

HackShield in Noord-Holland

Een evaluatie van de implementatie en resultaten van HackShield in Noord-Hollandse gemeenten



SAXION
HOGESCHOOL

HACKSHIELD
FUTURE CYBERHEROES

NH Samen
Veilig

Auteurs:

Jim Schiks MSc

Senna Hansen MSc

Elsa Foppen BSc

Dr. Rutger Leukfeldt

Dr. Remco Spithoven

De Haagse Hogeschool,
Centre of Expertise Cybersecurity

Hogeschool Saxion, Lectoraat
Maatschappelijke Veiligheid

In opdracht van: Regionaal Samenwerkingsverband
Noord Holland Samen Veilig

let's change
YOU. US. THE WORLD.

DE HAAGSE
HOGESCHOOL

© 2021 De Haagse Hogeschool

De Haagse Hogeschool
Johanna Westerdijkplein 75
2521 EN Den Haag
www.dehaagsehogeschool.nl

Auteurs:

Jim Schiks MSc
Senna Hansen MSc
Elsa Foppen BSc
Dr. Rutger Leukfeldt
Dr. Remco Spithoven

De Haagse Hogeschool, Centre of Expertise Cybersecurity
Hogeschool Saxion, Lectoraat Maatschappelijke Veiligheid
In opdracht van: Regionaal Samenwerkingsverband Noord Holland Samen Veilig

Foto's/illustraties omslag en binnenwerk: www.joinhackshield.nl, Shutterstock.com
Vormgeving: Dienst Onderwijs, Kennis & Communicatie

Niets uit deze uitgave mag worden verveelvoudigd, door middel van druk, fotokopieën, geautomatiseerde gegevensbestanden of op welke andere wijze ook zonder voorafgaande schriftelijke toestemming van de uitgever.

INHOUDSOPGAVE

Samenvatting	5
1 Inleiding	6
1.1 Achtergrond	6
1.2 Aanleiding	6
1.3 Doelstelling en onderzoeksvragen	6
1.4 Leeswijzer	6
2 Interventies voor cybercriminaliteit	7
2.1 Inleiding	7
2.2 Criminaliteitspreventie	7
2.3 Cybercriminaliteit & preventie	7
3 Methodische verantwoording	8
3.1 Onderzoeksmethoden	8
3.2 Selectieprocedure	8
3.3 Interviewprocedure	9
4 De plannen van 'HackShield in gemeenten Noord-Holland'	10
4.1 Inleiding	10
4.2 Aanleiding	10
4.3 Betekenis, doelen en doelgroep	11
4.4 Onderbouwing	12
4.5 Inhoud project	14
4.6 Samenwerkingspartners	15
4.7 Resumé	16
5 De uitvoering van HackShield	17
5.1 Inleiding	17
5.2 Casus 1: gemeente A	17
5.3 Casus 2: gemeente B	18
5.4 Casus 3: gemeente C	18
5.5 Casus 4: gemeente D	19
5.6 Selectie en bereik van deelnemers	20
5.7 Resumé	22
6 De ervaringen rondom HackShield	23
6.1 Inleiding	23
6.2 Waardering betrokkenen	23
6.3 Bijdrage cyberweerbaarheid	24
6.4 Bevorderende en belemmerende factoren	25
6.5 Resumé	27
7 Conclusie en discussie	28
7.1 Conclusies	28
7.2 Discussie	29
Referenties	30



Samenvatting

In de provincie Noord-Holland is in 2019 een op de zeven inwoners weleens slachtoffer geworden van een vorm van cybercriminaliteit. Door regionaal samenwerkingsverband Noord Holland Samen Veilig (NHSV) wordt cybercriminaliteit dan ook aangemerkt als een geprioriteerd thema. Een van de projecten die dient bij te dragen aan deze prioritering is 'HackShield in gemeenten Noord-Holland'. HackShield is een cybersecurity spel voor kinderen tussen de 8 en 12 jaar en heeft tot doel om een cyberveilige generatie kinderen te creëren. In de samenwerking met gemeenten roepen burgemeesters en politieagenten kinderen op om het spel te spelen en 'cyber-agent' van de gemeente te worden. Spelers met de meeste punten worden gehuldigd door de gemeenten. Vanuit NHSV en HackShield is er de behoefte om het project te evalueren.

Het huidige onderzoek bestaat uit een beknopte plan- en procesevaluatie waarin de beleidstheorie, uitvoering en ervaringen van het project in kaart worden gebracht. De gebruikte onderzoeksmethoden betreffen een documentanalyse en 30 interviews met ontwikkelaars, uitvoerders en deelnemers. Een belangrijke beperking van het onderzoek is de representativiteit van de geïnterviewde deelnemers: de helft van de deelnemers die bereid waren om deel te nemen aan het onderzoek waren 'testers' van het spel en daarmee de meest fanatieke spelers. Verder is het van belang om te vermelden dat de dataverzameling heeft plaatsgevonden tussen september 2020 en februari 2021. Dit betekent dan ook dat de huidige evaluatie een momentopname betreft, aangezien projecten tussentijds kunnen worden aangepast.

