen alle onderdelen van een programma te worden uitgevoerd. De kwaliteit van de uitvoering – ook wel implementatie genoemd – is namelijk bepalend voor de effectiviteit van een interventie (Durlak & Dupre, 2008; Lipsey, 2009). Er is echter discussie of interventies volledig moeten worden geïmplementeerd zoals beoogd of dat aanpassingen aan lokale behoeften en voorkeuren toe moeten worden gelaten of zelfs moeten worden aangemoedigd (Durlak & Dupre, 2008; Nas et al., 2011). Enige mate van vrijheid voor uitvoerders lijkt wenselijk en kan zelfs leiden tot een effectievere interventie. Echter de theoretisch belangrijke componenten van de interventie dienen volledig te worden uitgevoerd zoals beoogd (Durlak & Dupre, 2008). Ten slotte stelt het *professionaliteitsbeginsel* dat een programma dient te worden uitgevoerd door professionals die goed zijn opgeleid en getraind (Van der Laan, 2004).

Vanuit de literatuur worden er ook enkele kanttekeningen geplaatst bij de 'what-works'-benadering (Van der Laan, 2004; Rovers, 2007; Harte, 2019). Ten eerste kan het werken volgens de 'what-works'-beginselen op gespannen voet komen te staan met bepaalde juridische beginselen zoals rechtsgelijkheid, proportionaliteit en legaliteit (Van der Laan, 2004; Rovers, 2007). Zo stelt het gelijkheidsbeginsel dat gelijke gevallen gelijk behandeld dienen te worden. Een sterk op het individu afgestemde interventie kan hiermee in strijd zijn. Ten tweede kunnen 'what-works'-beginselen ook elkaar in de weg staan (Rovers, 2007; Harte, 2019). Zo is er een spanning tussen het uitvoeren van een interventie zoals deze van tevoren is bepaald (programma-integriteit) en het afstemmen van de interventie op individuele behoeften en capaciteiten (responsiviteit). Een derde kanttekening is dat de 'what-works'-beginselen sterk gericht zijn op speciale preventie[5] (Van der Laan, 2004). Naast preventie bij een individuele dader zijn er echter ook andere strafdoelen zoals vergelding, generale preventie en normbevestiging.[6] Ten vierde kunnen de 'what-works'-beginselen worden aangemerkt als algemeen, waardoor de beginselen lastig zijn te operationaliseren en weinig sturing geven voor implementatie in de praktijk (Ferguson, 2002; Rovers, 2007). Het biedt bijvoorbeeld geen uitkomst bij dilemma's rondom de eerdergenoemde spanning tussen de responsiviteit en programma-integriteit van een interventie. Ten slotte stelt Rovers (2007) dat een te sterke nadruk op de 'what-works'-beginselen ervoor zorgt dat er weinig ruimte wordt overgelaten voor innovatie. De beginselen zijn gebaseerd op kennis uit het verleden en laten daarbij weinig ruimte om nieuwe inzichten of theoretische paden te ontdekken.

5 Speciale preventie richt zich op het voorkomen van recidive bij een individuele dader.
6 Bij vergelding beoogt een straf leed toe te voegen, generale preventie verwijst naar normbevestiging en afschrikking. Normbevestiging verwijst op haar beurt naar het bevestigen van geldende regels.

3.3 Het 'Good-Lives-Model'

Een tweede rehabilitatietheorie die vaak aangehaald wordt om uit te leggen hoe therapeutische behandelingen op effectieve wijze recidive kunnen terugdringen, is het 'Good-Lives-Model' (GLM) (Ward & Stewart, 2003; Ward & Brown, 2004). Het GLM stelt dat recidive kan worden voorkomen als een programma in staat is om deelnemers handvatten te bieden waarmee zij een bevredigender leven kunnen leiden (Ward & Stewart, 2003). Volgens de theorie van het GLM richt het RNR-model van Andrews et al. (1990) zich enkel op risicofactoren en te weinig op versterkende of positieve factoren. Waar het RNR-model wordt gezien als een 'risk-based'-model, wordt het GLM gezien als een 'strength-based'-model (Ward & Brown, 2004; Whitehead et al., 2007; Wormith et al., 2007). Het GLM is onderdeel van de opkomst van de positieve psychologie, een stroming binnen de psychologie die er voor pleit dat behandelprogramma's zich niet alleen moeten richten op tekortkomingen van personen, maar ook op de sterktes van personen om succesvol te zijn (Seligman, 2002; Wormith et al., 2007). Personen dienen door een behandeling in staat te worden gesteld om een voorspoedig leven te leiden met een betere gezondheid, welzijn en betekenis (Wormith et al., 2007).

Het GLM stelt dus dat een behandelprogramma deelnemers beter in staat moet stellen om in hun basisbehoeften te voorzien zodat recidive kan worden voorkomen (Ward & Stewart, 2003; Ward & Brown, 2004). Volgens de theorie zijn mensen van nature geneigd om deze basisbehoeften te vervullen. Voorbeelden van basisbehoeften zijn leven (een gezond leven en fysiek optimaal functioneren), kennis, uitblinken in spel en werk (meesterschap), zelfstandigheid (vermogen tot handelen), innerlijke rust (vrij zijn van emotionele opschudding en stress), vriendschap, gemeenschap, spiritualiteit (betekenis geven aan het leven), geluk en creativiteit (Ward & Brown, 2004). Wanneer niet of slechts gedeeltelijk in de basisbehoeften wordt voorzien, dan resulteert dat in een lagere mate van welzijn.

Of deelnemers kunnen voorzien in hun basisbehoeften op een manier waarop individueel welzijn kan worden gestimuleerd, is afhankelijk van interne capaciteiten (zoals vaardigheden, competenties, overtuigingen en attitudes) en externe omstandigheden (zoals een goede opvoeding en sociale ondersteuning) (Ward & Stewart, 2003; Ward & Brown, 2004; Ward & Gannon, 2006). Een interventie dient zich volgens het GLM naast het verminderen of vermijden van risico's ook te richten op het ontwikkelen of versterken van de interne en externe condities die voor een individu nodig zijn om zijn of haar 'goede leven' te kunnen leiden. Eerst moeten obstakels (risicofactoren) worden geïdentificeerd en vervolgens dient de deelnemer te worden voorzien van vaardigheden, overtuigingen en ondersteuning om de invloed van deze obstakels tegen te gaan. Hierbij dient rekening te worden gehouden met de unieke omstandigheden, talenten, voorkeuren en sterke punten van het individu (Ward & Brown, 2004).

Ten slotte benadrukt het GLM het belang van 'treatment readiness' als een voorwaarde voor een effectieve interventie (Ward & Brown, 2004); het aanwezig zijn van kenmerken binnen de deelnemer of therapeutische setting die betrokkenheid bevorderen en daarmee de kans op gedragsverandering door de interventie vergroten (Ward et al., 2004). Hiermee wordt verwezen naar het 'Multi Offender Readiness Model' (Ward et al., 2004), waarbij een deelnemer kan worden aangemerkt als gereed of bereid als hij of zij gemotiveerd is, in staat is om te reageren op de behandeling, de behandeling betekenisvol vindt en de capaciteiten heeft om succesvol een programma te voltooien (Howells & Day, 2003).

Er zijn ook kanttekeningen te plaatsen bij de GLM-benadering. Zo is het ten eerste onduidelijk of een rehabilitatiebenadering vanuit het GLM effectiever is dan andere benaderingen in het terugdringen van recidive (Wormith et al., 2007). Er is nog weinig empirisch onderzoek dat het effect van GLM-behandelingen aantoont op recidive (Looman & Abracen, 2013). Looman en Abracen (2013) merken op dat de principes uit de positieve psychologie nog niet getest zijn in de forensische psychologie. Daarnaast wordt er ook uitgebreid gediscussieerd over of er wel fundamentele, betekenisvolle verschillen zijn tussen het GLM en het RNR-model (Wormith et al., 2007; Andrews et al., 2011; Looman & Abracen, 2013). Sommige auteurs stellen dat het RNR-model ook al gericht was op versterkende factoren en dat er dat het GLM dan ook weinig heeft toegevoegd aan het bestaande model (Andrews et al., 2011). Andere auteurs stellen dat er wel degelijk fundamentele verschillen zijn tussen de twee modellen (Ward et al., 2012; Looman & Abracen, 2013).

3.4 Lessen uit evaluatieonderzoek

Studies van Martinson (1974) en Lipton en collega's (1975) worden in de interventieliteratuur als een soort startpunt gezien voor een grote hoeveelheid vervolgonderzoek naar effectieve interventies (Lipsey, 2007; Rovers, 2007; Wartna et al., 2013; Weisburd et al., 2017). Martinson (1974) concludeerde namelijk dat de tot dan toe uitgevoerde pogingen om daders te resocialiseren geen merkbaar effect hadden op recidive. Het idee dat niks werkte leidde tot veel kritiek op rehabilitatieprogramma's en heeft er voor gezorgd dat er sinds de jaren tachtig een grote hoeveelheid evaluatiestudies zijn uitgevoerd om te onderzoeken welke factoren van een programma wel kunnen zorgen voor effectiviteit (bijvoorbeeld Andrews et al., 1990; Farrington & Welsh, 2005; Lipsey & Cullen, 2007; Wormith et al., 2007; Lipsey, 2009; Koehler et al. 2013; Weisburd et al., 2017). De meeste van de evaluatiestudies betreffen meta-analyses, een methode waarbij onderzoeksresultaten van grote hoeveelheden relevante studies worden samengevat in een kwantitatieve maat; de gemiddelde effectgrootte (Rovers, 2007).

De uitgevoerde meta-analyses tonen aan dat er wel degelijk interventies zijn die bijdragen aan criminaliteitspreventie. Zo laat een recente studie van Weisburd en collega's (2017) zien dat er in verschillende gebieden van criminaliteitspreventie consistent be-

wijs is gevonden voor programma's die werken. Voorbeelden zijn programma's op het gebied van politiewerk, rehabilitatieprogramma's, gemeenschapsinterventies en situationele preventie. Er zijn echter ook veel programma's die niet werken (Weisburd et al., 2017). Zo is bijvoorbeeld bekend dat gevangenisstraf niet bijdraagt aan recidivevermindering (Cullen et al., 2011). Een ander belangrijk inzicht is dat sommige interventies zelfs schade toe kunnen brengen aan de personen die eraan deelnemen (McCord, 2003). Een bekend voorbeeld hiervan is het 'Scared Straight'-programma, waarin jeugdige delinquenten of risicojongeren gevangenissen bezoeken (Petrosino, 2003). Tijdens deze bezoeken wordt jongeren duidelijk gemaakt hoe verschrikkelijk het leven in detentie is, met het idee dat dit hen zou afschrikken om criminaliteit te plegen. Het onderzoek van Petrosino (2003) laat echter zien dat 'Scared Straight' en soortgelijke interventies juist een negatief effect kunnen hebben op de deelnemers en de kans vergroten dat jongeren criminaliteit plegen.

In verschillende meta-analyses is specifiek gekeken naar effecten van interventies op recidive van individuele daders die een delict hebben gepleegd (Lipsey & Cullen, 2007; Wormith et al., 2007; Lipsey, 2009; Koehler et al., 2013). Dergelijke interventies zijn gericht op effecten in de vorm van speciale preventie, waarbij het gedrag van een individuele dader wordt veranderd om toekomstig crimineel gedrag te voorkomen (Van der Laan, 2004). Een duidelijke conclusie die uit de onderzoeken naar voren komt, is dat interventies die zijn gestoeld op therapeutische benaderingen effectiever zijn dan interventies die zijn gebaseerd op toezicht en sanctionering. Interventies die gestoeld zijn op toezicht en sanctionering gebruiken controle, dwang, afschrikking en disciplinering om recidive te voorkomen. Interventies vanuit een therapeutische benadering bestaan daarentegen uit begeleiding, advies geven en het trainen van vaardigheden. Therapeutische benaderingen zijn doorgaans effectief in het verminderen van recidive bij zowel volwassenen (Wormith et al., 2007) als jongeren (Lipsey, 2009). Wel wordt opgemerkt dat er een aanzienlijke variatie te vinden is in de effecten van dergelijke op rehabilitatie gerichte behandelingen (Lipsey & Cullen, 2007). Deze variatie hangt samen met het type behandeling, de kwaliteit van de implementatie en de aard van de daders op wie de behandeling zich richt (Lipsey & Cullen, 2007).

3.5 Evaluatieonderzoek in Nederland

Ook in Nederland is onderzoek verricht naar effectieve interventies met behulp van meta-analyses. In dit kader is het onderzoek van Wartna et al. (2013) relevant. In deze meta-analyse zijn alle beschikbare recidivestudies op Nederlands taalgebied meegenomen. De auteurs identificeerden 141 empirische studies naar de effectiviteit van interventies. Van de 141 empirische studies maakten 83 studies gebruik van een controlegroep om de recidivecijfers van deelnemers van de interventie, de experimentele groep, mee te vergelijken. Alleen deze studies zijn in de meta-analyse meegenomen. De resultaten laten zien dat in 26 van de 83 studies een significant lager recidiveniveau te zien is bij de experimentele groep dan bij de controlegroep. Een andere bevinding is dat bij

18 van de onderzochte interventies de experimentele groep een significant hoger recidiveniveau bleek te hebben dan de controlegroep. Deze interventies lijken dus een averechts effect te hebben (Wartna et al., 2013). In lijn met internationale literatuur (zie paragraaf 3.2) zijn in de bestudeerde Nederlandse interventies die zich richten op resocialisatie (behandeling en begeleiding) effectiever in het verminderen van recidive dan interventies die zijn gericht op afschrikking (Wartna et al., 2013).

In Nederland wordt belang geacht aan interventies die zijn gebaseerd op wetenschappelijke inzichten en aantoonbaar recidive terugdringen. In 2005 heeft het ministerie van Veiligheid en Justitie dan ook besloten om een commissie in te stellen die gedragsinterventies dient te toetsen: de Erkenningscommissie Justitiële Interventies (Ooyen-Houben et al., 2011). Op basis van verschillende kwaliteitscriteria kan de commissie bepalen of een interventie wordt erkend. De vier niveaus waarop de commissie een interventie erkend zijn: goed onderbouwd, effectief volgens eerste aanwijzingen, effectief volgens goede aanwijzingen of effectief volgens sterke aanwijzingen (Justitiële interventies, 2020). Sinds 2015 is de erkenning van interventies overgenomen door de Erkenningscommissie Justitiële Interventies. Op dit moment zijn er volgens deze commissie 32 erkende interventies, waarvan slechts twee interventies als effectief volgens goede aanwijzingen worden aangemerkt en twee interventies als effectief volgens sterke aanwijzingen (Justitiële interventies, 2020). Effectief volgens sterke aanwijzingen zijn de Multidimensionele familietherapie (MDFT) en de Multisysteem therapie (MST), bedoelt om probleemgedrag tegen te gaan bij jongeren tussen de 12 en 18 jaar oud. Deze zogenoemde systeemtherapieën richten zich niet alleen op de jongeren zelf, maar ook op de familie en de bredere sociale omgeving van de jongeren.

Een bekende justitiële interventie die in Nederland wordt ingezet voor jongeren is de Halt-interventie. De Halt-interventie is een mogelijkheid voor jongeren van 12 tot 18 jaar die een licht strafbaar feit hebben begaan om een strafblad te ontlopen (Ferwerda et al., 2006; Abraham & Buysse, 2013). Tijdens de Halt-interventie worden de jongeren zich bewust gemaakt van de gevolgen van hun gedrag (door middel van gesprekken, leer- en werkopdrachten) en krijgen zij de kans om eventuele schade te herstellen. Een van de doelen van de Halt-interventie is dat de jongeren niet opnieuw crimineel gedrag vertonen. Een uitgebreide effect-evaluatie in 2006 heeft laten zien dat jongeren die aan de Halt-interventie hebben deelgenomen na een jaar geen ander recidivepatroon vertonen dan jongeren die niet aan Halt hebben deelgenomen (Ferwerda et al., 2006). Naar aanleiding van dit onderzoek is Halt op verschillende aspecten vernieuwd. De conclusie van een procesevaluatie van de vernieuwde Halt-interventie is dat Halt op dit moment zodanig wordt uitgevoerd dat wel een positief effect verwacht kan worden (Abraham & Buysse, 2013). In hoeverre de Halt-interventie op dit moment recidive voorkomt, is echter op dit moment onduidelijk.

3.6 Interventies gericht op daders van online criminaliteit

Oosterwijk en Fischer (2017) voerden een systematische literatuurstudie uit naar alle beschikbare interventies gericht op de preventie en/of het tegengaan van online criminaliteit onder jongeren. De studie laat zien dat de meeste interventies zijn gericht op algemene populaties en daarmee ook op de preventie van slachtofferschap of daderschap onder potentiële daders. Interventies specifiek gericht op cybercriminelen die reeds een cyberdelict hebben begaan, zijn zeldzamer. Er worden door de onderzoekers vier dadergerichte hackinterventies geïdentificeerd.

Een eerste interventie die wordt genoemd is het gebruik van 'warning banners' (Maimon et al., 2014). Tijdens deze interventie worden personen die zichzelf illegaal toegang hebben verschaft tot computersystemen geïnformeerd over de strafbaarheid op het moment dat zij het systeem binnenkomen. Een experimenteel onderzoek met een controlegroep laat zien dat de 'warning banners' er voor zorgen dat daders minder lang in het systeem blijven, maar dat de banners er niet voor zorgen dat de daders hun hacking-activiteiten afbreken of dat zij minder snel geneigd zijn om nog een keer in hetzelfde systeem in te breken (Maimon et al., 2014). Een kanttekening bij de interventie is dat het onduidelijk is of de 'warning banners' worden gelezen door personen of dat het gaat om automatische aanvallen.

Twee andere interventies proberen daders op het rechte pad te houden door hen diensten of structuren aan te bieden waarmee daders op een verantwoorde en legale manier hun hack-activiteiten kunnen uitoefenen. Een van de interventies is 'duty to report' (Wible, 2003) en is te vergelijken met het 'responsible disclosure' beleid in Nederland (Weulen Kranenbarg et al., 2018a). Met dit beleid worden hackers uitgenodigd om kwetsbaarheden in ICT-systemen te rapporteren aan de eigenaar van het systeem, zonder de kwetsbaarheid met anderen te bespreken. De andere interventie is de 'hack-in-contest' (Wible, 2003). Dit is een wedstrijd waarin hackers uitgedaagd worden om een systeem te hacken van een partij die meedoet aan de wedstrijd. Vaak krijgt de persoon die het lukt een vergoeding of andere (symbolische) prijs (ook wel 'bug-bounty'-programma's genoemd). De interventies worden inhoudelijk geëvalueerd (planevaluatie) in de studie van Wible (2003), waarin 'hack-in-contests' worden geprefereerd boven 'duty to report', omdat 'duty to report' er niet in zou slagen om een duidelijk signaal af te geven dat hacken strafbaar is. Hackers zouden zelf kunnen bepalen of zij een melding doen of niet. De 'hack-in contest' daarentegen creëert een veilige omgeving waar hacken is toegestaan. Doordat het binnendringen van private systemen buiten deze omgeving verboden is, worden voorkeuren voor gedrag duidelijker gevormd. Het is onduidelijk wat het daadwerkelijke effect is van de zojuist genoemde interventies.

De vierde interventie richt zich op jeugdige hackers en maakt gebruik van de 're-integrative shaming theorie' (Kao et al. 2009). 'Shaming' kan worden gedefinieerd als alle sociale processen waarin afkeuring wordt geuit, die als gevolg berouw of schaamte op-

roepen bij de persoon die wordt afgekeurd of veroordeeld. 'Re-integrative' shaming veroordeelt niet *de persoon* in het *openbaar*, maar *het strafbare feit* in een *besloten setting,* zodat de persoon de mogelijkheid krijgt om terug te keren in de gemeenschap. Resultaten van de studie van Kao en collega's suggereren dat re-integrative shaming negatieve gevolgen kan hebben wanneer jongeren vasthouden aan hun geloof in de huidige hackers-ethiek. Jongeren moeten daarom volgens de auteurs eerst worden geleid richting een volwassener hackers-ethiek waarin een duidelijk onderscheid wordt gemaakt tussen de definities van een 'computer intruder' en een 'ethical hacker', zodat re-integrative shaming tot betere resultaten kan leiden. Onduidelijk blijft of een interventie gebaseerd op 're-integrative shaming' waarbij jongeren richting een andere hackersethiek worden geleid effectief is in het terugdringen van recidive.

Op basis van de overzichtsstudie van Oosterwijk en Fischer (2017) kan worden geconcludeerd dat er ten tijde van dat onderzoek geen effectief geëvalueerde interventie was gericht op daders van cybercriminaliteit. Wel geven Oosterwijk en Fischer en daarna Van der Wagen en collega's (2019) aan dat er aanknopingspunten zijn voor potentieel effectieve interventies voor (jeugdige) cyberdaders. Vooral interventies die zich richten op bewustwording worden als potentieel effectief gezien. De gedachte is dat daders bewust moeten worden gemaakt van de schadelijkheid van hun gedrag voor anderen en voor henzelf. 'Mentaliseren' (inleven in de ander) zou hiervoor als specifieke methode geschikt kunnen zijn. Daarnaast zouden interventies voor hackers gericht moeten zijn op kansen voor de jongeren, door hen uitdagende, legale alternatieven aan te bieden. Andere elementen die belangrijk zouden zijn voor effectieve interventies zijn snel handelen, in contact blijven met de daders door controlerende instanties, en het betrekken van leeftijdsgenoten bij de interventie. Ten slotte worden ook traditionele interventies die zich richten op specifieke criminogene factoren zoals verslaving, schulden of gebrek aan sociale vaardigheden als mogelijk effectief benoemd voor jongere en oudere cybercriminelen die andere drijfveren hebben dan nieuwsgierigheid en mentale uitdaging. Wel wordt opgemerkt dat de effectiviteit van de traditionele interventies tegen kan vallen omdat de bestaande interventies niet inspelen op de online context van de problematiek.

Ondanks dat er geen effectieve interventies zijn voor daders van cybercriminaliteit, zijn er wel verschillende initiatieven die (nog) niet geëvalueerd zijn. Zo worden jongeren die door de politie worden gearresteerd voor cyberdelicten in het Verenigd Koninkrijk door de 'National Crime Agency' (NCA) naar zogenoemde 'rehab-camps' gestuurd (Ward, 2017). Gedurende een tweedaagse bijeenkomst leren de jongeren daar hoe zij hun vaardigheden op een positieve, legale manier in kunnen zetten. Hiervoor worden de jongeren ingelicht over het verantwoordelijk inzetten van vaardigheden en vertellen professionals die werkzaam zijn bij cybersecuritybedrijven over hun werk. Een andere interventie die ook door de NCA wordt gebruikt zijn zogenoemde 'knock-and-talk' of 'cease-and-desist' bezoeken bij personen die in beeld zijn gekomen tijdens opsporingsonderzoeken (NCA, 2017; Chan, 2019). Tijdens deze interventies brengen

politieagenten een bezoek aan het huis van jongeren om hen te waarschuwen dat zij in beeld zijn bij opsporingsinstanties.

3.7 Resumé

In dit hoofdstuk is inzicht gegeven in factoren die kunnen bijdragen aan een effectieve interventie. In de literatuur worden twee dominante rehabilitatie theorieën onderscheiden: het 'Risk-Need-Responsivity'-model (RNR) en het 'Good-Lives-Model' (GLM). Het RNR-model stelt dat een effectief programma moet worden afgestemd op het risico dat de dader in herhaling valt, de criminogene behoeften van de dader en de responsiviteit van de dader. Het GLM stelt dat recidive kan worden teruggedrongen wanneer een programma in staat is om de deelnemer aanknopingspunten te bieden waarmee hij of zij een bevredigender leven kan leiden. Uit evaluatieonderzoek is gebleken dat er verschillende interventies bestaan die recidive bij daders van criminaliteit kunnen verminderen, maar dat zeker niet alle interventies effectief zijn en dat er zelfs interventies zijn die de kans op recidive bij daders kunnen vergroten. Interventies die zijn gebaseerd op therapeutische benaderingen (begeleiding, advies geven en het trainen van vaardigheden) zijn doorgaans effectiever in het verminderen van recidive dan interventies die zijn gericht op toezicht en sanctionering. Ook in Nederlandstalige effectstudies blijft deze conclusie overeind. Uit de literatuur is verder duidelijk geworden dat er tot op heden geen effectieve dadergerichte interventies zijn op het gebied van online criminaliteit.

4. Methoden

4.1 Inleiding

In dit onderzoek staat de interventie 'Hack_Right' centraal en wordt deze interventie geëvalueerd. In dit hoofdstuk wordt verantwoord op welke wijze het onderzoek is uitgevoerd. Allereerst komen in paragraaf 4.2 het onderzoeksdoel en de onderzoeksvragen aan bod. Vervolgens staan in paragraaf 4.3 de gebruikte onderzoeksmethoden centraal. Ten slotte bespreekt paragraaf 4.4 de beperkingen van de gebruikte onderzoeksmethoden.

4.2 Onderzoeksdoel en -vragen

Het doel van dit onderzoek is om Hack_Right en de tot nu toe uitgevoerde Hack_Right-trajecten te evalueren. Uit de voorgaande hoofdstukken blijkt dat een interventie op verschillende manieren kan worden geëvalueerd. Gebruikelijke vormen van evaluatie zijn de planevaluatie, procesevaluatie en effectevaluatie. Aangezien Hack_Right pas kortgeleden is gestart en er slechts een beperkt aantal casussen is afgerond, is het op dit moment niet mogelijk om een effectevaluatie uit te voeren. Het huidige onderzoek omvat daarom een planevaluatie en een procesevaluatie. Daarnaast worden de ervaringen van alle betrokkenen met betrekking tot de mogelijke effecten van de interventie onderzocht.

Voor de planevaluatie is onderzocht wat Hack_Right is, wat de doelen van de interventie zijn, welke partijen aan de interventie samenwerken en hoe de interventie theoretisch is onderbouwd. De onderzoeksmethoden die zijn gebruikt voor de planevaluatie zijn de analyse van beschikbare beleidsdocumenten en wetenschappelijke literatuur en interviews met de interventieontwikkelaars.

De procesevaluatie zoomt vervolgens in op hoe de tot nu toe uitgevoerde Hack_Right-trajecten zijn uitgevoerd in de praktijk en in hoeverre dit overeenkomt met de plannen die van tevoren zijn gemaakt. Een procesevaluatie kan worden opgedeeld in drie verschillende onderdelen: bereik, programma-integriteit en dosering (Durlak & DuPre, 2008; Sondorp et al., 2019). Om het bereik van de interventie te onderzoeken, is gekeken of de beoogde doelgroep wordt bereikt. Vervolgens is onderzocht in welke mate de interventie wordt uitgevoerd zoals beoogd (programma-integriteit). Ten slotte is bekeken of de interventie met voldoende intensiviteit en compleet wordt uitgevoerd (dosering). Voor de

procesevaluatie zijn registraties van individuele Hack_Right-trajecten geanalyseerd en interviews afgenomen met toewijzers, uitvoerders en deelnemers van de interventie.

De ervaringen van de betrokkenen zijn in kaart gebracht door de gevolgen voor deelnemers na het afronden van de interventie en het oordeel van betrokkenen over de interventie te onderzoeken. Hiervoor zijn interviews afgenomen met uitvoerders van de interventie en met jongeren die aan de interventie hebben deelgenomen. De verschillende onderzoeksmethoden die zijn gebruikt worden verder toegelicht in paragraaf 4.3.

Onderzoeksvragen

Op basis van de literatuur over evaluatieonderzoek zijn de volgende onderzoeksvragen geformuleerd:

1. Wat is Hack_Right en hoe is Hack_Right theoretisch onderbouwd?
   a) Waarom en hoe is Hack_Right ontstaan?
   b) Wat is de definitie van Hack_Right?
   c) Wat is het doel van Hack_Right?
   d) Hoe is Hack_Right theoretisch onderbouwd?
   e) Wat is de doelgroep van Hack_Right?
   f) Hoe ziet de inhoud/invulling van Hack_Right eruit?
   g) Welke partijen zijn betrokken bij de opzet en uitvoering van Hack_Right?
   h) Hoe past Hack_Right in het huidige strafrechtsysteem?

2. Hoe zijn de tot nu toe uitgevoerde Hack_Right-trajecten verlopen?
   a) Wordt in de tot nu toe uitgevoerde Hack_Right-trajecten de beoogde doelgroep bereikt?
   b) Verloopt het programma van de tot nu toe uitgevoerde Hack_Right-trajecten volgens plan?
   c) Zijn de tot nu toe uitgevoerde Hack_Right-trajecten voldoende intensief en compleet uitgevoerd?

3. Hoe hebben alle betrokkenen de tot nu toe uitgevoerde Hack_Right-trajecten ervaren?
   a) Worden de gestelde doelen voor de deelnemers van Hack_Right behaald?
   b) Welke mogelijke positieve of negatieve gevolgen zijn er volgens betrokkenen voor deelnemers van Hack_Right?
   c) Hoe verloopt het contact tussen uitvoerders en deelnemers van Hack_Right?
   d) Hoe tevreden zijn personen die betrokken zijn geweest bij de tot nu toe uitgevoerde Hack_Right-trajecten?
   e) Wat zijn bevorderende en belemmerende factoren voor een goed verloop van Hack_Right volgens betrokkenen?

4.3 Onderzoeksmethoden

Voor de evaluatie van Hack_Right zijn kwalitatieve onderzoeksmethoden gebruikt. Kwalitatief onderzoek is een geschikte methode om de werkelijkheid van binnenuit te bestuderen en zodoende zicht te krijgen op de verschillende processen die een rol spelen bij een fenomeen (Decorte & Zaitch, 2016). Daarnaast is er maar een klein aantal deelnemers dat Hack_Right tot op heden heeft gevolgd, waardoor kwantitatief onderzoek nog niet haalbaar is. Om een complex fenomeen zoals de Hack_Right-interventie te kunnen onderzoeken en daarbij sterke en zwakke punten van de interventie bloot te leggen, zijn kwalitatieve onderzoeksmethoden dan ook geschikt. Voor het onderzoek zijn twee kwalitatieve onderzoeksmethoden gebruikt: documentanalyse en interviews. De onderzoeksmethoden worden hierna uitgebreid besproken. In tabel 1 staat een overzicht van welke methoden gebruikt zijn om iedere onderzoeksvraag te beantwoorden.

Tabel 1: Methodenmatrix

	Documenten-analyse	Interviews ontwikkelaars	Interviews toewijzers	Interviews uitvoerders	Interviews deelnemers
Vraag 1a	X	X			
Vraag 1b	X	X	X	X	
Vraag 1c	X	X	X	X	
Vraag 1d	X	X			
Vraag 1e	X	X			
Vraag 1f	X	X			
Vraag 1g	X	X			
Vraag 1h	X	X			
Vraag 2a	X		X	X	X
Vraag 2b	X		X	X	X
Vraag 2c			X	X	X
Vraag 3a			X	X	
Vraag 3b				X	X
Vraag 3c				X	X
Vraag 3d			X	X	X
Vraag 3e			X	X	X

Documentanalyse

Het doel van de documentanalyse is om inzicht te krijgen in de plannen van Hack_Right, zoals die op papier staan. Zo kan worden onderzocht wat Hack_Right is, hoe Hack_Right theoretisch is onderbouwd en welke trajecten tot nu toe zijn uitgevoerd. Verschillende documenten zijn hiervoor geraadpleegd. Ten eerste is er vanuit de projectgroep Hack_Right een casusoverzicht aangeleverd van de Hack_Right-trajecten die

zijn aangemeld. In dit casusoverzicht is opgenomen door wie Hack_Right is opgelegd, via welke strafmodaliteit Hack_Right is gevolgd, welke strafrechtketenpartner betrokken is geweest, welke modules zijn gevolgd, hoe het traject is ingevuld, welk bedrijf of welke organisatie betrokken is geweest, wat de omvang van het traject was en of de casus afgerond is of nog loopt. Ten tweede zijn er projectplannen van Hack_Right geraadpleegd: 'Hack_Right projectplan 1.0' en 'Hack_Right projectplan 2.0'. Ten derde is het document 'Samenvatting literatuur Hack_Right' geanalyseerd om inzicht te krijgen in de theoretische onderbouwing van Hack_Right. Verder is het 'schema strafmodaliteiten' geraadpleegd waarin de verschillende strafmodaliteiten zijn opgenomen waarin Hack_Right kan plaatsvinden. Ten slotte is het document 'one-pager + checklist' geraadpleegd waarin verschillende selectiecriteria zijn opgenomen voor deelnemers van Hack_Right.

Interviews

Het doel van de interviews was drieledig. Ten eerste was het doel om in aanvulling op de beleidsdocumenten een beter inzicht te krijgen in de plannen omtrent Hack_Right. Een tweede doel was om inzicht te krijgen in het verloop van de tot nu toe uitgevoerde Hack_Right-trajecten. Het derde doel van de interviews was om de ervaringen met Hack_Right van alle betrokkenen in kaart te brengen. In totaal zijn 28 interviews afgenomen met respondenten die op verschillende manieren betrokken zijn bij de Hack_Right interventie: twee interventieontwikkelaars, vijf toewijzers, elf uitvoerders en tien deelnemers (zie tabel 2). De interviews duurden tussen de 53 minuten en 128 minuten. Alle interviews waren semigestructureerd. Dit betekent dat de meeste topics en vragen van tevoren zijn vastgesteld, maar dat er ook ruimte is overgelaten voor de interviewer om andere vragen te stellen en verder in te gaan op relevante zaken die ter sprake komen. Een overzicht van de interviewprotocollen die gebruikt zijn om de interviews af te nemen staan in bijlage 1.

Tabel 2: Overzicht respondenten

Code	Rol respondent	Organisatie	Geslacht	Duur
RE1	Uitvoerder	Reclassering	Man	1h16m
RE2	Uitvoerder	Reclassering	Man	1h11m
HA1	Uitvoerder	Halt	Man	1h8m
HA2	Uitvoerder	Halt	Vrouw	1h24m
CS1	Uitvoerder	(Cybersecurity-)organisatie	Man	1h12m
CS2	Uitvoerder	(Cybersecurity-)organisatie	Man	58m
CS3	Uitvoerder	(Cybersecurity-)organisatie	Man	53m
CS4	Uitvoerder	(Cybersecurity-)organisatie	Man	1h32m
CS5	Uitvoerder	(Cybersecurity-)organisatie	Man	56m
CS6	Uitvoerder	(Cybersecurity-)organisatie	Man	1h9m

Code	Rol respondent	Organisatie	Geslacht	Duur
CS7	Uitvoerder	(Cybersecurity-)organisatie	Man	55m
OM1	Toewijzer	Openbaar Ministerie	Vrouw & man[1]	1h23m
OM2	Toewijzer	Openbaar Ministerie	Vrouw	1h8m
OM3	Toewijzer	Openbaar Ministerie	Man	1h27m
OM4	Toewijzer	Openbaar Ministerie	Man	1h22m
OM5	Toewijzer	Openbaar Ministerie	Vrouw	1h37m
IO1	Ontwikkelaar	Politie	Vrouw	1h22m
IO2	Ontwikkelaar	Openbaar Ministerie	Vrouw	1h37m
DN1	Deelnemer	n.v.t.	Man	1h20m
DN2	Deelnemer	n.v.t.	Man	1h4m
DN3	Deelnemer	n.v.t.	Man	1h19m
DN4	Deelnemer	n.v.t.	Man	1h39m
DN5	Deelnemer	n.v.t.	Man	1h35m
DN6	Deelnemer	n.v.t.	Man	1h12m
DN7	Deelnemer	n.v.t.	Man	1h35m
DN8	Deelnemer	n.v.t.	Man	1h41m
DN9	Deelnemer	n.v.t.	Man	2h08m
DN10	Deelnemer	n.v.t.	Man	Onbekend[2]

1 Dit interview heeft plaatsgevonden met twee personen van het OM uit hetzelfde arrondissement.
2 Deze respondent is door een ander onderzoeksteam geïnterviewd en wij beschikken alleen over een uitgewerkt transcript. Voor meer informatie, zie de paragraaf 'Deelnemers Hack_Right'.

In tabel 2 staat een overzicht van alle respondenten. Hierna gaan we per doelgroep dieper in op de uitgevoerde interviews.

– *Ontwikkelaars*. Ten eerste zijn er twee interviews gehouden met personen die betrokken zijn geweest bij de ontwikkeling van de Hack_Right interventie. Een respondent is werkzaam bij de politie, de andere respondent is werkzaam bij het Openbaar Ministerie. De interviewonderwerpen en vragen die zijn gesteld tijdens de interviews met de interventieontwikkelaars zijn weergegeven in bijlage 1.1.
– *Toewijzers.* Er zijn vijf interviews gehouden met personen die betrokken zijn geweest bij de oplegging van de Hack_Right interventie aan deelnemers. Een van deze interviews betrof een interview met twee personen. De respondenten waren allen werkzaam bij het Openbaar Ministerie in de functie van (cyber)officier, parketsecretaris of interventiespecialist. Ook deze respondenten zijn benaderd via de projectgroep Hack_Right. In bijlage 1.2 is een overzicht van de verschillende interviewonderwerpen en vragen die zijn gesteld tijdens de interviews met toewijzers van de interventie.
– *Uitvoerders Hack_Right*. Er zijn elf interviews gehouden met personen die betrokken zijn bij de uitvoering van de interventie. Vier van de elf respondenten zijn werkzaam bij toezichthoudende instanties. Er zijn twee respondenten geïnterviewd

die werkzaam zijn bij Reclassering Nederland en twee respondenten die werkzaam zijn bij Halt. De overige zeven respondenten zijn werkzaam bij praktijkorganisaties (bedrijven die raakvlakken hebben met cybersecurity en cybercriminaliteit) die de jongeren verder hebben begeleid. Vanuit de projectgroep Hack_Right is aan uitvoerders gevraagd of zij bereid waren mee te werken aan een onderzoek naar de interventie Hack_Right. Zodra instemming was verkregen, konden de contactgegevens gedeeld worden met de onderzoekers om afspraken in te plannen. Voor de selectie van respondenten zijn de onderzoekers daarom afhankelijk geweest van projectgroep Hack_Right en de bereidheid van deelnemers. Zo werd bijvoorbeeld bekend dat er na twee interviews met Halt-medewerkers geen nieuwe interviews meer konden worden afgenomen, omdat er vanuit Halt werd aangegeven dat respondenten al veelvuldig belast zijn geweest met het meewerken aan onderzoeken of gesprekken omtrent de Hack_Right interventie. Buiten deze signalen van Halt zijn er naar kennis van de onderzoekers geen respondenten of organisaties geweest die niet wilden meewerken aan het onderzoek. De interviewonderwerpen en vragen die tijdens de interviews met uitvoerders van de interventie zijn gesteld zijn weergegeven in bijlage 1.3.

– *Deelnemers Hack_Right*. In totaal zijn tien van de veertien deelnemers geïnterviewd die ten tijde van het onderzoek Hack_Right hebben afgerond. Zeven van de deelnemers zijn specifiek geworven voor dit onderzoek. Drie andere deelnemers zijn geworven en geïnterviewd voor een ander onderzoek naar cybercriminaliteit dat gelijktijdig liep (Van der Wagen e.a., 2019). Om de jongeren niet onnodig te belasten, zijn door Van der Wagen en collega's[7] vragen over Hack_Right gesteld aan de respondenten. De uitgewerkte gespreksverslagen zijn – nadat ze geanonimiseerd waren – gedeeld met het onderzoeksteam van onderhavig onderzoek. Toegang en contactgegevens van zes deelnemers die specifiek zijn geworven voor onderhavig onderzoek zijn verkregen via Reclassering Nederland of Halt. Vanuit deze organisaties is aan deelnemers die Hack_Right hebben afgerond, gevraagd of ze mee wilden werken met het onderzoek. Verder zijn er nog twee Hack_Right deelnemers geweest die in eerste instantie aan Reclassering Nederland of Halt hebben aangegeven hebben dat ze wilden meewerken, maar waarmee de onderzoekers geen contact gekregen hebben (de jongeren reageerden niet op het verzoek tot contact via de door hen opgegeven e-mailadressen of telefoonnummers). Een respondent is geworven vanuit het netwerk van de onderzoekers. Deze respondent heeft Hack_Right dus afgerond voordat onze dataverzamelingsperiode begon. Alle deelnemers (en ouders bij jongeren onder de 18 jaar) hebben een informed consent ondertekend (zie bijlage 1.5). Het interviewprotocol is weergegeven in bijlage 1.4. Alle respondenten waren mannen, met leeftijden tussen de 15 en 20 jaar ten tijde van het interview.

7 Zie Van der Wagen e.a. (2019) voor een uitgebreide methodische verantwoording.

Toestemming ethische commissie
Aangezien voor dit onderzoek jongeren zijn geïnterviewd die Hack_Right hebben doorlopen, is voorafgaand aan het onderzoek toestemming gevraagd aan de ethische commissie van de Vrije Universiteit Amsterdam.[8] De ethische commissie heeft goedkeuring gegeven voor het onderzoek. Belangrijke aspecten van de aanvraag waren:

– *Toestemmingen*. Om in contact te kunnen komen met de respondenten was medewerking van de reclassering vereist. De reclassering is betrokken bij het Hack_Right initiatief en heeft aangegeven medewerking te verlenen. De reclassering vroeg de beoogde respondenten na afronding van Hack_Right of ze geheel vrijwillig mee wilden werken aan onderhavig onderzoek. De beoogde respondenten konden dan contact opnemen met de onderzoeker of na ondertekening van een informed consent formulier hun telefoonnummer en/of e-mailadres doorgeven aan de onderzoeker. In het geval van een minderjarige respondent moest ook een ouder of voogd het informed consent formulier ondertekenen. In alle gevallen hebben respondenten voorafgaand aan het interview (nogmaals) het informed consent formulier met de onderzoeker doorgenomen en ingevuld (zie bijlage 1.5).
– *Anonimiteit*. Voordat een respondent medewerking toezegt heeft de onderzoeker geen informatie over de beoogde respondent. Na toestemming werd indien van toepassing een formulier met contactinformatie uitsluitend verstuurd via de beveiligde mailbox van het Openbaar Ministerie aan de onderzoeker. De onderzoeker plaatste het formulier vervolgens in het Secure Analytics Lab (SAL)[9] van het NSCR. De interviews worden opgenomen met een voicerecorder die geencrypt is. Derden kunnen dus niet de opnames beluisteren. De onderzoeker plaatste het audiobestand vervolgens in het Secure Analytics Lab (SAL) van het NSCR. Dit bestand werd uitgewerkt tot een interviewverslag dat volledig gepseudonimiseerd is (in lijn met de richtlijnen hieromtrent van het NSCR).
– *Risico voor respondent*. Het risico voor de respondent van deelname aan dit onderzoek kan worden geclassificeerd als nihil. De respondenten hebben een interventietraject afgerond, waardoor directe gezinsleden op de hoogte zijn. De interviews gaan over de ontwikkelpaden die hebben geleid tot het delict waarvoor ze zijn veroordeeld. De onderzoeker benadrukte dat respondenten geen informatie dienen te delen over eventuele andere strafbare feiten.

4.4 Beperkingen van de onderzoeksmethoden

De zojuist genoemde onderzoeksmethoden voor het onderzoek naar Hack_Right en de tot nu toe uitgevoerde Hack_Right trajecten kennen enkele beperkingen. Ondanks dat beide interventieontwikkelaars en het merendeel van zowel de uitvoerders als de

8 Zowel de Haagse Hogeschool als het NSCR heeft geen eigen ethische commissie, daarom maken NSCR onderzoekers standaard gebruik van de ethische commissie van de Vrije Universiteit Amsterdam.
9 Een gecertificeerd netwerk dat niet op internet is aangesloten. Binnen dit SAL wordt bij het NSCR alle gevoelige informatie opgeslagen. De informatie is alleen toegankelijk voor de onderzoeker.

deelnemers zijn geïnterviewd, heeft er toch een selectie van respondenten plaatsgevonden die zijn geïnterviewd. De onderzoekers waren voor contactgegevens van respondenten afhankelijk van andere partijen. De projectgroep Hack_Right heeft toewijzers en uitvoerders van de interventie benaderd en gevraagd of contactgegevens gedeeld konden worden met de onderzoekers. Daarnaast is er vanuit Halt aan de onderzoekers doorgegeven dat er slechts twee medewerkers geïnterviewd konden worden, omdat dit anders te veel tijd van medewerkers zou kosten. Ook met betrekking tot de deelnemers heeft er een selectie plaatsgevonden, doordat via Halt en de reclassering deelnemers zijn aangedragen die bereid waren mee te werken met het onderzoek. Aangezien niet alle toewijzers, uitvoerders en deelnemers zijn gesproken kan er een selectie*bias* hebben plaatsgevonden, waarbij de resultaten mogelijk een vertekend beeld geven.

Een tweede beperking heeft te maken met de validiteit van de antwoorden van respondenten. Zo is het mogelijk dat respondenten sociaal wenselijke antwoorden hebben gegeven. De beperking is geprobeerd te ondervangen door enerzijds open vragen te stellen en anderzijds zo veel mogelijk perspectieven te belichten, ook van bijvoorbeeld deelnemers. Echter blijft de validiteit van de antwoorden van respondenten lastig vast te stellen.

Een derde beperking van het onderzoek is dat er voor de mogelijke gevolgen van Hack_Right volgens respondenten alleen is gekeken naar gevolgen voor de deelnemers. Het blijft echter onduidelijk welke gevolgen de interventie Hack_Right bijvoorbeeld kan hebben voor slachtoffers of de samenleving.

Ten vierde is het onderzoek naar Hack_Right retrospectief, wat inhoudt dat er is teruggekeken op de tot nu toe uitgevoerde Hack_Right trajecten. Voor de interviews met respondenten betekent dit dat er vragen zijn gesteld over casussen die soms al geruime tijd geleden hebben plaatsgevonden. Enerzijds heeft dit soms geleid tot onvolledige antwoorden, anderzijds kan dit hebben geleid tot minder betrouwbare antwoorden.

5. Hack_Right: het plan

5.1 Inleiding

In dit hoofdstuk zullen de plannen, ideeën en aannames rondom Hack_Right in kaart worden gebracht op basis van een analyse van beleidsdocumenten en interviews met de interventieontwikkelaars (n=2). Zo wordt duidelijk wat Hack_Right is en hoe Hack_Right is onderbouwd. In dit hoofdstuk wordt eerst in paragraaf 5.2 besproken hoe Hack_Right is ontstaan. Vervolgens gaat paragraaf 5.3 in op de betekenis van Hack_Right, paragraaf 5.4 op de doelen van Hack_Right, paragraaf 5.5 op de theoretische onderbouwing van Hack_Right en paragraaf 5.6 op de doelgroep van Hack_Right. De inhoudelijke invulling van Hack_Right wordt besproken in paragraaf 5.7. Welke partijen er bij de interventie zijn betrokken, wordt duidelijk in paragraaf 5.8. Ten slotte geeft paragraaf 5.9 inzicht in het proces van instroom tot uitstroom van deelnemers van Hack_Right. Per paragraaf wordt steeds eerst beschreven hoe het onderwerp op papier in de beleidsplannen staat beschreven en vervolgens hoe dit zich in de praktijk heeft ontwikkeld volgens de interventieontwikkelaars. Het hoofdstuk sluit af met een resumé in paragraaf 5.10.

5.2 Aanleiding Hack_Right

In deze paragraaf wordt de aanleiding voor de ontwikkeling van Hack_Right beschreven. Het blijkt dat Hack_Right is ontstaan vanwege een toename in verdachten van computercriminaliteit, het afwijkende profiel van cybercrimedaders ten opzichte van traditionele daders en het gebrek aan werkzame interventies.

5.2.1 *Op papier*

Uit de projectplannen van Hack_Right (Projectplan 1.0, z.d.; Projectplan 2.0, 2018) volgen drie redenen die de aanleiding zijn geweest voor het opstarten van Hack_Right:

– Een toename in het aantal verdachten van computercriminaliteit.[10]

10 In bijlage 2 is een overzicht opgenomen van de verschillende delicten die volgens de definitie van het OM vallen onder computercriminaliteit, ook wel cybercrime in enge zin genoemd door het OM (Ministerie van Justitie en Veiligheid, 2018).

– Het profiel van cybercrime daders.
– Het gebrek aan werkzame interventies .

Ten eerste ziet het Openbaar Ministerie (OM) een toename in het aantal verdachten van computercriminaliteit dat bij hen instroomt in de leeftijdscategorie 12 tot 23 jaar. In de projectplannen staat dat de verwachting is dat deze toename van het aantal verdachten door zal zetten. Enerzijds door de intensivering van de aanpak computercriminaliteit door de politie en het OM, anderzijds door de verwachte toename in cybercrimedelicten als gevolg van technologische ontwikkelingen en de achterblijvende mate van beveiliging van burgers en organisaties.

Ten tweede wordt in de plannen genoemd dat cybercriminelen een nieuwe groep daders betreft, die verschillen van traditionele criminelen. Zo wordt er gesteld dat cybercriminelen jonger zijn dan verdachten van vergelijkbare traditionele criminaliteit. De jongeren zouden zich niet altijd bewust zijn van de grote consequenties die hun daden kunnen hebben, doordat grenzen in de online wereld niet zo duidelijk zijn als in de fysieke wereld. Naast het verschil in leeftijd wordt gesteld dat de jongeren de cyberdelicten veelal plegen vanwege intrinsieke motieven zoals nieuwsgierigheid, uitdaging, indruk maken op leeftijdsgenoten, bij een groep willen horen of vanwege politieke motieven (op basis van: Weulen Kranenbarg, 2018; NCA, 2017). Bij traditionele vormen van criminaliteit zoals winkeldiefstal zou het eerder gaan om financiële motieven en/of druk van vrienden (Weulen Kranenbarg, 2018). In de projectplannen wordt verder verwezen naar andere verschillen tussen cyber- en traditionele criminaliteit die naar voren komen in studies van Weulen Kranenbarg (2018) en Janssen (2017). Het projectplan 1.0 gaat bovendien verder in op daderprofielen. Er zijn meerdere daderprofielen te onderscheiden op basis van leeftijd, technische kennis en motieven. Aan de ene kant van het spectrum zijn er oudere daders, met veel technische vaardigheden en financieel gewin als belangrijkste motief. Aan de andere kant zijn er jonge 'scriptkiddies' die vanuit nieuwsgierigheid de grenzen van internet verkennen met recent opgedane kennis. De laatste groep wordt als een risicogroep aangemerkt en de verwachting wordt uitgesproken dat deze jonge daders een positieve bijdrage aan de maatschappij kunnen leveren indien ze op tijd worden bijgestuurd. Wanneer dit niet gebeurt of wanneer interventies een averechts effect hebben, zouden de jongeren een criminele carrière kunnen ontwikkelen en richting de andere kant van het spectrum opschuiven. Ook wordt genoemd dat er veel ICT-talent zit in de doelgroep van de interventie, die goed gebruikt kan worden in de publieke of private sector in Nederland (Projectplan 1.0, z.d.).

Ten slotte stelt men dat er nog geen effectieve interventies zijn beschreven die bedoeld zijn als strafrechtelijke reactie op het plegen van cybercriminaliteit door jeugdigen (op basis van: Oosterwijk & Fischer, 2017). De strafrechtketen is volgens de plannen nog niet toegerust op cybercriminelen en heeft een sterke behoefte aan interventies die gericht zijn op het voorkomen van cybercrime daderschap onder jongeren (Projectplan 1.0, z.d.).

5.2.2 *In de praktijk*

Tijdens interviews met personen die betrokken zijn geweest bij de opzet en ontwikkeling van Hack_Right (n=2) wordt meer inzicht gegeven in hoe Hack_Right is ontstaan. Een van de interventieontwikkelaars is werkzaam bij de politie en geeft aan dat de daders in cybercrime-opsporingsonderzoeken een afwijkend profiel hadden ten opzichte van bijvoorbeeld daders in opsporingsonderzoeken op het gebied van georganiseerde misdaad (IO1). Bij de opsporingsonderzoeken cybercriminaliteit ging het veelal om jongeren, die delicten plegen waar relatief zware straffen op staan. De respondent noemt een voorbeeld van een casus waarbij vitale infrastructuur op instorten stond door toedoen van een 17-jarige jongen. Ook vanuit het Openbaar Ministerie en het Nationaal Cyber Security Centrum (NCSC) werd het probleem van jonge cybercriminelen geconstateerd volgens deze respondent. Vervolgens ontstond samen met twee collega's van het OM en NSCS het idee voor Hack_Right.

> *"Toen dachten we: we moeten een oplossing gaan vinden waarbij de jongeren leren wat er eigenlijk mis is gegaan, wat wel en niet mag en hoe ze het de volgende keer beter kunnen doen. En daar hebben we al die partijen voor nodig." (IO1)*

Partijen die vervolgens zijn betrokken bij de ontwikkeling van Hack_Right zijn uitvoerders van straffen – zoals Reclassering, Halt en de Raad voor de Kinderbescherming – en bedrijven uit de private sector die een belangrijke kennispositie hebben op dit onderwerp. De respondent van de politie geeft aan dat de bedrijven kennis hebben van ethisch hacken en waar de grenzen liggen tussen legaal en illegaal gedrag op internet. Uitvoerders van straffen hebben daar doorgaans geen verstand van volgens de respondent. Het moment dat alle partijen voor het eerst bij elkaar werden gebracht, kan worden gezien als de start van Hack_Right (IO1). De eerste twee Hack_Right trajecten zijn eind 2017 uitgevoerd.

5.3 De betekenis van Hack_Right

De betekenis van Hack_Right wordt in deze paragraaf beschreven op basis van projectplannen en interviews met zowel ontwikkelaars als toewijzers en uitvoerders. Volgens de projectplannen en ontwikkelaars is Hack_Right een alternatief of aanvullend straftraject voor jeugdige daders van cybercriminaliteit. Toewijzers en uitvoerders geven verschillende omschrijvingen aan Hack_Right, waarbij het leerelement van de interventie centraal lijkt te staan. De meningen lopen uiteen over of Hack_Right een straffunctie dient te vervullen.

5.3.1 *Op papier*

Hack_Right wordt in de projectplannen omschreven als een alternatief of aanvullend straftraject voor jonge daders van computercriminaliteit (Projectplan 1.0, z.d.; Project-

plan 2.0, 2018). Hack_Right staat daarmee niet op zichzelf, maar zoekt volgens eigen zeggen aansluiting bij bestaande (jeugd)interventies van andere organisaties die deelnemen aan Hack_Right (Projectplan 2.0, 2018). Voorbeelden die worden genoemd, zijn de leeropdracht van Halt of een gedragsinterventie van Reclassering. Naast de eerdergenoemde omschrijving wordt Hack_Right in de projectplannen ook aangemerkt als '(gedrags)interventie' en 'project'.

5.3.2 *In de praktijk*

Ontwikkelaars – Aan ontwikkelaars is gevraagd wat Hack_Right is. Beide respondenten noemen Hack_Right een aanvulling of alternatief op de huidige strafafdoeningen (IO1 en IO2), net zoals Hack_Right is omschreven in de plannen. Het volgende citaat illustreert dit:

> *"Dat is waar Hack_Right dan voor deze doelgroep erin stapt en zorgt dat er een traject wordt aangeboden waarmee iemand op het rechte pad blijft. Normaal is een dergelijk traject interessegebied van Halt of Reclassering. […] Maar inhoudelijk zul je technische expertise erbij moeten halen. En dat zie ik echt als Hack_Right: de aanvulling op het bestaande reclasseringstoezicht of de Halt-straf vanuit het Hack_Right programma." (IO2)*

Omtrent de betekenis van Hack_Right leggen de ontwikkelaars uit op welke wijze Hack_Right zich volgens hen tot het strafelement dient te verhouden. De respondenten geven aan dat er verschillende strafdoelen zijn. Waar bestaande strafelementen zoals een boete, werkstraf of gevangenisstraf ervoor zorgen dat het vergeldingsdoel wordt behaald, richt Hack_Right zich op het voorkomen van recidive. Het antwoord van een van de interventieontwikkelaars illustreert dit en laat zien welke rol Hack_Right volgens de respondent heeft in het huidige strafrechtsysteem:

> *"Van tevoren hebben we gedacht, is Hack_Right wel genoeg een straf? We dachten: we kunnen hier wel een heleboel strafelementen in stoppen, maar die bestaan al. Er zijn genoeg strafelementen voorhanden: een boete, gevangenisstraf of wat dan ook. Dat bestaat al, daar hoeven we niets nieuws voor te maken. Maar wel met het idee van: dat kun je dus heel goed combineren met Hack_Right. Want alle strafdoelen moeten natuurlijk afgevinkt worden: je wilt een beetje vergelding, maar je wilt vooral die recidivepreventie en daar zit Hack_Right op. Dus als iemand een zwaar delict pleegt, kun je hem een straf geven en erna Hack_Right." (IO1)*

Uitvoerders en toewijzers – Ook aan toewijzers en uitvoerders van Hack_Right (n=16) is gevraagd wat zij onder Hack_Right verstaan. Uit de antwoorden blijkt dat er in de praktijk verschillende labels worden gegeven aan Hack_Right. Respondenten omschrijven Hack_Right als project (n=5), (gedrags)interventie (n=4), gedragstraining (n=3), aanvullende of alternatieve straf(afdoening) (n=2), werkstraf (n=1), leer-/werkopdracht (n=1)

en 'een soort opvoedcursus' (n=1). De grote diversiteit aan definities lijkt voor een deel te wijten aan de organisaties waar de respondenten werkzaam zijn en (daarmee) van de strafmodaliteit (zie paragraaf 5.8) waarin Hack_Right wordt ingezet. Zo geeft een Halt-medewerker aan de betekenis van Hack_Right alleen vanuit Halt te kunnen linken als Halt-afdoening (HA2), leggen reclasseringswerkers uit dat Hack_Right bij de reclassering als leer-/werkopdracht (RE2) of werkstraf (RE1) in het systeem binnenkomt en omschrijven personen die werkzaam zijn bij cybersecuritybedrijven Hack_Right vanuit de voortrekkersrol (CS2) en maatschappelijke intenties (CS6) die de bedrijven hebben om hackers aan de goede kant van de wet te houden. Het volgende citaat van een reclasseringswerker is illustratief voor de context-afhankelijke definitie van Hack_Right:

> *"We hebben het project Hack_Right bij de werkstraffen ingehangen, speciaal gecreeerd, waardoor we het een naam konden geven en waardoor we de uren konden verantwoorden." (RE1)*

Een verdere analyse van de antwoorden laat zien dat het leerelement centraal staat bij Hack_Right (zie ook paragraaf 5.4). Een duidelijke rode draad in de antwoorden is namelijk dat Hack_Right jongeren leert om hun vaardigheden op een positieve manier in te zetten (n=12). De volgende antwoorden illustreren de wijze waarop respondenten dit omschrijven:

> *"Een mooie alternatieve sanctiemogelijkheid om mensen te leren van hun fouten om aan de goede kant van de wet te blijven staan." (RE1)*

> *"Ik zie Hack_Right als een pilotproject waarmee jonge daders de kans krijgen om aan te tonen dat ze hun kennis ook op een goede manier kunnen inzetten." (CS4)*

Een punt van discussie dat gedurende de interviews naar voren komt is of Hack_Right, naast de leerfunctie, niet ook een straffunctie zou moeten vervullen. Enkele respondenten geven namelijk aan dat Hack_Right ook een straf dient te zijn (RE2, CS1, OM3) of zou kunnen zijn (RE1, OM2, CS7). Ook wordt met betrekking tot de invulling bij Halt gesproken van een Halt-straf en over de reclassering dat zij toezicht houden op de uitvoering van een taakstraf (n=6). Andere respondenten zeggen dat Hack_Right niet per se een straf hoeft te zijn, maar dat het wel een dwingend karakter heeft en dat deelnemers er wel iets voor moeten doen (HA1, OM2, OM5). De volgende citaten zijn illustratief voor de uiteenlopende meningen:

> *"Wat het voor mij vooral is, is een combinatie van een straf en iemand inzicht verschaffen in positievere alternatieven voor skills die hij al heeft of aan het ontwikkelen is." (CS1)*

> *"Hack_Right is, ondanks dat het geen strafblad oplevert, er wel een, het moet ervaren worden als een straf." (OM3)*

"Hack_Right is meer maatwerk op de persoon zelf, waarin niet alleen – en soms helemaal niet – de straf in verdisconteerd zit." (OM2)

"Toen wij de verdachte lieten meedoen aan Hack_Right, weet ik niet zozeer, ik denk niet dat we het als een straf zagen, maar meer als een poging om hem het goede pad op te krijgen. […] En dwingend, want als hij er niet aan zou meedoen dan zou hij wel gewoon een taakstraf krijgen." (OM5)

5.4 Doel(en) van Hack_Right

De doelen van Hack_Right worden in deze paragraaf beschreven op basis van de projectplannen en interviews met ontwikkelaars, toewijzers en uitvoerders van Hack_Right. De hoofddoelen zijn volgens de projectplannen en ontwikkelaars (1) recidive verminderen en (2) ICT-talent verder ontwikkelen. Toewijzers en uitvoerders noemen diverse doelen, waarin de rode draad is dat deelnemers leren om hun vaardigheden op een goede manier in te zetten.

5.4.1 *Op papier*

Het hoofddoel van Hack_Right wordt in de projectplannen (Projectplan 1.0, z.d.; Projectplan 2.0, 2018) als volgt omschreven:

"Doel van Hack_Right is het resocialiseren van computercriminelen tussen 12 en 23 jaar en te voorkomen dat ze recidiveren door hun talent te ontwikkelen binnen de kaders van de wet." (Projectplan 2.0, 2018)

In het hoofddoel klinken drie verschillende doelen door die met elkaar samenhangen: resocialisatie, recidive voorkomen en talent ontwikkelen binnen de kaders van de wet. Naast het hoofddoel worden er ook verschillende subdoelen beschreven welke samenhangen met vier verschillende modules waar Hack_Right uit bestaat: (1) 'herstel', (2) 'training', (3) 'coaching' en (4) 'alternatief'. Deze modules zijn de verschillende onderdelen waar de inhoudelijke invulling van Hack_Right uit kan bestaan (zie voor een uitgebreide beschrijving paragraaf 5.7). Elke module heeft een eigen doel, die hier zullen worden beschreven.

Volgens de beleidsstukken heeft de module 'herstel' tot doel om de jongere inzicht te geven in de gevolgen van zijn of haar handelen en de gevolgen die zijn of haar daad voor het slachtoffer heeft gehad. De module 'training' heeft drie doelen. Ten eerste om de jongere te leren wat wel en niet mag volgens Nederlandse wetgeving. Ten tweede om de jongere na te laten denken over ethisch verantwoord hacken, waarom dit ethisch is en om zijn of haar eigen opvattingen hier aan te toetsen. Ten derde dient de module de cognitieve vaardigheden van de jongere te versterken zodat hij of zij beter in staat is om de gevolgen van zijn of haar handelen te overzien, zodat in de toekomst 'de juiste keu-

zes' gemaakt kunnen worden. De module 'coaching' heeft tot doel om de jongere intensief kennis te laten maken met personen, organisaties en locaties waarin de jongere zijn kennis en behoeften op een positieve manier kwijtkan. De module 'alternatief' heeft tot doel om positieve alternatieven voor cybercriminaliteit onder de aandacht te brengen van de jongere.

5.4.2 *In de praktijk*

Ontwikkelaars - Tijdens interviews met interventieontwikkelaars is gevraagd wat volgens hen het doel is van Hack_Right (n=2). Net als beschreven in de projectplannen benoemen beide ontwikkelaars 'recidive verminderen' en 'ICT-talent verder ontwikkelen' als de belangrijkste doelen van Hack_Right. De volgende citaten illustreren dit:

> *"Aan de ene kant recidive voorkomen en de andere kant talent winnen of talent door ontwikkelen. Dat zijn de belangrijkste pijlers van Hack_Right." (IO1)*

> *"Bijdragen aan het voorkomen van recidive is het belangrijkste doel, dus iemand op het rechte pad helpen. Het tweede doel is het stimuleren en verder helpen ontwikkelen van IT-talent." (IO2)*

Met het verder ontwikkelen van ICT-talent wordt verwezen naar de technische vaardigheden van de jongeren. Een van de interventieontwikkelaars legt uit wat er wordt bedoeld met het verder ontwikkelen van talent:

> *"We proberen vooral te zoeken naar: hoe kunnen we zorgen dat ze door de juiste mensen begeleid worden om op een veilige manier hun talenten verder te ontwikkelen? Dus het talent ontwikkelen zelf besteden we minder aandacht aan, het gaat meer om het in goede banen leiden van die technische carrières." (IO1)*

Volgens de respondent staat niet het leren van technische vaardigheden centraal, maar deelnemers leren op welke manier zij hun technische vaardigheden voor goede doelen kunnen inzetten (IO1). Beide respondenten geven aan dat de doelgroep van Hack_Right breed is, waardoor het verschilt op welke manier het ICT-talent van de jongeren kan worden gestimuleerd. Zo kan een jongere van 13 jaar die een DDoS-aanval heeft gepleegd, gestimuleerd kunnen worden om te kijken welke opleidingen interessant zijn. Oudere deelnemers die meer technische vaardigheden hebben, kunnen bijvoorbeeld stage lopen bij een bedrijf of worden gestimuleerd om hun talenten op een goede manier te blijven inzetten.

Uitvoerders en toewijzers – Ook aan uitvoerders en toewijzers van Hack_Right (n=16) is gevraagd wat volgens hen het doel is van Hack_Right. Zowel in de antwoorden van individuele respondenten als tussen de antwoorden van verschillende respondenten komen diverse doelen naar voren. De rode draad in de antwoorden is dat Hack_Right

ervoor dient te zorgen dat deelnemers hun vaardigheden op een goede manier inzetten (n=12). Dit wordt ook wel omschreven als de deelnemers 'het goede of rechte pad op brengen'. De volgende citaten illustreren hoe respondenten dit doel verwoorden:

> *"Voor ons is dat uiteindelijk heel erg van; de jonge cybercrime daders het rechte pad op krijgen en uiteindelijk ook houden. Ze een perspectief aanbieden." (CS3)*

> *"Het Hack_Right project probeert zulke jongeren te begeleiden om ze naar de goede kant te trekken van het hacken. Van het slechte hacken naar het ethisch hacken. Black-hat en white-hat." (OM5)*

> *"Waarbij je, omdat het gaat om iemand met technische kennis, die wellicht ook nog niet helemaal de criminele weg is ingeslagen, die je dus door een andere interventie eigenlijk op het goede spoor krijgt zodat hij zijn technische kennis kan inzetten voor iets goeds." (OM4)*

In aansluiting op het doel om de vaardigheden op een positieve manier in te zetten, klinkt in de antwoorden van respondenten door dat een doel is om de deelnemers iets bij te brengen of te leren. Enkele respondenten benoemen als doel van Hack_Right deelnemers leren wat goed en fout is of wat wel en niet mag (n=4). Hiermee lijkt te worden gedoeld op de juridische en ethische grenzen van hacken.

Het talent ontwikkelen binnen de kaders van de wet, zoals in het projectplan benoemd als een van de hoofddoelen, klinkt in de zojuist beschreven doelen van respondenten duidelijk door. Een ander hoofddoel volgens het projectplan is het verminderen van recidive. Een kleine groep respondenten noemt recidive verminderen of voorkomen van strafbaar gedrag als expliciet doel (n=3).

5.5 Theoretische onderbouwing

In deze paragraaf wordt de theoretische onderbouwing van Hack_Right besproken aan de hand van projectplannen en interviews met ontwikkelaars. Het blijkt dat Hack_Right probeert in te spelen op criminogene factoren voor daders van cybercriminaliteit. Ontwikkelaars geven aan dat de criminogene factoren zijn geïdentificeerd op basis van literatuuronderzoek. Een deel van de geïdentificeerde criminogene factoren zijn technisch gezien echter geen criminogene factoren zoals omschreven door de 'what-works'-benadering, maar gelegenheidsfactoren die een omgeving creëren waarin crimineel gedrag tot stand kan komen.

5.5.1 *Op papier*

In de projectplannen van Hack_Right (projectplan 1.0, z.d., projectplan 2.0, 2018) wordt verwezen naar enkele theoretische invalshoeken waar Hack_Right op is geba-

seerd. Een belangrijk ingrediënt bij de ontwikkeling van dadergerichte recidive-interventies is volgens de plannen de 'what-works'-benadering.[11] In de projectplannen worden de volgende acht criminogene factoren genoemd voor daders cybercriminaliteit:

– De invloed van 'peers'.
– De lage pakkans.
– Anonimiteit online.
– Onduidelijke regels op internet.
– Financiële beloning.
– Emotionele/cognitieve beloning.
– Weinig sociale controle.
– Onzichtbaarheid/ontkennen van schade en slachtoffers.

Het blijft in de projectplannen onduidelijk hoe de acht criminogene factoren zijn bepaald. Wel wordt in projectplan 1.0 gesteld dat de criminogene factoren uit criminologisch onderzoek blijken. Er worden in de projectplannen geen concrete bronnen genoemd. Hierbij dient te worden vermeld dat een deel van de door Hack_Right geformuleerde factoren technisch gezien niet kunnen worden aangeduid als criminogene factoren zoals omschreven in de 'what-works'-benadering. Uit paragraaf 3.2 is gebleken dat criminogene factoren die factoren zijn die rechtstreeks samenhangen met het plegen van het delict en in potentie te veranderen zijn. Factoren zoals een lage pakkans, anonimiteit online, onduidelijke regels op internet en emotionele of financiële beloningen van criminaliteit zijn vooral gelegenheidskenmerken die een omgeving creëren waarin crimineel gedrag makkelijker kan ontstaan. Aan deze factoren zelf kan een op het individu gerichte interventie niets veranderen. Wel kan een interventie deelnemers inzicht geven in hoe de gelegenheidsfactoren kunnen leiden tot crimineel gedrag en hoe deelnemers hiermee om kunnen gaan.

De eerdergenoemde factoren zijn de basis geweest voor het ontwikkelen van de verschillende modules van Hack_Right. Per criminogene factor is een doel gesteld, dat bereikt kan worden met verschillende strategieën die worden ingezet in de verschillende modules (paragraaf 5.7 gaat verder in op de vertaling van criminogene factoren naar modules). Hoe rekening wordt gehouden met de responsiviteit van de dader en het risico op recidive wordt niet direct benoemd in de projectplannen. Wel wordt opgemerkt dat het kiezen van modules maatwerk is en afhangt van de criminogene factoren en persoonlijke omstandigheden van de deelnemer.

Naast de 'what-works'-benadering worden er nog andere theoretische aspecten in de plannen genoemd die een rol spelen bij Hack_Right. Zo wordt er gesteld dat de aanwe-

11 De 'what-works'-benadering stelt dat interventies effectief zijn wanneer zij inspelen op criminogene factoren, rekening houden met de responsiviteit van de dader en rekening houden met het risico op recidive van de dader – zie paragraaf 3.2 voor meer details.

zigheid van motivatie bij een deelnemer van belang is voor het tot stand komen van houding en gedragsveranderingen (McMurran & Ward, 2010). Ook wordt er verwezen naar het belang van programma-integriteit, wat inhoudt dat een interventie daadwerkelijk wordt uitgevoerd op de manier waarop deze ontwikkeld is. Het blijft in de projectplannen onduidelijk hoe Hack_Right invulling geeft aan dit aspect.

5.5.2 *In de praktijk*

Aan ontwikkelaars van de interventie (n=2) is gevraagd waarom zij denken dat Hack_Right haar doelstellingen zal behalen. In het volgende citaat geeft een van de ontwikkelaars aan dat dit nog niet duidelijk is:

> *"Ik denk dat wij het nog niet zeker weten. Toen we begonnen, was er nog weinig wetenschappelijk onderzoek naar de doelgroep gedaan." (IO2)*

De ontwikkelaars verwijzen in de interviews naar de kennis die wel aanwezig was op het moment dat zij de interventie ontwikkelden en geven aan dat Hack_Right op deze kennis is gebaseerd (IO2 en IO1). Zo wordt er verwezen naar een WODC-onderzoek dat liet zien dat er geen passende interventies waren (IO2), een onderzoek naar 'pathways into cybercrime' (IO2), experimenten met een hackers-bootcamp die in Engeland plaatsvonden (IO2) en naar een onderzoek dat door twee collega's is uitgevoerd naar criminogene factoren voor cybercriminaliteit (IO2 en IO1). Op basis van de onderzoeken ontstond informatie over de *modus operandi* (IO2), hoe de doelgroep in het criminele wereldje terechtkomt (IO2) en dat veel hackers de stap naar criminele activiteiten onbewust maken (IO2 en IO1). De modules van Hack_Right zijn volgens de respondenten gebaseerd op criminogene factoren (IO2 en IO1). Ook bevat Hack_Right volgens een van de ontwikkelaars (IO2) elementen van 're-integrative shaming', doordat de 'hacker-community' zelf de straf uit voert, in de vorm van cybersecuritybedrijven en ethisch hackers (IO1). Ten slotte benadrukt de respondent dat er een tweesporenbeleid is omtrent Hack_Right, waarin enerzijds wetenschappelijk onderzoek gedaan blijft worden naar de doelgroep en de mate waarin Hack_Right werkt, en anderzijds ook vast wordt gestart met de interventie.

> *"Door te proberen, kom je er veel sneller achter of iets werkt of niet, of het aanslaat en of het haalbaar is." (IO1)*

5.6 Doelgroep Hack_Right

De doelgroep van Hack_Right wordt in deze paragraaf beschreven op basis van de projectplannen en interviews met ontwikkelaars. Hack_Right richt zich op jongeren tussen de 12 en 23 jaar, die een eerste delict computercriminaliteit plegen, een gedeeltelijke bekentenis hebben afgelegd en gemotiveerd zijn voor deelname aan Hack_Right.

In aanvulling op de plannen is het volgens ontwikkelaars ook belangrijk dat deelnemers beschikken over technische interesse of vaardigheden.

5.6.1 *Op papier*

In de projectplannen is een vastomlijnde doelgroep voor Hack_Right opgesteld (Projectplan 1.0, z.d.; Projectplan 2.0, 2018). De doelgroep is volgens de documenten bepaald op basis van wetenschappelijk onderzoek en praktijkervaring en zal worden aangescherpt aan de hand van de uitgevoerde pilots (Projectplan 1.0, z.d.). Studies waar naar wordt verwezen, zijn onderzoek van Van Dijk (2012), Zebel en collega's (2015), Aiken en collega's (2016) en Stavenuiter (2017). In de plannen wordt een checklist beschreven met vier voorwaarden waar jongeren aan moeten voldoen om in aanmerking te komen voor Hack_Right (Projectplan 2.0, 2018):

– Eerste delict computercriminaliteit.
– Leeftijd tussen de 12 en 23 jaar.
– Gedeeltelijke bekentenis.
– Gemotiveerd zijn voor deelname.

De checklist stelt dat er ten eerste sprake moet zijn van een eerste delict computercriminaliteit (zie bijlage 2 voor een overzicht van delicten computercriminaliteit). Het gepleegde delict moet voor de verdachte het eerste cyberdelict zijn dat hij of zij pleegt ('first offenders'). Men veronderstelt dat het criminele pad voor deze jongeren relatief nieuw is en dat recidive voorkomen daarom een haalbare doelstelling is. Ook wordt er gesteld dat het bij een eerste cyberdelict nog aannemelijk is dat de verdachte niet doorhad dat zijn of haar gedrag niet mag binnen de grenzen van de wet.

De tweede voorwaarde houdt in dat potentiële deelnemers een leeftijd moeten hebben tussen de 12 en 23 jaar. Er wordt gesteld dat de meeste delicten door deze doelgroep worden gepleegd en dat deze personen vatbaarder zijn voor gedragsverandering. Ook wordt er gesteld dat impulsiviteit en risicozoekend gedrag toeneemt in de jonge tienerjaren, waardoor de kans bestaat dat jongeren gaan kijken waar de grens ligt van hun kwaliteiten en deze grens bewust of onbewust overschrijden.

Een derde voorwaarde voor deelname aan Hack_Right is dat de verdachte moet inzien dat zijn of haar handelen ten minste een aandeel heeft gehad in de schade die is ontstaan in de vorm van een gedeeltelijke bekentenis. Er wordt gesteld dat Hack_Right geen gepaste interventie is als de verdachte betrokkenheid ontkent of de strafbaarheid niet inziet. Bij de voorwaarde wordt de kanttekening geplaatst dat wanneer een slachtoffer zelf de beveiliging niet op orde heeft, een klein delict grote schade kan aanrichten en daarom bij de dader zou kunnen leiden tot frustratie en minder inzicht in zijn of haar aandeel in de schade. In dit geval zou een gedeeltelijke bekentenis voldoende zijn.

Ten slotte dient de verdachte gemotiveerd te zijn om mee te doen aan Hack_Right. De interventie wordt als ongeschikt geacht wanneer er geen wil is om meer te leren, schade te herstellen of te werken aan ethisch verantwoord gedrag. Indien een dader niet gemotiveerd is, of niet voldoet aan een van de andere criteria, volgt het reguliere strafproces zonder Hack_Right.

In het document 'Samenvatting literatuur Hack_Right' (z.d.) wordt een verdere beschrijving gegeven van de doelgroep 'jonge cybercriminelen'. Ten eerste wordt gesteld dat het vaak om adolescenten gaat met een hoog IQ, die nieuwsgierig zijn naar technologie en vaardig zijn met de computer. Verder wordt over de doelgroep gezegd dat zij niet tot een specifieke sociale klasse behoren, maar dat zij vaak nog bij hun ouders wonen. De sociale controle van de kinderen door ouders is daarbij vaak gering. Daarnaast wordt gesteld dat het vaak gaat om een sociaal geïsoleerde jongen, maar dat de dader zich soms ook in een netwerk bevindt met soortgelijke adolescenten. Andere kenmerken die worden genoemd, zijn dat de jonge cybercriminelen kwetsbaar, sociaal ongemakkelijk en teruggetrokken zijn. Verder hebben zij grote behoefte aan online aansluiting en bevestiging, is de online reputatie in het netwerk belangrijk en speelt hiërarchie een rol. Ten slotte beleeft de doelgroep veel intrinsiek plezier aan meer online uitdaging, zoals vaak gezien in online criminaliteit van een hoger niveau. Er worden ook enkele risicofactoren genoemd met betrekking tot de doelgroep. Zo hebben jongeren volgens de projectplannen vaak geen strafblad, maar kan het hebben van antecedenten worden gezien als een risicofactor voor het plegen van cybercrimedelicten. Andere risicofactoren die worden genoemd zijn het online-disinhibitie-effect, weinig ouderlijke controle en het hebben van vrienden die cybercrimedelicten plegen.

5.6.2 *In de praktijk*

Interventieontwikkelaars (n=2) omschrijven de doelgroep van Hack_Right aan de hand van de checklist die is opgesteld. Hack_Right is voor verdachten die een eerste cyberdelict plegen en tussen de 12 en 23 jaar zijn ten tijde van het plegen van het delict (IO2, IO1). Ook is er een gedeeltelijke bekentenis nodig (IO2). De respondent geeft aan dat dit criterium niet altijd haalbaar is wanneer iemand bijvoorbeeld door zijn of haar advocaat wordt gewezen op het zwijgrecht of omdat het niet altijd duidelijk is wat precies het motief was. Op dit criterium is men minder streng wanneer de verdachte bijvoorbeeld bij de reclassering opener is en aangeeft berouw te hebben en een tweede kans te willen. Bovendien dient de verdachte gemotiveerd te zijn om deel te nemen aan Hack_Right (IO2, IO1). Dit is volgens de respondenten enerzijds wenselijk voor het bedrijf dat er tijd in stopt en anderzijds nodig voor gedragsverandering tijdens een leerstraf.

Naast de zojuist genoemde criteria worden ook technische interesse of vaardigheden van de verdachte genoemd (IO2, IO1). Volgens de respondenten stond dit een criterium eerder ook op de checklist, maar bleek dit in de praktijk lastig te meten en subjectief (IO2, IO1). Het volgende citaat laat zien hoe de ontwikkelaars tegen dit criterium aankijkt:

"Maar in principe is het dus gericht op jongeren waarvan we verwachten dat ze in de toekomst gaan experimenteren met IT en met hacken, waarvan we verwachten dat dat een risico gaat vormen." (IO1)

Uit de interviews blijkt dat er gewerkt wordt aan een intake-assessment die kan worden gebruikt tijdens de eerste ontmoeting tussen de deelnemer en medewerker van Halt of Reclassering om te kunnen adviseren of de jongere geschikt is (IO2). Een ander criterium dat eerst op de checklist stond als contra-indicatie was dat financieel gewin niet het hoofdmotief mocht zijn (IO1). Dit criterium is uit de lijst gehaald omdat het in de praktijk lastig bleek vast te stellen en omdat men vanuit Hack_Right liever zelf naar het profiel kijkt, zodat jongeren die een klein financieel gewin hebben gehad niet bij voorbaat afvallen. Ten slotte wordt benoemd dat de ernst van het delict geen criterium is vanuit Hack_Right (IO1). Dit wordt overgelaten aan de officier van justitie of rechter. Wel wordt er vanuit Hack_Right nagedacht of iemand die een zwaarder delict pleegt nog kan leren om zijn vaardigheden op een goede manier in te zetten.

5.7 Inhoud Hack_Right

In deze paragraaf wordt besproken hoe het programma van Hack_Right eruitziet op basis van de projectplannen en interviews met ontwikkelaars. Het blijkt dat Hack_Right op papier bestaat uit vier verschillende modules die zijn gebaseerd op de eerdergenoemde criminogene factoren. In de praktijk worden volgens ontwikkelaars echter geen modules opgelegd, maar komen elementen van de modules terug in de invulling die per deelnemer wordt bepaald.

5.7.1 *Op papier*

Hack_Right bestaat volgens de projectplannen uit vier verschillende modules: 'herstel', 'training', 'coaching' en 'alternatief' (Projectplan 1.0, z.d.; Projectplan 2.0, 2018). De modules zijn volgens de plannen gebaseerd op criminogene factoren[12] voor het plegen van delicten cybercriminaliteit. Hack_Right speelt met de modules in op zes[13] van de acht criminogene factoren die in het projectplan worden genoemd: invloed van peers, onduidelijke regels op het internet, financiële beloning, emotionele of cognitieve beloning, weinig sociale controle en de onzichtbaarheid van schade en/of slachtoffers (Projectplan 2.0, 2018). In tabel 3 is een overzicht opgenomen van de criminogene factoren, de doelen die gesteld zijn om diens invloed zo veel mogelijk proberen te verkleinen, de strategieën die worden ingezet om dit te bereiken en de verschillende modules van Hack_Right.

12 Kenmerken en omstandigheden van mensen en hun omgeving die bijdragen aan het plegen van delicten en daardoor ook ten aanzien van recidive een voorspellende waarde kunnen hebben (Projectplan 2.0, 2018).

13 Hack_Right speelt niet in op de criminogene factoren 'anonimiteit online' en 'lage pakkans'. Een interventieontwikkelaar (IO2) geeft in een interview aan dat Hack_Right op sommige criminogene factoren niet of minimaal inspeelt, omdat deze lastig zijn om op in te spelen of dat deze door andere modules al gedeeltelijk worden ondervangen.

Tabel 3: vertaling van criminogene factoren naar modules (Projectplan 2.0, 2018)

Criminogene factor	Doel	Strategie	Module(s)
1. Onduidelijkheid of ontkennen van morele en juridische grenzen op het internet	Inzicht in juridische en morele grenzen van de samenleving en hoe deze grenzen ook online gelden	Training om het besluitvormingsproces bij jonge cybercriminelen te verbeteren	Training, Alternatief
2. Onzichtbaarheid of ontkennen van schade en slachtoffers	Herstel relatie dader en slachtoffer. Verantwoordelijkheid en zelfinzicht van de dader	Restorative justice Inspelen op emotionele en cognitieve vaardigheden	Herstel
3. Gebrek aan sociale controle	Verbreding en verdieping van sociale controle	Coaching, inbedden in ethical hacker community	Herstel, Coaching, Alternatief
4. Negatieve invloed peers	Invloed negatieve peers verkleinen en invloed positieve peers vergroten.	Introduceren van positieve rolmodellen	Training, Coaching, Alternatief
5. Financiële beloning	Legale carrière perspectief van de daders verbeteren	Aantrekkelijk maken van positieve alternatieven in het bedrijfsleven	Training, Coaching, Alternatief
6. Emotionele of cognitieve beloning	Vaardigheden van daders verbeteren op een legale manier	Legale uitdagingen promoten	Training, Coaching, Alternatief

Per module wordt nu beschreven wat het doel is, op welke criminogene factoren de module zich richt en met welke strategie de module probeert in te spelen op deze criminogene factoren. De eerste module, 'herstel', probeert de dader inzicht te geven in de gevolgen van zijn of haar handelen voor het slachtoffer. De criminogene factoren waar de module zich op richt, zijn zowel de onzichtbaarheid of het ontkennen van schade en slachtoffers als het gebrek aan sociale controle. Onderdelen die bij de module worden genoemd zijn een dader-slachtoffergesprek, een herstelconferentie en een herstelplan.