De resultaten van het onderzoek laten zien dat HackShield een project, spel en maatschappelijke beweging is waarin de 'Hero-Centred-Design' filosofie van de makers van het spel centraal staat. In deze filosofie staat de eindgebruiker in het middelpunt en krijgt deze een (fictieve) rol die de gebruiker niet heeft in de echte wereld. Binnen de onderzochte gemeenten bestaat het project uit een promotiecampagne om kinderen HackShield te laten spelen, een spelperiode en een huldiging van de beste spelers door de burgemeester en politie. Vooraf hebben gemeenten informatie en instructies gehad over de invulling van het initiatief en tegelijkertijd ruimte gehad om hiervan af te wijken. Verschillen in de uitvoering bestaan in de communicatiekanalen die zijn gebruikt en de wijze waarop huldigingen hebben plaatsgevonden.

Deelnemers, ouders en uitvoerders zijn tevreden over het verloop van het project. Uitvoerders zijn tevreden omdat er duidelijke instructies en goede begeleiding was en omdat er door het project meer aandacht is voor cybercriminaliteit. Bijna alle uitvoerders zouden bij een toekomstige projectronde opnieuw meedoen. Deelnemers zijn enthousiast omdat zij het spel leuk en leerzaam vinden. Alle ouders zouden het spel aanbevelen aan anderen. De inzet van partners die betrokken zijn bij het initiatief, de goede ondersteuning vanuit de initiatiefnemers en de kleine inspanning die het vraagt voor gemeenten om mee te doen zorgen voor een goed verloop van het initiatief. Winst is te behalen door scholen beter bij het project te betrekken en door meer levels aan het spel toe te voegen. Daarnaast worden de maatregelen rondom het COVID-19 virus door verschillende uitvoerders benoemd als belemmerende factor, omdat het ondernemen van fysieke activiteiten hierdoor beperkt mogelijk was.

Voor de meeste uitvoerders is het onduidelijk in hoeverre de doelen van HackShield worden behaald. Deelnemers geven allemaal aan iets te hebben geleerd, bijvoorbeeld over sterke wachtwoorden, het herkennen van phishing mails en hoe je kunt voorkomen dat je wordt gehackt. Het blijft echter onduidelijk wat de daadwerkelijke effecten zijn van het initiatief. Vervolgonderzoek in de vorm van een effectevaluatie is een noodzakelijke volgende stap. Toekomstig evaluatieonderzoek in de vorm van (kwantitatieve) effectevaluaties kan aantonen wat de daadwerkelijke effecten zijn van het initiatief. Zo kan er een voor- en nameting plaatsvinden met betrekking tot de kennis die deelnemers en ouders daadwerkelijk opdoen, door vragenlijsten op te stellen die deze kennis toetsen. Verder verdient het de aanbeveling om ook kwalitatief onderzoek te blijven uitvoeren, zodat zowel positieve effecten als mogelijke ongewenste consequenties van het initiatief in kaart kunnen worden gebracht. Interviews met deelnemers en ouders zijn hiervoor geschikt, mits de steekproeven representatief zijn voor alle deelnemers.

1 Inleiding

1.1 Achtergrond

Cybercriminaliteit is inmiddels niet meer weg te denken uit de huidige samenleving. Uit cijfers van het CBS blijkt dat in 2019 14% van de inwoners uit de provincie Noord-Holland weleens slachtoffer is geworden van een vorm van cybercriminaliteit (CBS, 2020a). Voorbeelden van vormen van cybercriminaliteit zijn identiteitsfraude, phishing, koop- en verkoopfraude en hacking. Zo werden in 2020 bijvoorbeeld twintig Noord-Hollanders slachtoffer van een 18-jarige hacker en afperser, die met behulp van phishing toegang kreeg tot Snapchat-accounts en privéfoto's van de slachtoffers (NH nieuws, 2020). Naast de hoge aantallen cybercrimedelicten, kunnen ook de gevolgen van dergelijke delicten voor slachtoffers groot zijn. Zo ervaren slachtoffers emotionele, psychologische en financiële gevolgen van de delicten (Leukfeldt et al., 2020).

Vanuit de overheid is er op lokaal en regionaal niveau aandacht voor de bestrijding en preventie van cybercriminaliteit. In de politie-eenheid Noord-Holland is de 'aanpak cybercrime en gedigitaliseerde vormen van criminaliteit' een van de vier geprioriteerde thema's van het Integraal Meerjarenbeleidsplan Veiligheid (Noord-Holland Samen Veilig, 2018). In het uitvoeringsplan van de regio Noord-Holland staan verschillende deelprojecten beschreven die dienen bij te dragen aan deze prioritering (Noord-Holland Samen Veilig, 2020).

Een van de deelprojecten in het uitvoeringsplan van de regio Noord-Holland is het uitrollen van het project 'HackShield en de gemeente'. HackShield wordt omschreven als een cybersecurity spel voor kinderen tussen de 8 en 12 jaar oud (Projectaanvraag, z.d.). In plaats van als potentiële slachtoffers, benadert HackShield de spelers als Future Cyber Hero's: de digitale helden van morgen. Het doel van HackShield is om een cyberveilige generatie kinderen te creëren. Om dit doel te bereiken krijgen kinderen tijdens het spel een reeks opdrachten – ook wel 'quests' genoemd - aangeboden. In de opdrachten maken deelnemers eerst kennis met thema's zoals 'phishing' en vervolgens worden de kinderen gestimuleerd om de opgedane kennis over te dragen aan hun omgeving, bijvoorbeeld aan hun (groot)ouders. HackShield en gemeenten in Noord-Holland zijn een samenwerking aangegaan om de digitale veiligheid van huidige en toekomstige generaties te verbeteren.