De tweede module 'training' heeft tot doel om de dader te leren wat wel en niet mag volgens Nederlandse wetgeving, leert de dader nadenken over ethisch verantwoord hacken en versterkt de cognitieve vaardigheden van de dader zodat hij of zij beter in staat is om de gevolgen van zijn of haar handelen te overzien. De module speelt in op de onduidelijkheid of het ontkennen van morele en juridische grenzen op internet, de emotionele of cognitieve beloning, de financiële beloning en de negatieve invloed van peers. Onderdelen die worden genoemd voor de module zijn een training juridische grenzen, een training ethisch hacken en bestaande trainingen of interventies. Het is echter onduidelijk welke bestaande trainingen of interventies hiermee worden bedoeld.

In de derde module, 'coaching', worden daders gekoppeld aan personen of organisaties waar de daders hun kennis en behoeften op een positieve manier kwijtkunnen. De

module speelt hiermee in op de negatieve invloed van peers, de emotionele of cognitieve beloning, de financiële beloning en het gebrek aan sociale controle. De module bestaat uit begeleiding van jongeren in hun persoonlijke ontwikkeling door een ethisch hacker of een werknemer van een cybersecuritybedrijf.

De laatste module, 'alternatief', brengt positieve alternatieven voor cybercriminaliteit onder de aandacht van de dader. Criminogene factoren waar de module op inspeelt zijn de negatieve invloed van peers, de financiële beloning, de emotionele/cognitieve beloning, het gebrek aan sociale controle en de onduidelijkheid of het ontkennen van morele en juridische grenzen op internet. Onderdelen die bij de module worden genoemd zijn leeropdrachten, workshops, (CTF-)challenges[14], presentaties door het bedrijfsleven en demo's door hackerspaces.

5.7.2 *In de praktijk*

Uit de interviews met ontwikkelaars (n=2) blijkt dat er inderdaad in eerste instantie vier modules zijn ontwikkeld. Deze modules zijn door zogenoemde 'tafels' met betrokken strafrechtketenpartners uitgewerkt (IO1). De tafels werden later werkgroepen, die niet zozeer op modules gericht waren, maar om bepaalde producten te ontwikkelen. De namen van de modules die vanuit Hack_Right werden gegeven, bleken bij de betrokken strafrechtketenpartners verschillende, andere benamingen en connotaties te hebben en daarom lastig werkbaar. Het volgende citaat illustreert dit:

> *"Dus we merkten dat het wel extreem ambitieus was om met drie verschillende uitvoerende overheidspartijen een plan te maken voor een relatief kleine dadergroep. Want iedereen werkt weer op een andere manier." (IO1)*

De concrete invulling van Hack_Right wordt daarom niet zozeer als module(s) ingevuld (IO2, IO1). Het volgende citaat illustreert hoe de invulling van Hack_Right tot stand komt:

> *"Er wordt eigenlijk niet heel erg vanuit modules benaderd. Eigenlijk is het, die jongere komt, je ziet wat hij gedaan heeft, je kijkt heel breed wat er nodig is om de jongere op het juiste pad te brengen en dan bedenk je een traject. Toevallig valt het meestal dan in de modules. Het is dus meer omgekeerd: je kijkt eerst naar wat gaat hij precies doen en dan verbind je daar modules aan vast. Ik denk in de toekomst dat het beter zou zijn om dat om te keren. Dus als er een handleiding af is, dan sluiten de modules ook wat logischer aan op het traject." (IO1)*

14 'Capture The Flag challenges' zijn opdrachten waarin deelnemers zoeken naar beveiligingskwetsbaarheden in vooropgezette programma's of websites.

Tijdens de interviews wordt door de respondenten verder toegelicht hoe elementen van de oorspronkelijke modules zijn verwerkt in de verschillende trajecten die deelnemers hebben doorlopen.

> *"De modules, het heeft wel overal in gezeten ofzo, we hebben niet iets gedaan wat compleet niet in die modules stond. Maar ik denk dat je het meer moet zien als een soort van ingrediënten ofzo, waar we een beetje van alles hebben doorgeroerd." (IO2)*

Per module wordt nu besproken hoe deze volgens de respondenten terugkomen in de Hack_Right trajecten die tot nu toe zijn uitgevoerd.

Herstel - Met betrekking tot herstel geeft een van de respondenten aan dat het herstellen van de schade die door de deelnemer aangericht is lastig is, omdat er vaak een lange tijd zit tussen het slachtofferschap en vervolging en omdat het bij cybercriminaliteit niet altijd duidelijk is wie of wat slachtoffer is geworden (IO1). Bij Halt hebben deelnemers wel excuusbrieven geschreven voor – of gesprekken gehad met – slachtoffers (IO2, IO1). Verder is het herstel vooral gericht op toekomstige schade voorkomen. Het volgende voorbeeld illustreert dit:

> *"Een jongere had een DDoS-aanval gepleegd en heeft iemand van de bank geïnterviewd om de gevolgen te horen. De herstelgedachte zat daar op die manier in." (IO2)*

Met een methodiekontwikkelaar bespreken de interventieontwikkelaars nu hoe de module herstel in de toekomst een vastere invulling kan krijgen.

Training - Voor de module training is er per casus gekeken wat de deelnemer dient te leren. De trainer was dan een persoon van het bedrijf waar de deelnemer heen is gegaan. Vaak is er een powerpointpresentatie gegeven over ethisch hacken en wat wel en niet mag (IO2). De bedrijven hebben zelf invulling gegeven aan de training (IO2, IO1). Op dit moment wordt een training ethisch hacken en juridische grenzen ontwikkeld voor de deelnemers (IO2, IO1).

Coaching - Met betrekking tot de module coaching hebben er coachingstrajecten plaatsgevonden waarin iemand een rolmodel aangeboden heeft gekregen vanuit de organisatie waar de deelnemer is geplaatst. De coach is iemand die ethisch hacker of IT'er is en laat aan de deelnemer zien hoe hij of zij zelf legaal geld verdient, welke online fora interessant zijn en stelt kritische vragen aan de deelnemer (IO2). Tijdens het interview met de tweede interventie-ontwikkelaar blijkt dat er wordt gedacht om coaching officieel geen onderdeel van de straf te laten zijn. Een coachingsgesprek kan dan wel onderdeel zijn, maar is volgens de respondent lastig om te zien als strafuren wanneer iemand de deelnemer gaat helpen (IO1).

> *"In het begin zaten we nog veel met de terminologie; wanneer noem je iets een coachingstraject en wanneer niet? Een jongen had behoorlijk aantal uren Hack_Right gekregen. Daar hebben twee coaches hem heel lang in begeleid. Maar het was ook een leeropdracht. Dus ja, we hebben het coachingstraject genoemd omdat we een van de twee begeleiders hadden gezien als coach en de ander was dan degene die de leeropdracht zou begeleiden. Maar in de praktijk hebben ze eigenlijk samen beide rollen op zich genomen omdat dat voor die jongen beter werkte. Dat is gewoon uitproberen." (IO1)*

Positief alternatief - Deelnemers leren over positieve alternatieven doordat zij naar een bedrijf gaan, kijken wat ze daar doen, meelopen, opdrachten krijgen en ideeën opdoen over mogelijke banen en/of opleidingen die gevolgd moeten worden (IO2).

> *"Uiteindelijk moeten we natuurlijk ook heel duidelijk gaan communiceren: wat is nou wat? Want ik merk ook als ik het probeer uit te leggen, het loopt allemaal een beetje door elkaar. En dat is denk ik ook gewoon de ontwikkelfase waar we inzitten. Uiteindelijk kristalliseert zich dat wel uit en dat moet dan in ieder geval in de handleiding die in april af is erin staan." (IO1)*

De concrete invulling van Hack_Right is dus nog sterk in ontwikkeling, zoals blijkt uit de interviews met interventieontwikkelaars. Het feit dat een handleiding in ontwikkeling is, heeft belangrijke implicaties voor evaluatieonderzoek. Een evaluatie van de handleiding (als onderdeel van een planevaluatie) en een evaluatie van de mate waarin trajecten worden uitgevoerd volgens de handleiding (als onderdeel van een procesevaluatie) zijn hierdoor namelijk niet mogelijk. Hoe verschillende individuele trajecten concreet zijn ingevuld wordt besproken in paragraaf 6.4.

5.8 Betrokken partijen

De partijen die betrokken zijn bij Hack_Right worden in deze paragraaf besproken. Bij de opzet van Hack_Right zijn het Openbaar Ministerie, de politie, Halt, de reclassering, wetenschappers en (cybersecurity)bedrijven betrokken. Ook bij de uitvoering van Hack_Right trajecten zijn de meeste van deze partners betrokken.

5.8.1 *Op papier*

De opdrachtgever van Hack_Right is de hoofdofficier van justitie van het Landelijk Parket van het Openbaar Ministerie (Projectplan 2.0, 2018). Een projectgroep is verantwoordelijk voor de vormgeving en implementatie van Hack_Right en bestaat uit vertegenwoordigers van de volgende ketenpartners: het Landelijk Parket van het Openbaar Ministerie, de High Tech Crime Unit van de Landelijke Eenheid van de Nationale Politie, Bureau Halt en Reclassering Nederland. De dagelijkse aansturing en casusregie liggen bij de projectgroep. Naast de ketenpartners wordt er samengewerkt

met bedrijven die zijn aangesloten bij de interventie. Deze bedrijven helpen bij het ontwikkelen of uitvoeren van de opdrachten binnen de verschillende modules. Ook wordt er samengewerkt met verschillende kennisinstellingen. Deze instellingen kijken kritisch mee met de werking en opzet van de interventie.

Er is verder een aantal werkgroepen (met vertegenwoordigers van diverse publieke en private organisaties) om specifieke onderdelen van het Hack_Right traject uit te werken. Er zijn werkgroepen ter ontwikkeling van een training juridische grenzen & ethisch hacken, ter bevordering van kennisuitwisseling en implementatie van Hack_Right in bestaande kaders, ter ontwikkeling van een begeleidend kader voor de leeropdrachten, ter ontwikkeling van een begeleidend kader voor de coaches en een werkgroep wetenschap. In de projectplannen staat verder beschreven dat op lange termijn de deelnemende organisaties zelfstandig de Hack_Right trajecten kunnen initiëren en uitvoeren (Projectplan 1.0, z.d.; Projectplant 2.0, 2018). De projectgroep en het project Hack_Right stoppen op het moment dat de interventie is verankerd in bestaande procedures van de betrokken partijen.

5.8.2 *In de praktijk*

Tijdens de interviews met interventieontwikkelaars wordt verder inzicht gegeven in de verschillende organisaties die in de praktijk betrokken zijn bij Hack_Right. Bij de opzet van Hack_Right zijn het Openbaar Ministerie, de politie, de reclassering, Halt, de Raad voor de Kinderbescherming, cybersecuritybedrijven, het ministerie van Justitie en Veiligheid en wetenschappers betrokken geweest (IO1). Vanuit deze organisaties hebben personen deelgenomen aan de tafels/werkgroepen van Hack_Right. Voor de uitvoering van Hack_Right zijn Halt, Reclassering en de Raad voor de Kinderbescherming betrokken als strafrechtketenpartners. Ook kunnen deze organisaties betrokken zijn bij het geven van een strafadvies aan het Openbaar Ministerie of de rechter. Een van de interventieontwikkelaars geeft aan dat men wil dat alle Hack_Right deelnemers bij Reclassering, Halt of RvK terechtkomen (IO2). Wanneer welke organisatie betrokken is wordt verder besproken in paragraaf 5.9. Naast de strafrechtketenpartners zijn er ook (cybersecurity)bedrijven of organisaties betrokken bij de uitvoering van Hack_Right.

5.9 Instroomproces Hack_Right

De huidige paragraaf beschrijft aan de hand van de projectplannen en interviews met ontwikkelaars hoe het proces van instroom tot uitstroom van Hack_Right eruitziet. Het blijkt dat Hack_Right is ingebed in de bestaande strafrechtketen. Afhankelijk van de leeftijd van de verdachte kan Hack_Right in de vorm van verschillende strafmodaliteiten aan verdachten worden opgelegd door de officier van justitie of rechter.

5.9.1 *Op papier*

In de documenten 'instroomschema Hack_Right' (z.d.), 'schema strafmodaliteiten' (z.d.) en in Projectplan 1.0 (z.d.) wordt beschreven op welke wijze een verdachte kan instromen in Hack_Right. Het startpunt is het opsporingsonderzoek dat wordt uitgevoerd door de politie. Hier komt de verdachte in beeld en ontstaat inzicht in de zaak en persoon van de verdachte. Wanneer de zaak rond is, wordt deze ingestuurd naar het OM. Een mogelijkheid is dat de zaak vervolgens wordt besproken aan de zogeheette ZSM-tafel. De ZSM-aanpak is een manier waarop veelvoorkomende criminaliteit zorgvuldig, snel en op maat (ZSM) kan worden afgedaan. Ook kan er onderzoek door de Reclassering of Raad van de Kinderbescherming worden uitgevoerd om strafadvies uit te brengen. De officier van justitie bepaalt vervolgens de strafafdoening. De projectgroep Hack_Right adviseert de officier van justitie of een verdachte in aanmerking komt voor Hack_Right. Er zijn verschillende strafmodaliteiten mogelijk waarin Hack_Right kan worden ingezet, die nu worden besproken.

Afhankelijk van de leeftijd van de verdachte wordt Hack_Right binnen een bestaande strafmodaliteit toegepast. Op het moment dat de verdachte onder het volwassenenrecht valt, zijn er drie vormen van Hackright mogelijk. Ten eerste kan Hack_Right worden opgelegd bij een voorwaardelijk sepot. Hackright wordt dan als bijzondere voorwaarde opgelegd met reclasseringstoezicht. Ten tweede kan Hackright worden opgelegd bij een Transactie Openbaar Ministerie (TOM), OM-hoor of OMSB-zitting. Hack_Right kan dan als aanwijzing in een strafbeschikking of als voorwaarde worden opgelegd met reclasseringstoezicht. Ten derde kan Hack_Right worden opgelegd bij een dagvaarding bij de Politierechter Zitting of Meervoudige Kamerzitting. Hack_Right kan dan als overige bijzondere voorwaarde worden opgelegd met reclasseringstoezicht. Ook kan Hack_Right in deze strafmodaliteit worden opgelegd als onderdeel van een gedragsbeïnvloedende maatregel met verplicht reclasseringstoezicht (Schema strafmodaliteiten, z.d.).

Wanneer de verdachte valt onder het Jeugdrecht of Adolescentenstrafrecht zijn er vijf vormen van Hack_Right mogelijk (Schema strafmodaliteiten, z.d.). Ten eerste kan er een Halt-afdoening worden opgelegd, waarbij Hack_Right een programma van maximaal twintig uur is. Ten tweede kan er een voorwaardelijk sepot plaatsvinden. Hack_Right kan dan als bijzondere voorwaarde met jeugdreclassering worden opgelegd. Ten derde kan er een Transactie in Persoon (TRIP)- of transactie Openbaar Ministerie Minderjarigen (TOMMi)-zitting plaatsvinden. Binnen deze strafmodaliteiten kan Hack_Right voor maximaal zestig uur worden opgelegd als bijzondere voorwaarde met jeugdreclasseringstoezicht. Ten vierde kan er een dagvaarding voor de kinderrechter plaatsvinden. Hack_Right kan dan als overige bijzondere voorwaarde met jeugdreclasseringstoezicht worden opgelegd bij een (deels) voorwaardelijke straf. Ten vijfde kan er een dagvaarding bij de meervoudige kamer plaatsvinden. Hack_Right kan dan als overige bijzondere voorwaarde worden opgelegd met jeugdreclasseringstoezicht.

Ook kan Hack_Right in dit geval worden opgelegd als onderdeel van een gedragsbeïnvloedende maatregel met verplicht jeugdreclasseringstoezicht (Schema strafmodaliteiten, z.d.).

Nadat duidelijk is welke strafafdoening van toepassing is voor de verdachte, wordt ook duidelijk welke justitiele ketenorganisatie betrokken is. De justitiele ketenorganisaties zijn Halt, (Jeugd)Reclassering of de Raad voor de Kinderbescherming. Uit de plannen wordt niet duidelijk wanneer de Raad voor de Kinderbescherming is betrokken bij een Hack_Right traject. Indien er nog geen intakeassessment heeft plaatsgevonden neemt een van deze organisaties een intakeassessment af. Vervolgens wordt er een interventieafstemming georganiseerd met de betrokken ketenpartner, eventueel de politie en/of het Openbaar Ministerie, het bedrijf of de organisatie waar de jongere activiteiten voor Hack_Right gaat uitvoeren en tijdens de pilots iemand van team Hack_Right. Ten slotte wordt het plan met betrekking tot de invulling van het Hack_Right traject uitgewerkt. Hiervoor zijn team Hack_Right (in de pilotfase), de ketenpartner en het bedrijf verantwoordelijk. Hoe modules precies worden ingezet, is afhankelijk van de doelgroep en het juridisch kader waarbinnen de specifieke casus zich afspeelt (Projectplan 2.0, 2018).

5.9.2 *In de praktijk*

Uit de interviews met interventieontwikkelaars blijkt dat verdachten van cybercriminaliteit in de praktijk op verschillende manieren bij Hack_Right terechtkomen (IO2 en IO1). Zoals uiteengezet in het projectplan zijn er ook in de praktijk verschillende plekken in het strafrechtsysteem waar Hack_Right kan worden geopperd als mogelijke interventie voor een verdachte: bij de politie, bij het OM of bij uitvoerende strafrechtketenpartners zoals Halt en reclassering. Ten eerste kan men bij de politie Hack_Right opperen, waar de verdachte als eerst in beeld komt. Ten tweede kan – als een zaak vervolgd wordt – een persoon binnen het OM Hack_Right als mogelijke interventie initiëren. Ten derde kunnen ook uitvoerende strafrechtketenpartners zoals Halt en de reclassering Hack_Right adviseren. Halt en reclassering kunnen al vroeg bij een zaak betrokken zijn in de vorm van vroeghulp en het geven van advies aan een officier van justitie of rechter en daarbij Hack_Right adviseren. Halt kan ook tijdens de uitvoering van een straf nog aan Hack_Right denken en aan de officier van justitie vragen of Hack_Right in de straf kan worden opgenomen. In tegenstelling tot het projectplan blijkt dat er in de praktijk ook een casus is geweest waarbij Hack_Right is geïnitieerd door het Leger des Heils, in een advies aan de rechter (IO2). Volgens de respondent vonden de projectgroep Hack_Right en het OM de verdachte niet geschikt voor Hack_Right en is het advies van het Leger des Heils buiten de projectgroep Hack_Right en het OM omgegaan. Een interventieontwikkelaar – en ook andere respondenten, zie paragraaf 7.6 – merkt op dat een probleem van Hack_Right is dat niet alle verdachten die in aanmerking komen voor Hack_Right daadwerkelijk een Hack_Right traject krijgen. Mogelijke verklaringen hiervoor worden in paragraaf 7.6 benoemd.

Nadat op een van de eerdergenoemde plekken in het strafrechtsysteem Hack_Right wordt geïnitieerd, wordt de casus – vaak telefonisch – aangemeld bij de projectgroep Hack_Right (IO2 en IO1). Zoals uiteengezet in de projectplannen brengt de projectgroep Hack_Right ergens in de vervolgprocedure een advies uit over de geschiktheid van de verdachte voor deelname en een mogelijke invulling voor een traject (IO2 en IO1). Dit gebeurt in overleg met verschillende strafrechtketenpartners. Er wordt dan gekeken naar wat voor persoon de verdachte is, wat hij of zij heeft gedaan, wat zijn of haar interesses en vaardigheden zijn en waar de verdachte woont. Een plan voor de invulling van een traject wordt vaak opgesteld samen met het bedrijf of de organisatie waar de deelnemer zal worden geplaatst. Het advies over de geschiktheid is volgens een van de ontwikkelaars redelijk dwingend: als de projectgroep zegt niks te kunnen doen, denkt de respondent dat de officier hierin mee zou gaan (IO1). Uiteindelijk ligt de beslissingsbevoegdheid voor het wel of niet opleggen van Hack_Right bij een officier van justitie of een rechter (IO2 en IO1). Zij bepalen of de verdachte wel of geen Hack_Right krijgt opgelegd.

5.10 Resumé

In dit hoofdstuk zijn de plannen, ideeën en aannames rondom Hack_Right in kaart gebracht, zodat duidelijk wordt wat Hack_Right is en hoe Hack_Right theoretisch is onderbouwd. De aanleiding van Hack_Right is duidelijk: Hack_Right is eind 2017 opgestart als reactie op de toename van het aantal jonge cybercrime verdachten dat bij het OM instroomt, de verschillen die men ziet tussen traditionele criminelen en cybercriminelen en omdat er nog geen effectieve interventie bestaat voor jeugdige daders van cybercrime. Het doel van Hack_Right is om recidive bij jonge cybercrimedaders te voorkomen en de ICT-talenten van de deelnemers verder te ontwikkelen binnen de kaders van de wet. Uitvoerders en toewijzers van de interventie benoemen verschillende definities en doelen van Hack_Right, waarin de rode draad is dat Hack_Right deelnemers leert hoe zij hun vaardigheden op een goede manier in kunnen zetten. Het leerelement staat volgens respondenten dus centraal. Er is geen consensus over of Hack_Right een strafelement zou moeten bevatten. Dat er geen consensus is onder toewijzers en uitvoerders over of Hack_Right een straffunctie dient te vervullen, is opvallend aangezien ontwikkelaars aangeven dat Hack_Right zich richt op het verminderen van recidive en een aanvulling of alternatief is voor huidige afdoeningsmogelijkheden.

Hack_Right richt zich op verschillende criminogene factoren voor online criminaliteit die in kaart zijn gebracht door de ontwikkelaars. Daarnaast wordt door de interventieontwikkelaars opgemerkt dat er verschillen zijn tussen het profiel van daders van traditionele criminaliteit en daders van cybercriminaliteit. Op basis van de literatuur kan een kritische kanttekening worden gemaakt bij deze onderbouwing. Zo is er op dit moment nog weinig empirisch onderzoek naar kenmerken van cybercriminelen en mogelijke verschillen die zij vertonen ten opzichte van traditionele criminelen (zie voor een overzicht bijvoorbeeld Holt & Bossler (2014), Leukfeldt (2017) en Maimon &

Louderback (2019)). Studies laten niet eenduidig zien dat we te maken hebben met een nieuw type dader. Bovendien zijn enkele van de criminogene factoren die in de plannen worden aangemerkt, technisch gezien geen individuele criminogene factoren zoals omschreven in de 'what-works'-methodiek. De factoren kunnen beter gezien worden als gelegenheidskenmerken die een omgeving creëren waarin crimineel gedrag makkelijker kan ontstaan. Aan deze factoren zelf kan een op het individu gerichte interventie niets veranderen. Wel kan een interventie deelnemers zich bewust maken hoe de gelegenheidsfactoren kunnen leiden tot crimineel gedrag en hoe deelnemers hiermee om kunnen gaan.

De doelgroep van Hack_Right bestaat uit 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. Ook is volgens ontwikkelaars affiniteit en/of interesse met ICT belangrijk om deel te kunnen nemen. De invulling van Hack_Right bestaat volgens de projectplannen uit verschillende modules, die inspelen op de aangemerkte criminogene factoren die een rol spelen bij jeugdige cybercrimedaders. In de praktijk is de invulling volgens ontwikkelaars niet zozeer als module(s) ingevuld, maar zijn elementen van de modules verwerkt in de trajecten. Een handleiding voor de uitvoering van Hack_Right trajecten is nog in ontwikkeling, wat betekent dat een evaluatie van deze handleiding en een evaluatie van de uitvoering van de handleiding in de praktijk nog niet mogelijk zijn. Met betrekking tot de inhoud kan Hack_Right afhankelijk van de leeftijd van de verdachte in de vorm van verschillende strafmodaliteiten aan verdachten worden opgelegd door de officier van justitie of rechter.

Ten slotte zijn er verschillende partijen betrokken bij de opzet en uitvoering van Hack_Right, waaronder de Politie en het OM, justitiële ketenpartners, (cybersecurity)bedrijven en wetenschappelijke instellingen. Op de lange termijn wil Hack_Right verankerd zijn in bestaande procedures van de betrokken organisaties.

6. Hack_Right: de uitvoering

6.1 Inleiding

In het vorige hoofdstuk is besproken wat Hack_Right inhoudt op basis van beleidsdocumenten en interviews met interventieontwikkelaars en uitvoerders en is gebleken dat de plannen nog in ontwikkeling zijn. In het huidige hoofdstuk wordt beschreven hoe de tot nu toe uitgevoerde Hack_Right-trajecten zijn verlopen. Er zal een analyse plaatsvinden op basis van de verschillende onderdelen die in een procesevaluatie centraal staan: bereik, programma-integriteit en dosering. Als het gaat om bereik geeft paragraaf 6.2 een beeld van de Hack_Right-casuïstiek aan de hand van enkele casusbeschrijvingen en laat paragraaf 6.3 zien hoe Hack_Right deelnemers zijn geselecteerd. Met betrekking tot de programma-integriteit wordt de invulling van de verschillende uitgevoerde Hack_Right-trajecten uitvoerig besproken in paragraaf 6.4 en laat paragraaf 6.5 zien hoe er wordt samengewerkt tussen de organisaties die betrokken zijn bij Hack_Right. Ten slotte bespreekt paragraaf 6.6 hoe intensief en compleet de Hack_Right-trajecten zijn uitgevoerd (dosering). Het hoofdstuk sluit af met een samenvatting in paragraaf 6.7.

6.2 Casusbeschrijvingen

In deze paragraaf worden Hack_Right casussen kort beschreven op basis van de interviews met deelnemers van Hack_Right en het casusoverzicht van de projectgroep Hack_Right. Zo wordt duidelijk wie bij Hack_Right terecht zijn gekomen, welk delict zij hebben gepleegd en wat zij voor Hack_Right hebben moeten doen. Uit het casusoverzicht van de projectgroep Hack_Right blijkt dat alle deelnemers die Hack_Right hebben gevolgd man zijn (n=18). De deelnemers zijn verdacht van – of veroordeeld voor – een DDoS-aanval (n=7) of (poging tot) computervredebreuk (n=5) of voor beide delicten (n=1). Andere deelnemers zijn verdacht van fraude en internetoplichting (n=1), medewerking aan een 'booter' service (n=1), het opzetten van phishing campagnes (n=1), of een combinatie van verschillende cybergerelateerde delicten (n=1). Een deelnemer heeft Hack_Right in een vrijwillig kader gevolgd en kan niet worden gekoppeld aan een delict. De casussen worden nu individueel besproken.

Casus 1 (DN1) – Een jongen van 15 jaar oud (14 jaar ten tijde van het delict) heeft een DDoS-aanval uitgevoerd en daardoor onder andere het wifinetwerk van zijn school platgelegd. De deelnemer heeft een Halt-straf opgelegd gekregen met Hack_Right in-

vulling en bij een cybersecuritybedrijf meegekeken op een afdeling, interviews gehouden en een presentatie gemaakt.

Casus 2 (DN2) – In deze casus heeft een jongen van 19 jaar oud (16 ten tijde van het delict) een SQL-aanval uitgevoerd op een gedeelte van de website van zijn school en zo toegang verkregen tot een database, wachtwoorden en uiteindelijk tot het account van de systeembeheerder. Zo kon de deelnemer bijvoorbeeld schoolcijfers, verzuim, roosters en andere zaken aanpassen. De rechter heeft als alternatieve straf Hack_Right opgelegd. Via de reclassering is de deelnemer een aantal keer naar een non-profitorganisatie gegaan op het gebied van cybersecurity.

Casus 3 (DN3) – Een 20-jarige jongen is veroordeeld door de rechter voor het hacken van een website, het hacken van een account van een persoon en het stelen van een domeinnaam. De jongen was 16 jaar ten tijde van de delicten en moest uiteindelijk een werkstraf uitvoeren bij de reclassering in de vorm van Hack_Right. Hiervoor heeft hij twee interviews moeten geven (waaronder een voor een groep scholieren) en voor publiek verteld wat voor delict hij gepleegd heeft.

Casus 4 (DN4) – In de vierde casus heeft een jongen van 17 jaar (16 jaar tijdens het delict) met behulp van een DDoS-aanval (een deel van) het netwerk van zijn school platgelegd en daarmee ook de netwerken van allerlei andere organisaties die op hetzelfde netwerk zaten aangesloten. De deelnemer heeft een Halt-straf gekregen met Hack_Right invulling en is bij een cybersecuritybedrijf geweest waar hij met ethisch hackers heeft gesproken en een Responsible Disclosure guideline heeft doorgenomen.

Casus 5 (DN5) – In deze casus heeft een 17-jarige jongen (14 jaar ten tijde van het delict) accounts gehackt. Nadat de politie de jongen heeft aangehouden, heeft hij een Halt-straf gekregen. Bij Halt heeft de deelnemer opdrachten gemaakt en is hij naar een cybersecuritybedrijf geweest. Hier heeft de jongen een presentatie gekregen over ethisch hacken en een applicatie mogen testen.

Casus 6 (DN6) – Een jongen van 19 jaar oud (17 jaar ten tijde van het delict) heeft zijn schoolnetwerk gehackt met behulp van een SQL-injectie. De deelnemer heeft een Halt-straf gekregen waarin hij opdrachten heeft gemaakt bij Halt en een programma van twee dagen heeft gevolgd bij een ICT-bedrijf. Hier heeft hij gesproken met medewerkers van het ICT-bedrijf en een richtlijn van het OM over cybercrime herschreven.

Casus 7 (DN7) – In een andere casus heeft een jongen van 16 jaar (15 jaar tijdens het delict) een laptop van school gehackt waardoor hij mee kon kijken met een andere scholier die de laptop gebruikte. Als Halt-straf heeft de deelnemer opdrachten gemaakt bij Halt en een programma van twee dagen gevolgd bij een bedrijf. Bij het bedrijf heeft de respondent mensen geïnterviewd, een reflectieverslag gemaakt en een technische opdracht ('capture the flag') uitgevoerd.

Casus 8 (DN8) – Een 18-jarige jongen (15 jaar ten tijde van het delict) heeft het systeem van een school gehackt en zo inloggegevens verkregen waarmee hij cijfers en roosters aan kon passen. De deelnemer heeft een werkstraf met reclasseringstoezicht gekregen en is daarvoor twaalf keer naar een non-profitorganisatie geweest op het gebied van cybersecurity. Bij deze organisatie leerde de jongen (Java-)programmeren, kwam af en toe een cryptograaf langs en werden lessen gegeven.

Casus 9 (DN9) – In de casus heeft een jongen van 19 jaar (ongeveer 16 jaar ten tijde van de delicten) verschillende websites en een online spel gehackt. Ook heeft de deelnemer hierdoor toegang verkregen tot databases. De jongen heeft een werkstraf gekregen met reclasseringstoezicht waarin een Hack_Right programma gevolgd moest worden. Hiervoor heeft de respondent het boek 'helpende hackers' moeten lezen, meegedaan aan programma waar men spreekt over informatietechnologie en twee interviews gegeven.

Casus 10 (DN10) – In deze casus heeft een jongen van 20 jaar (17 of 18 jaar ten tijde van het delict) zich schuldig gemaakt aan online oplichting. De jongen kocht pakketjes bij bedrijven, gaf vervolgens zijn gegevens aan een tussenpersoon, die op zijn beurt het bedrijf belde dat het pakketje niet was aangekomen zodat de jongen het geld weer terugkreeg. De deelnemer heeft tijdens een TOM-zitting een werkstraf gekregen waarin hij Hack_Right heeft gevolgd. Ook heeft de jongen een geldbedrag moeten betalen aan slachtoffers. Tijdens Hack_Right heeft de jongere meegedaan aan een programma waar men spreekt over informatietechnologie, twee interviews gegeven en een presentatie gegeven over cybercriminaliteit.

6.3 Selectie deelnemers en strafmodaliteiten

In deze paragraaf staat centraal hoe personen werden geselecteerd voor Hack_Right. De criteria en overwegingen die bij het OM centraal stonden om wel of geen Hack_Right op te leggen, worden besproken in sectie 6.3.1. In sectie 6.3.2 worden de bereidheid tot deelname en motivatie van deelnemers besproken. Ten slotte laat sectie 6.3.3 zien via welke strafmodaliteiten Hack_Right is opgelegd aan deelnemers.

6.3.1 *Selectiecriteria en overwegingen Openbaar Ministerie*

Personen uit verschillende arrondissementen die vanuit het Openbaar Ministerie betrokken zijn geweest bij de oplegging van Hack_Right (n=5) zijn gevraagd naar hun overwegingen voor het wel of niet opleggen van Hack_Right aan verdachten. Uit de antwoorden van de respondenten blijkt dat alle respondenten aangeven dat de ernst van het feit (n=5) en de affiniteit van de verdachte met ICT (n=5) van belang zijn voor het opleggen van Hack_Right. Bijna alle respondenten vinden de leeftijd van de verdachte (n=4), persoonlijke omstandigheden (n=4) en het motief (n=4) belangrijk. Een overzicht van alle factoren is weergegeven in tabel 4. Na de tabel gaan we uitgebreid in op de door de respondenten genoemde factoren.

Tabel 4: selectiecriteria op basis van interviews met respondenten van het OM (n=5)

Factor	Aantal respondenten (n=5)
Ernst van het delict	5
Affiniteit/kennis ICT	5
Leeftijd	4
Persoonlijke omstandigheden	4
Motief	4
Bereidheid deelname	2
Ouderdom feit	2
Delict geschiedenis	2
Bekentenis	1
Wensen slachtoffer	1
Duur Halt-straf	1
Normbesef	1
Criteria voor Halt^{+}-straf	1

Ernst van het feit - De ernst van het feit speelt bij alle respondenten een rol bij de keuze voor Hack_Right. Het feit moet volgens de meeste respondenten van geringe ernst zijn om in aanmerking te komen voor Hack_Right (n=4). Zo geven twee respondenten aan dat deelnemers niet in aanmerking kwamen voor Hack_Right omdat de delicten te zwaar waren (OM2, OM4) en geeft een andere respondent aan dat Hack_Right geen reële optie zou zijn geweest als de verdachte vitale infrastructuur had aangevallen (OM3). Aan de andere kant kan Hack_Right volgens een van de respondenten ook te zwaar zijn, bijvoorbeeld voor gamers die DDoS-aanvallen uitvoeren en niet doorhebben dat het strafbaar is (OM2). Deze respondent geeft tegelijkertijd ook aan dat een van de casussen te zwaar was voor een Halt-afdoening en dat daarom Hack_Right is opgelegd (OM2). Ten slotte sluit een van de respondenten niet uit dat Hack_Right ook in zwaardere gevallen zou kunnen worden opgelegd, maar dat dan niet alleen Hack_Right wordt opgelegd als straf (OM5).

Affiniteit/kennis van ICT – Alle respondenten geven aan dat de verdachte affiniteit of kennis van ICT nodig heeft om in aanmerking te komen voor Hack_Right. Enkele respondenten verwijzen hiervoor naar de criteria die vanuit de projectgroep Hack_Right zijn gegeven (n=2). Het volgende citaat laat zien welke rol affiniteit met ICT speelt voor de respondenten:

> *"Die jongen moest zijn toekomstige werk, waarvoor hij studeert, in die ICT-wereld hebben. Dus het leek mij vanuit die hoedanigheid heel zinvol dat hem duidelijk wordt gemaakt – want hij was al meerderjarig – wat nou de grens is en wat de consequenties zijn van het overtreden van die grens." (OM3)*

Ook een verdachte die voor het specifieke delict geen gebruik heeft gemaakt van veel technische kennis – maar wel zoveel ICT-kennis had dat hij wel dingen zelf aan het bouwen was – kwam in aanmerking voor Hack_Right (OM4). Een voorbeeld van een verdachte die niet in aanmerking is gekomen voor Hack_Right vanwege zijn ICT-vaardigheden is iemand die niet zelf maar met behulp van een dienst – waar hij via vrienden aan gekomen was – DDoS-aanvallen uitvoert (OM5).

Leeftijd – Vier van de vijf respondenten geven aan dat de leeftijd een rol speelt bij het opleggen van Hack_Right. Een van de respondenten refereert naar specifieke leeftijden tussen de 12 en 23 jaar (OM5). Andere respondenten geven aan Hack_Right in principe te overwegen voor jeugdigen tot 18 jaar (OM1, OM4). Het volgende citaat illustreert dit:

> *"En eentje die hadden we wel op het oog voor Hack_Right, maar die bleek net, volgens mij 19 te zijn geweest ten tijde van de pleegdatum. Dus die kwam niet in aanmerking daarvoor." (OM1)*

De respondent geeft aan niet geheel op de hoogte te zijn geweest van de ruime inzetbaarheid van Hack_Right in de vorm van andere strafmodaliteiten dan Halt.

Persoonlijke omstandigheden – Bijna alle respondenten van het OM benoemen ook persoonlijke omstandigheden als een factor die meespeelt bij het opleggen van Hack_Right (n=4). Zo werd bijvoorbeeld een verdachte met mogelijk autisme spectrum problematiek voor Hack_Right niet naar een bedrijf verwezen maar naar een organisatie die ervaring heeft met deze doelgroep (OM1). Bij een andere verdachte werd Hack_Right niet opgelegd omdat er al een andere zaak liep met een intensief begeleidingstraject (OM5). Ten slotte wordt bij de persoonlijke omstandigheden ook gerefereerd naar een verdachte die een ICT-opleiding volgde, waardoor het niet wenselijk zou zijn geweest om een straf op te leggen omdat dit een aantekening oplevert op zijn justitiële documentatie (OM3). De verdachte is daarom doorverwezen naar Hack_Right.

Motief – Vier van de vijf respondenten benoemen het motief als een factor die een rol speelt bij de keuze voor Hack_Right. In relatie tot motief wordt vooral benoemd dat een financieel motief een contra-indicatie zou zijn voor het opleggen van Hack_Right. Volgens respondenten is er bij een financieel motief forsere problematiek en recidivegevaar (OM1) en is er een strengere straf nodig voor deze doelgroep (OM5). Een andere respondent geeft aan dat een rechter wel Hack_Right heeft opgelegd bij iemand met een financieel oogmerk (OM4). Ten slotte verwijst een respondent – bij het noemen van motief als selectiecriterium – naar de mate waarin iemand weet dat hij of zij strafbare feiten heeft gepleegd (OM2). Iemand die niet wist dat hij of zij strafbare feiten heeft gepleegd, komt volgens de respondent eerder in aanmerking voor Hack_Right dan iemand die volledige opzet op het feit had.

Naast de zojuist besproken factoren worden er door individuele respondenten ook andere factoren genoemd. Zo wordt genoemd dat de verdachte bereid moet zijn om aan Hack_Right deel te nemen (n=2). Daarnaast geeft een respondent aan dat een verdachte van een relatief ernstigere zaak die langer geleden heeft plaatsgevonden toch Hack_Right heeft gekregen, waar dit bij een kersverse zaak wellicht anders was geweest (OM1). Ook benoemen twee respondenten dat het moet gaan om een eerste delict. Ten slotte wordt door individuele respondenten genoemd dat de verdachte een bekentenis moet afleggen, dat de wensen van het slachtoffer worden meegewogen, dat de duur van een eventuele Halt-straf wordt meegewogen en dat de juridische criteria voor een Halt-straf worden meegenomen.

Een van de respondenten maakt echter duidelijk dat het lastig is om zwart op wit te krijgen waarom iemand nu precies wel of geen Hack_Right krijgt opgelegd. Het gaat uiteindelijk om een weging van de verschillende factoren:

> *"De ernst van het feit, iemand zijn achtergrond, wat het voor iemand inhoudt om justitiële documentatie te krijgen en dat soort dingen. Maar dat zijn allemaal wegingsfactoren. Het is zo lastig om te zeggen, je slaat de ene keer rechtsaf en de andere keer linksaf." (OM2)*

6.3.2 *Bereidheid deelname & motivatie*

Uit de interviews met uitvoerders van Hack_Right blijkt dat de meeste verdachten/deelnemers bereid zijn om aan Hack_Right deel te nemen. Tijdens de uitvoering van de trajecten is een enkele deelnemer volgens uitvoerders echter minder of niet gemotiveerd.

Met betrekking tot de bereidheid tot deelname van deelnemers aan Hack_Right geven toewijzers van het OM aan dat verdachte(n) hebben ingestemd (OM3), bereid zijn om deel te nemen (OM1), openstonden voor Hack_Right (OM5) of het zelfs geweldig vinden om deel te nemen aan Hack_Right (OM4). Bij twee casussen weten de toewijzers van het OM niet precies of de verdachte bereid was om deel te nemen (OM1, OM2).

Met betrekking tot de motivatie tijdens de uitvoering van de trajecten geven respondenten van Halt aan dat deelnemers gemotiveerd waren (HA2 en HA1). De reclasseringswerker vertelt dat de deelnemers redelijk enthousiast waren en dat er ten tijde van het interview geen deelnemers waren die iets met tegenzin deden of het lieten lopen (RE1). Een wisselvalliger beeld omtrent de motivatie komt naar voren tijdens de interviews met respondenten van bedrijven. Zo geeft een van de respondenten aan dat de twee deelnemers er niet per se op zaten te wachten (CS2). De eerste deelnemer kon in de loop van de dag bewogen worden om gemotiveerd te zijn, de tweede deelnemer was erg ongemotiveerd en had geen idee waarom hij bij het bedrijf zat en niet 'mest aan het scheppen was op de kinderboerderij'. (CS2). Een andere respondent laat weten dat een

eerste deelnemer erg gemotiveerd was en een tweede deelnemer er niet was geweest als hij niet verplicht was om te komen (CS5). Weer een andere respondent geeft aan dat de deelnemer van zijn traject wel gemotiveerd was (CS1). Een respondent die langere trajecten heeft begeleid, vertelt dat de jongeren allebei wel een kans zagen (CS4). Wel stelden de deelnemers veel uit tot het laatste moment, waar ze op zijn aangesproken door de respondent. Ten slotte geeft een respondent aan dat de jongere tijdens zijn traject niet gemotiveerd was, erg passief was en weinig teruggaf (CS7). Deze deelnemer heeft het traject niet afgemaakt.

6.3.3 *Strafmodaliteiten*

Uit een casusoverzicht[15] van achttien Hack_Right trajecten blijkt dat er dertien trajecten zijn opgelegd door een officier van justitie, vier trajecten door een rechter en dat er één traject vanuit een vrijwillig kader heeft plaatsgevonden. Een overzicht van de verschillende strafmodaliteiten waarin Hack_Right heeft plaatsgevonden is te vinden in tabel 5.

Tabel 5: strafmodaliteiten van de tot nu toe uitgevoerde Hack_Right casussen.

Strafmodaliteit	N	Opgelegd door	Toezichthouder
Halt-straf	10	OvJ	Halt
Transactie	2	1 OvJ, 1 rechter	1 OM, 1 reclassering
Voorwaardelijk sepot	2	OvJ	Reclassering
Taakstraf en reclasseringstoezicht	1	Rechter	Reclassering
Voorwaardelijke jeugddetentie, reclasseringstoezicht, meewerken aan HR	1	Rechter	Reclassering
Vrijwillig kader	1	N.v.t.	Halt
Bijzondere voorwaarde voor schorsing	1	Rechter	Reclassering

Van de trajecten die zijn opgelegd, hebben tien trajecten plaatsgevonden in het kader van een Halt-straf, opgelegd door officieren van justitie. Verder waren twee trajecten onderdeel van een transactie. Een van deze transacties vond plaats bij een officier van justitie, de andere transactie vond plaats bij een rechter. Twee trajecten waren onderdeel van een voorwaardelijk sepot bij officieren van justitie. Ook is Hack_Right een keer uitgevoerd als onderdeel van een taakstraf met reclasseringstoezicht, een keer in combinatie met voorwaardelijke jeugddetentie en reclasseringstoezicht en een keer als bijzondere voorwaarde voor schorsing. In deze gevallen heeft de rechter Hack_Right opgelegd. Uit interviews met toewijzers van het OM komt eenzelfde beeld naar voren met betrekking tot de verschillende strafmodaliteiten die zijn opgelegd.

15 Een casusoverzicht met informatie over de tot nu toe uitgevoerde Hack_Right-trajecten is opgesteld door de casemanager van Hack_Right. Het overzicht is verkregen op 9 maart 2020 en daarom een momentopname. Op de zojuist genoemde datum waren veertien van de achttien casussen afgerond en vier casussen nog lopend.

6.4 Invulling casussen

Zoals in paragraaf 5.7 is besproken, is de invulling van de tot nu toe uitgevoerde Hack_Right-trajecten niet duidelijk te herleiden tot concrete modules. Ook tijdens interviews met respondenten die betrokken zijn bij de uitvoering (n=11) blijkt dat sommige respondenten niet (geheel) bekend zijn met de modules die worden beschreven in de projectplannen (n=4). Uit de interviews volgt dat er een onderscheid gemaakt kan worden tussen deelnemers die een Hack_Right traject via Halt hebben gevolgd en deelnemers die een traject via de reclassering hebben gevolgd. De Halt-straf bestaat enerzijds uit opdrachten en gesprekken bij Halt en anderzijds uit een programma van een of twee dagen bij een (cybersecurity)organisatie. Voor de reclasseringstrajecten verschillen de activiteiten die zijn uitgevoerd onder Hack_Right sterk per deelnemer. In deze paragraaf wordt per organisatie (Halt, reclassering en bedrijven) aangegeven hoe zij invulling hebben gegeven aan de verschillende Hack_Right trajecten die zij hebben uitgevoerd.

6.4.1 *Invulling Halt-straf*

Uit de interviews met Halt-medewerkers is gebleken dat de Hack_Right deelnemers die zij hebben begeleid een maximale Halt-straf van twintig uur hebben gekregen (HA2 en HA1). HA1 heeft twee Hack_Right-trajecten uitgevoerd en HA2 heeft één Hack_Right-traject uitgevoerd. De invulling van de Halt-straf bestaat uit een programma bij Halt en een programma bij een bedrijf of organisatie.

Het programma dat de deelnemers bij Halt volgen is voor alle Hack_Right deelnemers hetzelfde (HA2 en HA1). Halt voert drie gesprekken van één uur met de jongeren en de jongeren dienen thuis drie opdrachten van één uur te maken. Tijdens de drie gesprekken wordt er gereflecteerd op het delict, worden de opdrachten die de deelnemers maken besproken en wordt eventuele problematiek in kaart gebracht aan de hand van het LIJ-instrument. Het LIJ-instrument is een signaleringsinstrument waarbij de problematiek van de jongere in kaart wordt gebracht aan de hand van voornamelijk risicofactoren, maar ook beschermende factoren (HA2). Een belangrijke opmerking is hier dat het LIJ-instrument is ontwikkeld voor traditionele vormen van criminaliteit. Het is vooralsnog onduidelijk of het instrument ook toepasbaar is op daders van online criminaliteit. Op basis van de signalering kunnen jongeren eventueel worden doorverwezen naar andere hulporganisaties (HA2 en HA1). De zojuist genoemde stappen vinden ook plaats met jongeren die niet aan Hack_Right deelnemen. De opdrachten die de jongeren moeten maken, zijn door Halt en ICT-medewerkers specifiek ontwikkeld voor Hack_Right (HA2, HA1). De eerste opdracht is een presentatie maken over hacking. De tweede opdracht is het schrijven van een verslag over onder andere de stappen die de jongere heeft ondernomen om te leren hacken, het delict dat de jongere gepleegd heeft, het motief voor het plegen van het delict en de gevolgen van het delict (HA1). Een derde opdracht bestaat uit het schrijven van een motivatiebrief voor het bedrijf of

de organisatie waar de jongere het tweede gedeelte van de Halt-straf doorbrengt (HA2, HA1). In de motivatiebrief dienen de jongeren aan te geven waarom ze naar een bepaald bedrijf moeten, willen en/of kunnen (HA2). In sommige gevallen moeten de jongeren ook een excuusopdracht maken (HA2 en HA1). Zo moest een van de deelnemers bij Halt een brief schrijven naar zijn school en naar zijn moeder (HA1). Andere deelnemers hebben geen excuusopdracht gemaakt omdat het excuus al had plaatsgevonden of omdat de school had besloten om geen aangifte te doen (HA2).

De uren die na de gesprekken en opdrachten nog overblijven van de Halt-straf worden bij het bedrijf of de organisatie ingevuld als stage of werkstraf (HA2 en HA1), zie ook paragraaf 6.4.3. In één geval heeft een deelnemer meegewerkt aan het opzetten van een politiecampagne rondom hacking, omdat er niet tijdig een bedrijf of organisatie gevonden kon worden (HA2).

6.4.2 *Invulling reclasseringstraject*

Bij de reclassering zijn de Hack_Right-trajecten (bijna) allemaal uitgevoerd door dezelfde reclasseringswerker (RE1). De respondent geeft aan vijf of zes Hack_Right-trajecten te hebben gehad ten tijde van het interview. Vaak zijn de trajecten een TOM (Taakstraf Openbaar Ministerie)-afdoening geweest met verplicht reclasseringscontact, waarbij Hack_Right bij de reclassering als werkstraf is ingehangen. Hoe de invulling van Hack_Right precies gedefinieerd wordt, is volgens de respondent niet belangrijk, zoals eerder is benoemd in paragraaf 5.3.

De taak van de reclasseringswerker is om zowel advies te geven als toezicht te houden. Tijdens de adviesfase legt de respondent contact met de deelnemer om inzicht te krijgen in het gedrag van de deelnemer in relatie tot het delict (RE1). Voor de Hack_Right-trajecten spreekt de respondent de deelnemers drie tot vier keer, waar dit bij reguliere trajecten één tot twee keer is. Zo ontstaat er een profiel van de verdachte omtrent de vaardigheden, kennis en problematiek die een rol spelen bij het delict. De respondent geeft aan dat deze eerste fase belangrijk is om tot deugdelijke adviezen te komen:

> *"Als je een goede interventie wilt doen, zou je goed moeten weten hoe iemand in elkaar zit om goede stappen te kunnen zetten." (RE1)*

Tijdens de adviesfase wordt er gebruikgemaakt van de RISC, een risicotaxatie-instrument dat de reclassering gebruikt. De respondent geeft aan dat de RISC handig is om te structureren, maar dat er ook belangrijke aandachtspunten zijn bij cyberdaders die niet in de RISC vermeld staan. Voorbeelden die de respondent benoemt, zijn computerkennis, online sociale netwerken en gamen. Samen met personen uit de projectgroep van Hack_Right kijkt de respondent naar een geschikte invulling en wordt een voorstel voor een Hack_Right-traject voorgelegd aan het OM. De respondent geeft aan

dat de reclassering uiteindelijk de opdracht krijgt van de rechter of officier van justitie om voor een bepaald aantal uren invulling te geven aan Hack_Right. Per activiteit kunnen de uren dan worden afgeschreven. Voor een ander traject stond geen aantal uren, maar was Hack_Right opgenomen als bijzondere voorwaarde.

De uiteindelijke invulling van de tot nu toe uitgevoerde Hack_Right-trajecten via de reclassering verschilt sterk per deelnemer. Zo hebben deelnemers bij de cyberwerkplaats werkzaamheden uitgevoerd, meegewerkt aan een praatprogramma waar de jongeren hebben moeten uitleggen wat ze gedaan hebben en waarom, bij ICT-bedrijven meegekeken, interviews gegeven voor een online politiekrant, presentaties gegeven en is er een deelnemer geïntroduceerd bij een hackerspace.

6.4.3 *Invulling bedrijven*

Vanuit zowel Halt als de reclassering zijn de Hack_Right deelnemers gekoppeld aan een bedrijf of organisatie. De invulling voor het programma dat de deelnemers volgen bij de bedrijven wordt (grotendeels) overgelaten aan de bedrijven zelf en voorgelegd of afgestemd met de projectgroep Hack_Right, Halt en/of reclassering (CS3, CS2, CS5, CS1, CS4, CS7). De invulling bij bedrijven vanuit een Halt- en reclasseringstraject wordt nu besproken.

Halt-trajecten
Cybersecurity bedrijf A is bij 5 Hack_Right-trajecten betrokken geweest die als Halt-straf zijn uitgevoerd. De directeur van dit bedrijf geeft tijdens het interview aan dat het bedrijf zelf een programma voor Hack_Right deelnemers heeft bedacht (CS3). Deelnemers krijgen eerst een deel theorie, waarbij wordt uitgelegd wat wel en niet mag met betrekking tot hacking, hoe men verantwoord een beveiligingslek kan melden en hoe er legaal geld mee verdiend kan worden. Ook wordt uitgelegd hoe hackers van het bedrijf in de praktijk te werk gaan. Bovendien wordt er met de deelnemer gesproken over de redenen en motivaties voor het hacken. Vervolgens krijgen de deelnemers opdrachten waarmee ze hun technische vaardigheden kunnen uitoefenen, zoals een *Juice Shop,* een standaardapplicatie waar beveiligingslekken in zitten, en *Hack In The Box*. Ook hebben enkele deelnemers met behulp van Raspberry Pi's in een eigen omgeving kunnen oefenen met hacken (CS5). De deelnemers krijgen tijdens de opdrachten begeleiding van medewerkers van het bedrijf. Afhankelijk van het soort jongere, het delict dat gepleegd is en de passie van de jongeren hebben zij een opdracht gekregen. Ten slotte hebben twee deelnemers een presentatie moeten geven over wat ze precies gedaan hebben en geleerd hebben bij het bedrijf. De derde deelnemer heeft een responsible disclosure uit moeten schrijven (CS6). De trajecten duurden allemaal één dag (acht uur) of zijn binnen twee kortere dagen uitgevoerd. Twee medewerkers die de jongeren hebben begeleid, zijn geïnterviewd (CS6 en CS5).

Een medewerker van IT-consultancy bedrijf B heeft twee Hack_Right-trajecten begeleid die onderdeel waren van een Halt-straf (CS2). De trajecten bestonden uit twee

dagen van zes uur. Het traject van de eerste deelnemer bestond de eerste dag uit een kennismaking en een uitleg van een medewerker van het Nationaal Cyber Security Centre (NCSC) over responsible disclosure en de wet Computercriminaliteit. Ook heeft de deelnemer tijdens de eerste dag een opdracht gemaakt waarin hij diende te reflecteren op het delict dat hij heeft gepleegd. Tijdens de tweede dag heeft de deelnemer aan een tweede opdracht gewerkt waarin hij een nieuwe versie van de jongerenrichtlijn voor cybercrime op de site van het OM heeft geschreven. Ook is de tweede dag met de deelnemer gesproken over een toekomstige carrière. De respondent geeft aan dat dit een soort coachende gesprekken zijn geweest. Het tweede traject heeft een vergelijkbaar programma gehad, maar dan afgestemd op DDoS-aanvallen.

Bij consultancybedrijf C is één Hack_Right-traject uitgevoerd vanuit een Halt-straf (CS1). Het programma bij dit bedrijf duurde twaalf uur. Eerst vond er een intakegesprek van één uur plaats met de deelnemer. Daarnaast heeft de deelnemer vier uur lang interviews afgenomen met werknemers binnen het bedrijf. Ten slotte heeft de jongere een presentatie gegeven van één uur waarin hij moest uitleggen wat hij had geleerd. De rest van de uren waren bestemd voor de voorbereiding van de interviews en het uitwerken van de presentatie (CS1).

Reclasseringstrajecten
Een medewerker van organisatie D heeft een Hack_Right traject uitgevoerd waar de reclassering bij betrokken was (CS7). De tijdsduur die aan het traject is verbonden, is niet bekend bij de respondent. De opdracht voor de deelnemer was om een presentatie te maken op basis van een interview/gesprek met de respondent. Er heeft een gesprek plaatsgevonden van één à anderhalf uur tussen de deelnemer, respondent en reclasseringswerker. Tijdens dit gesprek is aan de deelnemer uitgelegd waar de jongere bij betrokken was (de deelnemer had een DDoS-aanval gekocht en uitgevoerd), dat hij door het delict een ecosysteem in leven houdt en hoe hij een presentatie kon maken. De presentatie zou worden gegeven aan de officier van justitie, maar de deelnemer is uitgevallen tijdens het traject (zie paragraaf 6.6).

Een laatste respondent die werkzaam is bij cybersecuritybedrijf E heeft twee gelijksoortige Hack_Right-trajecten uitgevoerd (CS4). De duur van de trajecten was gemiddeld 120 uur in een periode van drie tot zes maanden. Een van de trajecten was in het kader van een reclasseringstraject en het andere betrof een vrijwillig traject. De respondent geeft aan dat de deelnemers zelf een of meerdere projecten hebben moeten bedenken. Eerst is er een introductiebijeenkomst geweest en vervolgens zijn er twee of drie bijeenkomsten geweest om de casus 'fijn te slijpen'. Vervolgens hebben de jongeren in de projecten iets moeten bouwen voor het bedrijf. Deze opdrachten voerden de deelnemers voornamelijk thuis uit. Tijdens overlegmomenten kwamen de respondent en deelnemer samen. Ook werd er overlegd via instant messaging. De deelnemers moesten logboeken bijhouden met de werkzaamheden die zij verrichtten. Ten slotte moeten de deelnemers aan het eind van het traject hun projecten presenteren aan het OM.

6.4.4 *Individuele afstemming*

Uit de vorige secties is gebleken dat de invulling van Hack_Right-trajecten sterk verschilt per deelnemer. Tijdens interviews met uitvoerders en ontwikkelaars van Hack_Right wordt duidelijk dat individuele factoren zoals technische kennis, risicofactoren en motieven een rol spelen bij de wijze waarop Hack_Right-trajecten worden ingevuld. Vooral de invulling van reclasseringstrajecten en het programma dat deelnemers volgen bij bedrijven probeert men af te stemmen op de eigenschappen van de deelnemers. Het volgende citaat van een ontwikkelaar illustreert dit:

> *"Het is nu nog extreem maatwerk. Het traject bij het bedrijf wordt echt per persoon op maat gemaakt. Dus bijvoorbeeld: 'Wat heeft deze jongere gedaan? Een DDoS-aanval? Dan is het wel handig dat we iets uitleggen over DDoS. Hij heeft technische affiniteit, of doet applicatie-ontwikkeling? Dan kunnen we hier iets over vertellen en daarover.'" (IO2)*

Een reclasseringswerker geeft aan dat het bij de invulling van Hack_Rigt-trajecten belangrijk is om te kijken hoe het best aansluiting bij de daders kan worden gevonden en wat daders kunnen leren om meer slachtoffers te voorkomen (RE1). Het volgende citaat illustreert waarom deze individuele afstemming volgens de respondent belangrijk is:

> *"Wat Hack_Right sterk maakt, is dat je steeds kunt kijken wat er voor iemand nodig is, zonder het in een mal te gieten. Dat maakt ook dat je, waar de een linksom moet, kan de ander rechtsom of dwars door het midden. Als dat binnen Hack_Right niet meer mogelijk is, dan is Hack_Right ten dode opgeschreven binnen vier jaar. De techniek verandert, alles verandert. Als je dat nu in een bepaald stramien gooit, dan is over drie jaar alles weer anders en ben je niet flexibel genoeg om met de veranderingen mee te gaan. Je moet steeds weer anticiperen op datgene waar ze mee bezig zijn geweest." (RE1)*

Specifieke individuele factoren die een rol spelen bij de invulling van Hack_Right zijn de technische kennis en vaardigheden, risicofactoren en het motief van de deelnemer. De factoren en wijze waarop hier wel of geen rekening mee gehouden wordt tijdens de invulling van Hack_Right casussen worden nu verder besproken.

Technische kennis en vaardigheden
Respondenten van bedrijven geven aan dat zij opdrachten graag afstemmen op de technische vaardigheden van de deelnemers. Het volgende citaat illustreert dit:

> *"Hoe meer iemand kan, hoe belangrijker het wordt dat we beter begrijpen wat hij dan echt al kan en weet, op welke deelgebieden ook." (CS1)*

In een van de Hack_Right-casussen, bijvoorbeeld, heeft een deelnemer – die zelf aangaf veel kennis en ervaring te hebben met JAVA – een JAVA-assessment doorlopen met

allerlei opdrachten (CS3). Er zijn verschillen in de mate waarin de opdrachten die deelnemers hebben gemaakt aansloten bij hun vaardigheden. Zo waren opdrachten bij bedrijven in sommige gevallen te lastig voor deelnemers (CS3, CS5) en waren opdrachten bij Halt soms te makkelijk voor deelnemers (HA2, IO2). Dat opdrachten bij Halt in sommige gevallen te makkelijk waren, wordt ook bevestigd door deelnemers (zie hiervoor paragraaf 7.5). Een van de ontwikkelaars benoemt dat men graag niveauverschil zou willen in de Halt-opdrachten (IO2). Respondenten van bedrijven of organisaties geven aan dat zij flexibel zijn in de opdrachten die aan deelnemers kunnen worden aangeboden. Bij bedrijf A is er bijvoorbeeld een groot arsenaal aan opdrachten waaruit gekozen kan worden (CS3) en kunnen oefenapplicaties worden voorgelegd aan jongeren met geavanceerde kennis en aan jongeren met minder kennis (CS5). Het volgende citaat illustreert hoe de afstemming ook tijdens het traject nog plaatsvindt:

> *"Dan pak je een jonge vent bij ons die al heel veel geleerd heeft, maar die begint dan eigenlijk al op een verkeerd niveau met zo'n jongere dan te sparren. En dan merk je al vrij snel van: 'Oké, hier gaat hij niet uitkomen.' Dan geef je hem wat meer hulp, of dan is deze opdracht eigenlijk een beetje te ver." (CS3)*

Het is daarom volgens respondenten belangrijk om de technische kennis en vaardigheden van deelnemers van tevoren in kaart te brengen (n=5). Er wordt op dit moment nagedacht over het ontwikkelen van een intake-assessment om de technische vaardigheden en interesses van deelnemers in te kunnen schatten (IO1).

Risicofactoren

Medewerkers van Halt geven aan dat er tijdens de gesprekken met deelnemers een signalering plaatsvindt waarbij verschillende leefgebieden van de deelnemer worden langsgelopen: school, werk, vrienden, sport, geweld, psychosociale problemen enzovoort. (HA1 en HA2). Op basis hiervan kan Halt jongeren doorverwijzen op het moment dat bepaalde problematiek een rol speelt. Zo is een autistische jongen vanuit Halt gekoppeld aan organisatie E, een ontwikkelingsgelegenheid op het gebied van ICT waar pedagogen en psychologen werkzaam zijn die hulpverlening kunnen bieden (HA2). Daarnaast geeft een van de ontwikkelaars aan hoe men tijdens overleg over de invulling van een Hack_Right-traject rekening probeert te houden met criminogene factoren:

> *"Het is niet altijd dat er een lijstje met criminogene factoren bij wordt gepakt, maar het zit wel in ons achterhoofd. Dus je maakt wel de match tussen de criminogene factor en de module. Als we in een delict terug zien komen dat online grenzen niet helder zijn, dan richten we wel op training ethische/juridische grenzen. Straks is daar een training voor, nu wordt meegegeven aan bedrijven dat daar aandacht aan moet worden besteed. Als diegene zich niet bewust is van de schade, geven we dat mee aan het bedrijf." (IO2)*

De risicofactoren worden volgens de ontwikkelaar uit zowel dossiers als uit beschrijvingen van de politie of gesprekken met Halt-medewerkers gehaald (IO2). Een respondent van een cybersecuritybedrijf is kritisch en geeft aan dat er tijdens werkgroepen veel is gesproken over leerbehoeften en risicofactoren, maar dat hij twijfelt of daar in de praktijk al invulling aan wordt gegeven (CS3).

Motief
Ten slotte geeft een ontwikkelaar aan dat ook het motief een belangrijke rol speelt bij de invulling. Het volgende citaat laat zien hoe dit volgens de respondent de invulling beïnvloedt:

> *"We willen zo veel mogelijk dat het traject inspeelt op het motief van iemand. Dus als er wel een beetje geld heeft meegespeeld, dan red je het niet alleen met een powerpoint met wat wel en niet mag bij ethisch hacken. Dan moet je meer denken aan een coachingstraject en het laten zien van een positief alternatief. De boodschap is dan meer van een schop onder de kont. Dat is een heel ander traject dan wanneer je zit met iemand van Halt die schrikt van de politie en uit nieuwsgierigheid zat te prutsen." (IO2)*

Ondanks dat de invulling van de tot nu toe uitgevoerde Hack_Right-trajecten sterk verschilt per deelnemer, hebben de deelnemers volgens de ontwikkelaar wel dezelfde ervaring gehad:

> *"De meeste jongeren zullen wel ongeveer dezelfde ervaring hebben gehad: er zal een wereld open zijn gegaan, ze hebben iemand gesproken met dezelfde interesses, misschien nieuwe interesses gekregen om zich op een bepaalde manier te oriënteren. Maar hoe dat heeft plaatsgevonden is wel bij iedereen net wat anders gegaan. En de producten die ze hebben opgeleverd zijn allemaal ongeveer anders." (IO2)*

6.5 Samenwerking tussen betrokken partijen

In deze paragraaf wordt de samenwerking tussen de verschillende partijen die betrokken zijn bij Hack_Right besproken. De partijen die met elkaar samenwerken, zijn de projectgroep Hack_Right, toewijzers van het Openbaar Ministerie, Halt-medewerkers, Reclasseringswerkers en uitvoerders van bedrijven of organisaties. Uit interviews met ontwikkelaars blijkt dat de samenwerking met strafrechtketenpartners tot september 2020 loopt (IO2). Om de samenwerking te kunnen verlengen, moeten alle partijen akkoord zijn met een verlenging en zijn financiële middelen nodig. Voor de samenwerking met bedrijven is een intentieverklaring getekend waarin bedrijven bevestigen dat ze willen meewerken aan Hack_Right (IO1). Het is onduidelijk of er een termijn is gekoppeld aan de intentieverklaring van de bedrijven. Er vindt samenwerking plaats tussen de zojuist genoemde partijen voorafgaand, tijdens en na afloop van de Hack_Right trajecten. Per fase wordt nu besproken hoe deze samenwerking bij de uitgevoerde Hack_Right-trajecten eruit heeft gezien.

Samenwerking voorafgaand aan trajecten
Voorafgaand aan de Hack_Right-trajecten wordt er volgens een ontwikkelaar vanuit de projectgroep Hack_Right een geheimhoudingsverklaring aan bedrijven voorgelegd (IO2). Zo kan er over bepaalde casussen worden gesproken met de bedrijven. Voordat een Hack_Right-traject van start gaat, wordt er ook een eenmalig contract (dus per Hack_Right-traject) getekend tussen het bedrijf en strafrechtketenpartners zoals Halt en de reclassering (IO2). In dit contract staan een aantal afspraken omtrent de casus. Persoonlijke informatie over de verdachte mag niet worden gedeeld vanuit Halt of de reclassering met het bedrijf, tenzij er toestemming wordt gegeven door de deelnemer (HA1, RE1). Verder vindt er voordat de Hack_Right-trajecten plaatsvinden veel overleg plaats tussen de verschillende partijen over de afstemming en invulling van de trajecten. Zo geeft een Halt-medewerker aan dat de werkopdracht wordt afgestemd met de projectgroep Hack_Right (HA1) en vertelt een reclasseringswerker dat er veel overleg plaatsvindt met het OM en de projectgroep Hack_Right over de duur, invulling en instelling die bij een traject wordt betrokken (RE1). Verschillende toewijzers van het OM benoemen dat zij afspraken maken met toezichthouders en de projectgroep Hack_Right over geheimhouding, verslaglegging en voorwaarden omtrent de trajecten (n=3).

Samenwerking tijdens trajecten
Tijdens de uitvoering van de Hack_Right-trajecten is er ook contact tussen verschillende partijen. Enkele uitvoerders geven aan dat zij tijdens het traject informatie delen en sparren met de projectgroep Hack_Right (n=3). Het volgende citaat illustreert hoe een van de respondenten de samenwerking vooraf en tijdens het traject met de projectgroep ervaart:

> *"Het voordeel van Hack_Right is voor mij eigenlijk, omdat het een soort neutraal eiland is, dat je de kans krijgt om ook als vrijwilliger even te sparren. Dat doen ze trouwens uitermate goed ook hoor. Ook tijdens de casus zijn er korte lijntjes met Hack_Right." (CS4)*

Wanneer een traject minder goed verloopt, kunnen uitvoerders van bedrijven contact opnemen met de projectgroep Hack_Right (IO2). De projectgroep schakelt dan weer met Halt en reclassering. Halt of reclassering kan vervolgens een waarschuwingsgesprek voeren met de deelnemer of besluiten dat een deelnemer wordt terugverwezen naar de officier van justitie of rechter (IO2). Ook hebben sommige uitvoerders van bedrijven en uitvoerders van Halt of reclassering contact met elkaar tijdens de trajecten. Zo hebben twee uitvoerders van bedrijven tussendoor contact gehad met een Halt-medewerker over het verloop van het traject (CS2, CS1). Een van de Halt-medewerkers heeft geen contact gehad met het bedrijf tijdens de uitvoering van het traject (HA1). Ten slotte blijkt uit interviews met respondenten van het OM dat zij tijdens de uitvoering van het traject meer op afstand staan (n=3). Wel is er een respondent die tussendoor contact heeft gehad met de reclasseringswerker (OM4) en een respondent die naar een afsluitende presentatie van de deelnemer is gegaan en een verslag heeft

gezien van de deelnemer (OM5). Respondenten van het OM geven aan dat zij meer betrokken zijn bij de uitvoering van een straf dan het geval is bij andere straffen of maatregelen (n=2). Het volgende citaat illustreert dit:

> *"Want dat vond ik het mooie, dat men je op de hoogte houdt van de vorderingen, wat er gebeurt, hoe men het plan heeft ingestoken. Ik moet zeggen, dat zie ik nooit terug bij andere modaliteiten. Bij een eventueel deels voorwaardelijke straf die wordt opgelegd, dat je daar nog over gecontacteerd wordt vanuit reclassering of iets dergelijks, dat zie je totaal niet. Behalve als iets niet goed gaat natuurlijk." (OM4)*

Samenwerking na afloop van trajecten
Na afloop van de Hack_Right-trajecten vindt er volgens verschillende uitvoerders van Hack_Right een evaluatie plaats met verschillende partijen (n=5). Zo geeft een Halt-medewerker aan dat er een evaluatie heeft plaatsgevonden met het OM, de projectgroep Hack_Right en Halt (HA1), vertelt een uitvoerder van een bedrijf dat er een evaluatie heeft plaatsgevonden met de projectgroep Hack_Right en Halt (CS1) en heeft weer een andere uitvoerder van een bedrijf een evaluatie gehad met de projectgroep Hack_Right en de politie (CS2). Het OM krijgt volgens toewijzers van Hack_Right een positief of negatief afloopbericht vanuit Halt of de reclassering (n=3). Ook zijn er respondenten die aangeven dat deelnemers een afsluitende presentatie hebben gehouden voor het OM (n=2).

6.6 Dosering

In deze paragraaf wordt besproken hoe intensief en hoe compleet de tot nu toe uitgevoerde Hack_Right-trajecten zijn uitgevoerd. In sectie 6.6.1 wordt besproken wat het tijdsverloop is geweest tussen de arrestatie van de deelnemers tot de afronding van Hack_Right. Het blijkt dat de tijdsduur tussen het plegen van het delict en de afronding van Hack_Right bij de meeste trajecten lang is geweest. Vervolgens wordt in sectie 6.6.2 besproken wat de duur is geweest van de Hack_Right-trajecten en wat uitvoerders van deze duur vinden. De duur van Halt-trajecten is meestal twintig uur en de duur van reclasseringstrajecten kan sterk verschillen: van veertig tot 144 uur. Ten slotte laat sectie 6.6.3 zien in hoeverre de Hack_Right-trajecten compleet zijn uitgevoerd. Het blijkt dat één Hack_Right-traject niet volledig is afgrond.

6.6.1 *Tijdsverloop van arrestatie tot afronding Hack_Right*

De tijdsduur tussen het plegen van het delict en de afronding van Hack_Right duurt bij de meeste trajecten lang, zo blijkt uit interviews met toewijzers, uitvoerders en deelnemers. De tijdsduur tussen het plegen van het delict en de afronding van Hack_Right heeft volgens de meeste respondenten één tot drie jaar geduurd (n=14). Voor een enkele respondent is het onduidelijk hoeveel tijd er tussen het delict en afronding van

Hack_Right zat. De volgende citaten illustreren hoe deelnemers de tijdsduur tussen het plegen van het delict en de afronding van Hack_Right hebben ervaren:

> *"Ja, eigenlijk duurde het hele traject echt moker-lang [erg lang]. Voor die rechtbank ook. Zoooo." (DN5)*

> *"Het was ook, weet je wat het ook is, het komt ook allemaal heel laat. […] Het is al meer dan 2,5 jaar geleden gebeurd en nu pas ga ik Hack_Right… In die tijd, in die 2,5 jaar is er ook zoveel gebeurd." (DN9)*

De respondenten geven verschillende verklaringen voor de lange tijdsduur. Zo was de casus die bijna drie jaar in beslag nam een zaak waar in eerste instantie onvoldoende bewijs was en later een extra zaak bij kwam waardoor er wel voldoende bewijs was (OM5). Verklaringen die door andere respondenten worden genoemd voor de langere doorlooptijd zijn langdurige opsporingsonderzoeken en grote dossiers (OM1, OM4, HA2), het afstemmen van vakanties en agenda's voor de formele afsluiting van Hack_Right (OM2) en door andere praktische zaken zoals een geheimhoudingsverklaring van de organisatie die moest worden aangepast voor een minderjarige deelnemer (CS1).

De lange tijd die over de zaken heen gaat, heeft volgens de respondenten ook gevolgen voor het verloop van het Hack_Right-traject. Zo is het volgens een respondent lastig om terug te blikken op het delict (HA2). Een andere respondent geeft aan dat de link tussen het delict en de straf door de lange doorlooptijd verwatert (CS2). Door de lange tijd die over de zaken heen gaat, is het volgens respondenten lastig om terug te blikken op het delict (HA2).

6.6.2 *Duur Hack_Right trajecten*

Halt-trajecten
Uit de interviews met uitvoerders en toewijzers van Hack_Right blijkt dat de Halt-trajecten een duur hebben gehad van twintig uur (HA2, HA1, OM1). Dit is de maximale duur van de Halt-straf. Het gedeelte van de Halt-straf dat bij Halt wordt uitgevoerd bestaat uit drie opdrachten van één uur[16] en drie gesprekken van éé uur (HA2, HA1). De uren die overblijven, vaak twaalf tot vijftien uur, worden ingevuld met een programma bij een bedrijf (HA2, HA1).

Reclasseringstrajecten
De duur van de reclasseringstrajecten is minder duidelijk en verschilt sterk per traject. Zo geeft de reclasseringswerker aan dat er één traject is geweest waar geen aantal uur is

16 Een van de deelnemers geeft echter aan dat hij met een vragenlijst tien minuten bezig is geweest, een presentatie in vijftien minuten heeft gemaakt en andere opdrachten in twintig minuten heeft ingeleverd.

opgelegd, dat er één traject geweest is van vijftig uur en dat bij andere trajecten een bepaald aantal opdrachten gedaan zijn waarvan niet kon worden ingeschat hoelang het zou duren (RE1). Respondenten van het OM spreken over een traject van 144 uur verspreid over drie maanden (OM2), een traject waarbij de rechter heeft opgenomen dat 'aanwijzingen van de reclassering gevolgd moeten worden zolang zij dit noodzakelijk acht' (OM4) en een traject dat verspreid is geweest over zes à zeven maanden (OM5). Ook is er een respondent die dacht dat er een traject was van twintig uur, maar dit niet zeker wist (OM3). Een van de respondenten die twee reclasseringstrajecten bij zijn bedrijf heeft uitgevoerd spreekt over zwaardere, langere trajecten die tussen de drie en zes maanden hebben geduurd. Ten slotte geeft een respondent van een bedrijf aan dat het traject van de officier van justitie kort moest zijn en dat de jongere het in een keer moest kunnen afronden (CS7).

Tijdens interviews met deelnemers van Hack_Right wordt een iets duidelijker beeld geschetst. Zo moest een van de deelnemers zes dagen naar de cyberwerkplaats (DN2), hadden andere respondenten een werkstraf met Hack_Right van veertig uur (DN3, DN9, DN10) en had een respondent een werkstraf van tachtig uur (DN8). Een deelnemer geeft aan dat de werkstraf weinig voorstelde (DN3). Zo telde volgens de respondent een scholiereninterview van één uur voor tien uur en telde een ander interview van drie uur voor twintig uur.

Mening respondenten over duur trajecten
Enkele respondenten hebben hun mening gegeven over de duur van de Hack_Right-trajecten. Zo geeft een medewerker van de reclassering aan dat er in het advies aan de officier van justitie of rechter wordt toegevoegd dat de duur is 'zolang de reclassering nodig acht' (RE2). De respondent vindt het belangrijk dat de reclasseringswerker de ruimte heeft om – op het moment dat er grote veranderingen in iemands leven plaatsvinden zoals het krijgen van een huis of werk – te bepalen of er met Hack_Right verder moet worden gegaan.

Respondenten die werkzaam zijn bij het OM en Hack_Right toewijzen aan de verdachte geven verschillende antwoorden. Zo geeft een van de respondenten aan dat de Haltstraf van twintig uur bij zijn casus passend is (OM3). Het moet volgens de respondent als bijzondere afdoening en als straf tegelijkertijd worden ervaren door de deelnemer, waardoor er wel wat tijd mee gemoeid mag gaan. Een andere respondent die een Haltstraf van twintig uur heeft opgelegd, vindt de duur 'niet per se te veel' (OM1). De respondent geeft aan dat Halt voor Hack_Right de maximale afdoening van twintig uur nodig heeft, waardoor er per verdachte moet worden gewogen of twintig uur passend is bij het delict en de verdachte. Andere respondenten geven aan dat het uiteindelijk om het resultaat gaat in plaats van de tijdspanne (OM2), dat het maatwerk is (OM4) en dat er een mate van vrijheid is gegeven aan de reclasseringswerker zodat bepaalde opdrachten en afspraken gepland konden worden (OM5).

Ook aan respondenten die werkzaam zijn bij een bedrijf of organisatie is gevraagd wat zij van de duur vonden. Een van de respondenten geeft aan dat het in zijn optiek meer een inspanningsverplichting is, omdat de strafmaat door de rechter of het OM vaak in aantal uren wordt bepaald (CS3). Wanneer de deelnemers dan het aantal uren hebben gemaakt, krijgen zij een vinkje en is het traject afgerond. Of de duur voldoende is, vindt de respondent lastig te bepalen. Het is vooral belangrijk om het idee te krijgen dat de deelnemer het traject serieus heeft genomen (CS3). Andere respondenten geven aan dat de Halt-trajecten die zij hebben uitgevoerd voldoende lang hebben geduurd (CS5) ten opzichte van het delict dat er tegenover staat (CS6, CS1, CS7). Het volgende citaat illustreert de overwegingen van een van de respondenten:

> *"En ik denk dat in die twaalf uur, doordat we ze even laten spreken met collega's, er echt een wereld voor ze opengaat. […] Dus zelfs in zes uur zou je dan al een grote impact kunnen maken. Maar ik denk: twaalf uur, dan zit er ook een beetje die strafcomponent in, ze moeten ook wel een beetje strafwerk hebben, denk ik. Dus in die zin vind ik het best wel een goede hoeveelheid. Bij serieuzere gevallen kan ik me een langer traject voorstellen." (CS1)*

Een andere respondent die serieuzere Hack_Right trajecten heeft begeleid, geeft aan dat er voor zwaardere casussen langer de tijd nodig is om het tot een succes te kunnen brengen (CS4). Het volgende citaat illustreert dit:

> *"Voor de zwaarte van het traject is het vooral belangrijk om te bepalen of je inderdaad dan dit kanon wilt inzetten. Want het is wel een veel langer traject dan andere trajecten." (CS4)*

6.6.3 *Uitval*

Van de tot nu toe uitgevoerde trajecten hebben bijna alle deelnemers Hack_Right compleet afgerond, zo blijkt uit de interviews. Van de afgeronde trajecten vertellen twee respondenten dat er trajecten waren die moeizaam of stroef verliepen (CS1, CS2). Zo heeft een van de respondenten een deelnemer gehad die tijdens de eerste dag niet gemotiveerd was, te laat kwam en er niks van opgestoken had (CS2). De respondent heeft contact opgenomen met Halt en vanuit Halt is er een gesprek geweest met de deelnemer en zijn moeder. Na de interventie is besloten om toch door te gaan met het traject. Ook de tweede dag kwam de deelnemer te laat, maar was de jongere wel iets gemotiveerder. Vanuit Halt is achteraf aangegeven dat de jongere op dat moment teruggestuurd had mogen worden, maar omdat de respondent van het traject wilde leren, is dit niet gebeurd (CS2). Ook een andere respondent heeft een casus gehad die moeizamer verliep (CS1). De respondent kreeg op een bepaald moment geen contact meer (telefonisch of via mail) met een deelnemer. Dit is teruggekoppeld aan de Halt-begeleider, waarna uiteindelijk de gezamenlijke conclusie is getrokken dat de jongere niet zozeer

ongemotiveerd was, maar dat de deelnemer vanwege zijn leeftijd niet gewend is aan het altijd nakomen van afspraken (CS1).

Zover bekend heeft één deelnemer zijn traject niet afgerond. Bij zowel de reclassering (RE1), het OM (OM3) als een organisatie (CS7) komt een bepaalde casus naar voren die niet goed is verlopen. Zo vertelt de reclasseringswerker over een traject waarbij iemand dreigde af te haken terwijl hij nog iets moest inleveren (RE1). De deelnemer reageerde niet meer, waarop een wijkagent is langs gestuurd om poolshoogte te nemen (RE1, OM3, CS7). Uit latere interviews blijkt dat de deelnemer heeft verzuimd om een afsluitende presentatie te geven (OM3, CS7). De jongere heeft aangegeven geen medewerking te verlenen aan de afsluiting, omdat hij het gevoel had een presentatie te moeten geven of verklaring te moeten afleggen over iets dat hij niet gedaan had (OM3, CS7). De verdachte komt nu weer in het reguliere strafproces terecht, waarmee hij zeer waarschijnlijk voor de strafrechter wordt gedaagd (OM3).

6.7 Resumé

In dit hoofdstuk is onderzocht hoe de tot nu toe uitgevoerde Hack_Right-trajecten in de praktijk zijn verlopen. Het bereik, de programma-integriteit en de dosering stonden centraal. Om te onderzoeken of de beoogde doelgroep van Hack_Right wordt bereikt, is gekeken naar een casusoverzicht, kenmerken die naar voren komen tijdens interviews met deelnemers en de selectiecriteria die toewijzers van het OM hanteren bij het wel of niet opleggen van Hack_Right. Op een enkele uitzondering na bereikt Hack_Right de doelgroep zoals deze is beschreven in de plannen. Deelnemers van Hack_Right zijn jonge mannen die verschillende vormen van cybercriminaliteit hebben gepleegd. De meeste delicten betreffen (D)DoS-aanvallen en hackaanvallen. Een van de geïnterviewde deelnemers is betrokken geweest bij online oplichting. Deze uitzondering is niet in overeenstemming met het plan om deelnemers te selecteren die verdacht zijn van computercriminaliteit. Bij de selectie van deelnemers zijn de ernst van het delict, affiniteit met – en kennis van – ICT, leeftijd, persoonlijke omstandigheden en het motief de belangrijkste criteria voor toewijzers om Hack_Right wel of niet op te leggen. Dat de ernst van het delict als belangrijk criterium wordt aangemerkt is opvallend, aangezien dit geen criterium is volgens de plannen van Hack_Right. Uit een casusoverzicht blijkt dat meer dan de helft van de Hack_Right-trajecten is uitgevoerd in het kader van een Halt-straf. De overige trajecten vonden plaats bij de reclassering, veelal in de vorm van reclasseringstoezicht (tijdens een werkstraf). Ten slotte blijkt uit de interviews met toewijzers en uitvoerders dat de deelnemers bereid zijn geweest om deel te nemen aan Hack_Right. Tijdens de uitvoering waren deelnemers volgens respondenten gemotiveerd, maar er zijn ook gevallen waarbij deelnemers minder of helemaal niet gemotiveerd waren. In hoeverre deelnemers affiniteit hebben met ICT, de schadelijkheid van hun gedrag inzien en 'first offender' zijn, is op basis van het onderzoek niet te concluderen.