1.2 Aanleiding

In maart 2020 is een pilot gestart van de samenwerking tussen HackShield en 7 gemeenten uit Noord-Holland, welke in september 2020 is uitgebreid naar 25 gemeenten. In de samenwerking worden kinderen door hun burgemeester en/of lokale politie (vlogger) via online kanalen opgeroepen om HackShield te spelen en 'Junior Cyber Agent' van hun gemeente te worden. De 'Junior Cyber Agents' die de meeste punten hebben gescoord worden gehuldigd door de burgemeester en politie

na afloop van een bepaalde spelperiode. Vanuit het samenwerkingsverband Noord-Holland Samen Veilig en HackShield is er de behoefte om de eerste pilots te evalueren.

1.3 Doelstelling en onderzoeksvragen

Het huidige onderzoek heeft tot doel om het initiatief 'HackShield in gemeenten Noord-Holland' te evalueren. Bij voorkeur verloopt de evaluatie van een programma of interventie volgens een bepaalde hiërarchie: (1) planevaluatie, (2) procesevaluatie en (3) effectevaluatie (Rossi et al., 2004; Ooyen-Houben & Leeuw, 2010). Dit onderzoek bestaat uit een beknopte plan- en procesevaluatie en zal daarnaast de eerste ervaringen in kaart brengen van de verschillende stakeholders die betrokken zijn bij dit initiatief. Het onderzoek is daarmee nadrukkelijk geen effectevaluatie. Voor de planevaluatie zal de beleidstheorie van het initiatief in kaart worden gebracht en kritisch worden bekeken. Vervolgens zal voor de procesevaluatie inzicht worden verkregen in de uitvoeringspraktijk van de pilot die is uitgevoerd. Ten slotte zullen ervaringen van betrokkenen met betrekking tot de pilot in kaart worden gebracht. De volgende onderzoeksvragen staan dan ook in het onderzoek centraal:

Het plan:

1. Wat is het initiatief 'HackShield in gemeenten Noord-Holland' en hoe is dit theoretisch onderbouwd?

Het proces:

2. In hoeverre verloopt de uitvoeringspraktijk van het initiatief zoals beoogd?
3. In hoeverre wordt de beoogde doelgroep van het initiatief bereikt?

De ervaringen:

4. Hoe waarden uitvoerders en deelnemers het initiatief?
5. In hoeverre draagt het initiatief volgens uitvoerders en deelnemers bij aan een cyber veilige maatschappij?
6. Welke onderdelen van de opzet en de uitvoering met betrekking tot de pilot worden door uitvoerders en deelnemers als succesvol of juist niet succesvol aangemerkt?

1.4 Leeswijzer

Dit rapport is op de volgende wijze opgebouwd. Eerst zal in hoofdstuk 2 een overzicht worden gegeven van wat er in wetenschappelijke literatuur bekend is over (effectieve) interventies voor cybercriminaliteit. In hoofdstuk 3 wordt vervolgens de methodische verantwoording van het onderzoek besproken. De resultaten van het onderzoek komen aan bod in de hoofdstukken 4, 5 en 6. Tot slot laat hoofdstuk 7 zien wat de belangrijkste conclusies en beperkingen zijn van het onderzoek.

2 Interventies voor cybercriminaliteit

2.1 Inleiding

Het huidige hoofdstuk geeft meer inzicht in interventies op het gebied van (cyber)criminaliteit. Eerst bespreekt paragraaf 2.2 wat bekend is vanuit de literatuur over traditionele criminaliteitspreventie strategieën. Vervolgens geeft paragraaf 2.3 inzicht in (het gebrek aan) kennis over criminaliteitspreventie strategieën voor cybercriminaliteit.

2.2 Criminaliteitspreventie

Met betrekking tot criminaliteitspreventie kan op basis van de reikwijdte van een interventie of strategie onderscheid gemaakt worden tussen primaire, secundaire en tertiaire preventie (Brantingham & Faust, 1976; Brewer et al., 2019). Primaire preventie richt zich op de gehele populatie potentiële slachtoffers of daders. Voorbeelden zijn voorlichting, opvoeding en onderwijs om criminaliteit te voorkomen. HackShield is dan ook een voorbeeld van primaire preventie. Bij secundaire preventie richt men zich op groepen die een verhoogd risico lopen om slachtoffer of dader te worden van criminaliteit. Hierbij kan worden gedacht aan interventies gericht op kwetsbare ouderen om slachtofferschap te voorkomen of een aanpak gericht op kwetsbare wijken waar jongeren meer risico lopen om betrokken te raken bij criminaliteit. Ten slotte richt tertiaire preventie zich op personen die reeds slachtoffer zijn geworden of al een delict hebben gepleegd. Het doel van tertiaire preventie is om herhaald slachtoffer- of daderschap te voorkomen. Voorbeelden zijn initiatieven van slachtofferhulp of reclasseringstrajecten voor daders. Eerder evaluatieonderzoek laat zien dat er interventies zijn op het gebied van criminaliteitspreventie die werken, maar dat er ook veel programma's worden ingezet die niet werken of zelfs schade toe kunnen brengen aan de personen die eraan deelnemen (Weisburd, 2017; McCord, 2003).

2.3 Cybercriminaliteit & preventie

Recent onderzoek laat zien dat er nog weinig tot geen onderzoek is dat de effectiviteit van criminaliteitspreventie strategieën op het gebied van cybercriminaliteit heeft geëvalueerd (Brewer et al., 2019; Oosterwijk & Fischer, 2017). Enkel op het gebied van situationele criminaliteitspreventie is schaars bewijs dat sommige vormen van situationele criminaliteitspreventie effectief zijn in het verminderen van cybercriminaliteit. Situationele criminaliteitspreventie (SCP) betreft het dusdanig ontwerpen of manipuleren van de omgeving dat het voor criminelen minder aantrekkelijk wordt om een bepaald delict te plegen of hierbij betrokken te raken (Clarke, 1995). De gelegenheid voor criminaliteit verminderen staat bij situationele criminaliteitspreventie centraal.

Voorbeelden van effectief gebleken SCP-strategieën voor cybercriminaliteit zijn het gebruik van antivirussoftware, het gebruik van 'warning banners' en het monitoren of bewaken van computersystemen (Brewer et al., 2019). Antivirussoftware is bedoeld om computersystemen schoon te houden van virussen, wormen en 'trojans'. Dergelijke programma's blijken een effectieve strategie te zijn om kwaadaardige software te ontdekken en voorkomen, indien de 'handtekening' van de kwaadaardige software in de database van de antivirussoftware staat. 'Warning banners' zijn afschrikkende banners die zijn bedoeld om het gedrag van potentiële daders te beïnvloeden en hen bewust te maken van de mogelijke risico's of gevaren. Dergelijke berichten zijn relatief ineffectief in het voorkomen van het binnendringen van computersystemen, maar kunnen wel effectief zijn in het beperken van de gevolgen en het beïnvloeden van het gedrag wanneer men al in een computersysteem is binnengedrongen. Ten slotte heeft het implementeren van monitoring of bewaking in computersystemen positieve effecten op het aantal incidenten.

Naar de effectiviteit van primaire, secundaire of tertiaire vormen van criminaliteitspreventie op het gebied van cybercriminaliteit is nog te weinig onderzoek gedaan (Brewer et al., 2019). Dergelijk onderzoek is echter essentieel om niet alleen te achterhalen of criminaliteitspreventie strategieën hun doelen behalen met betrekking tot het verminderen van criminaliteit, maar ook of zij het geld waard zijn en of de strategieën geen onvoorziene of ongewenste consequenties met zich mee brengen.

3 Methodische verantwoording

3.1 Onderzoeksmethoden

Voor het onderzoek is gebruik gemaakt van twee kwalitatieve onderzoeksmethoden: documentanalyse en interviews. Kwalitatief onderzoek is geschikt om de perspectieven van betrokken actoren inzichtelijk te krijgen (Decorte & Zaitch, 2016). Beleidstheorieën zijn vaak impliciet in beleidsdocumenten geformuleerd. Dit betekent dat men het doel en de in te zetten middelen beschrijft, maar niet expliciet vermeld *waarom* de ingezette middelen het doel doen behalen. Voor het blootleggen van de beleidstheorie (planevaluatie) zijn enerzijds documenten geanalyseerd met betrekking tot de plannen van het initiatief (inhoud, doelen, onderbouwing) en anderzijds interviews gehouden met ontwikkelaars die het initiatief hebben opgestart. Voor het evalueren van de uitvoeringspraktijk (procesevaluatie) zijn interviews gehouden met stakeholders die betrokken zijn geweest bij de uitvoering van het project en met (ouders van) deelnemers. Ook is documentatie met betrekking tot de uitvoering geanalyseerd. Ten slotte zijn de ervaringen van uitvoerders en (ouders van) deelnemers in kaart gebracht aan de hand van interviews. In tabel 1 is een overzicht weergegeven van de gebruikte onderzoeksmethoden in relatie tot de onderzoeksvragen die in het onderzoek centraal staan.

3.2 Selectieprocedure

In totaal hebben 25 Noord-Hollandse gemeenten deelgenomen in de tweede projectronde van HackShield tussen september en december 2020. Gezien de beperkte omvang van onderhavige onderzoek, is het niet mogelijk om het verloop van HackShield binnen alle gemeenten te onderzoeken. Er is daarom een selectie gemaakt van vier gemeenten die mee zijn genomen in de evaluatie. De gemeenten zijn geselecteerd op basis van (1) het aantal inwoners en (2) het relatieve bereik met betrekking tot het aantal deelnemers¹. Gemeente A is een kleine gemeente met een relatief klein bereik, gemeente B is een kleine gemeente met een relatief groot bereik, gemeente C is een grote gemeente met een relatief klein bereik en gemeente D is een grote gemeente met een relatief groot bereik.

Tabel 1: Gebruikte onderzoeksmethoden

	Document-analyse	Interviews ontwikkelaars	Interviews stakeholders	Interviews deelnemers
Vraag 1: de plannen	X	X		
Vraag 2: verloop uitvoeringspraktijk	X		X	
Vraag 3: bereik beoogde doelgroep	X		X	X
Vraag 4: waardering betrokkenen			X	X
Vraag 5: bijdrage cyberweerbaarheid			X	X
Vraag 6: (niet) succesvolle onderdelen			X	X

¹ Via HackShield is een overzicht verkregen met informatie over het aantal 'cyber-agents' per gemeente op 30 november 2020 en het percentage 'cyber-agents' ten opzichte van het totaal aantal kinderen van 7 tot en met 12 jaar in de gemeente.