De invulling van de tot nu toe uitgevoerde Hack_Right-trajecten is niet duidelijk te herleiden tot concrete modules zoals die in de plannen worden besproken. Dat hoeft overigens niet te betekenen dat de inhoud van de modules niet aan bod gekomen zijn in de trajecten, alleen dat dit niet herkenbaar was voor de respondenten. Verder kan er een onderscheid worden gemaakt tussen deelnemers die een Hack_Right-traject via Halt hebben gevolgd en deelnemers die een traject via de reclassering hebben gevolgd. Via Halt hebben deelnemers een maximale Halt-straf van twintig uur gekregen. De Halt-straf bestaat enerzijds uit opdrachten en gesprekken bij Halt en anderzijds uit een programma van een of twee dagen bij een (cybersecurity)organisatie. Hoe resterende uren bij bedrijven worden ingevuld, verschilt per deelnemer. Sommige deelnemers hebben eerst een uitleg gekregen over hacken, de juridische grenzen ervan en mogelijkheden om verantwoord te hacken en vervolgens (technische) opdrachten uitgevoerd. Andere deelnemers hebben bijvoorbeeld interviews afgenomen met werknemers van een bedrijf of meegewerkt aan een politiecampagne rondom hacking. Voor de reclasseringstrajecten verschillen de activiteiten die zijn uitgevoerd onder Hack_Right sterk per deelnemer. Deelnemers hebben bijvoorbeeld werkzaamheden uitgevoerd bij een cyberwerkplaats, meegewerkt aan een praatprogramma over hacken, meegekeken bij ICT-bedrijven en interviews en presentaties gegeven. Individuele factoren die een rol spelen bij de invulling van Hack_Right-trajecten zijn de technische kennis en vaardigheden, risicofactoren en het motief van de deelnemer. Ten slotte blijkt dat er tussen betrokken organisaties veelvuldig wordt samengewerkt en overlegd, zowel vooraf, tijdens als na de uitvoering van de individuele Hack_Right-trajecten.

Met betrekking tot de intensiviteit van de Hack_Right-trajecten is gebleken dat de tijd tussen het plegen van het delict en de afronding van Hack_Right bij de meeste trajecten een tot enkele jaren duurt. Verklaringen voor de lange doorlooptijd zijn onder andere langdurige dossieropbouw van cyberdelicten bij de politie en het OM. De Hack_Right-trajecten zelf duren bij Halt vaak twintig uur, waarbij twaalf tot vijftien uur wordt ingevuld bij een (cybersecurity)organisatie. De duur van reclasseringstrajecten verschilt sterk per traject en kan variëren van bijvoorbeeld veertig uur tot 144 uur, verspreid over enkele dagen tot maanden. Uit de interviews blijkt ten slotte dat op een traject na bij alle trajecten het programma compleet is afgerond. Een deelnemer is uitgevallen omdat hij verzuimd heeft een afsluitende presentatie te geven. De deelnemer leek uiteindelijk niet de schadelijkheid van zijn gedrag in te zien. Enkele andere trajecten verliepen moeizaam, maar zijn uiteindelijk wel compleet afgerond.

7. Hack_Right: ervaringen

7.1 Inleiding

Het vorige hoofdstuk heeft inzicht gegeven in de wijze waarop de tot nu toe uitgevoerde trajecten zijn verlopen, waarbij de selectie, invulling en dosering van de Hack_Right-trajecten centraal stonden. In het huidige hoofdstuk staan de ervaringen van respondenten centraal. Zo wordt duidelijk in hoeverre volgens respondenten doelen van Hack_Right (besproken in 5.3) worden behaald (7.2), welke mogelijke gevolgen Hack_Right heeft op deelnemers (7.3), hoe het contact verloopt tussen deelnemers en uitvoerders (7.4), hoe tevreden betrokkenen zijn over de uitgevoerde trajecten (7.5) en hoe Hack_Right volgens respondenten verbeterd kan worden (7.6). Het hoofdstuk sluit af met een conclusie in paragraaf 7.7.

7.2 Doelen bereikt?

Per groep respondenten die betrokken zijn bij de toewijzing en uitvoering van Hack_Right wordt in deze paragraaf inzicht gegeven in de mate waarin beoogde doelen worden bereikt. De beoogde doelen verschillen per respondent, zoals is gebleken uit de vorige paragraaf. De meeste respondenten geven aan dat de doelen die zij gesteld hebben, worden behaald. Of sommige doelen zoals recidive verminderen worden behaald, blijft onduidelijk. Bij één Hack_Right casus is het doel volgens respondenten niet behaald, omdat de deelnemer is uitgevallen tijdens het traject.

7.2.1 *Toezichthouders*

Een van de Halt-medewerkers geeft aan dat er per jongere wordt bekeken wat het doel is dat men uit het traject wil halen (HA2). Bij een van de Hack_Right deelnemers was het doel om te zorgen dat de straf uitgevoerd wordt, dat de deelnemer niet opnieuw de fout in gaat en dat er bewustwording plaatsvindt dat het niet kan en niet geaccepteerd wordt wat de deelnemer heeft gedaan. Deze doelen zijn grotendeels bereikt volgens de respondent. De deelnemer heeft de straf uitgevoerd en er heeft volgens de respondent bewustwording plaatsgevonden bij de deelnemer dat het 'niet geaccepteerd wordt wat hij heeft gedaan'. Dit komt doordat de jongere tijdens de campagne die hij moest opzetten op een bewuste manier moest nadenken over wat hij zou moeten horen of zien om

het niet nog een keer te gaan doen. Of de deelnemer daadwerkelijk niet meer in herhaling valt, is lastig te controleren volgens de respondent (HA2).

Een andere Halt-medewerker benoemde 'de jongeren in hun kracht zetten' en 'talent verder ontwikkelen' als doelen van het traject (HA1). Dit is volgens de respondent bij zijn traject gelukt omdat de jongere na het traject nog steeds contact heeft met het bedrijf waar hij is geweest. De jongere nam bijvoorbeeld met het bedrijf contact op omdat hij met hen wilde schakelen over een situatie die hij had gevonden op internet. De jongere is er zich volgens de respondent daarom van bewust dat hij geen fouten meer wil maken (HA1).

De reclasseringswerker geeft aan dat er van tevoren geen doelen worden gesteld, maar dat je alleen achteraf kunt zeggen wat er is gebeurd (RE1). Bij de trajecten die de respondent heeft begeleid, hebben twee deelnemers inmiddels een baan, is er iemand die een technische tool heeft ontwikkeld en 'zich met Artificial Intelligence wilt gaan bezighouden' en heeft een deelnemer meer gedaan dan vanuit de reclassering werd gevraagd (RE1).

7.2.2 *Bedrijven en organisaties*

Voor de eerste respondent zijn de doelen van het traject om 'de deelnemer binnen de lijnen te houden' (zorgen dat de jongere het niet nog een keer doet) en 'om de deelnemer in stelling te brengen voor de goede kant van hacking' (CS2). Volgens de respondent zijn bij de eerste casus beide doelen bereikt. Na het traject is er nog contact met de jongere geweest en heeft de jongere gevraagd of hij bij de organisatie zou kunnen komen werken. Uiteindelijk is dit niet gebeurd omdat er geen invulling kon worden gegeven aan een functie, door een studie die de deelnemer nog volgt. Bij de tweede casus geeft de respondent aan dat er misschien een licht effect is geweest op het zorgen dat de jongere het niet nog een keer doet, omdat de gevolgen voor de deelnemer vervelend kunnen zijn. Het in stelling brengen voor de goede kant van hacking is bij de tweede casus niet gelukt (CS2). De deelnemer vond het programma niet interessant en was niet gemotiveerd.

Een tweede respondent geeft aan dat het doel is om de deelnemers te laten zien hoe zij op een goede manier kunnen hacken (CS6). Bij beide casussen heeft de respondent het gevoel dit te hebben bereikt. Bij de eerste casus was de jongere anders dan aan het begin van de dag:

> *"Hij kwam met zo van: 'Ik mag nu mijn computer niet meer aanraken, ik moet nu wat anders bedenken en dat vind ik eigenlijk helemaal niet leuk.' En dat was volgens mij aan het eind van de dag helemaal anders. […] Dan zie je wel dat je een soort ervaring mee hebt gegeven." (CS6)*

Twee deelnemers uit een ander traject hebben er wel wat van opgestoken, maar waren nog niet zo ver als de andere deelnemer: 'Zij waren wel nieuwsgierig, maar hadden gewoon iets doms gedaan.' (CS6).

De derde respondent ziet het 'laten zien dat wat de deelnemers hebben gedaan niet oké is en hoe je het anders kunt doen zonder mensen te benadelen' als doel van Hack_Right (CS5). Volgens de respondent is dit bij beide deelnemers in zekere zin gelukt omdat ze intensief bezig zijn geweest, maar is het bij de ene deelnemer beter gelukt dan de andere. De ene deelnemer is een stuk bewuster geworden, zag het probleem en zag dat het in zijn eigen belang was om niet verder te gaan met illegale activiteiten. Over de andere deelnemer heeft de respondent aan de projectgroep Hack_Right teruggekoppeld dat de jongere zichzelf in de toekomst wel weer in de problemen zou kunnen werken (CS5).

De vierde respondent omschrijft 'het voorkomen dat mensen de fout ingaan' en 'ervoor zorgen dat deelnemers hun technische vaardigheden positief inzetten' als doelen van Hack_Right (CS1). Met betrekking tot recidive denkt de respondent zeker niet dat de deelnemer nogmaals een dergelijk delict zou plegen, maar dat dit ook voor het Hack_Right traject al het geval was. Het proces met een verhoor bij de politie van een paar uur draagt hier volgens de respondent aan bij (CS1).

Voor een vijfde respondent zijn 'het verbeteren van de wereld' en 'het goed gebruiken van talenten' de doelen van Hack_Right (CS4). De respondent geeft aan dat je nooit voor honderd procent doelen kunt afvinken, maar dat het het belangrijkst is hoeveel tijd en energie iemand erin heeft gestoken. Uiteindelijk is er bij beide trajecten iets succesvols opgeleverd (CS4).

Ten slotte geeft een respondent aan dat het laten zien welke positieve dingen jongeren kunnen doen met hun skills het belangrijkste doel is. Het is volgens de respondent 'ongetwijfeld niet gelukt om hem duidelijk te maken dat hij onderdeel uitmaakt van een keten van misdaad'. De respondent geeft aan dat hier achteraf gezien langer de tijd voor nodig was (CS7). De deelnemer heeft na het gesprek met de respondent en reclasseringswerker niks meer van zich laten horen en is terugverwezen naar het OM.

7.2.3 *Openbaar Ministerie*

De eerste respondent geeft aan dat het doel formeel is bereikt wanneer het OM een positieve teruglegging[17] krijgt (OM3). In de casus waar de respondent bij betrokken is geweest, is dit niet gebeurd waardoor het doel formeel niet is bereikt. Een ander doel dat de respondent noemt is om 'de doelgroep ethisch en moreel besef mee te geven'

17 Een positieve teruglegging houdt in dat het OM een bericht krijgt vanuit Halt of reclassering dat een deelnemer een traject of straf positief heeft afgerond.

zodat strafbaar gedrag in de toekomst voorkomen wordt. Of dit recidivedoel behaald is, blijft voor de respondent onduidelijk (OM3).

Een tweede respondent benoemt ook een positieve teruglegging als doel voor het OM (OM1). Dit is bij de twee casussen het geval geweest. In hoeverre andere doelen worden bereikt, krijgt het OM niet mee, dit ligt volgens de respondent bij Halt en de reclassering. Zij doen een beoordeling en daar moet het OM op vertrouwen (OM1).

Een derde respondent is betrokken geweest bij een vrijwillig Hack_Right traject dat door het OM aan de verdachte is aangeboden. De respondent geeft aan dat het traject positief is afgerond 'als je het gevoel hebt en ziet dat je verdachte gegroeid is, het besef heeft en het waarschijnlijk niet nog een keer gaat doen'. Gedurende het traject kreeg het OM positieve signalen en is uiteindelijk de beslissing genomen om het bij het Hack_Right traject te laten (OM2).

Een vierde respondent benoemt het 'laten zien dat deelnemers op een positieve manier hun technische vaardigheden kunnen inzetten' als doel van Hack_Right. In hoeverre het doel is bereikt, is voor de respondent onduidelijk omdat het traject nog niet is afgerond. Wel krijgt de respondent positieve berichten over dat de jongere zich aan de afspraken houdt (OM4).

Een laatste respondent geeft aan dat het doel van Hack_Right is 'om jongeren van de slechte kant van hacken naar het ethisch hacken te begeleiden' (OM5). De respondent denkt dat het doel bereikt is in de zin dat de jongere zich niet meer bezighoudt met de activiteiten van het delict. De deelnemer is tot nu toe niet terug gezien bij het OM (OM5).

7.3 Mogelijke gevolgen van Hack_Right

In de interviews met uitvoerders van de interventie is gevraagd welke mogelijke positieve of negatieve gevolgen het Hack_Right-traject heeft gehad voor de deelnemer. Ook is aan de uitvoerders gevraagd wat jongeren mogelijkerwijs hebben geleerd van het traject. Aan deelnemers van Hack_Right is gevraagd of zij Hack_Right als straf hebben ervaren en of zij iets van Hack_Right hebben geleerd.

Uit de antwoorden van respondenten komen signalen naar voren dat Hack_Right ervoor kan zorgen dat ouders meer betrokken zijn en dat jongeren worden geleid richting een opleiding, stage of werk op het gebied van IT. Soms is het bij respondenten onduidelijk wat de gevolgen zijn van Hack_Right. Een enkele respondent benoemt het risico dat jongeren kennis opdoen die zij kunnen misbruiken. Daarnaast blijkt dat deelnemers Hack_Right zelf niet als straf zien en verschillen van mening of zij wat hebben geleerd. De mogelijke gevolgen van Hack_Right die toezichthouders, bedrijven en deelnemers hebben benoemd, worden nu per groep uitgebreid besproken.

7.3.1 *Toezichthouders*

Uit de interviews met Halt- en reclasseringswerkers komen verschillende gevolgen naar voren voor de thuis-, school- en werksituatie van de deelnemers na deelname aan Hack_Right. Met betrekking tot de thuissituatie zijn ouders aanwezig geweest bij Halt-gesprekken (HA2, HA1), waardoor ouders pedagogische handvatten mee hebben gekregen (HA2). Op het gebied van school heeft een deelnemer tips en adviezen meegekregen over wat hij zou kunnen gaan studeren (HA2). Hack_Right heeft volgens de Halt-medewerkers niet zozeer gevolgen gehad voor de werksituatie van de deelnemers (HA2, HA1). De reclasseringswerker geeft aan dat twee deelnemers nu aan het werk zijn terwijl zij voor het traject geen werk hadden (RE1). Daarnaast is er een deelnemer die er tijdens het traject achter is gekomen dat hij iets met Artificial Intelligence wil gaan doen in de toekomst. De reclasseringswerker geeft aan dat deze gebeurtenissen mogelijk zijn wanneer je inzicht krijgt in het leven van de deelnemers en het programma aan laat sluiten bij de kennis, vaardigheden en interesses van de deelnemers (RE1).

Hiernaast worden er ook mogelijke andere gevolgen benoemd door de respondenten. Zo hebben sommige deelnemers na de Hack_Right-trajecten nog contact met de organisatie waar zij zijn geweest. Ook hebben deelnemers mogelijkerwijs wat geleerd van de trajecten. Zo geeft een Halt-medewerker aan dat de deelnemer bewust is geworden van hetgeen hij fout heeft gedaan en is de deelnemer geschrokken van hoe groot de gevolgen hadden kunnen zijn (HA1). De andere Halt-medewerker geeft in eerste instantie aan dat de jongere er net zoveel van geleerd had als wanneer de jongen geen opdrachten zou hebben gekregen. Later in het interview geeft de respondent aan dat de jongere er wel inhoudelijk wat van heeft opgestoken. De reclasseringswerker geeft aan dat het onduidelijk is wat de effecten zijn op zaken als kennis en recidive, omdat deze effecten lastig te bepalen zijn en niet zijn gemeten. Het volgende citaat illustreert dit:

> *"Bij een HEMA-cursus[18] weet je ook niet in welke mate de cursus effect heeft op het gedrag, dat weet je niet. Je kunt het alleen maar hopen, niet weten. Ook bij kennis: dan zou je kennis vooraf en achteraf, moeten meten. Maar dat doe je niet, dus kun je het niet zeggen." (RE1)*

Ten slotte geeft een van de Halt-medewerkers aan dat er een mogelijkheid is dat deelnemers de kennis die zij opdoen misbruiken. Het is voor de Halt-medewerker namelijk onbekend of de deelnemer dingen heeft geleerd die hij op een slechte manier zou kunnen inzetten:

> *"Ik hoop altijd vooral dat ze niet veel slimmer worden dan dat ze nu zijn. Maar dat is het stukje dat ik hoop dat de juiste bedrijven binnen zijn, die ze daarin uit kunnen leggen dat je er toch de positieve kanten van kan gaan benutten, en wat er vooral niet*

18 De HEMA-academie is een opleidingsinstituut en biedt verschillende opleidingen en cursussen aan.

mag en waarom niet. Maar goed dat is natuurlijk met alles, zodra je meer weet over wetgeving weet je ook beter hoe je dat dan op een andere manier kunt doen. Ik denk vooral dat het positief is dat hij nu weet wat de gevolgen zijn. En daar is hij zich niet bewust van geweest van tevoren." (HA2)

7.3.2 *Bedrijven en organisaties*

Ook tijdens interviews met begeleiders vanuit de bedrijven en organisaties komen verschillen gevolgen naar voren voor de thuis-, school- en werksituatie van de deelnemers. Met betrekking tot de thuissituatie geeft een van de respondenten aan dat de ouders van de deelnemer bij het traject betrokken geweest zijn en achteraf nog mails hebben verstuurd dat ze blij waren met het traject (CS1). Op het gebied van school en studie geeft een respondent aan dat een deelnemer gedurende het traject erachter kwam dat hij graag in Engeland wilde studeren, maar vanwege planning en/of financien is dit nog niet gebeurd (CS4). Een andere deelnemer heeft besloten om een opleiding mbo-applicatie ontwikkeling te gaan doen (CS3). De deelnemer loopt nu ook stage bij het bedrijf waar hij zijn Hack_Right-programma heeft gevolgd (CS3, CS5). Volgens een andere respondent wilde een deelnemer graag bij de organisatie gaan werken, maar vanwege de studie die de deelnemer nog volgde, was het niet mogelijk om een geschikte invulling te geven aan een functie bij het bedrijf (CS2). Andere respondenten laten weten dat zij van sommige trajecten verder geen idee hebben of Hack_Right mogelijk gevolgen heeft gehad op de thuis-, school- en werksituatie van de deelnemers (CS3, CS2, CS6).

In de interviews geven respondenten aan dat er zowel deelnemers zijn die wat geleerd hebben tijdens hun Hack_Right-traject, als deelnemers die minder of niks hebben geleerd. Zo vertellen respondenten dat deelnemers tijdens het traject een beter handelingsperspectief hebben gekregen over hoe zij op een goede manier geld kunnen verdienen (CS5, CS1). Jongeren hebben geleerd dat er platformen zijn die je kunnen inhuren als hacker of waar je geld krijgt als je iets rapporteert en dat er hackers en specialisten bij bedrijven werkzaam zijn (CS1). Ook geven respondenten aan dat er deelnemers zijn die zich bewuster zijn geworden van de gevolgen (CS5, CS4). Het volgende citaat laat zien hoe een respondent – die langere Hack_Right trajecten heeft begeleid – dit heeft ervaren:

"Maar als iemand letterlijk, die jonge jongen van 15, die gebruikt het woord moraal in zijn eindpresentatie. Nou ja, dat vind ik niet een standaardwoord voor zijn leeftijd. En dat zijn moraal echt veranderd was, dat ook zwart op wit heeft geschreven. Nou, dat is voor mij wel een teken dat je hebt nagedacht van: 'Wat is moraal? En waarom wil ik dit wel of niet?'" (CS4)

Ook zijn de deelnemers die de respondent heeft begeleid volwassener geworden, doordat ze hebben geleerd om projectmatig te werken. De deelnemers hebben een missie en

visie op moeten schrijven, doelstellingen moeten opschrijven en geleerd hoe ze hun projecten presenteren aan het OM. Het volgende citaat illustreert hoe de deelnemers volgens de respondent volwassener zijn geworden:

> *"Want soms waren ze ook wel een beetje bang van; moet ik niet te veel communiceren? Van: willen jullie dat dan wel weten? Ja, als het belangrijk is, of als jij vindt dat je dat moet communiceren, dan is het jouw verantwoording om dat te communiceren. Ik ga niet voor je verzinnen wat je moet communiceren. En daarmee maak je ze wel een stuk volwassener hoor." (CS4)*

Een van de respondenten vertelt over een traject waarbij de deelnemer heeft aangegeven alleen geleerd te hebben hoe een auto werkt en dat hij verder niets heeft geleerd (CS2). De deelnemer vond zoals eerder genoemd het programma niet interessant en was niet gemotiveerd. Er is daarom besloten om een 'interventie te doen' waarbij de deelnemer is gevraagd wat hij dan wel interessant vond. Hieruit bleek dat de deelnemer snelle auto's interessant vond en is vervolgens door het bedrijf uitgelegd hoe auto's steeds meer digitaal worden en hoe hacking in potentie ook gevaarlijk kan zijn voor auto's. Ook een andere respondent geeft aan dat een van de deelnemers zich niet zozeer bewuster is geworden tijdens het traject wat wel en niet een goede manier van hacken is (CS5).

Verschillende respondenten geven aan dat het ook mogelijk is dat het volgen van Hack_Right geen of negatieve gevolgen kan hebben voor deelnemers. Zo vertelt een van de respondenten dat jongeren simpelweg de consequenties van hun handelen niet kunnen overzien:

> *"Je kunt na zo'n alternatieve strafafdoening ook niet opeens verwachten dat jongeren wel de consequenties van hun daden gaan overzien. Dat zit gewoon niet in hun hersenen, nog niet. Daar zijn ze vaak gewoon nog niet volwassen genoeg voor." (CS3)*

Andere respondenten vragen zich net als de Halt-medewerker af of deelnemers tijdens Hack_Right niet te veel kennis krijgen die ze wellicht kunnen gebruiken voor illegale activiteiten. De volgende citaten zijn hiervoor illustratief:

> *"Maar wat ik me wel bij die eerste jongens afvraag is: maak je ze niet wijzer dan ze al zijn of zo? Ze waren bij wijze van spreken, ja, op de al… Ja, als je jong bent, dan ben je altijd bezig om dingen te ontdekken, dat is heel normaal. Dus dan heb je daar eigenlijk op aangegrepen en je helpt ze eigenlijk nog verder op weg om nog meer te ontdekken. Dus dat moet je dan wel op de goede manier doen." (CS6)*

> *"Ik denk wel, het enige gevaar dat je hebt bijvoorbeeld als je wat meer gaat uitleggen over hacken, dat je mensen wat meer, ze te veel geïnteresseerd maakt. […] Ik weet niet*

of dat erg is, maar ik kan me voorstellen dat als iemand te veel weet, terwijl hij eigenlijk alleen maar slechte bedoelingen heeft, dat dat niet heel verstandig is." (CS5)

Bij één Hack_Right traject heeft de deelnemer niks meer van zich laten horen na een gesprek waarin de respondent en reclassering duidelijk hebben proberen te maken dat het niet goed was wat de deelnemer had gedaan (CS7):

"Je kon wel technische vragen aan hem stellen van: hoe heb je dat dan gedaan? Daar ging hij wel over vertellen, dat vond hij dan wel interessant om te vertellen. Maar als je vervolgens dan probeerde uit te leggen van: ja, wat je me nu vertelt is eigenlijk een misdrijf. Maar dan was hij ook echt zo van: 'Nou ja, echt niet, want het staat op internet'. […] Deze jongen had wel iets meer nodig dan dit." (CS7)

Ten slotte geven respondenten aan dat het uiteindelijk onduidelijk is wat precies de effecten zijn van Hack_Right op de deelnemers (n=3). Zo is het onduidelijk wat de criteria zijn voor een geslaagd traject (CS2), of de effectiviteit daarvan gemeten kan worden (CS2) en welke mechanismen tot eventuele effecten hebben geleid (CS3). Ook bestaat de mogelijkheid dat bepaalde effecten op jongeren al voor het Hack_Right-programma plaatsvinden. Twee uitvoerders (en ook deelnemers, zie hiervoor de volgende sectie) geven namelijk aan dat arrestatie en het verhoor door de politie een behoorlijke impact hebben op de jongeren (CS1, CS4).

7.3.3 *Deelnemers*

Aan deelnemers is tijdens de interviews gevraagd of zij wat hebben geleerd van Hack_Right en of zij Hack_Right als straf hebben ervaren. De deelnemers verschillen van mening over de mate waarin ze iets hebben geleerd van Hack_Right. Een deel van de jongeren geeft aan in meer of mindere mate iets te hebben geleerd tijdens het traject (n=5). Zo vertelt een van de deelnemers dat hij bij het bedrijf geleerd heeft over Responsible Disclosure. De jongere heeft na Hack_Right enkele andere bedrijven berichten gestuurd over hun kwetsbaarheden (DN5). Ook heeft de deelnemer een powerpoint moeten opstellen waarin hij heeft geleerd dat mensen op legale wijze geld kunnen verdienen met hacken. Een andere deelnemer heeft wel wat geleerd, maar geeft aan dat de grenzen bij hem al redelijk duidelijk waren (DN7). Ouders van de respondent geven tijdens het interview aan dat de jongere heeft geleerd om een 'pentest'[19] uit te voeren en over welke grenzen de jongere met toestemming heen mag en waar je zonder toestemming moet stoppen. Andere deelnemers hebben geleerd over white- en blackhat hackers (DN1), de goede en slechte kanten van hacken (DN1), DDoS-aanvallen (DN1) en Java-programmeren (DN8). Een andere deelnemer geeft aan dat hij vooral wat geleerd

19 'Pentest' is een afkorting van 'penetration testing' en is het penetreren van software en/of hardware zodat zwakke plekken in de software en/of hardware gevonden kunnen worden.

heeft bij het cybercrimeteam van de politie, waar de jongere is uitgelegd wat de impact was van het gepleegde delict (DN4). Bij Halt heeft de jongere minder geleerd:

> *"Ik denk dat nu nog niet eens 10 procent van de mensen die het volgt hier echt wat van leert. Of ze moeten echt 11 zijn en zoiets hebben van; white-hat hacker, wat is dat?" (DN4)*

Verschillende deelnemers benoemen dat Hack_Right voor de jongere zelf niet veel heeft toegevoegd, maar dat het voor anderen wel leerzaam had kunnen zijn (n=3). Zo vertelt een deelnemer dat hij het meeste dat hij leerde bij organisatie F al wist, maar dat andere leerlingen wel redelijk wat dingen leerden (DN2). Andere deelnemers geven duidelijk aan dat zij niks hebben geleerd van Hack_Right en dat Hack_Right niks heeft toegevoegd voor hen (n=2). Zo is er een deelnemer die vertelt dat de Halt-opdrachten te makkelijk waren en dat er geen programma lag bij het bedrijf toen de deelnemer aankwam (DN4).

Uit de interviews blijkt dat bijna alle deelnemers Hack_Right niet of nauwelijks als straf ervaren (n=7). De volgende citaten illustreren hoe de deelnemers dit verwoorden:

> *"Tenminste, wat ik heb gedaan vond ik niet echt een straf. En ik denk, je wordt meer eigenlijk, het was meer eigenlijk een beloning ofzo. Want daardoor loop ik nu hier stage, doe ik nu mijn opleiding. En ja, als je daarnaast nog een straf krijgt, heb je toch nog het idee van; ik heb wel wat fout gedaan zeg maar." (DN5)*

> *"Nee, [lacht]. Dat moet je eigenlijk wel voelen, maar… lukt niet." (DN7)*

> *"Dus ja, als ik het zelf mag zeggen een heel softe straf. Ik vind dat ik er heel makkelijk vanaf kom." (DN9)*

Tussen deze deelnemers zitten zowel jongeren die een traject bij Halt hebben gevolgd als jongeren die een traject bij de reclassering hebben gevolgd. Een andere deelnemer noemt Hack_Right een 'soort van verplichte studieopdracht' (DN4). Uit andere interviews is niet gebleken of respondenten Hack_Right als straf hebben ervaren (n=2). Wat wel als strafelement wordt gevoeld door enkele respondenten is de inval door de politie en inbeslagneming van spullen zoals laptops (n=5) De volgende citaten illustreren dit:

> *"Ja dat was echt de sanctie, want ik kon nergens meer bij. Ik ben daar zoveel door kwijtgeraakt, dat was eigenlijk mijn straf wel. Wat daarna allemaal is gebeurd maakt niet echt meer uit." (DN9)*

> *"Nou ik vond het, kijk, het is natuurlijk niet alleen het Hack_Right wat echt de straf was. Het is natuurlijk ook überhaupt, los ook van die Halt-opdrachten, gewoon drie*

dagen vast zitten is niet echt leuk. En alle spullen die waren meegenomen en eigenlijk heb ik daar bijna niks van terug gekregen enzo." (DN6)

Naast het leer- en strafeffect geven enkele respondenten aan dat zij zich niet meer bezighouden met hacken en het niet nog een keer zouden doen (n=6). Zo vertellen deelnemers dat zij vooral gestopt zijn nadat de politie hen heeft opgepakt (DN2, DN7) en geeft een deelnemer aan dat hij niet nog meer problemen wil (DN1). Een andere respondent geeft heel specifiek aan dat hij was doorgegaan met illegale activiteiten als hij Hack_Right niet had gehad (DN5). Andere respondenten geven aan dat zij al gestopt waren voordat zij Hack_Right hebben gehad (n=2). Ten slotte blijkt dat Hack_Right voor enkele deelnemers ook andere gevolgen heeft gehad (n=3). Zo gaan twee respondenten – die voor hun straf naar organisatie F moesten – nog steeds naar de organisatie terwijl hun straf al is afgelopen (DN2, DN8). Ook is er een deelnemer die aangeeft dat hij door het Hack_Right-traject nu stage loopt en een opleiding is gaan volgen (DN5). Een duidelijk beeld over hoe tevreden deelnemers zijn met Hack_Right wordt geschetst in paragraaf 7.5.

7.4 Contact tussen deelnemers en uitvoerders Hack_Right

Uit de literatuur is gebleken dat het contact tussen deelnemers en uitvoerders een factor kan zijn die tot een effectieve interventie kan leiden. Tijdens interviews is gevraagd of er vaste contactpersonen zijn geweest, is gesproken over competenties van uitvoerders en is gevraagd hoe uitvoerders en deelnemers het contact met elkaar hebben ervaren. De resultaten laten zien dat deelnemers bij Halt, reclassering en bedrijven een of meerdere vaste contactpersonen hebben gehad. Verder blijkt dat Halt- en reclasseringswerkers over weinig tot geen technische kennis te beschikken, maar dat is volgens respondenten niet per definitie van groot belang voor een goed verloop van het traject. Zowel deelnemers als uitvoerders zijn grotendeels tevreden over het contact dat zij met elkaar hebben gehad. Het lijkt er vooral op dat jongeren zich gehoord en begrepen voelen bij de (cybersecurity)organisaties.

Contactpersonen
Vanuit Halt hebben de Hack_Right deelnemers in principe één vaste contactpersoon gehad die hen tijdens het traject heeft begeleid (HA2, HA1, DN4, DN6). Een van de Halt-medewerkers geeft aan dat hij de opstart van een traject samen met een collega heeft gedaan, omdat Hack_Right nieuw was (HA1). Later in het traject heeft de respondent de casus alleen voortgezet.

Bij de reclasseringstrajecten is er één reclasseringswerker die het grootste deel van de Hack_Right deelnemers heeft begeleid (RE1). De respondent geeft aan dat alle zaken in zijn regio die met computers te maken hebben op zijn naam instromen. De respondent is voor de deelnemers de vaste contactpersoon geweest vanuit de reclassering (RE1).

Tijdens het programma dat deelnemers van Hack_Right uitvoeren bij bedrijven is er vaak een medewerker van de organisatie die de gehele dag aanwezig is bij de deelnemer (CS2, CS6, CS5, CS1). Dit is meestal het vaste aanspreekpunt voor de deelnemer. Daarnaast komen de deelnemers met verschillende andere medewerkers in aanraking. Zo vertellen respondenten over een (DN6, DN7), twee (CS6, CS5, DN4, CS7), drie (HA1, DN4) of meerdere (CS1) medewerkers die hebben meegekeken (HA1) vanuit het bedrijf of de organisatie. Bij de twee langere trajecten van bedrijf E waren er weliswaar één of twee vaste aanspreekpunten, maar voerden de deelnemers de werkzaamheden vooral thuis uit (CS4).

Competenties begeleiders
Halt & Reclassering – Een terugkerend onderwerp tijdens de interviews is de technische kennis van Halt- en reclasseringswerkers. Uit de interviews met uitvoerders blijkt dat medewerkers van Halt en reclassering over het algemeen niet over technische kennis of een technische achtergrond beschikken (CS3, HA2, RE1, CS6, CS1). Het volgende citaat van een Halt-medewerker is hiervoor illustratief:

> *"Die opdrachten wil ik best een keer met de jongeren doornemen, maar die gaan grotendeels mee naar de bedrijven waar de jongeren heen gaan, want ik weet niet eens waar het over gaat. Ik vind het vooral boeiend hoe ze het mij uitleggen, of het ze lukt om het mij uit te leggen." (HA2)*

Respondenten van Halt en reclassering verschillen van mening over de noodzaak van deze technische kennis. Zo geven een Halt-medewerker en reclasseringswerker aan dat inhoudelijke ICT-kennis niet belangrijk is (HA2, RE1). Vooral het pedagogische aspect is volgens hen belangrijk. De respondenten geven beiden aan dat de kennisachterstand ten opzichte van de jongeren er juist voor kan zorgen dat jongeren beginnen met praten (HA2, RE1). Het volgende citaat illustreert dit:

> *"Geen technische achtergrond heeft een voordeel. Je kunt alles vragen wat ze gedaan hebben, ze leggen het dan vaak uit. Zo kun je zien op welke momenten ze beslissingen hebben genomen die ze achteraf gezien beter niet hadden kunnen nemen. Als je heel goed technisch op de hoogte bent dan zit je meer van; waarom heb je het niet anders gedaan." (RE1)*

Andere medewerkers van Halt en reclassering geven aan dat enige kennis van ICT wel van belang kan zijn (RE2, HA1). Een Halt-medewerker geeft bijvoorbeeld aan dat het moeilijker is om je in de casus in te leven als je geen affiniteit hebt met ICT (HA1). Ook wil de respondent de jongeren graag iets mee kunnen geven vanuit 'een stukje begrip en kennis'. Een reclasseringswerker geeft aan dat het belangrijk is om te weten wat het delict inhoudt en dat meer specifieke kennis een pre is (RE2). Inhoudelijke vakkennis kan volgens de respondent eventueel het vertrouwen van de cliënt in de competenties van de reclasseringswerker verhogen.

Respondenten die werkzaam zijn bij ICT-bedrijven vinden ook dat technische kennis van Halt- en reclasseringswerkers belangrijk is. Zo hebben Halt-medewerkers hulp nodig om in te kunnen schatten hoe digitaal vaardig iemand is en of iemand daarom geschikt is voor een Hack_Right traject (CS3) en kunnen Halt-medewerkers niet goed inschatten wat er daadwerkelijk inhoudelijk gebeurt tijdens een traject en of het daadwerkelijk goed verloopt (CS3, CS6). Ook is kennis over informatica en security nodig om contact te kunnen maken met de doelgroep (CS5):

> *"Anders is het denk ik wel onmogelijk om contact met ze te maken. Dan is het weer gewoon iemand die ze al duizend keer gesproken hebben, die wil weten hoe het met ze gaat of weet ik het wat. Dat is niet echt waar ze op inhaken." (CS5)*

Een van de respondenten denkt ook dat technische kennis waardevol is om goed te kunnen weten of jongeren niet iets op de mouw van bijvoorbeeld een reclasseringswerker spelden:

> *"[Een reclasseringswerker] had dan al een jaar iemand begeleid waardoor die persoon er inmiddels wel een klein beetje in thuis was, maar zei ook: 'Af en toe word ik gewoon om de tuin geleid. En als iemand dat echt wil; die kan me van alles op de mouw spelden, ik heb geen enkele manier om door te vragen.'" (CS1)*

Het kan volgens de respondent daarom waardevol zijn om – bij wat zwaardere trajecten – iemand met een technische achtergrond aan te laten sluiten bij de gesprekken tussen de deelnemers en reclasseringswerkers (CS1).

Ten slotte geven deelnemers ook hun mening over de technische kennis van Halt- en reclasseringswerkers tijdens de interviews. Uit de interviews blijkt dat Halt-medewerkers helemaal niks wisten (DN5) of er niet veel vanaf wisten (DN1, DN4, DN7) en dat een reclasseringswerker wel meerdere cyberzaken had gedaan, maar niet zozeer technisch onderlegd was (DN3). Deelnemers lijken het minder belangrijk te vinden vinden dat een Halt- of reclasseringswerker over veel technische kennis beschikt (DN1, DN3, DN4). Zo vindt een respondent het niet vervelend (DN1), neemt een andere respondent de medewerkers serieus (DN4) en weet een andere respondent niet of het uitmaakt dat de medewerkers niet over technische kennis beschikken (DN3). Een andere deelnemer vindt het wel storend en irriteerde zich zelfs aan de Halt-medewerker omdat zij er niks vanaf wist (DN5):

> *"Net zoals bij mijn opleiding, heb ik ook een paar docenten die dan niet kunnen programmeren. En die lopen dan wel rond om je te helpen. Dat zijn meestal dan, van die filosofische vragen stellen ze dan. Van hoe je dat eerder hebt gedaan, loop al je stappen maar langs. En daar heb je gewoon niks aan. En dan moet je uitleggen van; luister, zo werkt het niet." (DN5)*

Bedrijven en organisaties – Uit interviews met uitvoerders die werkzaam zijn bij bedrijven en organisaties blijkt dat verbinding kunnen maken met de deelnemer (n=4) en didactische/pedagogische vaardigheden (n=4) belangrijk zijn voor begeleiders. Met betrekking tot het in verbinding staan met de deelnemer merken respondenten op dat het belangrijk is dat begeleiders geïnteresseerd zijn (CS6, CS5), niet direct hun oordeel uiten (CS5) en dat deelnemers zich kunnen identificeren met de begeleiders (CS6). Ook moet er aansluiting zijn met de belevingswereld en het opleidingsniveau van de deelnemers (CS2, CS1). De volgende citaten zijn illustratief voor het belang van aansluiting met de belevingswereld van de deelnemer:

> *"Hij moet ook kunnen herkennen van: 'Hey, dat is ook iemand die dat soort dingen interessant vindt'. Daar krijg je dan wel snel een klik op." (CS6)*

> *"Ik denk dat je veel makkelijker met elkaar kan praten over een geïnteresseerd gebied. […] Maar als jij die kennis niet hebt, dan houdt het op. Al meteen, in het begin. Maar als je daarop door kan gaan, op kan doorvragen van: 'Hoe heb je dat dan gedaan en kan je er wat meer over vertellen?' Dan wordt iemand wakker en denkt: 'Oh, wacht, er zit iemand tegenover me die wel weet waar het over gaat'. Dat is denk ik ook wat je hier ziet: technische mensen praten een stuk sneller met elkaar over zo'n onderwerp." (CS5)*

In het kader van pedagogische vaardigheden merken respondenten op dat pedagogische kennis en vaardigheden belangrijk kunnen zijn voor het begeleiden van een Hack_Right traject (CS4, CS5). De reclasseringswerker heeft op dit vlak input kunnen geven aan uitvoerders bij bedrijven of organisaties (CS4, CS7). Het volgende citaat illustreert dit:

> *"En dan merk je dat de relatie met [naam reclasseringswerker] ook wel handig was. Af en toe [zeiden wij] van: 'Hey [reclasseringswerker], moet je horen, we zien nu dit, maar we snappen dat niet helemaal'. [En dan zei reclasseringswerker:] 'Ja, maar je moet weten dat dit en dit bij hem speelt'. Dus wat dat betreft was het ook handige reflectie weer." (CS4)*

Een andere respondent merkt op dat het voor langdurige trajecten belangrijk is om sociale en psychologische achtergronden van de deelnemers te begrijpen (CS7). Ook worden kennis van het strafrechtsysteem (CS4, CS7), 'voelsprieten en intuïtie' (CS7) en een 'bullshit-detector' genoemd als belangrijke competenties:

> *"Je moet ook een soort bullshit-detector hebben. Dat je ook denkt van: 'Onzin jongens, praat nou eens even verder van wat je nou echt bedoelt. Je hebt drie treinen gemist? Ja, ja.'" (CS4)*

Verschillende respondenten geven aan dat niet al hun collega's geschikt zouden zijn om Hack_Right deelnemers te begeleiden (CS6, CS1, CS7). Niet alle collega's beschikken over communicatieve en pedagogische kwaliteiten (CS4) en sommige medewerkers kunnen gestrest raken omdat ze het erg spannend vinden en niet weten wat ze kunnen verwachten (CS6, CS4). Het volgende citaat illustreert dit:

> *"Vanuit [organisatie X] zien wij ook best een hoop mensen en ook autisten. Ik denk niet dat iedereen uit het juiste hout gesneden is om dit [begeleider te zijn] te kunnen doen." (CS4)*

Relatie tussen deelnemers en uitvoerders
Halt – Een van de Halt-medewerkers geeft aan dat ze nooit zoveel moeite heeft met jongeren en altijd probeert te 'levellen' met jongeren (HA2). Tijdens de gesprekken komt de respondent er dan achter wat de jongeren nodig hebben. Het contact met de deelnemers heeft volgens de respondent veel invloed:

> *"Het staat of valt met het contact denk ik. Maar de complete Halt-afdoening. Want je kunt heel streng en strak een gesprek inzetten, hoewel dat soms nodig is, maar over het algemeen; het leerproces ga je niet bereiken als je er strak op gaat zitten. De jongere gaat leren door te spiegelen, door steeds terug te pakken naar wat ze zelf denken, zeggen en doen." (HA2)*

De andere Halt-medewerker geeft aan dat er niet zozeer sprake was van een klik met de deelnemer, maar meer van een gezonde, zakelijke werkrelatie (HA1). Tijdens interviews met jongeren geeft een jongere aan dat hij het contact met de Halt-medewerker als irritant heeft ervaren door het gebrek aan kennis (DN5) en zegt een jongere dat een andere Halt-medewerker de deelnemer wellicht beter had begrepen (DN1). Een derde respondent geeft daarentegen aan dat de Halt-medewerker erg enthousiast was, veel energie in het traject heeft gestoken en er veel mee bezig was (DN7).