3.3 Interviewprocedure

Voor het onderzoek zijn in totaal 30 respondenten geïnterviewd. Twee van de respondenten zijn interventie-ontwikkelaar, acht respondenten zijn betrokken geweest bij de uitvoering van de HackShield pilots en negentien respondenten waren deelnemers van de HackShield pilots. In tabel 2 is een overzicht weergegeven van alle respondenten. Per doelgroep wordt nu de procedure en informatie omtrent de interviews besproken:

Ontwikkelaars – Twee interventieontwikkelaars zijn voor het onderzoek geïnterviewd om de plannen en ideeën rondom het initiatief 'HackShield in de gemeente Noord-Holland' in kaart te brengen. Een van de respondenten is betrokken vanuit samenwerkingsverband Noord-Holland Samen Veilig (publieke sector), de andere respondent is oprichter van HackShield (private sector). De interviews duurden 1 uur en 39 minuten en 2 uur en 17 minuten.

Uitvoerders - Voor de interviews met uitvoerders is van elk van de geselecteerde gemeenten gesproken met zowel een medewerker van de desbetreffende gemeente als met een medewerker van de politie die betrokken waren bij de uitvoering van HackShield. Contactgegevens van de medewerkers van gemeenten zijn verkregen via de projectleiders van HackShield in Noord-Holland. Via de medewerkers van gemeenten zijn de contactgegevens van medewerkers van de politie verkregen. In totaal zijn 4 medewerkers van gemeenten, 4 medewerkers van de politie en 1 communicatie-manager van HackShield geïnterviewd. De duur van de interviews varieerde van 26 minuten tot 59 minuten.

Deelnemers – De PR- en communicatiemanager van HackShield heeft wekelijks vijf deelnemers en hun ouders benaderd met de vraag of zij deel wilden nemen aan dit onderzoek. Zodra ouders instemden met het interview hebben de onderzoekers een afspraak ingepland voor het gesprek. In totaal zijn 19 deelnemers en 16 ouders van deelnemers geïnterviewd vanuit 11 verschillende gemeentes. Het verschil in het aantal kinderen en ouders wordt veroorzaakt doordat soms meerdere kinderen uit één gezin afkomstig waren en omdat in één geval de ouders niet in de mogelijkheid waren om deel te nemen aan het gesprek. Wel gaven zij toestemming voor het deelnemen van hun kind. Deze interviews duurden tussen de 11 en 40 minuten. Dit was vooral het gevolg van een beperkte spanningsboog van de deelnemende kinderen.

Alle interviews hebben plaatsgevonden via Microsoft Teams en één interview is afgenomen middels WhatsApp videobellen. Voorafgaand aan de interviews is toestemming gevraagd aan de respondent – of hun ouders in het geval

van de deelnemende kinderen - om het gesprek op te nemen. De opnames zijn vervolgens verwerkt tot een geanonimiseerd gespreksverslag en verwijderd. Ter validatie zijn de gespreksverslagen voorgelegd aan ontwikkelaars en uitvoerders. In een enkel geval zijn onjuistheden gecorrigeerd, wat uiteindelijk geen inhoudelijke verschillen heeft opgeleverd. De gespreksverslagen vormden de basis voor de rapportage in de resultaat hoofdstukken 4, 5 en 6. De dataverzameling heeft plaatsgevonden tussen september 2020 en februari 2021.

Tabel 2: Overzicht respondenten

Code	Rol	Functie	Organisatie
I01	Ontwikkelaar	Projectleider cybercrime en gedigitaliseerde criminaliteit	Noord Holland Samen Veilig
I02	Ontwikkelaar	Co-CEO	HackShield
COM1	Uitvoerder	Communicatie-manager	HackShield
GM1	Uitvoerder	Medewerker openbare Orde en Veiligheid	Gemeente A
GM2	Uitvoerder	Projectcoördinator openbare Orde en Veiligheid / Projectleider Cybercrime	Gemeente B
GM3	Uitvoerder	Junior adviseur openbare Orde en Veiligheid	Gemeente C
GM4	Uitvoerder	Beleidsadviseur openbare Orde en Veiligheid	Gemeente D
POL1	Uitvoerder	Wijkagent	Politie
POL2	Uitvoerder	Operationeel specialist	Politie
POL3	Uitvoerder	Wijkagent	Politie
POL4	Uitvoerder	Teamchef	Politie
DN1	Deelnemer	n.v.t.	n.v.t.
DN2 ²	Deelnemer	n.v.t.	n.v.t.
DN3	Deelnemer	n.v.t.	n.v.t.
DN4	Deelnemer	n.v.t.	n.v.t.
DN5	Deelnemer	n.v.t.	n.v.t.
DN6	Deelnemer	n.v.t.	n.v.t.
DN7	Deelnemer	n.v.t.	n.v.t.
DN8	Deelnemer	n.v.t.	n.v.t.
DN9	Deelnemer	n.v.t.	n.v.t.
DN10	Deelnemer	n.v.t.	n.v.t.
DN11	Deelnemer	n.v.t.	n.v.t.
DN12	Deelnemer	n.v.t.	n.v.t.
DN13	Deelnemer	n.v.t.	n.v.t.
DN14	Deelnemer	n.v.t.	n.v.t.
DN15	Deelnemer	n.v.t.	n.v.t.
DN16	Deelnemer	n.v.t.	n.v.t.
DN17	Deelnemer	n.v.t.	n.v.t.
DN18	Deelnemer	n.v.t.	n.v.t.
DN19	Deelnemer	n.v.t.	n.v.t.