Reclassering – De reclasseringswerker die de meeste Hack_Right-trajecten heeft begeleid, geeft aan dat waar hij normaal gesproken niet zo goed met jongeren overweg kan, het op een of andere manier met de Hack_Right doelgroep erg goed gaat (RE1). Een mogelijke verklaring hiervoor ligt volgens de respondent in de manier waarop hij zich opstelt:

> *"Het heeft vooral te maken met de manier van opstellen: 'Vertel maar, laat maar weten, leg mij maar uit hoe het werkt, ik snap er toch niks van.' Als je op regels gaat zitten, daar moet je bij jongeren niet mee aankomen." (RE1)*

De respondent geeft aan dat hij eerst iemand leert kenen en van daaruit gaat kijken wat de mogelijkheden zijn. Vertrouwen is volgens de reclasseringswerker het belangrijkste (RE1). Respondenten die vanuit een reclasseringstraject aan Hack_Right hebben deel-

genomen, bevestigen dat zij prettig contact hebben gehad met de reclasseringswerker (DN2, DN3). De volgende citaten illustreren dit:

> *"Nou, ik moet zeggen dat reclassering mij heel erg beviel. Je hoort altijd van: 'Ja, reclassering, dit dat. Gezeik en zo.' Maar het heeft mij eigenlijk alleen geholpen. Dus ja, dat beviel me eigenlijk. Terwijl ik verwachtte van niet." (DN2)*

> *"Ja, [naam reclasseringswerker] is op zich wel een aardige gozer. Hij komt ook, af en toe is hij ook gewoon hier naar toegekomen. Ik ben nog maar twee keer of zo bij reclassering geweest. Dan is het even een kort gesprekje hoe het gaat, waar ik mee bezig ben en dan is het allemaal prima." (DN3)*

Bedrijven of organisaties – Tijdens interviews met uitvoerders van Hack_Right die bij bedrijven of organisaties werkzaam zijn, is gebleken dat zij het contact met deelnemers wisselend hebben ervaren. De meeste respondenten hebben het contact met de deelnemers als positief ervaren (CS6, CS5, CS1, CS4). Zo geeft een van de respondenten aan dat hij absoluut een klik – en goed contact – heeft gehad met de deelnemers (CS6). Een andere respondent geeft aan dat hij en de deelnemer makkelijk met elkaar konden praten. Ook zijn er respondenten die aangeven dat hier wel eerst meer tijd voor nodig was (CS1, CS4). Zo was er een traject dat in eerste instantie wat stroef verliep en waarbij de jongere eerst een gesloten houding had (CS1). Dit bleek te komen door een gebeurtenis in de privésfeer van de deelnemer en doordat de respondent het lastig vond om te werken met een jongen van veertien jaar van een ander niveau. Later merkte de jongere dat medewerkers van het bedrijf dezelfde interesse hadden en ging het contact beter (CS1). Ook een andere respondent geeft aan dat de jongeren tijdens zijn trajecten eerst de kat uit de boom keken (CS4). Gedurende het traject werden de jongeren steeds opener in hun communicatie en gingen zij steeds meer vertellen. De respondent heeft het contact als erg positief en opbouwend ervaren. Ook na Hack_Right is er nog contact met de deelnemer over hoe het gaat en waar hij mee bezig is (CS4). Ten slotte zijn er twee respondenten die het contact met een deelnemer als minder goed hebben ervaren (CS2, CS4). Zo vond een respondent het lastig om zich te verplaatsen in de belevingswereld van de deelnemer en is er daarom een jongere collega bij gevraagd (CS2). Een andere respondent geeft aan dat het moeilijk was om contact te maken met de deelnemer en dat de jongere weinig teruggaf (CS7).

Respondenten die werkzaam zijn bij bedrijven geven aan dat het contact dat zij hebben met de deelnemer belangrijk is voor het verloop van het traject (n=4). Zo vertellen respondenten dat het contact ervoor zorgt dat jongeren erg open zijn (CS5), dat een goede klik belangrijk is voor het leerproces (CS2), dat er zo een relatie opgebouwd wordt waardoor je iemand beter op het spoor kunt zetten (CS4) en dat het inspirerend werkt en invloed heeft op het vertrouwen tussen de deelnemer en begeleider (CS6). Het volgende citaat laat zien wat wordt bedoeld met een inspirerende werking:

> *"Wat ook wel een beetje inspirerend werkt bij die jongens is het contact wat je met die jongens hebt gedurende de dag. Je legt dan wat uit over hoe een kwetsbaarheid werkt. Zij vertellen dan over wat zij hebben gedaan en waarom en ook over of het nou, dan zeggen ze het was eigenlijk niet netjes of zo, of gewoon uit nieuwsgierigheid dat ze dat deden. En dat raakt best wel aan onze leefwereld. Daar hebben we best wel goed contact met ze over. Dus dat, als je iets niet weet, daar zijn we ook voor, om ze dan uit te leggen hoe dat werkt." (CS6)*

Voor het strafelement zou het contact er volgens een respondent eigenlijk niet toe moeten doen (CS2).

Ten slotte laten enkele deelnemers merken dat zij het contact met de begeleiders bij bedrijven als positief hebben ervaren (n=3). Zo vertelt een respondent dat het aardige mensen waren die hem hielpen met hoe alles werkt (DN5), voelde een andere respondent zich begrepen en gehoord bij het bedrijf (DN4) en noemt weer een andere respondent de begeleider een 'supertoffe gozer' die de respondent veel tips heeft gegeven wat hij later kan doen met zijn talenten (DN6). Het volgende citaat laat zien hoe het contact door een van de respondenten is ervaren:

> *"Maar het was wel echt heel fijn om gewoon… het was eigenlijk voor het eerst dat ik het idee had dat iemand gewoon meer begreep over wat ik zei dan...ik heb eigenlijk nooit echt mensen om me heen waarmee ik gewoon vrij kan praten over dingen waarmee ik bezig ben. En hij was eigenlijk de eerste. Dus dat vond ik wel tof." (DN6)*

Een respondent die bij de cyberwerkplaats is geweest, geeft daarentegen aan dat hij een vaste contactpersoon miste die er regelmatig is, verstand heeft van zaken en die je kunt berichten als je een vraag hebt en ergens op vastloopt (DN2).

7.5 Tevredenheid uitvoerders en deelnemers

In deze paragraaf wordt besproken hoe tevreden de uitvoerders en deelnemers van Hack_Right zijn over het traject (of de trajecten) waar zij bij betrokken zijn geweest. Eerst wordt de tevredenheid van toezichthouders besproken (7.5.1), vervolgens de tevredenheid van bedrijven en organisaties (7.5.2) en ten slotte de tevredenheid van deelnemers (7.5.3). Uit de resultaten blijkt dat uitvoerders over het algemeen tevreden zijn over de verloop van de Hack_Right-trajecten. Deelnemers zelf verschillen echter van mening over de mate waarin zij tevreden zijn over het traject dat zij hebben gevolgd.

7.5.1 *Toezichthouders*

De twee Halt-medewerkers geven allebei aan dat zij redelijk tevreden zijn over het verloop van de Hack_Right-trajecten die zij hebben begeleid (HA2, HA1). Voor de

eerste respondent heeft het negatieve aspect vooral te maken met de lange opstarttijd voordat de deelnemer daadwerkelijk kon beginnen met Hack_Right (HA2). De andere Halt-medewerker merkt op dat de opdrachten die de jongere bij Halt heeft gemaakt uitdagender hadden gekund omdat de deelnemer er nu relatief makkelijk vanaf kwam (HA1). Over het traject bij het bedrijf is de respondent tevreden en heeft hij niks aan te merken. De reclasseringswerker geeft aan dat de deelnemers allemaal binnen de eindtermijn het traject positief hebben afgerond (RE1).

7.5.2 *Bedrijven en organisaties*

Ook respondenten die deelnemers vanuit bedrijven of organisaties hebben begeleid, zijn over het algemeen tevreden over het verloop van het traject. Een eerste respondent is tevreden over het eerste traject en minder tevreden over het tweede traject (CS2). In het tweede traject was het namelijk niet goed gelukt om met de jongere in contact te komen, kwam de jongere zijn afspraken niet na en was de jongere ongemotiveerd. Een tweede respondent geeft aan dat hij over het geheel gezien tevreden is over de trajecten, maar dat de trajecten wel veel tijd hebben gekost (CS6). De derde respondent geeft aan dat er achteraf gezien bepaalde dingen anders konden worden aangepakt (CS5). Dit had vooral te maken met de informatievoorziening richting het bedrijf en het ontbreken van een duidelijk plan van aanpak. Een vierde respondent is over het algemeen tevreden over zijn traject (CS1). De vijfde respondent is tevreden met beide trajecten die hij heeft uitgevoerd omdat hij bij beide trajecten heeft gezien dat het nut heeft gehad (CS4). De respondent geeft als voorbeeld dat een van de deelnemers in een afsluitende presentatie benoemde dat zijn moraal veranderd was. De laatste respondent is ondanks dat de deelnemer is uitgevallen tevreden over het traject, omdat het traject voor de respondent erg leerzaam is geweest (CS7). De respondent zou bijvoorbeeld in het vervolg eerst een voorgesprek willen hebben om de motivatie en situatie van de deelnemer te kunnen inschatten.

7.5.3 *Deelnemers*

Aan jongeren die Hack_Right hebben doorlopen is tijdens de interviews gevraagd om een cijfer van 0 tot 10 te geven aan Hack_Right (n=7).[20] Cijfers variëren van een 2 tot een 9, waaruit blijkt dat er verschillen zitten in de mate waarin jongeren tevreden zijn over het Hack_Right-programma. De meeste jongeren geven een ruime voldoende aan Hack_Right (n=5). Zo geeft een deelnemer die een Halt-straf heeft gehad een 7.5, omdat hij het niet saai vond (DN1). Een andere deelnemer die via de reclassering naar organisatie F is gegaan geeft een 8.5 aan de organisatie tijdens het Hack_Right-traject (DN2). De respondent is blij dat hij kennis heeft kunnen maken met de organisatie en heeft door Hack_Right een baan kunnen vinden. Op dit moment gaat de respondent

20 Niet alle geïnterviewde deelnemers (n=10) zijn dezelfde vragen gesteld. In de methodische verantwoording (paragraaf 4.3) wordt dit verder toegelicht.

nog steeds naar de organisatie (ondanks dat de straf al is voltooid), maar is minder tevreden omdat er steeds projectmatiger gewerkt wordt. De respondent geeft daarom op dit moment een 6,5/7 aan de organisatie. Weer een andere respondent geeft een 6 of 7 aan Hack_Right (DN5). De respondent vond dat Hack_Right goed verliep, maar geeft aan dat het onderzoek van de politie lang duurde. Respondent DN6 geeft een 7 of 8 aan Hack_Right. De jongere vertelt dat hij zelf nooit kwade bedoelingen heeft gehad en vraagt zich af of mensen met kwade bedoelingen gecorrigeerd kunnen worden. Als deze mensen corrigeerbaar zijn dan had Hack_Right dat kunnen doen volgens de jongere. Ten slotte geeft een laatste respondent een 9 (DN7). De respondent vond Hack_Right een erg goed programma, vooral het gedeelte bij het bedrijf. Wel duurde het lang voordat er met Hack_Right gestart kon worden. Respondenten die onvoldoendes geven, beoordelen Hack_Right met een 2 (DN3) en een 3 (DN4). De jongere die een 2 geeft, vindt Hack_Right wel leuk en denkt wel dat het een positieve impact heeft gehad, maar vond de opdrachten erg makkelijk en heeft Hack_Right niet als een straf gezien (DN3). De jongere die een 3 geeft aan Hack_Right is teleurgesteld dat er geen duidelijk programma was bij het bedrijf en dat de jongere weinig kon doen doordat er geen geheimhoudingsverklaring was (DN4). Wel geeft de respondent een 'dikke 10' aan het bedrijf waar hij was, als het bedrijf niet verantwoordelijk was voor het ontbreken van een programma.

7.6 Belemmerende factoren en verbeterpunten

Uit interviews is gebleken dat respondenten over het algemeen enthousiast zijn over Hack_Right en dat zij tevreden zijn over de goede communicatie tussen de verschillende partners tijdens de verschillende fasen van de Hack_Right-trajecten. Naast deze bevorderende factoren voor een goed verloop van Hack_Right, worden ook factoren benoemd die volgens respondenten Hack_Right belemmeren of tot verbetering zouden kunnen leiden. De verschillende factoren die tot verbetering van Hack_Right kunnen leiden, worden in deze paragraaf besproken. Het blijkt dat vooral de lange tijd tussen het delict en de start van Hack_Right, de lage instroom van Hack_Right deelnemers en de ondersteuning voor uitvoerders een goed verloop van Hack_Right verbeterd kunnen worden.

Tijd tussen delict en Hack_Right – Veel van de respondenten merken op – zoals besproken in paragraaf 6.6 – dat er een lange tijd zit tussen het moment dat deelnemers van Hack_Right het delict plegen en het moment dat Hack_Right begint (n=10). Respondenten geven aan dat hierdoor voor deelnemers lastig is om terug te blikken op het delict (HA2, OM4) en vragen zich af of het na zo'n lange periode nog pedagogisch zinvol is of effect heeft (OM1, DN1).

Lage instroom Hack_Right – Een tweede factor die door respondenten wordt genoemd, is de lage instroom van geschikte casussen bij Hack_Right (n=4), waardoor de beoogde doelgroep niet altijd wordt bereikt. Een eerste mogelijke verklaring hiervoor is dat er zaken blijven liggen bij de politie en het OM (RE2, OM1). Ook wordt opgemerkt dat het mogelijk is dat de reclassering, politie en het OM niet goed op de hoogte zijn van Hack_Right als mogelijkheid (IO1, OM4). Ook de strafmodaliteiten waarbinnen Hack_Right opgelegd kan worden, zijn niet altijd bekend bij toewijzers (OM1). Ten slotte wordt opgemerkt dat het uiteindelijk een beslissing van individuen is om een zaak wel of niet aan te melden voor Hack_Right (IO1).

Ondersteuning uitvoerders – Tijdens interviews met uitvoerders komt naar voren dat er op verschillende gebieden meer ondersteuning kan worden gegeven aan uitvoerders (n=4). Ten eerste op het gebied van kennis en vaardigheden. Zo is in paragraaf 7.4 al besproken dat respondenten het belangrijk vinden om over pedagogische vaardigheden te beschikken. Respondenten geven aan dat een technisch-pedagogisch medewerker (CS5) of een begeleider met didactische vaardigheden (CS2) welkom waren geweest. Een van de respondenten vertelt daarnaast over een deelnemer met ADD/PDD-NOS-problematiek die bij het bedrijf zijn traject heeft uitgevoerd (CS3). Achteraf gezien is dit goed gegaan, maar de respondent geeft aan dat het bedrijf hier geen papieren voor heeft en dat meer begeleiding hierin nodig is. Ook zouden Halt-medewerkers volgens de respondent meer digitale vaardigheden moeten bezitten, om de digitale vaardigheden van een deelnemer in te kunnen schatten. De respondent zou graag zien dat er iets objectiefs komt om de technische kennis van deelnemers te kunnen bepalen (CS3). Ten tweede oppert een respondent ondersteuning in de vorm van faciliteiten, zoals centrale documentverwerking en een server die nodig is voor de projecten waar deelnemers aan werken (CS4). Nu regelt het bedrijf van de respondent deze zaken zelf. Ten slotte geeft de respondent aan dat op het moment dat een traject niet goed verloopt of een deelnemer later in de problemen komt, dit impact kan hebben op de begeleider/coach van het traject. Het zou wenselijk zijn dat er in zulke gevallen (psychologische) hulp wordt aangeboden.

Geschiktheid deelnemers – Enkele uitvoerders van Hack_Right-trajecten geven aan dat sommige deelnemers niet in aanmerking zouden moeten komen voor Hack_Right (n=3). Zo zou volgens een van de respondenten iemand die een DDoS-aanval pleegt niet in het traject moeten komen omdat dit weinig tot geen technische vaardigheden vereist (CS2). Ook zouden volgens een respondent mensen met financieel gewin of met slechte bedoelingen niet moeten deelnemen aan Hack_Right omdat dan skills aangeleerd kunnen worden die ze nog slechter kunnen gaan inzetten (OM5). Ook geeft een respondent aan dat ongemotiveerde deelnemers bij de selectie er beter uit gefilterd moeten worden (CS7). Verschillende respondenten erkennen dat de opdrachten bij Halt (IO2, DN4) en bij het bedrijf (DN1) bijvoorbeeld niet (technisch) uitdagend waren. De respondenten pleiten voor niveauverschillen (IO2), lastigere opdrachten (DN4) en criteria waaraan moet worden voldaan om opdrachten te halen (DN4).

Veel contacten – Uit enkele interviews blijkt dat Hack_Right intensief kan zijn voor zowel uitvoerders als deelnemers (n=3). Zo vraagt Hack_Right volgens een respondent veel van een Halt-medewerker (HA2) en geeft een andere respondent aan dat er veel contacten over het traject heen gaan en dat het wel praktisch moet blijven (OM1). Een derde respondent merkt op dat het belangrijk is om het aantal contactpersonen met de verdachte tot een minimum te beperken (OM3).

Opvolging of monitoring – Een ander punt dat wordt benoemd door uitvoerders van bedrijven, is dat zij graag nog een vinger aan de pols zouden willen houden bij de deelnemers (n=3). Zo opperen respondenten om jongeren 'te blijven triggeren' na Hack_Right (CS3), de mogelijkheid tot opvolging of monitoring (CS1) of om na het traject nog een contactmoment te hebben om te kijken hoe het met de jongere gaat en of hij of zij echt veranderd is (CS7). Een andere respondent benoemt tijdens een interview dat hij geen voorstander is van een lang monitoringssysteem (CS6).

Informatie-uitwisseling en communicatie - Verbetering is mogelijk in de communicatie tussen zowel organisaties die betrokken zijn bij Hack_Right (n=3) als richting deelnemers (n=2). Met betrekking tot het uitwisselen van informatie tussen partners, geeft een respondent aan dat de richtlijn hiervoor vaag is geformuleerd, waardoor het onduidelijk is wat nu wel en niet gedeeld mag worden met andere organisaties (CS1). Daarnaast zouden uitvoerders bij bedrijven graag vooraf meer informatie krijgen over de deelnemer (CS1, CS4). Een van de respondenten stelt voor om een standaard format op te stellen of een standaard briefing te geven aan het bedrijf waarin staat welke partijen er betrokken zijn en welke besluiten er genomen zijn (CS1). Bij een traject liep bijvoorbeeld nog een ontnemingsprocedure tijdens het Hack_Right-traject (OM4, CS4). De uitvoerder bij het bedrijf was hier niet van op de hoogte en geeft aan dat zulke zaken afgerond moeten zijn vóór het traject, omdat dit veel invloed heeft gehad op de motivatie van de deelnemer (CS4). Met betrekking tot het uitwisselen van informatie richting deelnemers had een respondent van het OM achteraf graag gewild dat er een intakebrief zou zijn gestuurd die de deelnemer kon ondertekenen met de duur en tijdspanne van het traject en wat er wordt verwacht van de deelnemer (OM3). Ten slotte geeft een van de deelnemers aan dat het voor hem onduidelijk was wat hij precies van het traject kon verwachten (DN10) en is er zoals eerder beschreven een deelnemer geweest die geen geheimhoudingsverklaring heeft getekend (DN4).

(Toe)zicht op bedrijven – Enkele respondenten merken op dat er weinig zicht is op wat er inhoudelijk bij de bedrijven gebeurt en wat bedrijven uiteindelijk aan de deelnemers vertellen (n=2). Zo geeft een respondent aan dat Halt en het OM weinig zicht hebben op wat er inhoudelijk gebeurt (CS3) en geeft een andere respondent aan dat men vanuit Hack_Right wellicht invloed wil hebben over wat bedrijven aan deelnemers vertellen (CS1):

> *"Ik denk bij wijze van spreken als iemand vanuit het NCSC aan tafel zou zitten in zo'n gesprek, dat ze af en toe misschien nog een beetje schrikken van wat wij dan zo'n deelnemer zouden vertellen, omdat zij er misschien met een andere bril naar kijken dan wij of een gemiddelde officier van justitie. Die hoort natuurlijk het liefste waarschijnlijk dat wij zeggen: 'Niet doen, wegblijven'. Waar wij er natuurlijk vanuit een breder perspectief naar kijken en zeggen: 'Het is gewoon belangrijk dat dit soort mensen dingen doen'. Maar goed, dat is een veel bredere discussie en debat dan Hack_Right alleen." (CS1)*

Ten slotte is er een respondent die aangeeft dat de selectie van uitvoerders professioneler zou kunnen door middel van een sollicitatie, screening of het opvragen van een vog (verklaring omtrent het gedrag) (CS4). Nu was er al vertrouwen en waren er korte lijntjes tussen de respondent en de projectgroep Hack_Right, maar dit kan belangrijk zijn als Hack_Right groter wordt, aldus de respondent.

Meerdere deelnemers tegelijkertijd – Een enkele respondent heeft een Hack_Right-traject begeleid of gevolgd waarbij twee deelnemers tegelijkertijd een traject hebben gevolgd (n=2). Beide respondenten merken op dat dit in de toekomst voorkomen moet worden. De ervaring van een deelnemer is hiervoor illustratief:

> *"Ja, die had [een DDoS-aanval gepleegd]. En hij zat een beetje stoer te praten over wat hij deed. En een beetje van: 'Daar wil ik het niet over hebben.' Een irritant jong. Ja, sorry. […] Ja, dat vond ik niet zo heel fijn dat hij erbij was. Vervelend." (DN5)*

Continuïteit Hack_Right – Tijdens de interviews komt ook de continuïteit van Hack_Right ter sprake. Zo zijn de financiering en het eigenaarschap op de lange termijn onduidelijk en loopt de formele samenwerking met ketenpartners tot september 2020 (IO2). Ondanks dat er genoeg bedrijven of organisaties zijn die Hack_Right deelnemers willen begeleiden (IO2, CS7), zijn er ook respondenten van bedrijven die aangeven dat het een investering is voor bedrijven en commercieel niet effectief is (CS2, CS4, CS6). De respondenten geven aan dat – ondanks dat ze er geen geld aan hoeven te verdienen – er wellicht mogelijkheden zijn om het voor bedrijven aantrekkelijker te maken om deelnemers te begeleiden. Voorbeelden die worden genoemd, zijn de kosten aftrekbaar maken van de belasting, te formaliseren dat partijen verantwoordelijkheid nemen en het eventueel betaald maken van het werk zoals dat ook bij Halt en reclassering het geval is.

7.7 Resumé

In dit hoofdstuk staan de ervaringen van Hack_Right betrokkenen centraal, zodat duidelijk wordt of volgens hen de doelen van Hack_Right worden behaald, wat mogelijke gevolgen zijn van Hack_Right en hoe Hack_Right verbeterd kan worden.

De meeste respondenten geven aan dat de doelen van Hack_Right die zij omschrijven worden behaald. Voor sommige doelen, waaronder het voorkomen van recidive, is het voor respondenten niet duidelijk of het doel is bereikt. Mogelijke gevolgen van Hack_Right volgens uitvoerders zijn dat deelnemers door Hack_Right werk hebben gekregen of een studie zijn gaan volgen, zich bewust zijn geworden van de gevolgen van hun handelen, handelingsperspectief hebben gekregen en nog contact hebben met de organisatie waar het programma is doorlopen. Negatieve gevolgen zouden kunnen zijn dat de deelnemers kennis die zij opdoen kunnen gebruiken voor negatieve doeleinden. Voor een aantal uitvoerders is het onduidelijk wat de effecten en gevolgen zijn voor deelnemers. Enkele deelnemers bevestigen dat zij nog steeds contact hebben of werkzaamheden verrichten bij de organisatie of een opleiding zijn gaan volgen. Sommige deelnemers geven aan wat te hebben geleerd, bijvoorbeeld over legale manieren om te hacken of verschillen tussen legaal en illegaal hacken. Anderen hebben minder of niets geleerd van Hack_Right, omdat opdrachten te makkelijk waren en zij de kennis zelf al hadden. Deelnemers hebben Hack_Right duidelijk niet als straf ervaren.

Met betrekking tot het contact tussen deelnemers en uitvoerders is gebleken dat deelnemers een vast contactpersoon hebben gehad vanuit Halt of reclassering en dat er vanuit bedrijven minimaal een medewerker de gehele dag aanwezig is bij de deelnemer. Halt en reclasseringswerkers weinig tot geen technische kennis hebben. Respondenten verschillen over de mate waarin dit voor het verloop van het Hack_Right-traject een probleem vormt. Uitvoerders bij bedrijven geven aan dat verbinding maken met de deelnemer en pedagogische vaardigheden belangrijke vaardigheden zijn om deelnemers te kunnen begeleiden vanuit een (cybersecurity)organisatie. Niet iedereen uit de organisaties is volgens respondenten geschikt om een deelnemer te begeleiden. Zowel deelnemers als uitvoerders zijn grotendeels tevreden over het contact dat zij hebben gehad met elkaar. Het lijkt er vooral op dat jongeren zich gehoord en begrepen voelen bij de (cybersecurity)organisaties.

Over het verloop van de Hack_Right-trajecten zijn uitvoerders over het algemeen tevreden. Deelnemers verschillen van mening over de mate waarin zij tevreden zijn over het traject dat zij hebben gevolgd. Deelnemers die minder tevreden zijn, geven aan dat er geen duidelijk programma was of dat opdrachten (vooral bij Halt) te makkelijk waren. Factoren die voor een minder goed verloop van Hack_Right zorgen of voor verbetering vatbaar zijn volgens uitvoerders, zijn onder andere de lange tijd tussen het delict en Hack_Right, de lage instroom van deelnemers bij Hack_Right, het gebrek aan ondersteuning voor uitvoerders, de geschiktheid van deelnemers, de vele contacten die nodig zijn tussen organisaties en het gebrek aan opvolging of monitoring.

8. Conclusie en discussie

8.1 Inleiding

We geven in dit hoofdstuk antwoord op de volgende drie 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 en (3) hoe hebben alle betrokkenen de tot nu toe uitgevoerde Hack_Right-trajecten ervaren? In paragraaf 8.2, 8.3 en 8.4 staan de conclusies per deelvraag beschreven. Tijdens de beantwoording van de onderzoeksvragen worden de belangrijkste conclusies van ons onderzoek weergegeven en wordt op deze bevindingen gereflecteerd. Voor de leesbaarheid zijn op enkele plekken deelvragen samengenomen en in een keer beantwoord. Paragraaf 8.5 bevat de aanbevelingen en mogelijkheden voor vervolgonderzoek.

8.2 Wat is Hack_Right en hoe is Hack_Right theoretisch onderbouwd? (Q1)

8.2.1 *Waarom en hoe is Hack_Right ontstaan? (Q1a)*

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.

De aanleiding van Hack_Right is aldus helder: een grote toestroom van verdachten met een 'nieuw' profiel waar nog geen effectieve interventie voor is ontwikkeld. 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 (zie bijvoorbeeld Oosterwijk & Fisher (2017) voor een overzicht van interventies). Echter ontbreekt empirisch onderzoek naar kenmerken van cybercriminelen nagenoeg. Enkele recente studies laten zien dat er weliswaar aanwijzingen zijn dat sommige cybercriminelen andere kenmerken hebben dan traditionele criminelen (Weulen Kranenbarg, 2018; Van der Wagen et al., 2019), maar een solide empirische basis hiervoor ontbreekt. Het merendeel van de studies die gedaan zijn, hebben een verkennend karakter, hebben aanzienlijke methodische beperkingen of laten op zijn minst zien dat er nog geen eenduidig beeld te schetsen is van de kenmerken van deze groep daders (zie voor een overzicht bijvoor-

beeld Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019). 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. Het 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. Feitelijk vormen dus deze signalen uit de praktijk de basis van het ontstaan van Hack_Right , waarbij met name het 'nieuwe' profiel van cyberdaders van belang is, omdat dit gegeven een nieuwe interventie noodzakelijk maakt. Er moet rekening 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.

8.2.2 *Wat is het doel en de theoretische onderbouwing van Hack_Right? (Q1c, Q1d)*

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, die interventieontwikkelaars in kaart hebben gebracht op basis van een literatuurstudie: onduidelijkheid of ontkennen van morele en juridische grenzen op internet, onzichtbaarheid of ontkennen van schade en slachtoffers, gebrek aan sociale controle, negatieve invloed peers, financiële beloning en emotionele of cognitieve beloning.

Hack_Right beoogt aldus in te spelen op de vermoedelijk criminogene behoeften ('needs') van de daders. Dit is een belangrijk principe voor een effectieve interventie om recidive te verminderen volgens het 'Risk-Need-Responsivity'-model. Ook hier is een kritische noot op zijn plek. De criminogene factoren die worden aangemerkt zijn technisch gezien namelijk geen 'needs' zoals omschreven in de 'what-works'-benadering. De lage pakkans, anonimiteit online, onduidelijke grenzen op internet en emotionele of financiële beloning zijn gelegenheidsfactoren die een omgeving creëren waarin crimineel gedrag mogelijk is. Het zijn echter geen factoren die direct relateren aan het individu en met Hack_Right veranderd kunnen worden. Wel kan Hack_Right deelnemers inzicht geven in hoe de gelegenheidsfactoren kunnen leiden tot crimineel gedrag en hoe deelnemers hiermee om kunnen gaan. Daarnaast speelt hier eenzelfde probleem als bij de onderbouwing van het 'nieuwe' profiel van cybercriminelen (zie beantwoording vorige deelvraag). Er zijn simpelweg nog bijna geen studies gedaan

naar criminogene factoren bij dit type dader en er is dus nog veel onbekend (zie Holt & Bossler, 2014; Leukfeldt, 2017; Maimon & Louderback, 2019) en is er 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 (Weulen Kranenbarg et al., 2018).

De interventieontwikkelaars erkennen dat de wetenschappelijk 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. Dat dit van belang is, blijkt niet alleen uit de literatuur – waar geen eenduidigheid is over of traditionele beschermende factoren nog wel zo beschermend zijn – maar ook uit de interviews. Zo geven enkele uitvoerders aan dat er een risico is dat de deelnemende jongeren wellicht de kennis die ze opdoen tijdens Hack_Right kunnen misbruiken. Het is onbekend of dat risico voor de Hack_Right doelgroep er daadwerkelijk is. In paragraaf 8.5 doen we aan aantal aanbevelingen voor vervolgonderzoek die kunnen helpen het wetenschappelijke fundament van Hack_Right steviger te maken.

8.2.3 *Hoe past Hack_Right in het huidige strafrechtsysteem en welke partijen zijn betrokken bij de opzet en uitvoering van Hack_Right? (Q1h, Q1g)*

Hack_Right kan gezien worden als een alternatief of aanvullend straftraject ingebed in het Nederlandse strafrechtsysteem. Hack_Right is eind 2017 ontwikkeld door de politie en het OM, in samenwerking met strafrechtketenpartners en (ICT-)bedrijven uit de private sector. In de praktijk komen verdachten van cybercriminaliteit op verschillende manieren bij Hack_Right terecht: via de politie, via het OM of via uitvoerende strafrechtketenpartners zoals Halt en reclassering. Iedere potentiële deelnemer wordt aangedragen bij de projectgroep Hack_Right en die projectgroep brengt advies uit over de geschiktheid van de verdachte voor deelname en een mogelijke invulling voor een traject.

8.3 Hoe zijn de tot nu toe uitgevoerde Hack_Right-trajecten verlopen? (Q2)

8.3.1 *Wat is de doelgroep van Hack_Right en wordt de doelgroep bereikt? (Q1e, Q2a)*

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.

Om te onderzoeken of de beoogde doelgroep van Hack_Right wordt bereikt in de tot nu toe uitgevoerde Hack_Right-trajecten, is enerzijds gekeken naar kenmerken van

deelnemers die naar voren komen tijdens interviews met Hack_Right jongeren en anderzijds gevraagd naar de selectiecriteria die toewijzers van het OM hanteren bij het wel of niet opleggen van Hack_Right.

– *Leeftijd.* Leeftijd speelt volgens de toewijzers een belangrijke rol: alleen jongeren komen in aanmerking voor Hack_Right. De leeftijd van de geïnterviewde deelnemers ten tijde van het delict varieert van 14 tot 18 jaar. Niet alle toewijzers blijken bekend met het feit dat ook personen boven de 18 jaar kunnen deelnemen aan Hack_Right.
– *Type delict.* Toewijzers van het OM geven aan dat de cyberdelicten van geringe ernst moeten zijn om in aanmerking te komen voor Hack_Right. Daarnaast mag het motief volgens enkele toewijzers geen financieel oogmerk hebben, iets dat niet is beschreven in de plannen van Hack_Right. In grote lijnen zijn de criteria genoemd door toewijzers terug te zien bij de delicten die de geïnterviewde jongeren hebben gepleegd. Dit zijn voornamelijk cyberdelicten zoals DDoS-aanvallen en hacks (op schoolsystemen) zonder financieel motief. Er is echter ook een deelnemer die Hack_Right kreeg toegewezen vanwege oplichting via internet. Bij deze deelnemer lijkt dus geen sprake te zijn van een delict computercriminaliteit en is wel een duidelijk financieel motief.
– *Motivatie*. Volgens uitvoerders en toewijzers van Hack_Right zijn jongeren die hebben deelgenomen vooraf bereid geweest om deel te nemen aan Hack_Right. Tijdens de uitvoering van Hack_Right is een enkele deelnemer echter minder gemotiveerd volgens uitvoerders. De deelnemers hebben op een persoon na wel allemaal het traject afgerond.
– *Affiniteit met ICT, schadelijkheid gedrag en 'first offender'*. Alle toewijzers geven aan dat affiniteit met ICT een belangrijke overweging is om wel of geen Hack_Right op te leggen. Een enkele toewijzer benoemt ook de schadelijkheid van het gedrag en delictsgeschiedenis van de deelnemer als selectiecriteria. In hoeverre de deelnemers daadwerkelijk aan deze voorwaarden voldoen, is op basis van dit onderzoek niet te concluderen.

In de regel bereikt Hack_Right dus de doelgroep zoals beschreven in de plannen. Er zijn ook uitzonderingen. Zo is er een deelnemer van Hack_Right die juist wel een financieel motief had. Deze deelnemer heeft via internet mensen opgelicht en past dus niet binnen de doelgroep van Hack_Right. Verder blijkt dat niet alle uitvoerders de leeftijdsgrens helder voor ogen te hebben: een uitvoerder is niet op de hoogte dat ook personen van ouder dan 18 jaar kunnen deelnemen aan Hack_Right. Deze uitzonderingen zijn opmerkelijk, juist omdat er nog maar een beperkt aantal Hack_Right-trajecten zijn afgerond (veertien ten tijde van de afronding van de dataverzameling voor dit onderzoek). Ook is het opvallend dat toewijzers de ernst van het delict een belangrijk criterium vinden, aangezien dit niet strookt met de plannen van Hack_Right.

We hebben 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.

8.3.2 *Verloopt het programma van de tot nu toe uitgevoerde Hack_Right-trajecten volgens plan? (Q1f, Q2b)*

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 module(s) gebruikt, maar zijn alleen elementen van de modules verwerkt in de trajecten. Producten zoals de training juridisch/ethisch hacken en een handleiding voor bedrijven zijn bijvoorbeeld ten tijde van het onderzoek nog in ontwikkeling.

De invulling van de tot nu toe uitgevoerde Hack_Right-trajecten is hierdoor niet duidelijk te herleiden tot concrete module(s) en bijbehorende producten die zijn beschreven in de plannen. De uitvoering van de trajecten verloopt daarmee niet zoals deze in de plannen zijn omschreven.

Een onderscheid kan worden gemaakt tussen deelnemers die Hack_Right hebben gevolgd in de vorm van een Halt-straf en deelnemers die Hack_Right hebben gevolgd bij de reclassering, vaak weggeschreven als werk- of leerstraf. De invulling van Halt-trajecten hebben een vaster karakter, waarin eerst opdrachten en gesprekken bij Halt plaatsvinden en vervolgens een (flexibel) programma bij een bedrijf wordt gevolgd. Deelnemers die Hack_Right hebben gevolgd via de reclassering hebben verschillende activiteiten uitgevoerd, zoals op projectbasis werken bij ICT-bedrijven, werkzaamheden uitvoeren bij een non-profitorganisatie op het gebied van cybersecurity en interviews of presentaties geven. Factoren die een rol spelen bij het bepalen van de invulling zijn technische kennis en vaardigheden, risicofactoren en het motief van de deelnemer.

De uitvoering van Hack_Right blijkt dus in de praktijk deels af te wijken van de plannen en bovendien verschilt de invulling van de uitgevoerde Hack_Right-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. Verschillen in trajecten kunnen echter ook worden toegeschreven aan het ontbreken van uitgewerkte 'producten' en handleidingen voor de uitvoering van die producten. Dit kan met name problematisch zijn omdat niet alle betrokken organisaties bij Hack_Right over de juiste kennis en kunde beschikken om de deelnemers te begeleiden. 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.

8.3.3 *Zijn de tot nu toe uitgevoerde Hack_Right-trajecten voldoende intensief en compleet uitgevoerd? (Q2c)*

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 trajecten die tot nu toe zijn uitgevoerd hebben bij Halt allemaal een duur gehad van twintig uur, verspreid over enkele dagen. Bij de reclassering variëren de trajecten van veertig tot 144 uur, verspreid over enkele dagen tot maanden. In beide soorten trajecten geven enkele van de deelnemende jongeren overigens aan dat het in de praktijk veel minder tijd kost. Volgens het risicoprincipe van het 'RNR-model' kunnen personen die een laag risico hebben om te recidiveren het best worden onderworpen aan een minimaal programma. Hoogrisicodaders dienen een intensiever programma te krijgen. Het is niet duidelijk in hoeverre er met de intensiteit van de invulling van Hack_Right rekening is gehouden met het risico op recidive. Verder blijkt dat de tijd tussen het plegen van het delict en de afronding van Hack_Right erg lang duurt – vaak een tot enkele jaren – mede dankzij langdurige dossieropbouw bij de politie en het OM. Hierdoor is het voor deelnemers lastig om tijdens Hack_Right terug te blikken op het gepleegde delict. Bovendien worden laagrisicodaders door de lange doorlooptijd lang blootgesteld aan de gevolgen van het gepleegde delict.

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. Een enkel traject van de compleet uitgevoerde Hack_Right-trajecten verliep moeizamer, door een gebrek aan motivatie van de deelnemer. De deelnemer die tijdens het traject is uitgevallen, heeft geen afsluitende presentatie gegeven, omdat de jongere het gevoel had een presentatie te moeten geven over iets dat hij in zijn ogen niet gedaan heeft. De deelnemer lijkt daarmee de schadelijkheid van zijn gedrag niet in te zien, een van de criteria voor deelname aan Hack_Right.

8.4 Hoe hebben alle betrokkenen de tot nu toe uitgevoerde Hack_Right-trajecten ervaren? (Q3)

8.4.1 *Worden de door betrokkenen gestelde doelen behaald? (Q1b, Q1c, Q3a)*

Personen die betrokken zijn bij de uitvoering of toewijzing van Hack_Right geven verschillende labels aan Hack_Right en noemen ook verschillende doelen van Hack_Right. Zo wordt Hack_Right omschreven als 'project', 'interventie', 'training' of 'straf' en variëren doelen van 'deelnemers het goede of rechte pad op brengen' tot 'bewustwording' of 'recidive voorkomen'. De variatie in antwoorden lijkt vooral te verklaren door de (strafrechtelijke) context waar respondenten werkzaam zijn.

Het leerelement staat centraal in de verschillende betekenissen en doelen die respondenten benoemen. Er is geen consensus over de mate waarin Hack_Right een strafelement dient te bevatten. Volgens enkele respondenten dient Hack_Right als straf te worden ervaren, voor sommige dient Hack_Right slechts een dwingend karakter te hebben en voor anderen hoeft het geen straf te zijn.

Aangezien respondenten een grote hoeveelheid verschillende doelen benoemen, is het niet mogelijk om eenduidig antwoord te geven op de vraag of de door betrokken gestelde doelen van Hack_Right worden behaald. Een groot deel van de respondenten geeft aan dat de doelen die zij benoemen zijn behaald. Voor andere respondenten – en bij sommige doelen die genoemd zijn zoals recidive verminderen – is het onduidelijk of de doelen zijn behaald. Een enkele respondent geeft aan dat de doelen niet zijn behaald. Zo is het bij de deelnemer die is uitgevallen niet gelukt om duidelijk te maken wat de gevolgen van het delict zijn voor slachtoffers en de samenleving.

8.4.2 *Welke mogelijke positieve of negatieve gevolgen zijn er volgens betrokkenen voor deelnemers? (Q3b)*

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.

Deelnemers geven een wisselend beeld over wat zij hebben geleerd van Hack_Right. Zo geven sommige deelnemers aan dat zij wat hebben geleerd over verschillen tussen goeden kwaadaardig hacken, mogelijkheden om op legale wijze geld te verdienen met hacken of een programmeertaal. Anderen geven aan dat zij weinig tot niets van Hack_Right geleerd hebben, omdat opdrachten te makkelijk waren en zij de kennis zelf al hadden. Verder blijkt dat deelnemers Hack_Right niet of nauwelijks als straf ervaren. Zij zien Hack_Right als een 'softe straf', een 'beloning' of vinden dat zij er makkelijk vanaf zijn gekomen. Vooral de arrestatie, het verhoor en inbeslagname van spullen worden gezien als straf.

8.4.3 *Hoe verloopt het contact tussen uitvoerders en deelnemers? (Q3c)*

Deelnemers hebben tijdens de uitvoering van de Hack_Right-trajecten vaak een vast contactpersoon gehad vanuit Halt of reclassering. Bij bedrijven is er een medewerker geweest die gedurende de hele dag(en) bij de deelnemer is geweest. Zowel deelnemers als uitvoerders zijn veelal tevreden over het contact dat zij hebben met elkaar. Deelnemers voelen zich vooral gehoord en begrepen bij de (cybersecurity)organisaties. Een match of klik tussen de uitvoerder en deelnemer kan een belangrijke factor zijn voor een effectieve interventie. Zo kan volgens de literatuur de persoonlijke behandelrelatie – ook wel 'who works' genoemd – tot een verbetering leiden van het gedrag van de deelnemer.

Uitvoerders van Halt en reclassering blijken over weinig tot geen technische kennis te beschikken. Respondenten verschillen van mening over de mate waarin dit een probleem vormt. Zo is volgens enkele respondenten technische kennis nodig om in contact te komen met de doelgroep, om in te schatten of een Hack_Right traject daadwerkelijk goed verloopt en kan meer technische kennis het vertrouwen van de deelnemer in de competenties van de begeleider verhogen. Andere respondenten geven aan dat vooral pedagogische kennis belangrijk is en dat de kennisachterstand er juist voor kan zorgen dat de doelgroep begint met praten.

Een bijzondere groep binnen de Hack_Right-interventie vormen de bedrijven. 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 – echter van belang dat een interventie wordt uitgevoerd door goed opgeleide en getrainde professionals. De deelnemers zijn over het algemeen tevreden over de begeleiding vanuit de ICT-bedrijven. Een belangrijke vraag blijft echter of verwacht kan worden dat de begeleiders vanuit de bedrijven over de juiste capaciteiten beschikken om de jongeren te begeleiden. Zeker wanneer Hack_Right wordt opgeschaald en er wellicht sprake is van een minder intensieve samenwerking tussen alle uitvoerende partijen.

8.4.4 *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? (Q3d, Q3e)*

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 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.

8.5 Aanbevelingen en vervolgonderzoek

Verbeter het fundament

Hack_Right is feitelijk ontstaan vanuit signalen uit de praktijk: een grote toestroom van verdachten met een 'nieuw' profiel waar nog geen effectieve interventie voor is ontwikkeld. Hack_Right is een initiatief dat met veel enthousiasme is opgezet door partijen binnen en buiten de strafrechtketen. Dit enthousiasme is tijdens de interviews met vrijwel alle betrokkenen overduidelijk. Over het algemeen vinden respondenten dat Hack_Right simpelweg nodig is. Dat wetenschappelijke inzichten in enkele belangrijke aspecten die ten grondslag liggen onder Hack_Right ontbreken, erkennen de ontwikkelaars, maar tegelijk geven ze aan dat het belangrijk is om te starten en daarbij nieuwe inzichten uit de wetenschap in de gaten te blijven houden. Een belangrijk punt is echter dat Hack_Right niet bij een enthousiast initiatief moet blijven. Om te kunnen doorgroeien tot een volwaardige interventie is daarom een stevigere basis nodig. Onderhavig onderzoek is daarbij een eerste stap, maar zeker niet de laatste. Inzichten in bijvoorbeeld kenmerken en criminogene factoren van de doelgroep zijn noodzakelijk om een effectieve interventie op te zetten. Enerzijds kan hierin inzicht worden verkregen door de uitgevoerde Hack_Right-trajecten te (blijven) evalueren. Ten tijde van dit onderzoek was er immers slechts een beperkt aantal trajecten afgerond. Anderzijds kunnen andere bronnen ge-

bruikt worden om meer inzicht te krijgen in kenmerken van de Hack_Right doelgroep. Data over verdachten die voorkomen in de politiesystemen kunnen bijvoorbeeld gebruikt worden om inzicht te krijgen in achtergrondkenmerken en criminele carrières.

Zorg dat de doelen duidelijk zijn

Ondanks dat het leerelement in Hack_Right centraal staat volgens alle uitvoerders van Hack_Right – deelnemers krijgen adviezen, begeleiding en ontwikkelen vaardigheden – leven er in de praktijk verschillende beelden bij wat de overige doelen van de interventie precies zijn. Ondanks dat de plannen van Hack_Right en interventieontwikkelaars benadrukken dat Hack_Right geen strafdoel heeft, verschillen de meningen van toewijzers en uitvoerders over de mate waarin Hack_Right een straf zou moeten zijn voor deelnemers. Hack_Right-deelnemers zelf rapporteren vaak tot hun eigen verbazing dat ze Hack_Right helemaal niet als straf hebben ervaren. Ook is de ernst van het delict voor toewijzers een belangrijk criterium om wel of geen Hack_Right op te leggen. Verwachtingsmanagement richting interne en externe partijen omtrent het strafelement is daarom belangrijk. Communiceer daarom naar interne en externe partijen duidelijk over de doelen van Hack_Right en zorg indien noodzakelijk dat het strafelement in een andere maatregel of straf tot uiting komt.

Verbeter de programma-integriteit

Bij de invulling van de tot nu toe uitgevoerde Hack_Right-trajecten bestaat er een spanning tussen een op het individu afgestemde interventie (responsiviteit) en een programma dat wordt uitgevoerd zoals in de plannen beschreven (programma-integriteit). Door de vele verschillende invullingen die Hack_Right-deelnemers hebben gehad, is niet duidelijk welke componenten van de interventie kunnen leiden tot bepaalde uitkomsten. Verder ontbreken op dit moment uitgewerkte producten en handleidingen voor de uitvoering van die producten. Zo zijn producten zoals de training juridisch/ethisch hacken en een handleiding voor bedrijven ten tijde van het onderzoek nog in ontwikkeling.

Voor de volgende stappen in het evaluatieonderzoek is het belangrijk dat duidelijker wordt wat de invullingsmogelijkheden zijn voor een Hack_Right-traject. Alleen dan kan – uiteindelijk met behulp van effectevaluaties – worden bepaald welke elementen van de interventie, onder welke omstandigheden, leiden tot bedoelde of onbedoelde gevolgen. Individuele afstemming is mogelijk en zelfs wenselijk, maar kernelementen van de interventie moeten duidelijk zijn en geborgd zijn tijdens de concrete invulling van Hack_Right.

Een belangrijk aspect binnen de programma-integriteit is de rol van de ICT-bedrijven. Er dient goed nagedacht te worden over de kennis, vaardigheden en denkbeelden die (cybersecurity)bedrijven deelnemers (zouden moeten) leren. Ga hierbij in overleg met partners, maak hier afspraken over en communiceer dit ook richting andere partijen. Beperk hierbij het risico dat deelnemers de vaardigheden die zij leren kunnen inzetten

voor nieuwe strafbare feiten. Dit kan bijvoorbeeld door alleen vaardigheden te leren aan deelnemers die aantonen dat zij zich ook inzetten voor het morele aspect van informatiebeveiliging. Ook kan hierbij rekening worden gehouden met de zwaarte van het delict en/of het risico op recidive: bij deelnemers met een hoog risico op recidive of deelnemers die een zwaar delict hebben gepleegd, lijkt terughoudendheid geboden in het leren van nieuwe vaardigheden.

Zorg voor een goede opleiding van de uitvoerders

Vanuit het professionaliteitsbeginsel is het voor een effectieve interventie van belang dat begeleiders die een interventie uitvoeren voldoende zijn opgeleid en getraind. Enerzijds betekent dit dat het belangrijk is om zorgvuldig geschikte uitvoerders te selecteren. Anderzijds kunnen er trainingen of cursussen worden aangeboden aan de uitvoerders. Halt- en reclasseringswerkers kunnen bijvoorbeeld worden voorzien van basale kennis over cybercriminaliteit. Uitvoerders van ICT-bedrijven kunnen worden ondersteund door pedagogisch medewerkers of, indien zij gedurende lange termijn betrokken zijn bij Hack_Right-trajecten, bijgeschoold worden in pedagogische kennis. Toekomstig onderzoek kan laten zien of – en welke – ICT-kennis nodig is voor toezichthouders om deelnemers effectief te kunnen begeleiden.

Verbeter de zichtbaarheid

Een belangrijke belemmerende factor volgens respondenten is de lage instroom van deelnemers bij Hack_Right. Het blijkt dat de selectie van deelnemers op dit moment afhankelijk is van individuen die op de hoogte zijn van Hack_Right als mogelijkheid en zelf beslissen om Hack_Right wel of niet aan te dragen aan de projectgroep Hack_Right. De overwegingen voor de selectie van deelnemers ligt niet alleen bij het OM, maar ook bij andere partners zoals de politie, Halt en reclassering. Het bereik van potentiële deelnemers is hierdoor afhankelijk van individuele kennis en keuzes. De zichtbaarheid van Hack_Right kan dan ook verhoogd worden, onder andere door het informeren van sleutelfiguren in het opleggen van Hack_Right over de mogelijkheden, doelen en selectiecriteria van Hack_Right.

Dat Hack_Right een alternatieve interventie is voor een zeer selecte groep verdachten, kan een vorm van rechtsongelijkheid met zich me meebrengen. Een juridisch vervolgonderzoek kan in kaart brengen hoe Hack_Right (als alternatieve interventie) en de selectie van deelnemers zich verhouden tot dergelijke rechtsbeginselen.

Onderzoek de schaalbaarheid

Hack_Right is eind 2017 ontwikkeld en heeft tot maart 2020 veertien afgeronde trajecten opgeleverd. Dit lijkt tegenstrijdig met de aanleiding van Hack_Right: een grote toename van daders computercriminaliteit. De verwachting is dan ook dat in de toekomst grotere stromen deelnemers Hack_Right zullen volgen. Op dit moment lijkt er echter sprake te zijn van een hoge mate van maatwerk: deelnemers worden aangereikt

vanuit verschillende onderdelen van de strafrechtketen, de projectgroep beoordeelt de aanvragen en een beperkt aantal personen binnen Halt en reclassering voeren de trajecten vervolgens uit met ICT-bedrijven. Om Hack_Right op grotere schaal te kunnen uitvoeren, is het daarom enerzijds van belang om de programma-integriteit te verbeteren: er zullen immers meer uitvoerders nodig zijn die moeten weten wat het doel is van de interventie en hoe de interventie moet worden uitgevoerd. Anderzijds moet goed bekeken worden hoeveel geschikte ICT-bedrijven er zijn die zich voor langere tijd willen committeren aan Hack_Right. Zonder de bedrijven vervalt immers een belangrijk deel van de interventie.

Mogelijkheden voor toekomstig onderzoek

Het onderzoek naar Hack_Right en de tot nu toe uitgevoerde Hack_Right-trajecten kent enkele beperkingen (zie ook paragraaf 4.4). Zo heeft er een selectie*bias* plaatsgevonden met betrekking tot de respondenten die zijn geïnterviewd, is de validiteit van de antwoorden van respondenten lastig vast te stellen, hebben respondenten vragen beantwoord over gebeurtenissen die enige tijd geleden plaatsvonden en heeft het onderzoek gekeken naar gevolgen voor deelnemers en niet naar gevolgen voor slachtoffers of de samenleving. Om de gevolgen van Hack_Right voor de samenleving en slachtoffers in kaart te brengen, kan met behulp van enquêtes onder de Nederlandse bevolking en interviews met slachtoffers worden onderzocht wat perspectieven zijn van deze groepen. Met betrekking tot de validiteit van de antwoorden – en selectie*bias* – van respondenten kunnen observaties een betrouwbaarder beeld van het verloop van de Hack_Right-trajecten schetsen. Daarnaast kunnen observaties beter inzicht geven in wat deelnemers precies leren bij (cybersecurity)organisaties tijdens de Hack_Right-trajecten.

Literatuurlijst

Abraham, M., & Buysse, W. (2013). *Halt vernieuwd. Procesevaluatie van de vernieuwde Halt-afdoening.* Den Haag/Amsterdam: WODC/DSP-groep.

Aiken, M., Davidson, J., & Amann, P. (2016). Youth pathways into cybercrime.

Andrews, D.A., Bonta, J., & Wormith, J.S. (2011). The risk-need-responsivity (RNR) model: Does adding the good lives model contribute to effective crime prevention? *Criminal Justice and Behavior*, *38*(7), 735-755.

Andrews, D.A., Zinger, I., Hoge, R.D., Bonta, J., Gendreau, P., & Cullen, F.T. (1990). Does correctional treatment work? A clinically relevant and psychologically informed meta-analysis. *Criminology, 28*(3), 369-404.

Anyon, Y., Roscoe, J., Bender, K., Kennedy, H., Dechants, J., Begun, S., & Gallager, C. (2019). Reconciling adaptation and fidelity: implications for scaling up high quality youth programs. *The journal of primary prevention, 40*(1), 35-49.

Boekhoorn, P. (2019). *De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging.* Den Haag: Politie & Wetenschap, Den Haag: Boekhoorn.

Bruijne, M. de (2018). Hack_Right: Een interventie voor jonge, naïeve cybercriminelen. *Opportuun*, *24*(2).

Centraal Bureau voor de Statistiek. (2019). Digitale veiligheid en criminaliteit 2018. Geraadpleegd van https://www.cbs.nl/nl-nl/publicatie/2019/29/digitale-veiligheid-criminaliteit-2018

Chan, D. (2019). Hack Right: How to Deter First Offenders Away from Cybercrime. Geraadpleegd van https://news.fordham.edu/university-news/hack-right-how-to-deter-first offenders-away-from-cybercrime/

Cullen, F., Jonson, C., & Nagin, D. (2011). Prisons do not reduce recidivism: The high cost of ignoring science. *The Prison Journal, 91*(3_suppl), 48.

Decorte, T. & Zaitch, D. (Ed.) (2016). *Kwalitatieve methoden en technieken in de criminologie* (3e ed.). Leuven: Uitgeverij Acco.

Denkers, A., & de Jong, J. D. (2020). Delinquentie, vrienden en 'boosheid met liefde'. *Tijdschrift voor Criminologie*, *62*(2-3).

Dijk, t. van (2012). Toegang en toezicht, online tijdsbesteding en –activiteiten. In: J. Kerstens & w. stol 9eds.), Jeugd en cybersafety: *Online slachtoffer- en daderschap onder Nederlandse jongeren* (pp. 55-72). Den Haag: Boom Lemma.

Durlak, J.A., & DuPre, E.P. (2008). Implementation matters: A review of research on the influence of implementation on program outcomes and the factors affecting implementation. *American Journal of Community Psychology, 41*(3-4), 327-350.

Farrington, D.P., & Welsh, B.C. (2005). Randomized experiments in criminology: What have we learned in the last two decades? *Journal of Experimental Criminology*, *1*(1), 9-38.

Farrington, D.P., Gottfredson, D.C., Sherman, L.W., & Welsh, B.C. (2003). The Maryland Scientific Methods Scale. In: *Evidence-based crime prevention* (pp. 27-35). Routledge.

Ferguson, J.L. (2002). Putting the 'what works' research into practice: An organizational perspective. *Criminal Justice and Behavior, 29*(4), 472-492.

Ferwerda, H., Leiden, I. van, Arts, N., & Hauber, A. (2006). *Halt: Het Alternatief? De effecten van Halt beschreven*. Den Haag: Boom Juridische uitgevers. Onderzoek en beleid 244.

Harte, J. (2019). *Zo werkt het: Over hoe onderzoek bijdraagt aan betere interventie.* Den Haag: Boom criminologie.

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20-40.

Howells, K., & Day, A. (2003). Readiness for anger management: Clinical and theoretical issues. *Clinical psychology review*, *23*(2), 319-337.

Justitiële interventies (2020). Erkende interventies. Geraadpleegd van https://www.justitieleinterventies.nl/erkende-interventies

Kao, D.-Y., Fu-Yuan Huang, F., & Wang, S.-J. (2009). Persistence and desistance: Examining the impact of re-integrative shaming to ethics in Taiwan juvenile hackers. *Computer Law & Security Review, 25*, 464-476.

Koehler, J.A., Lösel, F., Akoensi, T.D., & Humphreys, D.K. (2013). A systematic review and meta-analysis on the effects of young offender treatment programs in Europe. *Journal of Experimental Criminology*, *9*(1), 19-43.

Laan, P.H. van der. (2004). Over straffen, effectiviteit en erkenning. De wetenschappelijke onderbouwing van preventie en strafrechtelijke interventie. *Justitiële Verkenningen, 30*(5), 31-48.

Leeuw, F.L. (2005). Trends and developments in program evaluation in general and criminal justice programs in particular. *European Journal on Criminal Policy and Research, 11*(3-4), 233-258.

Leukfeldt, E.R., Kleemans, E.R., & Stol, W.P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. *The British Journal of Criminology, 57*(3), 704-722.

Leukfeldt, E.R. (ed.) (2017). *Research Agenda: The Human Factor in Cybercrime and Cybersecurity.* Den Haag: Eleven International Publishing.

Leukfeldt, E.R., Domenie, M.M.L. & Stol, W.P. (2010). *Verkenning cybercrime in Nederland 2009.* Den Haag: Boom Juridische uitgevers.

Leukfeldt, E. R., Notté, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims & Offenders*, *15*(1), 60-77.

Lipsey, M.W. (2009). The primary factors that characterize effective interventions with juvenile offenders: A meta-analytic overview. *Victims and Offenders*, *4*(2), 124-147.

Lipsey, M.W., & Cullen, F.T. (2007). The Effectiveness of Correctional Rehabilitation: A Review of Systematic Reviews. *Annual Review of Law and Social Science*, *3*(1), 297-320.

Lipsey, M.W., Chapman, G.L., & Landenberger, N.A. (2001). Cognitive-behavioral programs for offenders. *The Annals of the American Academy of Political and Social Science, 578*(1), 144-157.

Looman, J., & Abracen, J. (2013). The risk need responsivity model of offender rehabilitation: Is there really a need for a paradigm shift? *International Journal of Behavioral Consultation and Therapy*, *8*(3- 4), 30-36.

Lowenkamp, C.T., & Latessa, E.J. (2004). Understanding the risk principle: How and why correctional interventions can harm low-risk offenders. Topics in community corrections, 2004, 3-8.

Lusthaus, J., & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice*, 1-11.

Maimon, D., Alper, M., Sobesto, B., & Cukier, M. (2014). Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, *52*(1), 33-59.

Maimon, D., & Louderback, E. (2019). Cyber-dependent crimes: An interdisciplinary review. *Annual Review of Criminology, 2*(1), 191-216.

McCord, J. (2003). Cures that harm: Unanticipated outcomes of crime prevention programs. *The Annals of the American Academy of Political and Social Science*, *587*(1), 16-30.

McGuire, M., & Dowling, S. (2013). Cybercrime: A review of the evidence. Summary of key findings and implications. Home Office Research report, 75.

McMurran, M., & Ward, T. (2010). Treatment readiness, treatment engagement and behaviour change. *Criminal Behaviour and Mental Health*, *20*(2), 75-85.

Nas, C.N., van Ooyen-Houben, M.M.J. & Wieman, V. (2011). *Interventies in uitvoering: Wat er mis kan gaan bij de uitvoering van justitiële (gedrags)interventies en hoe dat komt*. Den Haag: WODC.

National Crime Agency. (2016). Pathways into Cybercrime.

NOS. (10 april 2020). Man (19) opgepakt voor DDoS-aanval op overheidssites. Geraadpleegd van https://nos.nl/artikel/2330050-man-19-opgepakt-voor-ddos-aanval-op-overheidssites.html

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

Ooyen-Houben, M.V., & Leeuw, F.L. (2010). *Evaluatie van justitiële (beleids)interventies: WODC-notitie.* Den Haag: WODC.

Ooyen-Houben, M.V., Nas, C.N. & Mulder, J. (2011). What Works en What goes Wrong ? *Justitiële Verkenningen*, *37*(5), 64-79.

Pawson, R., & Klein Haarhuis, C. (2005). Evaluatie van complexe programma's. Een theoriegestuurde aanpak. *Justitiële Verkenningen, 31*(8), 42-53.

Pawson, R., Tilley, N., & Tilley, N. (2004). *Realistic evaluation*. Sage.

Petrosino, A., Turpin-Petrosino, C., & Buehler, J. (2003). Scared Straight and Other Juvenile Awareness Programs for Preventing Juvenile Delinquency: A Systematic Review of the Randomized Experimental Evidence. *Annals of the American Academy of Political and Social Science*, *589*(March), 41–62.

Rechtspraak, de. (23 maart 2020). Man veroordeeld voor hacken computersysteem ROC Aventus. Geraadpleegd van https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Gelderland/Nieuws/Paginas/Man-veroordeeld-voor-hacken-computersysteem-ROC-Aventus.aspx

Rossi, P., Lipsey, M., & Freeman, H. (2004). *Evaluation : A systematic approach (7th ed.)*. Thousand Oaks, CA: Sage.

Rovers, B. (2007). What works; kanttekeningen bij een populair programma. *Tijdschrift Voor Veiligheid, 6*(3), 7-22.

Seligman, M.E.P. (2002). Positive psychology, positive prevention, and positive therapy. In C.R. Snyder and S.J. Lopez (Eds.), *Handbook of Positive Psychology* (pp. 3-9). New York: Oxford University Press.

Sondorp, J.E., Torregrosa, L.D.R., Höing, M., & Mebel, K. te. (2019). *Procesevaluatie pilot Halt-interventie Sexting.* Den Haag/Woerden: WODC/VanMontfoort.

Wagen, W. V., van 't Zand-Kurtovic, E.G., Matthijsse, S.R., & Fischer, T.F.C. (2019). *Cyberdaders: uniek profiel, unieke aanpak? Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin*. Den Haag: WODC.

Ward, M. (2017). Rehab camp aims to put young cyber-crooks on right track. BBC. Geraadpleegd via https://www.bbc.com/news/technology-40629887

Ward, T., & Brown, M. (2004). The good lives model and conceptual issues in offender rehabilitation. *Psychology, Crime and Law*, *10*(3), 243-257.

Ward, T., & Gannon, T.A. (2006). Rehabilitation, etiology, and self-regulation: The comprehensive good lives model of treatment for sexual offenders. *Aggression and Violent Behavior*, *11*(1), 77-94.

Ward, T., & Stewart, C. (2003). Criminogenic needs and human needs: A theoretical model. *Psychology, Crime and Law*, *9*(2), 125-143.

Ward, T., Yates, P.M., & Willis, G.M. (2012). The good lives model and the risk need responsivity model: A critical response to Andrews, Bonta, and Wormith (2011). *Criminal Justice and Behavior*, *39*(1), 94-110.

Wartna, B.J.S., Alberda, D.L. & Verweij, S. (2013). *Wat werkt in Nederland en wat niet? Een meta-analyse van Nederlands recidiveonderzoek naar de effecten van strafrechtelijke interventies.* Den Haag: Boom Lemma.

Weisburd, D., Farrington, D.P., Gill, C., Ajzenstadt, M., Bennett, T., Bowers, K., Wooditch, A. (2017). What Works in Crime Prevention and Rehabilitation: An Assessment of Systematic Reviews. *Criminology and Public Policy*, *16*(2), 415-449.

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison* (Doctoral dissertation, 2018). Amsterdam: Vrije Universiteit.

Weulen Kranenbarg, M.W., Holt, T.J., & van der Ham, J. (2018a). Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure. *Crime Science*, *7*(1), 16.

Whitehead, P.R., Ward, T. & Collie, R.M. (2007). Time for a change: Applying the good lives model of rehabilitation to a high-risk violent offender. *International journal of offender therapy and comparative criminology, 51*(5), 578-59.

Wible, B. (2003). A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime. *The Yale Law Journal, 112*(6), 1577-1623.

Wormith, J. S., Althouse, R., Simpson, M., Reitzel, L. R., Fagan, T. J., & Morgan, R. D. (2007). The rehabilitation and reintegration of offenders: The current landscape and some future directions for correctional psychology. *Criminal Justice and Behavior*, *34*(7), 879–892.

Zebel, S., de Vries, P. W., Giebels, E., Kuttschreuter, M., Stol, W., Karemaker, M., & Ufkes, E. G. (2015). Een screenshot van jeugdige daders van cybercrime in Nederland. *Jeugdcriminologie: Achtergronden van jeugdcriminaliteit*, 355-372.

Bijlage 1

Bijlage 1.1: Interviewprotocol interventieontwikkelaars

Te bespreken fases: 1 (Beschrijving van Hack_Right) en 2 (Plan evaluatie)

Algemeen:
- Wat is uw naam en leeftijd?
- *Noteer: geslacht*
- Bij welke organisatie bent u werkzaam? (eventueel: vanuit welke organisatie bent u betrokken bij Hack_Right?)
- Wat is, in uw organisatie, uw functie en met welke werkzaamheden houdt u zich bezig?
- Op welke wijze bent u betrokken bij Hack_Right?

Hack_Right:

Fase 1
- Wat is Hack_Right?
- Wat zijn de doelen van Hack_Right?
- Hoe en waarom is Hack_Right ontstaan?
- Welke partijen zijn betrokken (geweest) bij het opzetten van Hack_Right?

Fase 2
- Doelgroep
  - Wat is de doelgroep van Hack_Right?
  - Is dit schriftelijk vastgelegd?
- Selectie deelnemers
  - Hoe komt de selectie van deelnemers tot stand?
  - Is dit schriftelijk vastgelegd?
- Onderbouwing van Hack_Right
  - Waarom verwachten jullie dat Hack_Right werkt, dat Hack_Right zijn doelen bereikt?
  - Is Hack_Right gefundeerd op bestaande theorieën?
  - Hoe is de keuze van criminogene factoren voor Hack_Right tot stand gekomen?
  - *[noem kort de vier modules]*

- Hoe is de keuze van criminogene factoren onderbouwd voor
  - module 1: herstel
  - module 2: training
  - module 3: coaching
  - module 4: alternatief
- Hoe zijn de gekozen criminogene factoren vertaald naar
  - module 1: herstel
  - module 2: training
  - module 3: coaching
  - module 4: alternatief

– Toewijzing modules
- Hoe komt de toewijzing van modules tot stand?
- Is dit schriftelijk vastgelegd?

– Ketenpartners
- Welke ketenpartners zijn betrokken bij Hack_Right?
- Welke ketenpartners zijn betrokken bij
  - module 1
  - module 2
  - module 3
  - module 4
- Welke afspraken zijn gemaakt met ketenpartners?
  - Zijn er afspraken over de rol van de ketenpartners?
  - Zijn er afspraken over de invulling van de modules?
    - In hoeverre is er ruimte voor ketenpartners om de modules/opdrachten aan te passen tijdens het traject?
  - Zijn er afspraken over terugkoppeling tijdens/na de uitvoering van een case?
  - Hoe wordt nagegaan of ze zich ook houden aan afspraken?
  - Zijn al deze afspraken schriftelijk vastgelegd?
- Hoe los of vast is de samenwerking?
  - Is dit schriftelijk vastgelegd?
- Wat is de duur van de samenwerking?
  - Is dit schriftelijk vastgelegd?
- Hoeveel Hack_Right deelnemers worden ondergebracht bij de ketenpartners?
  - Is dit schriftelijk vastgelegd?

– Wilt u verder nog iets toevoegen?

Bijlage 1.2: Interviewprotocol toewijzers

Te bespreken fases: 1 (beschrijving van Hack_Right) en 3 (implementatie/proces evaluatie)

Algemeen:
- Wat is uw naam en leeftijd?
- *Noteer: geslacht*
- Bij welke organisatie bent u werkzaam? (eventueel: vanuit welke organisatie bent u betrokken bij Hack_Right ?)
- Wat is, in uw organisatie, uw functie en met welke werkzaamheden houdt u zich bezig?
- Op welke wijze bent u betrokken bij Hack_Right?
  - Voor start uitvoering Hack_Right
  - Tijdens en na uitvoering Hack_Right

Hack_Right:
Fase 1
- Wat is Hack_Right?
- Wat zijn de doelen van Hack_Right?
- Bij hoeveel Hack_Right casussen bent u betrokken geweest?
- Kunt u deze casussen kort beschrijven?
  - Indien >drie casussen; kunt u de twee meest recente casussen beschrijven?
    - Indien beide succesverhaal; kunt u ook een niet-succesverhaal beschrijven?

Fase 3
Bereik
Deel 1: wie doet er mee aan Hack_Right?
- Selectie
  - Hoe komt de selectie van deelnemers tot stand?
    - Wat zijn de selectiecriteria voor deelname?
  - Is dit schriftelijk vastgelegd?
  - Hoe is de bereidheid van deelnemers tot deelname aan Hack_Right?
  - Wat gebeurt er met deelnemers die niet willen deelnemen aan Hack_Right?
  - Is er uitval in het proces van case-screening/acceptie deelnemer? (zo ja, waar in het proces vindt uitval plaats en waarom?)
    - Door casescreener (zo ja, waar in het proces vindt uitval plaats en waarom?)
    - Door deelnemer (zo ja, waar in het proces vindt uitval plaats en waarom?)
    - Andere oorzaak (zo ja, waar in het proces vindt uitval plaats en waarom?)

Deel 2: welke modules worden doorlopen door deelnemers Hack_Right?
- Bent u bekend met de vier modules van Hack_Right?
  - Zo ja, wordt Hack_Right ook in de vorm van deze modules opgelegd?
  - Zo nee, op welke manieren kan Hack_Right worden ingevuld?

– Hoe komt de toewijzing van modules/invulling van Hack_Right tot stand?
  - Is dit proces schriftelijk vastgelegd?
  - Wat is de rol van de casescreener/toewijzer binnen Hack_Right?
  - Wat is de rol van de strafoplegger (OM, Politie, rechter enzovoort)?
  - Wat is de rol van de uitvoerders van de modules/Hack_Right?
  - Zijn deze rollen schriftelijk vastgelegd?
  - Hoe spelen individuele factoren een rol bij de keuze en toewijzing van de modules/invulling van Hack_Right? (risicofactoren en behoeften die samenhangen met delinquente gedrag, leervermogen)?
  - Wordt er vooraf gelet op de match/klik tussen deelnemers en module uitvoerder (persoon, niet bedrijf)?
– Komt het voor tijdens de toewijzing van modules/onderdelen aan personen dat
  - gekozen modules / onderdelen (door casescreener/OM/Politie) afwijken van uiteindelijk opgelegde modules/onderdelen?
  - opgelegde modules/onderdelen naderhand nog worden gewijzigd?

Integriteit: Uitvoering modules in de praktijk
Deel 1: uitvoering per module
– Welke doelen worden nagestreefd?
– Welke (keten)partners zijn betrokken bij de module?
  - Is dit schriftelijk vastgelegd?
– Hoeveel Hack_Right deelnemers zijn er tot nu toe ondergebracht bij de (keten) partners van de module?
  - Is er een maximaal aantal deelnemers dat per ketenpartner wordt ondergebracht?
  - Is dit schriftelijk vastgelegd?
– Samenwerking (keten)partners
  - Hoe ziet de samenwerking eruit?
  - Hoe verloopt de samenwerking met de (keten)partners? (goed, moeizaam)
  - Worden afspraken nagekomen?
– Heeft/hebben de uitvoerder(s) van de module ruimte bij het invullen van de module? Ofwel, heeft/hebben de uitvoerder (s) vrijheid tot het aanpassen van modules in individuele gevallen?
– Hoe ziet de invulling van de module eruit?
– Worden de volgende onderdelen doorlopen? En zo ja, hoe zien de onderdelen er precies uit?:
[let op: alleen huidige module kiezen!]

Module 1

– dader-slachtoffergesprek,
– herstel gesprek,
– herstel plan,
– herstel conferentie

Module 2

– training juridische grenzen en ethisch hacken,
– training sociale vaardigheden

Module 3	*Module 4*
– koppeling coach, – begeleidend kader voor coaches	– workshops, – challenges, – presentaties door bedrijfsleven, – demo's door hackerspaces

– Zijn alle jongeren geschikt voor deelname aan de module?
– Hoe is de bereidheid van deelnemers tot deelname aan de module?
– Hoe verloopt tot nu toe de uitvoering van de module?
– Worden de beoogde doelen bereikt? Waarom wel/niet?
– Welke factoren zorgen ervoor dat de uitvoering van de module goed verloopt?
– Welke factoren zorgen ervoor dat de uitvoering van de module minder goed verloopt?

Deel 2: Alle modules
– Contact tijdens uitvoering, tussen uitvoerder module en casescreener/toewijzer Hack_Right:
  • Welke informatie ontvangen jullie over het verloop van de uitvoering van de module?
  • Is bij jullie bekend wat de frequentie van contact is tussen deelnemer en uitvoerder van module?
  • Op welke/hoeveel momenten vernemen jullie of de deelname goed verloopt?
    ▪ In het geval van een niet goed lopende deelname, op welke manier en wanneer bereikt dit nieuws jullie?
  • Wat gebeurt er vervolgens?
– Wordt er tijdens doorloop module gelet op de match/klik tussen deelnemers en module uitvoerder (persoon, niet bedrijf)? Zo ja, heeft dit invloed op doorloop van module?
– Is jullie bekend of beoogde doelen zijn bereikt na voltooiing Hack_Right, in individuele gevallen?
– Uitval
  • Is er uitval in het proces van voltooiing van modules? (zo ja, waar in het proces vindt uitval plaats en waarom?)
  • Is er uitval in het proces van voltooiing van modules:
    ▪ Door deelnemer (zo ja, waar in het proces vindt uitval plaats en waarom?)
    ▪ Door ketenpartner van gekozen module (Halt, IT bedrijf enzovoort) (zo ja, waar in het proces vindt uitval plaats en waarom?)
    ▪ Door casescreener (zo ja, waar in het proces vindt uitval plaats en waarom?)
    ▪ Andere oorzaak (zo ja, waar in het proces vindt uitval plaats en waarom?)
– Duur proces van start Hack_Right en toewijzing modules
  • Hoeveel tijd zit er tussen arrestatie en oplegging Hack_Right?
  • Hoeveel tijd zit er tussen oplegging Hack_Right en start van module?

- Duur interventie
  - Wat is de beoogde duur van de interventie/voltooiing van module(s)?
    - Module 1
    - Module 2
    - Module 3
    - Module 4
  - Wat is de werkelijke duur van de interventie/voltooiing van module(s)?
  - Hoe tevreden bent u met deze duur: is dit te kort, precies goed, te lang?
  - Hoe tevreden zijn deelnemers met deze duur: is dit te kort, precies goed, te lang?
  - Hoe tevreden zijn ketenpartners met deze duur: is dit te kort, precies goed, te lang?
- Wilt u verder nog iets toevoegen?

Bijlage 1.3: Interviewprotocol uitvoerders

Algemeen/introductie:

- Wat is uw naam en leeftijd?
- *Noteer: geslacht*
- Bij welke organisatie bent u werkzaam?
- Wat is uw functie en met welke werkzaamheden houdt u zich bezig?
- Op welke wijze bent u betrokken bij Hack_Right?
  - Vóór de tenuitvoerlegging van de straf/start module
  - Tijdens en na straf/module
- Wat is volgens u Hack_Right?
- Wat zijn volgens u de doelen van Hack_Right?
- Bij welke Hack_Right module(s) bent u betrokken, en kunt u deze module(s) kort beschrijven?
- Bij hoeveel Hack_Right casussen bent u betrokken geweest? (afgerond of nog bezig)
- Kunt u kort beschrijven wat uw ervaringen in deze casus(sen) zijn?

Indien de respondent bij meerdere casussen betrokken is geweest, zullen de volgende vragen zo veel mogelijk samengevoegd worden gesteld; waar nodig worden de vragen per individuele jongere gesteld.

Beschrijving casus:

- Wat waren achtergrondkenmerken van de jongere die u heeft begeleid?
  - Sekse, leeftijd, studie/werk, woonsituatie (bij ouders/op kamers/zelfstandig/met partner/begeleid wonen), relatie met ouders/vrienden, psychiatrische problematiek zoals autisme
- Welk delict had de jongere gepleegd?
- Wat waren zijn/haar motieven?
- Wat was de omvang van de opgelegde Halt-straf/taakstraf?
- Had de jongere daarnaast nog andere straffen of maatregelen opgelegd gekregen?
- Heeft u een rol gehad bij de keuze voor een bepaalde straf/module voor de jongere?
- In hoeverre was de jongere bereid tot deelname aan/gemotiveerd voor uw Hack_Right module?

Beschrijving module(s)/opdracht(en):

- Hoe is de Hack_Right interventie voor deze jongere ingevuld?
  - Omvang
    - Zit er verschil tussen de beoogde duur en werkelijke duur?
    - Hoe tevreden bent u met deze duur: is dit te kort, precies goed, te lang?
    - Hoe tevreden zijn deelnemers met deze duur: is dit te kort, precies goed, te lang?

- Welke module(s) en opdracht(en)? (eventueel modules/opdrachten bij andere organisaties)
- Hoe is de selectie van modules/opdrachten tot stand gekomen?
- Wat is uw rol geweest bij de invulling van de modules/opdrachten bij de jongere? Heeft u ruimte gehad om de module/opdrachten aan te passen?
- Door wie begeleid
- Ouders en/of andere belangrijke personen betrokken

– Welke Hack_Right specifieke modules en opdracht(en) heeft de jongere uitgevoerd?

Module 1 (herstel)

– dader-slachtoffergesprek,
– herstel gesprek,
– herstel plan,
– herstel conferentie

Module 2 (training)

– training juridische grenzen en ethisch hacken,
– training sociale vaardigheden

Module 3 (coaching)

– koppeling coach,
– begeleidend kader voor coaches

Module 4 (alternatief)

– workshops/challenges
– presentaties door bedrijfsleven,
– demo's door hackerspaces

- Omschrijving module(s) en opdracht(en)
- Doel module(s) en opdracht(en)
- Benodigde hulpmiddelen (vragenlijsten, protocollen, cursussen, websites)
- Opgeleverd(e) eindproduct(en)
- Aanvangs- en einddatum
- Omvang (aantal uur)
- Ouders en/of andere belangrijke personen betrokken

– In hoeverre sloten de opdrachten aan bij het niveau/leervermogen, risicofactoren en behoeften van de jongere? Hoe kan deze aansluiting waar nodig verbeterd worden?
– Loopt het Hack_Right traject nog, heeft de deelnemer het traject inmiddels afgerond of is de deelnemer uitgevallen?
  - In geval van uitval: waarom en waar in het proces en door wie vond uitval plaats?)
    - Door deelnemer
    - Door u, als uitvoerder van module (Halt, IT-bedrijf enzovoort)
    - Door Hack_Right medewerker
    - Andere oorzaak
– Wat vond de deelnemer van de module/opdrachten?
– Hoe en door wie is de opdracht beoordeeld? Welke criteria zijn hierbij gehanteerd?
– In hoeverre hield de jongere zich aan de gemaakte afspraken, zoals rondom werktijden, resultaten en wijzigingen aanbrengen in systemen?
– Zijn er extra maatregelen nodig om naleving van deze afspraken te borgen?

Contact tussen deelnemer en uitvoerder:

- Was er een vaste contactpersoon vanuit de organisatie voor de Hack_Right deelnemer?
- Wat was de frequentie van contact tussen de Hack_Right deelnemer en de begeleider?
- In hoeverre was er sprake van een match/klik tussen u en de jongere?
  - vooraf (Zzo ja, heeft dit invloed op start van module?)
  - tijdens doorloop module (zo ja, heeft dit invloed op doorloop van module?)
- In hoeverre was er sprake van een match/klik tussen de deelnemer en het ICT-bedrijf?
- Hoe heeft u het contact met de deelnemer ervaren?
- Heeft het contact met de deelnemer invloed gehad op het verloop van de module? Oftewel, was de module voor de deelnemer mogelijk anders verlopen als iemand anders de begeleiding op zich had genomen?
- In hoeverre voelde u uzelf voldoende toegerust om de jongere te begeleiden?
- Over welke kennis dient een begeleider van Hack_Right jongeren volgens u te beschikken? Welke minimale kennis van ICT, relevante wet- en regelgeving, … is nodig?
- Wat zijn volgens u essentiële vaardigheden waarover een begeleider van Hack_Right jongeren dient te beschikken? (bijvoorbeeld: actief luisteren, vragen stellen, confronteren, gemotiveerd om jonge cyberdaders te begeleiden, een duidelijke anti-criminele attitude, bewustzijn van de voorbeeldfunctie die hij vervult, …)

Ervaringen uitvoerder/evaluatie:

- Hoe tevreden bent u met het verloop van de module(s)/opdracht(en) voor de jongere:
  - Wat zijn bevorderende factoren voor de uitvoering van uw module(s)/opdracht(en)?
  - Wat zijn belemmerende factoren voor de uitvoering van uw module(s)/opdracht(en)?
- Zijn de beoogde doelen bereikt bij de jongere na voltooiing van uw module(s)/opdracht(en)?
  - Waarom wel/waarom niet
- Hebben de module(s)/opdracht(en) een positieve en/of negatieve invloed gehad op de volgende factoren voor de deelnemer:
  - School
  - Werk
  - Thuis
  - Recidive
  - IT-talent
  - Overig
- Wat denkt u dat de jongere heeft geleerd van de module(s)/opdracht(en)?
  - Kennis (over online grenzen, mogelijke schade, …)

  - Vaardigheden
  - Gedrag/houding
- Hebben de module(s)/opdracht(en) onbedoelde bijeffecten gehad, voor deelnemers of daarbuiten?
- In hoeverre schat u in dat deze jongere geschikt is voor het werkveld, en zo ja, in welke functie?