2 Deelnemer 1 en deelnemer 2 zijn tegelijkertijd geïnterviewd.

4 De plannen van ‘HackShield in gemeenten Noord-Holland’

4.1 Inleiding

De plannen en ideeën rondom het initiatief ‘HackShield in gemeenten Noord-Holland’ worden in dit hoofdstuk in kaart gebracht. De resultaten worden weergegeven op basis van beschikbare documenten en interviews met interventie-ontwikkelaars. Eerst laat paragraaf 4.2 zien wat de aanleiding is geweest voor het initiatief en welke partijen betrokken zijn geweest bij de opzet. Vervolgens gaat paragraaf 4.3 in op de betekenis, doelen en doelgroep. De onderbouwing van HackShield wordt toegelicht in paragraaf 4.4 en in paragraaf 4.5 wordt inzicht gegeven in de inhoud van het initiatief. Daarna bespreekt paragraaf 4.6 de samenwerking tussen verschillende partners die betrokken zijn. Het hoofdstuk sluit af met een resumé in paragraaf 4.7.

4.2 Aanleiding

Tijdens de documentanalyse en interviews met ontwikkelaars komen verschillende aanleidingen naar voren voor het initiatief ‘HackShield in gemeenten Noord-Holland’. De rode draad hierin is de behoefte om bij te dragen aan de digitale weerbaarheid van kinderen en het tegengaan van cybercriminaliteit. Zo blijkt uit de documentanalyse dat HackShield en de gemeenten in Noord-Holland een samenwerking zijn aangegaan om een impuls te geven aan de digitale veiligheid van de huidige en toekomstige generaties (Projectaanvraag, z.d.). Verder wordt in de Collegia-omgeving³ benoemd dat cybercriminaliteit de snelst groeiende vorm van criminaliteit is, dat mensen een gebrek hebben aan basis cybersecurity-vaardigheden om zichzelf en anderen te beschermen en dat kinderen op dit moment niet digitaal opgeleid worden (Collegia, 2020).

In aanvulling op de documentanalyse geeft een van de ontwikkelaars - werkzaam bij het regionale samenwerkingsverband Noord-Holland Samen Veilig - verschillende bestuurlijke aanleidingen voor het initiatief (IO1). Zo is er volgens de respondent vanuit het openbare orde en veiligheidsperspectief behoefte om slachtofferschap van cybercriminaliteit te voorkomen, moet de overheid slimmer gaan werken en meebewegen met private partijen en moeten burgemeesters zich bewuster zijn van wat er online gebeurt omdat de openbare orde en veiligheid zich steeds meer online afspeelt (IO1). De tweede ontwikkelaar is werkzaam bij Flavour – een bedrijf gespecialiseerd in ‘applied gaming’ - en heeft HackShield ontwikkeld (IO2). De reden voor het ontwikkelen van HackShield was dat de respondent graag iets wilde

doen met trans mediale projecten en een beweging wilde creëren rondom een maatschappelijk relevant onderwerp. Bij trans mediale projecten komen karakters die in een verhaalwereld een rol spelen, ook in de werkelijkheid terug. De doelgroep van 8 tot en met 12 jaar is volgens de respondent erg geschikt om een beweging te creëren met een spel en verhaal, vanwege onder andere het hoge ethisch besef en de fantasie die deze doelgroep heeft. In overleg met collega’s is besloten dat digitale geletterdheid en potentiële gevaren van cybercriminaliteit het meest relevante onderwerp was voor deze doelgroep en de maatschappij (IO2).

Bij de opzet van HackShield en het project zijn een grote hoeveelheid partijen betrokken geweest. Zo geeft een van de ontwikkelaars aan dat Flavour de organisatie is die HackShield is gestart, heeft de Rabobank geïnvesteerd in HackShield, is het regionaal samenwerkingsverband Noord-Holland Samen Veilig vanuit de overheid de samenwerking met Flavour aangegaan, hebben verschillende gemeenten deelgenomen aan het initiatief en zijn er voor het project subsidies ontvangen van het Centrum voor Criminaliteitspreventie en Veiligheid en het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (IO1). Bij het ontwikkelen van de inhoud van het spel HackShield door Flavour zijn volgens de respondent ook partijen zoals TNO, het Team High Tech Crime van de politie, cybersecurity bedrijf ESET en andere organisaties betrokken geweest (IO2). Voor alles waar geen expertise was heeft men mensen benaderd en gevraagd om mee te helpen (IO2). In de projectaanvraag (z.d.) staat verder vermeld dat HackShield is ontwikkeld met behulp van Flavour, KraBé Academy, het SIDN fonds, de Rabo Foundation, de Rabobank, het platform voor de Informatie Samenleving en Interpolis. In paragraaf 4.6 staat verder beschreven hoe de samenwerking met verschillende partners eruitziet.

3 Collegia is een online platform waarin HackShield informatie deelt met betrokken partners omtrent het spel en het project binnen de gemeenten.