Samenwerking projectgroep Hack_Right en (keten)partners:
- Contact tijdens uitvoering, tussen uitvoerder module en projectgroep Hack_Right:
  - Hoe ziet de samenwerking eruit en hoe verloopt deze?
  - Welke informatie ontvangen jullie vooraf over de deelnemer?
  - Welke informatie geven jullie door aan projectgroep Hack_Right over het verloop van de uitvoering van de module?
  - Wat is de frequentie van contact tussen jouw organisatie en projectgroep Hack_Right?
  - Informeren jullie projectgroep Hack_Right over het verloop van de deelname?
  - In het geval van een niet goed lopende deelname, op welke manier en wanneer nemen jullie hierover contact op met projectgroep Hack_Right?
- Zijn er nog overige afspraken gemaakt met de projectgroep Hack_Right en worden afspraken nagekomen?
  - Zijn er nog andere (keten)partners betrokken bij uw module? Zo ja:
  - Hoe ziet de samenwerking eruit en verloopt deze goed?
  - Welke afspraken zijn er gemaakt met (keten)partners?
  - Worden afspraken nagekomen?

Verbeterpunten Hack_Right/input handleiding
- Wat is uw oordeel over uw module(s)/opdracht(en) en welk rapportcijfer zou u hieraan verbinden?
- Wat is uw algemene oordeel over Hack_Right en welk rapportcijfer zou u hieraan verbinden?
- Heeft u verbetersuggesties voor Hack_Right, module(s) en opdrachten?
- Heeft u suggesties voor opdrachten die geschikt zouden zijn voor Hack_Right jongeren?
- Waar moeten we op letten bij het formuleren van opdrachten? (taalgebruik, …)
- Welke onderdelen zouden er in de handleiding van Hack_Right moeten staan om deze zo helder en bruikbaar mogelijk te maken voor uw organisatie?
  - Halt: vormgeving in leeropdrachten; afstemming met andere vaste onderdelen Halt-afdoening, zoals gesprek met ouders en excuses aanbieden
  - (Jeugd)Reclassering: …
  - ICT-bedrijf: …

Bijlage 1.4: Interviewprotocol deelnemers

Achtergrond
- Leeftijd, geslacht, studie/werk
- Gezinssamenstelling, school, vrienden, hobby's
- Zelfperceptie, hoe anderen je zien

Pathways
- Wanneer en hoe ontwikkelde je interesse in computers en technologie?
  - Waarom/waardoor had je toen je jonger was interesse in computers/technologie? (leeftijd, tijd per dag)
  - Waardoor/door wie bleef die interesse bestaan? (zowel online/offline)
  - Wat heb je gedaan om jezelf verder te ontwikkelen op het gebied van computers/technologie?
  - Hoe/waar heb je dat geleerd? (zowel online/offline)
  - Van welk niveau zijn jouw computervaardigheden? Kun je programmeren? Welke programmeertalen? Vertel me over je beste prestatie.

- Wanneer en hoe ontwikkelde je interesse in [activiteit x]?
  - Wat trok je als jongere aan tot [activiteit x]? (leeftijd, tijd per dag)
  - Kun je me vertellen over de eerste keer dat je zelf [activiteit x] hebt uitgevoerd? Hoe wist je wat te doen? Hoe voelde je je?
  - Waardoor/door wie bleef die interesse bestaan? (zowel online/offline)
  - Wat heb je gedaan om jezelf verder te ontwikkelen op het gebied van [activiteit x]?
  - Hoe/waar heb je dat geleerd? (zowel online/offline)
  - Welk niveau hebben jouw computervaardigheden met betrekking tot [activiteit x]? Vertel me over je beste prestatie.
  - Heb je je ooit zorgen gemaakt over het aangetrokken worden tot [activiteit x]? Angst voor politie/justitie?

Over [activiteit x]
- Beschrijf de werkwijze, alle stappen die je moet nemen, selectie van doelwit en benodigde skills.
- Wat was je persoonlijke motivatie?
- Beschrijf jouw rol in het crime script. Rol/taak/taakverdeling.
- Beschrijf hoe vaak je alleen werkte versus samenwerkte met anderen.
- Beschrijf een gemiddelde dag waarin je [activiteit x] uitvoerde.

Samenwerking/samenplegen
- Alleen/met anderen/netwerk?
- Indien relevant: beschrijf het netwerk (omvang, rollen, interactie, communicatie, contacten met nieuwe mensen).

– Hoe ontmoette je mensen met dezelfde interesses in [activiteit x]?
– Hoe kom je aan de kennis/skills om dit te doen? Hoe weet je welke tools goed zijn? (rol peers/forums). Hoe veel tijd breng je door op forums (en wat doe je daar dan)?

Community
– Is er een community rondom [activiteit x]? Hoe kwam je daar achter? Hoe ben je daar geïntroduceerd?
– Maak jij onderdeel uit van die gemeenschap? Wat is je status?
– Heb je vrienden binnen die gemeenschap? (beschrijf online en offline interacties)

Ethiek
– Zie jij jezelf als een pleger van [activiteit x]? Zie jij jouw vrienden als pleger van [activiteit x]?
– Wat is jouw definitie/beschrijving van een pleger van [activiteit x]?
– Waarom denk je dat jongeren zich aangetrokken voelen tot [activiteit x]? Wat zijn hun motieven?
– Is [activiteit x] slecht? Geldt dat ook voor andere activiteiten? Hoe kijk je aan tegen bedrijven of personen die hun systemen niet goed beveiligen? Hoe kijk je aan tegen eventuele slachtoffers?
– Weet iemand binnen je directe kring van familie en vrienden van [activiteit x]?
– Wist je voor je [activiteit x] uitvoerde dat dit strafbaar is?

Stoppen/over deze interventie
– Hoe kijk je aan tegen je aanhouding? (jammer, einde periode, opluchting enzovoort)
– Over het hack_right programma
  • Datum begin en eind programma.
  • Zijn je ouders/verzorgers op de hoogte van je deelname? Hoe reageerden ze? (meelevend, verrast, boos enzovoort).
  • Gevolgde module(s). Geef een korte beschrijving van wat je hebt gedaan tijdens de module. Helemaal afgerond? [doorvragen bij herstel, confrontatie slachtoffer? Bij training: wat heb je geleerd?]
  • Wat denk je dat het doel is van Hack_Right? En wat denk je dat het doel is van de gevolgde module(s)? Waren de doelen duidelijk bij het begin van het traject? Was het makkelijk of moeilijk om de modules te voltooien?
  • Denk je dat het programma werkt/zin heeft? Waarom? Wat heb je geleerd? Zijn die skills dagelijks bruikbaar?
  • Persoonlijke ervaring. Voelde je je begrepen en gehoord? Ben je tevreden over hoe de politie/Halt/bedrijf de interventie heeft uitgevoerd (kwaliteit behandeling)? (schaal van 1-10) Heb je het gevoel dat je jouw kant van het verhaal kon vertellen? Heb/had je vertrouwen in de organisaties die betrokken waren? Hoe ging iedereen met je om?

- Vond je het leuk/interessant om de module(s) te volgen? (helemaal niet– heel erg). Heb je tips over hoe de module beter kan worden gemaakt?
- Wat vond je van de duur van de module(s)/trainingen? ◊ intensiviteit (dosering)
- Heb je het programma als een straf ervaren? Heb je het ervaren als iets dat invloed heeft gehad op je leven?
- Hoe wat het contact met behandelaars? Met welke mensen heb je contact gehad tijdens de interventie? (afhankelijk van gevolgede modules: onder andere reclasseringsmedewerker, ethisch hacker, mensen van de politie, toezichthouders)
- [één persoon kiezen die 'de voornaamste behandelaar' (persoon X) kan worden genoemd] Vervolgens per persoon doorvragen: Hoe vaak heb je contact gehad met persoon X? Hoe heb je het contact met persoon X ervaren? Klikte het tussen jou en persoon X? Heb je het idee dat deze persoon moeite voor je doet en het beste met je voor heeft? Heeft persoon X invloed gehad op jouw ervaringen met hackright/de module? Was je module anders verlopen als je een andere behandelaar had gehad?

– Ben je op dit moment gestopt met [activiteit x]? Zo niet, hoeveel tijd besteed je aan deze activiteit vergeleken met de tijd voor de interventie?
– In het algemeen: hoe kunnen we voorkomen dat jongeren [activiteit x] gaan plegen?

Bijlage 1.5: Informed consent

INFORMATIE
over het interview en de onderzoeken:
'Evaluatie Hack_Right' & 'The Offline side of Cybercrime: Mapping involvement mechanisms'

Achtergrond

Dit interview zal gebruikt worden voor twee wetenschappelijke onderzoeken. Onderzoek 1 is de evaluatie van het programma Hack_Right. Het doel van dat onderzoek is om meer inzicht te krijgen in hoe effectief het Hack_Right programma is. Hack_Right is opgezet om recidive te voorkomen en om jongeren te leren hun cybertalent verder te ontwikkelen binnen de kaders van de wet. Onderzoek 2 is een onderzoek getiteld 'The offline side of cybercrime'. In dat onderzoek bestuderen we wat de rol van online en offline sociale contacten en ontmoetingsplaatsen zijn bij de ontwikkeling van je ICT-skills.

Door jouw deelname aan dit onderzoek leren we welke elementen van het Hack_Right programma wel en niet werken, hoe het programma verbeterd kan worden en hoe we kunnen voorkomen dat jongeren strafbare delicten plegen.

Interview

Een interview duurt ongeveer een uur tot anderhalf uur en zal plaatsvinden op een nader te bepalen plaats. In overleg wordt vastgesteld op welk tijdstip en plaats het interview wordt gehouden.

Privacy

De informatie die je in het interview geeft, wordt alleen voor de hier beschreven wetenschappelijke onderzoeken gebruikt. Je gegevens worden anoniem verwerkt. Dit betekent dat je niet met naam en toenaam in het onderzoeksrapport wordt genoemd: je blijft volledig onbekend. Ook zal de informatie die je men ons deelt over uw zaak niet rechtstreeks naar jou herleidbaar zijn.

De onderzoekers

Rutger Leukfeldt – NSCR en De Haagse Hogeschool
Susanne van 't Hoff-de Goede – De Haagse Hogeschool

INFORMATIE
over het interview en de onderzoeken:
'Evaluatie Hack_Right' & 'The Offline side of Cybercrime: Mapping involvement mechanisms'

– Ik ben over het interview en de onderzoeken geïnformeerd;

– Ik heb de schriftelijke informatie gelezen;

– Ik ben in de gelegenheid gesteld om vragen over het interview en het onderzoek te stellen;

– Ik heb over mijn deelname aan het interview en het onderzoek kunnen nadenken;

– Ik heb het recht om mijn toestemming op ieder moment weer in te trekken, zonder dat ik daarvoor een reden hoef op te geven.

Ik stem toe met deelname aan het onderzoek.

Naam:
Geboortedatum:
Handtekening:
Indien minderjarige naam en handtekening ouder/voogd:

Ondergetekende verklaart dat de hierboven genoemde persoon zowel schriftelijk als mondeling over het onderzoek is geïnformeerd. Hij/zij verklaart tevens dat een voortijdige beëindiging van de deelname door bovengenoemde persoon, van geen enkele invloed zal zijn op de begeleiding binnen de reclassering.
Naam:
Functie:
Paraaf
Datum:

Bijlage 2

Cybercrime in enge zin (computercriminaliteit) volgens de 'Uitwerking veiligheidsagenda 2019-2022' (Ministerie van Justitie en Veiligheid, 2018).

- Art. 138ab Sr: Computervredebreuk.
- Art. 138b Sr: Opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmeren door daaraan gegevens aan te bieden of toe te zenden.
- Art. 139c Sr: Met technisch hulpmiddel gegevens afluisteren.
- Art. 139d Sr: Plaatsen opname of aftapapparatuur.
- Art. 139e Sr: Hebben en gebruiken van door wederrechtelijk afluisteren, aftappen c.q. opnemen verkregen gegevens.
- Art. 161sexies Sr: Opzettelijke vernieling geautomatiseerd werk of werk voor telecommunicatie.
- Art. 161septies Sr: Culpose vernieling van enig geautomatiseerd werk of werk voor telecommunicatie.
- Art. 350a Sr: Aantasting/manipulatie computergegevens (het doleuze misdrijf).
- Art. 350b Sr: Aantasting/manipulatie computergegevens (het culpose misdrijf).
- Art. 350c Sr: Aantasting/manipulatie geautomatiseerd werk (het doleuze misdrijf).
- Art. 350d Sr: Faciliteren van artikel 350a of artikel 350c.
- Art. 317 Sr lid 2: Afpersing middels bedreiging gegevens middels een geautomatiseerd werk op te slaan, onbruikbaar of ontoegankelijk te maken.
- Art. 138C Sr: (nieuw artikel, in combinatie met ingangsdatum Wet CCIII).
- Art. 139G Sr: (aangepast artikel, in combinatie met ingangsdatum Wet CCIII).

Leden Redactieraad Programma Politie & Wetenschap

Uitgaven in de reeks Politiewetenschap

1. ***Kerntaken van de politie. Een inventarisatie van heersende opvattingen***
   C.D. van der Vijver, A.J. Meershoek & D.F. Slobbe, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2001
2. ***Bevoegdheden overd(r)acht. Een onderzoek naar delegatie en mandaat van beheersbevoegdheden in de politiepraktijk***
   H.B. Winter & N. Struiksma, Pro Facto B.V., Universiteit Groningen, 2002
3. ***Sturing van politie en politiewerk. Een verkennend onderzoek tegen de achtergrond van een veranderende sturingscontext en sturingsstijl***
   J. Terpstra, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2002
4. ***Woninginbrekers en zware jongens. Daders vanuit het voormalig Joegoslavië aan het woord***
   M. van San, E. Snel & R. Boers, Risbo, Erasmus Universiteit Rotterdam, 2002
5. ***Zeg me wie je vrienden zijn. Allochtone jongeren en criminaliteit***
   F.M.H.M. Driessen, B.G.M. Völker, H.M. Op den Kamp, A.M.C. Roest & R.J.M. Molenaar, Bureau Driessen, Utrecht, 2002
6. ***Op deugdelijke grondslag. Een explorerende studie naar private forensische accountancy***
   J. van Wijk, W. Huisman, T. Feuth & H.G. van de Bunt, Vrije Universiteit, Amsterdam, 2002
7. ***Voorbij de dogmatiek. Publiek-private samenwerking in de veiligheidszorg***
   A.B. Hoogenboom & E.R. Muller, COT, Den Haag, 2003
8. ***Hennepteelt in Nederland. Het probleem van de criminaliteit en haar bestrijding***
   F. Bovenkerk, W.I.M. Hogewind, D. Korf & N. Milani, Willem Pompe Instituut, Universiteit Utrecht, 2003
9. ***Politiekennis in ontwikkeling. Een onderzoek naar het verzamelen en veredelen van informatie voor het Politie Kennis Net***
   I. Bakker & C.D. van der Vijver, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2003

10a. Politie en geweld. Een verkenning van politiereacties op geweldsincidenten in vier Nederlandse regiokorpsen

C.J.E. In 't Velt, W.Ph. Stol, P.P.H.M. Klerks, H.K.B. Fobler, R.J. van Treeck & M. de Vries, NPA-Politie Onderwijs- en Kenniscentrum, LSOP, Apeldoorn, 2003

10b. Geweldige informatie? Onderzoek naar de informatiehuishouding van geweldsmeldingen bij de politie

R. van Overbeeke, O. Nauta, A. Beerepoot, S. Flight & M. Rietveld, DSP-groep, Amsterdam, 2003

11. Blauwe Bazen. Het leiderschap van korpschefs

R.A. Boin, P. 't Hart & E.J. van der Torre, Departement Bestuurskunde, Universiteit Leiden/COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2003

12. Over de grens. Een verkenning van projecten voor probleemjeugd in Duitsland, Engeland en Zweden

I. van Leiden, G. Verhagen & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2003

13. Integriteit in het dagelijkse politiewerk. Meningen en ervaringen van politiemensen

J. Naeyé, L.W.J.C Huberts, C. van Zweden, V. Busato & B. Berger, Centrum voor Politiewetenschappen, VU Amsterdam, 2004

14. Politiestraatwerk in Nederland. Noodhulp en gebiedswerk: inhoud, samenhang, verandering en sturing

W. Ph. Stol, A.Ph. van Wijk, G. Vogel, B. Foederer & L. van Heel, Nederlandse Politieacademie, Onderzoeksgroep, LSOP, Apeldoorn, 2004

15. De kern van de taak. Kerncompetenties van de politie als criterium voor de afbakening van kerntaken in de praktijk

A. Mein, A. Schutte & A. van Sluis, ES&E, Den Haag, 2004

16. Professionele dienstverlening en georganiseerde criminaliteit. Hedendaagse integriteitsdilemma's van advocaten en notarissen

F. Lankhorst & J.M. Nelen, Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid, Sectie Criminologie, Amsterdam, 2004

17. Paradoxaal Politiebestel. Burgemeesters, Openbaar Ministerie en Politiechefs over de sturing van de politie

L.W.J.C. Huberts, S. Verberk, K. Lasthuizen & J.H.J. van den Heuvel, Vrije Universiteit Amsterdam/B&A Groep, 's-Gravenhage, 2004

18. Illegale vuurwapens in Nederland: smokkel en handel

A.C. Spapens & M.Y. Bruinsma, IVA, Tilburg, 2004

19. Samenwerking en netwerken in de lokale veiligheidszorg

J. Terpstra & R. Kouwenhoven, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2004

20. Uit balans: politie en bestel in de knel. State-of-the-art: bundeling van kennis en inzicht

H.G. van de Bunt, A.B. Hoogenboom, LW.J.C. Huberts, E.R Muller, J. Terpstra, C.D. van der Vijver & C. Wiebrens, 2004 Redactie: G.C.K. Vlek, C. Bangma, C. Loef & E.R. Muller

21. Politie en media. Feiten, fictie en imagopolitiek

H. Beunders & E.R. Muller, Erasmus Universiteit Rotterdam/COT, Instituut voor Veiligheids- en Crisismanagement, Leiden, 2005 (2e druk 2009)

22. Integriteit van de politie. State-of-the-art: wat we weten op basis van Nederlands onderzoek

L.W.J.C. Huberts & J. Naeyé, Centrum voor Politie- en Veiligheidswetenschappen/ Vrije Universiteit, Amsterdam, 2005

23. De sociale organisatie van mensensmokkel

R. Staring, G. Engbersen, H. Moerland, N. de Lange, D. Verburg, E. Vermeulen & A. Weltevrede; m.m.v. E. Heyl, N. Hoek, L. Jacobs, M. Kanis & W. van Vliet, Erasmus Universiteit Rotterdam: Criminologie – Sociologie – Risbo, 2005

24. In elkaars verlengde? Publieke en private speurders in Nederland en België

U. Rosenthal, L. Schaap J.C. van Riessen, P. Ponsaers & A.H.S. Verhage, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Universiteit Gent, 2005

25. De strafrechtelijke rechtshulpverlening van Nederland aan de lidstaten van de Europese Unie. De politieke discussie, het juridische kader, de landelijke organisatie en de feitelijke werking

C.J.C.F. Fijnaut, A.C. Spapens & D. van Daele, Universiteit van Tilburg, Vakgroep Strafrechtwetenschappen, 2005

26. Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie

J. Naeyé, Faculteit der Rechtsgeleerdheid, Vrije Universiteit Amsterdam, 2005

27. Preventief fouilleren. Een analyse van het proces en de externe effecten in tien gemeenten

E.J. van der Torre & H.B. Ferwerda, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Advies- en Onderzoeksgroep Beke, Arnhem, 2005

28. Zedenmisdrijven in Nederland. Aangiften- en verdachtenanalyses op basis van HKS-gegevens

A.Ph. van Wijk, S.R.F. Mali, R.A.R. Bullens, L. Prins & P.P.H.M. Klerks, Politieacademie Onderzoeksgroep, Apeldoorn, Vrije Universiteit Amsterdam. KLPD, 2005

29. Groepszedenmisdrijven onder minderjarigen. Een analyse van een Rotterdamse casus

I. van Leiden & J. Jakobs, Advies- en Onderzoeksgroep Beke, Arnhem, 2005

30. Omgaan met conflictsituaties: op zoek naar goede werkwijzen bij de politie

O. Adang, N. Kop, H.B. Ferwerda, J. Heijnemans, W. Olde Nordkamp, P. de Paauw & K. van Woerkom, Onderzoeksgroep Politieacademie, Apeldoorn/ Advies en Onderzoeksgroep Beke, Arnhem, 2006

31. De strategische analyse van harddrugsscenes. Hoofdlijnen voor politie en beleid

E.J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2006

32a. Cijfers en stakeholders. Prestatiesturing en de gevolgen voor de maatschappelijke en politiekbestuurlijke relaties van de politie

A. van Sluis, L. Cachet, L. de Jong, C. Nieuwenhuyzen & A. Ringeling, Centre for Local Democracy, Erasmus Universiteit Rotterdam, 2006

32b. Operationele betrokkenheid. Prestatiesturing en bedrijfsvoering Nederlandse politie

A.B. Hoogenboom, Nivra-Nyenrode, Breukelen, 2006

32c. Op prestaties gericht. Over de gevolgen van prestatiesturing en prestatieconvenanten voor sturing en uitvoering van het politiewerk

M.P.C.M. Jochoms, F. van der Laan, W. Landman, P.S. Nijmeijer & A. Sey, Politieacademie, Apeldoorn/Twynstra Gudde, Amersfoort/Universiteit van Amsterdam, 2006

33. Het nieuwe bedrijfsmatig denken bij de politie. Analyse van een culturele formatie in ontwikkeling

J. Terpstra & W. Trommel, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente, 2006

34. De legitimiteit van de politie onder druk? Beschouwingen over grondslagen en ontwikkelingen van legitimiteit en legitimiteitstoekenning

Bundel onder redactie van C.D. van der Vijver & G.C.K. Vlek, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente/Politie & Wetenschap, 2006

35. Naar beginselen van behoorlijke politiezorg

M.J. Dubelaar, E.R. Muller & C.P.M. Cleiren, Faculteit der Rechtsgeleerdheid, Universteit Leiden, 2006

36a. Asielmigratie en criminaliteit

J. de Boom, G. Engbersen & A. Leerkes, Risbo Contractresearch BV/ Erasmus Universiteit, Rotterdam, 2006

36b. Criminaliteitspatronen en criminele carrières van asielzoekers

M. Althoff & W.J.M. de Haan, m.m.v. S. Miedema, Vakgroep Strafrecht en Criminologie, Faculteit der Rechtsgeleerdheid, Rijksuniversiteit Groningen, 2006

36c. 'Ik probeer alleen maar mijn leven te leven'. Uitgeprocedeerde asielzoekers en criminaliteit

A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam; Amsterdamse School voor Sociaal Wetenschappelijk Onderzoek/Universiteit van Amsterdam, Amsterdam, 2006

37. Positie en expertise van de allochtone politiemedewerker

J. Broekhuizen, J. Raven & F.M.H.M. Driessen, Bureau Driessen, Utrecht, 2007

38. Lokale politiechefs. Het middenkader van de basispolitiezorg

E. J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2007

39. Niet verschenen

40. Conflict op straat: strijden of mijden? Marokkaanse en Antilliaanse jongeren in interactie met de politie

N. Kop, Martin Euwema, m.m.v. H.B. Ferwerda, E. Giebels, W. Olde Nordkamp & P. de Paauw, Politieacademie, Apeldoorn, Universiteit Utrecht, 2007

41. Opsporing onder druk

C. Liedenbaum & M. Kruijsen, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

42. Symbolen van orde en wanorde. Broken windows policing en de bestrijding van overlast en buurtverval

B. van Stokkom, Centrum voor Ethiek, Radboud Universiteit Nijmegen, 2008

43. Verkeershandhaving: prestaties leveren, problemen aanpakken

G. Meershoek & M. Krommendijk, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

44. De frontlinie van opsporing en handhaving. Stelselmatige bedreigingen door burgers als contrastrategie

M.J.G. Jacobs, M.Y. Bruinsma & J.W.M.J. van Poppel, IVA Tilburg, 2008

45a. 'Kracht van meer dan geringe betekenis'. Deel A: Politiegeweld in de basispolitiezorg

R. Bleijendaal, J. Naeyé, P. Chattellon & G. Drenth, Vrije Universiteit, Amsterdam, 2008

45b. 'Kracht van meer dan geringe betekenis'. Deel B: Sturing en toetsing van de politiële geweldsbevoegdheid

G. Drenth, J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45c. Agressie en geweld tegen politiemensen. Beledigen, bedreigen, tegenwerken en vechten

J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45d. Belediging en bedreiging van politiemensen

J. Naeyé, m.m.v. M. Bakker & C. Grijsen, Vrije Universiteit Amsterdam, 2009

45e. Uitgangspunten voor politieoptreden in agressie- en geweldssituaties

J. Naeyé, Vrije Universiteit Amsterdam, 2010

46. Wijkagenten en hun dagelijks werk. Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk

J. Terpstra, 2008

47. Bijzonder zijn ze allemaal! Vergelijkend onderzoek naar reguliere en bijzondere opsporing

W. Faber, A.A.A. van Nunen & C. la Roi, Faber Organisatievernieuwing, Oss, 2009

48. Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak

Y.M.M. Schoenmakers, E. de Vries Robbé & A.Ph. van Wijk, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2009

49. Het betwiste politiebestel. Een vergelijkend onderzoek naar de ontwikkeling van het politiebestel in Nederland, België, Denemarken, Duitsland, Engeland & Wales

A. Cachet, A. van Sluis, Th. Jochoms, A. Sey & A. Ringeling, Erasmus Universiteit Rotterdam/Politieacademie, Apeldoorn/Korps landelijke politiediensten, Driebergen, 2009

50. Leven met bedreiging. Achtergronden bij aangiften van bedreiging van burgers

B. Bieleman, W.J.M. de Haan, J.A. Nijboer & N. Tromp, Intraval & Rijksuniversiteit Groningen, 2010

51a. Het publieke belang bij private preventie. Een economische analyse van inbraakpreventiebeleid

B.A. Vollaard, TILEC/Universiteit van Tilburg, 2009

51b. Het effect van langdurige opsluiting van veelplegers op de maatschappelijke veiligheid

B.A. Vollaard, TILEC/Universiteit van Tilburg, 2010

52. Lokale politiek over politie

T.B.W.M. van der Torre-Eilert, H. Bergsma & M.J. van Duin, met medewerking van R. Eilert, LokaleZaken, Rotterdam, 2010

53a. Trainen onder stress. Effecten op de schietvaardigheid van politieambtenaren

R.R.D. Oudejans, A. Nieuwenhuys & G.P.T. Willemsen, Vrije Universiteit Amsterdam, 2010

53b. Schieten of niet schieten? Effecten van stress op schietbeslissingen van politieambtenaren

A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2012

53c. Politievaardigheden onder stress. Het optimaliseren van aanhouding en zelfverdediging in de praktijk

P.G. Renden, A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

53d. Effectief omgaan met acute stress. Effecten van aanleg en trainingservaring op de schietprestatie onder druk

A. Landman, A. Nieuwenhuys & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

54. Politie en publiek. Een onderzoek naar de communicatievormen tussen burgers en blauw

H.J.G. Beunders, M.D. Abraham, A.G. van Dijk & A.J.E. van Hoek, DSP-groep, Amsterdam/Erasmus Universiteit, Rotterdam, 2011

55. Managing collective violence around public events: an international comparison

O.M.J. Adang with cooperation from: S.E. Bierman, E.B. Brown, J. Dietermann, C. Putz, M. Schreiber, R. van der Wal, J. Zeitner, Police Science & Research Programme, Apeldoorn, 2011

56. Stads- en regioscan in de grootste Brabantse gemeenten. De achtergronden van onveilige GVI-scores

B.M.W.A. Beke, E.J. van der Torre, M.J. van Duin, COT, Den Haag; LokaleZaken, Rotterdam & Beke Advies, Arnhem, 2011

57. De mythe ontrafeld? Wat we weten over een goed politieleiderschap

W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2011

58. Proactief handhaven en gelijk behandelen

J. Svensson, H. Sollie & S. Saharso, Vakgroep Maatschappelijke Risico's en Veiligheid, Institute of Governance Studies, Universiteit Twente, Enschede, 2011

59a. De sterkte van de arm: feiten en mythes

J.H. Haagsma, T.M. Rumke, I. Smits, E. van der Veer & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

59b. Blauw, hier en daar. Onderzoek naar de sterkte van de politie in Nederland, België, Denemarken, Engeland & Wales en Nordrhein-Westfalen

J.H. Haagsma, I. Smits, H. Waarsing & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

60. De nachtdienst 'verlicht'

M.C.M. Gordijn, Rijksuniversiteit Groningen, 2012

61. Opsporing Verzocht. Een quasi-experimentele studie naar de bijdrage van het programma Opsporing Verzocht aan de oplossing van delicten

J.G. van Erp, F. van Gastel & H.D. Webbink, Erasmus Universiteit, Rotterdam, 2012

62. Jeugdige zedendelinquenten en recidive. Een onderzoek bij jeugdige zedendelinquenten naar de voorspellende waarde van psychiatrische stoornissen en psychosociale problemen voor (zeden)recidive

C. Boonmann, L.M.C. Nauta-Jansen, L.A. 't Hart-Kerkhoffs, Th.A.H. Doreleijers & R.R.J.M. Vermeiren, VUmc De Bascule, Duivendrecht, 2012

63. Hoe een angsthaas een jokkebrok herkent

J. Jolij, Rijksuniversiteit Groningen, 2012

64. Politie en sociale media. Van hype naar onderbouwde keuzen

A. Meijer, S. Grimmelikhuijsen, D. Fictorie, M. Thaens, P. Siep, Universiteit Utrecht, Center for Public Innovation, Rotterdam, 2013

65. Wapengebruik. Van inzicht in modus operandi naar een effectieve aanpak

M.S. de Vries, Universiteit Twente, Enschede, 2013

66. Politieverhalen. Een etnografie van een belangrijk aspect van politiecultuuren

M.J. van Hulst, Tilburg University, Tilburg, 2013

67. Recherchebazen. Een empirisch onderzoek naar justitieel politieleiderschap

E.J. van der Torre, M.J. van Duin & E. Bervoets, LokaleZaken, Rotterdam, 2013

68. Driehoeken: overleg en verhoudingen. Van lokaal tot nationaal

E.J. van der Torre & T.B.W.M. van der Torre-Eilert, m.m.v. E. Bervoets & D. Keijzer, LokaleZaken, Rotterdam, 2013

69. Overvallen vanuit daderperspectief. Situationele aspecten van gewelddadige, niet-gewelddadige en afgeblazen overvallen

W. Bernasco, M.R. Lindegaard & S. Jacques, NSCR, Amsterdam, 2013

70. Geweld tegen de politie. De rol van mentale processen van de politieambtenaar

L. van Reemst, T. Fischer & B. Zwirs, Erasmus Universiteit, Rotterdam, 2013

71. Vertrouwen in de politie: trends en verklaringen

L. van der Veer, A. van Sluis, S. Van de Walle & A. Ringeling, Erasmus Universiteit, Rotterdam, 2013

72. Mobiel banditisme. Oost- en Centraal-Europese rondtrekkende criminele groepen in Nederland

D. Siegel, i.s.m. R. Koenraadt, D. Lyubenova, N. Sovre & A. Troscianczuk, Universiteit Utrecht, 2013

73. De ontwikkeling van de criminaliteit van Rotterdamse autochtone en allochtone jongeren van 12 tot 18 jaar. De rol van achterstanden, ouders, normen en vrienden

F.M.H.M. Driessen, F. Duursma & J. Broekhuizen, Bureau Driessen, Utrecht, 2014

74. Speciaal blauw. Verschijningsvormen en overwegingen van specialisatie en despecialisatie binnen de Nederlandse politieorganisatie

R.J. Morée, W. Landman & A.C. Bos, Twynstra Gudde, Amersfoort, 2014

75. Gevangene van het verleden. Crisissituaties na de terugkeer van zedendelinquenten in de samenleving

M.H. Boone, H.G. van de Bunt & D. Spiegel, m.m.v. K. van de Ven, Erasmus Universiteit, Rotterdam, Universiteit Utrecht, 2014

76. Brandstichters onder vuur. Een empirisch onderzoek naar zaken van brandstichting en hun daders

L. Dalhuisen & F. Koenraadt, Universiteit Utrecht, 2014

77. Van stadswacht naar nieuwe gemeentepolitie? Gemeentelijk toezicht en handhaving in de openbare ruimte

T. Eikenaar & B. van Stokkom, Radboud Universiteit, Nijmegen, 2014

78. Politiemensen over het strafrecht

J. Kort, M.I. Fedorova & J.B. Terpstra, Radboud Universiteit, Nijmegen, 2014

79. Kijken, luisteren, lezen. De invloed van beeld, geluid en schrift op het oordeel over verdachtenverhoren

M. Malsch, R. Kranendonk, J. de Keijser, H. Elffers, M. Konter & M. de Boer, NSCR, Amsterdam, 2015

80. De mentale gesteldheid van de familierechercheur. Een onderzoek naar werkgerelateerde stress en secundaire posttraumatische groei binnen een bijzondere groep politieambtenaren

L.J.A. Bollen, M.C. Saan, M.J.J. Kunst, B.W.C. Zwirs & K.F. Kuijpers, Universiteit Leiden, 2015

81. Na de vrijlating. Een exploratieve studie naar recidive en re-integratie van jihadistische exgedetineerden

D.J. Weggemans & B.A. de Graaf, Universiteit Leiden, Universiteit Utrecht, 2015

82. Dat heeft iemand anders gedaan! Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland

L. Paulissen & J. van Wilsem, Universiteit Leiden, 2015

83. Demonstratieve kampementen

B. Roorda, Rijksuniversiteit Groningen, 2015

84. Private ordebewaarders bij betogingen

B. Roorda, Rijksuniversiteit Groningen, 2015

85. Spelen met weerbarstigheid. Belemmerende patronen en doorbrekende handelingsperspectieven bij het ontwikkelen van basisteams

W. Landman, R. Kouwenhoven & M. Brussen, Twynstra Gudde, Amersfoort, 2015

86. 'Onnodige' bureaucratie binnen het basispolitiewerk. Onderzoek naar de achtergronden van een hardnekkig verschijnsel

J. Kort & J.B. Terpstra, Radboud Universiteit Nijmegen, 2015

87. Politie en GHB-problematiek op het platteland

T. Nabben & D.J. Korf, Universiteit van Amsterdam, 2016

88. Basisteams in de Nationale Politie. Organisatie, taakuitvoering en gebiedsgebonden werk

J. Terpstra, I. van Duijneveldt, T. Eikenaar, T. Havinga & B. van Stokkom, Radboud Universiteit Nijmegen, 2016

89. Samen of apart. De invloed van overleg tussen agenten bij het opstellen van het proces-verbaal

A. Vredeveldt, L. Kesteloo & P.J. van Koppen, Vrije Universiteit Amsterdam, 2016

90. ***Overvallen in beeld. Gedrag van daders, slachtoffers en omstanders***

M.R. Lindegaard, W. Bernasco & T. de Vries, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2016

91. ***Boeven vangen. Een onderzoek naar proactief politieoptreden***

W. Landman & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

92. ***VVC onder de aandacht. Een onderzoek naar ZSM en de gevolgen voor het politiewerk***

R. Salet & J. Terpstra, m.m.v. P. Frielink, Radboud Universiteit Nijmegen, 2017

93. ***De mogelijke meerwaarde van bodycams voor politiewerk. Een internationaal literatuuronderzoek***

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2017

93A ***Focus. Evaluatie pilot bodycams Politie Eenheid Amsterdam 2017-2018***

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

93b ***Evaluatie bodycams Landelijke Eenheid; Proeftuin bodycams Dienst Infrastructuur 2018***

S. Flight, Sander Flight Onderzoek & Advies, Amsterdam, 2019

94. ***Criminele families in Noord-Brabant. Een verkenning van generatie-effecten in de georganiseerde misdaad***

H. Moors & T. Spapens, EMMA, Den Haag; Tilburg University, Tilburg, 2017

94a. ***Interveniëren in criminele families***

A. Boer, R. Ceulen, H. Moors, T. Spapens, EMMA/Tilburg University, 2020

95. ***Effectiviteit van het verdachtenverhoor. Een veldstudie naar de relatie tussen verhoortechnieken, de verklaring van verdachten en de aanwezigheid van de advocaat in zware zaken***

W.J. Verhoeven & E. Duinhof, Erasmus Universiteit, Rotterdam, 2017

96. ***Van meerdere markten thuis? Overlap in markten van zware en georganiseerde misdaad en de consequenties voor de opsporing***

T. Spapens, m.m.v. M. Bruinsma, Tilburg University, Tilburg, 2017

97. ***Horen, zien en zwijgen. Opsporing in dorpen en stadsbuurten met een gesloten leefgemeenschap***

E. Bervoets & M. Bruinsma, Bureau Bervoets, Amersfoort, 2017

98. ***Geweld tegen hulpverleners in de psychiatrie. Aard, omvang en aangifte bij de politie***

J.M. Harte, I. van Houwelingen & M.E. van Leeuwen, Vrije Universiteit, Amsterdam, 2017

99. Geëiste en opgelegde straffen bij de strafrechtelijke afhandeling van georganiseerde criminaliteit. Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit

C.G. van Wingerde & H.G. van de Bunt, Erasmus School of Law, Rotterdam, 2017

100. Doorgroeiers in de misdaad. De criminele carrières en achtergrondkenmerken van jonge daders van een zwaar delict

V. van Koppen, V. van der Geest & E.R. Kleemans, Vrije Universiteit, Amsterdam, 2017

101. Profielen van Nederlandse outlawbikers en Nederlandse outlawbikerclubs

A. Blokland, W. van der Leest & M. Soudijn (m.m.v. E. Kleinheerenbrink & I. van Die), Leiden Law School, Leiden, 2017

102. Verdachten van terrorisme in beeld. Achtergrondkenmerken, 'triggers' en eerdere politiecontacten

F. Thijs, E. Rodermond & F. Weerman, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2018

103. Burgemeesters in cyberspace. Handhaving van de openbare orde door bestuurlijke maatregelen in een digitale wereld

W. Bantema, S.M.A. Twickler, S.A.J. Munneke, M. Duchateau & W.Ph. Stol, NHL Stenden Hogeschool, Leeuwarden; Rijksuniversiteit Groningen, Groningen, 2018

104. Een bittere pil. Het fenomeen en de aanpak van illegale medicijnenhandel

I. van Leiden, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

105. Vastzitten zonder straf. Over inverzekeringstellingen en schadevergoedingen op basis van artikel 89 Sv

P. Kruize & P. Gruter, Bureau Ateno, Amsterdam, 2018

106. 'Ik hou het hier wel uit, hoor'. Mentale weerbaarheid binnen de districtsrecherche

H. Sollie, Twynstra Gudde, Amersfoort, 2018

107. Bestuurlijke bevoegdheden, politie en de lokale aanpak van onveiligheid

R. Salet & H. Sackers, Radboud Universiteit, Nijmegen, 2019

108. Politie en actief burgerschap: een veilig verbond? Een onderzoek naar samenwerking, controle en (neven)effecten

V. Lub & T. de Leeuw, m.m.v. A.S. Leerkes & R.J. Kleinhans, Bureau voor Sociale Argumentatie, Rotterdam; Erasmus Universiteit, Rotterdam; Bureau voor Maatschappij, Veiligheid & Deviantie, Rotterdam, 2019

109. Wijkagenten en veranderingen in hun dagelijks werk. Verslag van een onderzoek

J. Terpstra, m.m.v. A. Evers, Radboud Universiteit, Nijmegen, 2019

110. Naar een efficiëntere noodhulp? Een verkennend actieonderzoek

A. Scholtens & I. Helsloot, m.m.v. S. Kraaijenbrink, J. Vlagsma, M. Jürgens, D. Mouris & M. Eising, Crisislab, Renswoude, 2019

111. Bestrijding van Outlaw Motorcycle Gangs. Een rechtsvergelijkende studie naar de aanpak van onrechtmatige organisaties in rechtsstatelijk perspectief.

J. Koornstra, B. Roorda, M. Vols & J.G. Brouwer, Rijksuniversiteit Groningen, 2019

112. Politiestraatgezag en (on)gehoorzaam burgergedrag

A. Scholtens, M. Helsloot, I. Helsloot, Crisislab, Renswoude, 2019

113. Verkeershandhaving op Nederlandse autosnelwegen; Evaluatie van de werkwijze van het Team EVT, de effecten en de acceptatie van politiecontroles

Ch. Goldenbeld, A. Stelling-Kończak, S. van der Kint, SWOV, Den Haag, 2019

114. Virtual reality als onderzoeksmethode om inbrekers te doorgronden

I. van Sintemaartensdijk, J.L. van Gelder, P.A.M. van Lange, M. Otte, J.W. van Prooijen, Vrije Universiteit Amsterdam, 2019

115. Wanneer blaffende honden bijten. Een vergelijking tussen fataal en niet-fataal huiselijk geweld

P. Aarten, C. Boelema Robertus, L. Alink, M. Liem, Universiteit Leiden, 2020

116. Kijk naar het systeem. Begrijpen en beïnvloeden van opsporingspraktijken

W. Landman, R. Kouwenhoven, M. Brussen, Twynstra Gudde, Amersfoort, 2020

117 Verbeelding in de verhoorkamer. De invloed van het gebruik van beeldmateriaal in het verhoor op verhoortechnieken en proceshouding

W.J. Verhoeven, G. Vanderveen, L. van Dillen, S. Kruit, Erasmus Universiteit, Universiteit Leiden, 2020

118 Met gepast geweld. Politiegeweld in Nederland in 2016

M. Kuin, F. Kriek, J. Timmer, m.m.v. Y. Bleeker en E. Verbeek, Regioplan, Amsterdam en Vrije Universiteit Amsterdam, 2020

119 De rol van bodycambeelden in de opsporing en bewijsvoering

A. Vredeveldt, L. Kesteloo, A. Hildebrandt, Vrije Universiteit Amsterdam, 2020

120 Slachtoffer van onlinecriminaliteit, wat nu?

S.G.A. van de Weijer, E.R. Leukfeldt, S. van der Zee, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Amsterdam, 2020