4.3 Betekenis, doelen en doelgroep

Betekenis

Met betrekking tot de betekenis van HackShield kan er een onderscheid worden gemaakt tussen het online spel HackShield en HackShield als grotere maatschappelijke beweging. HackShield wordt in de projectaanvraag (z.d.) bijvoorbeeld omschreven als 'een trans mediale cybersecurity game voor kinderen tussen de 8 en de 12 jaar oud waarin zij zich op speelse wijze leren wapenen tegen digitale gevaren'. In de collegia-omgeving wordt HackShield echter breder omschreven als 'een digitale scouting', waarbij kinderen digitale vaardigheden leren in plaats van knopen leggen en waarbij een dialoog wordt gecreëerd tussen kinderen en (groot) ouders (Collegia, 2020). Ook tijdens de interviews komt dit verschil in betekenis naar voren. Zo omschrijft een van de ontwikkelaars HackShield als een digitaal instrument (een spel) om op een speelse manier aan digitale weerbaarheid te werken (IO1). De tweede ontwikkelaar geeft aan het lastig te vinden om een definitie van HackShield te geven (IO2). HackShield is volgens de respondent een beweging, waarin kinderen de hoofdrol spelen. Dat een van de grootste onderdelen van HackShield een spel-platform is, is volgens de respondent minder belangrijk dan dat het een beweging is. HackShield heeft bijvoorbeeld ook een kaartspel voor in de klas. Het volgende citaat illustreert de visie van de respondent:

“ Ik moet je heel eerlijk zeggen, zodra je het project in een hokje probeert te zetten, dan raak je de opzet kwijt. [...] Ik weet vaak duidelijker te zeggen wat het project is dan wat het product is. Want het product is niet alleen een spel.

We hebben een hele digitale omgeving ingericht voor gemeentes met allemaal tekst en uitleg hoe ze het kunnen uitleggen in hun gemeentes.

Ja, is dat dan ons product? Ik weet het niet, wij doen het gewoon want het is er niet. ” (IO2)

Doelen

In de documenten en interviews worden verschillende doelen geformuleerd met betrekking tot HackShield, die neerkomen op het cyberveiliger en cyberweerbaar maken van kinderen en Nederland als geheel. Zo staat in de projectaanvraag dat HackShield als doel heeft om een volledig cyberveilige generatie kinderen te creëren die zorgeloos over het web kan navigeren en de oudere generatie hierin kan bijstaan (Projectaanvraag, z.d.). In de Collegia-omgeving wordt als doel het verhogen van de cyberweerbaarheid van een generatie kinderen genoemd (Collegia, 2020). Onder cyberweerbaarheid verstaan wij in navolging van Spithoven (2020) een combinatie van een accurate risicoperceptie en afdoende zelfbeschermend gedrag. Beide documenten omschrijven ook verschillende subdoelen. Zo zijn in de collegia-omgeving specifieke leerdoelen en competenties gekoppeld aan het spel HackShield (Collegia, 2020) en staan in de projectaanvraag (z.d.) subdoelen gekoppeld aan het project zoals bijdragen aan een preventieve en bestuurlijke aanpak van criminaliteit, experimenteren met een publiek private samenwerking en burgers digitaal weerbaarder maken via jeugd. Deze verschillende subdoelen komen ook terug in het interview met de ontwikkelaar vanuit NHSV (IO1). Het HackShield project moet volgens de respondent de overheid slimmer maken, mobiliseren en ook innovatiekracht geven. Het einddoel van HackShield moet volgens de respondent zijn dat Nederland cyberveiliger wordt. De ontwikkelaar vanuit Flavour heeft als doel om met HackShield 'de 'security-mindset' te verhogen met kinderen in de hoofdrol zodat we een mooie, veilige digitale toekomst tegemoet gaan waarin alles mogelijk is en waar gevaren die voorkomen kunnen worden, worden voorkomen' (IO2). Met de 'security-mindset' verwijst de respondent naar een bepaalde alertheid: het leren denken als de tegenstander en snel kunnen schakelen zodat je dingen herkent.

De doelgroep & selectie

Uit de documenten en interviews blijkt dat er een duidelijke doelgroep is omschreven voor HackShield: kinderen tussen de 8 en 12 jaar oud (Collegia, 2020; Projectaanvraag, z.d.; IO1; IO2). Deze doelgroep is vastgelegd in projectplannen en wordt meegenomen in de communicatie (IO1). Flavour heeft volgens een respondent voor deze doelgroep gekozen omdat kinderen van deze leeftijd een groot ethisch besef hebben en veel bezig zijn met goed en kwaad en met welke rol zij spelen in de buitenwereld (IO2). Men wil er graag voor zorgen dat vóór de pubertijd bewustwording op het gebied van veilig online gedrag heeft opgetreden, omdat de doelgroep dan nog goed te bereiken is. De respondent geeft verder aan dat er veel informatie is verzameld en onderzoek is gedaan naar de doelgroep. Voorbeelden zijn hoe kinderen met 'devices' omgaan, welke spellen ze spelen en waar ze mee in aanraking komen op school (IO2). In de toekomst wil men wellicht ook andere doelgroepen toevoegen (IO2). Tot nu toe is dit niet gedaan omdat men graag eerst de gehele doelgroep wil bereiken, door heel Nederland en alle lagen van de samenleving. De respondent denkt dat HackShield eerder zal groeien naar hogere leeftijden dan lagere leeftijden. Enerzijds omdat kinderen van 13 of 14 jaar zich gaan oriënteren op de arbeidsmarkt en anderzijds omdat de benadering (met betrekking tot het gebruik van tekst en de interpretatie van digitale middelen) voor kinderen van 8 tot en met 12 jaar beter is te hergebruiken voor een oudere doelgroep dan een jongere doelgroep (IO2).

Op twee manieren kan er (al dan niet automatisch) selectie plaatsvinden binnen HackShield. Ten eerste is er een selectie van wie het spel gaat spelen. Tijdens de interviews merken beide ontwikkelaars op dat er geen criteria zijn om deel te kunnen nemen aan het spel, omdat het spel voor iedereen toegankelijk moet zijn (IO1, IO2). In de praktijk kan er volgens respondenten echter een selectie plaatsvinden, bijvoorbeeld omdat kinderen over een (mobiel) apparaat dienen te beschikken om het spel te spelen (IO1), kinderen van hoger opgeleide ouders sneller het spel zullen spelen omdat deze ouders het belang van een dergelijk project inzien (IO2) en omdat jongens makkelijker mee te krijgen zijn in 'gaming' dan meisjes (IO2). Bij het ontwerp van het spel probeert men hier rekening mee te houden, door bijvoorbeeld de kleuren, karakters en spelvormen te richten op meisjes, zodat jongens en meisjes evenveel vertegenwoordigd zijn (IO2). Ook heeft de promotie van HackShield invloed op wie het spel spelen. In de samenwerking met gemeenten worden filmpjes, posters en flyers verspreid zodat kinderen het spel gaan spelen. Een tweede wijze waarop selectie plaatsvindt is dat de best presterende kinderen in het spel worden gehuldigd door de deelnemende gemeenten (zie paragraaf 4.5 voor meer informatie over de huldiging). Deze selectie vindt automatisch plaats, op basis van het aantal punten dat kinderen verzamelen tijdens het spelen van het spel.

4.4 Onderbouwing

Mogelijke werking

Aan de ontwikkelaars is gevraagd waarom zij verwachten dat het initiatief de eerder genoemde doelen zal bereiken. De ontwikkelaar vanuit Noord-Holland Samen Veilig geeft aan te verwachten dat de geformuleerde doelen worden bereikt vanwege professionaliteit, innovatie, enthousiasme, een moreel doel, idealisme en vertrouwen. Zo is HackShield volgens de respondent een professioneel spel, heeft de ontwikkelaar vanuit Flavour een moreel doel waar de overheid gevoelig voor is en is er vertrouwen tussen deze particuliere organisatie en de overheid. Hoe HackShield bij de doelgroep tot gedragsverandering kan leiden vindt de respondent moeilijk om te bepalen. Wel wordt verwezen naar het ethische besef van de doelgroep en de toegankelijkheid van het spel voor alle kinderen. De ontwikkelaar vanuit Flavour geeft aan dat hij alleen verwacht dat HackShield zoveel enthousiasme opwekt bij mensen, dat mensen vanuit allerlei verschillende perspectieven gaan meehelpen om het te laten slagen (IO2). De respondent benadrukt dat het een bewustwordingscampagne, een bredere beweging is. Beide respondenten verwachten dat HackShield impact maakt op drie doelgroepen: (1) het kind, (2) de volwassenen eromheen en (3) de maatschappij als geheel (IO1, IO2). De maatschappelijke beweging – het activeren van beleid, besluitvorming en private partijen – is het eerste doel (IO2). Wanneer op dat niveau beweging wordt gecreëerd, ontstaan volgens de respondent de financiën, tijd en expertise van anderen om uiteindelijk een goed middel te creëren voor de kinderen:

“ Veel mensen begrijpen dat niet, maar dat is succes. Dus waarom denk ik dat het werkt: omdat we in staat zijn om de hele maatschappij in beweging te krijgen rondom het onderwerp. ” (IO2)

Inhoudelijk gelooft de respondent verder in publieksactivatie, spel-mechanismen, 'immersiviteit' en 'Hero Centred Design' (IO2). Met spel-mechanismen kunnen mensen volgens de respondent worden gemotiveerd om te leren en vol te houden. Met betrekking tot de 'immersiviteit' geeft de respondent aan dat wanneer kinderen worden meegenomen en een mooie rol krijgen in een verhaal dit veel in beweging zet bij de kinderen. Er wordt dan ingespeeld op trots, intrinsieke motivatie en plezier (IO2). In de volgende sectie wordt meer uitgelegd over het 'Hero Centred Design'.

Theorieën en professionele aannames

Uit de documentanalyse blijkt dat HackShield is ontwikkeld aan de hand van 'Hero Centred Design', een design waarbij het publiek een belangrijke maatschappelijke taak toebedeeld krijgt (Collegia, 2020). Het Hero Centred Design is gebaseerd op de overtuiging en ervaring van de makers van HackShield dat publiek pas in beweging komt wanneer zij zelf de hoofdrol spelen in hun eigen verhaal. Dit dient te resulteren in een trans mediale productie: een productie waarbij verhalen zich over verschillende media (spellen, sociale-media en andere platformen) heen bewegen en 'het publiek meeneemt in een multimediale verhaalwereld waar het invloed kan uitoefenen op de uitkomst van het verhaal' (Collegia, 2020). Daarnaast is HackShield volgens de projectaanvraag (z.d.) gebaseerd op 'adversarial thinking', waarbij het verplaatsen in – en anticiperen op – een tegenstander dient bij te dragen aan het verhogen van een 'security mindset'.

Tijdens de interviews met ontwikkelaars is gevraagd op welke theorieën of andere professionele aannames HackShield is gebaseerd. De ontwikkelaar vanuit Noord-Holland Samen Veilig is hier niet precies van op de hoogte en geeft aan dat de andere ontwikkelaar hier meer over weet (IO1). De ontwikkelaar vanuit Flavour benoemt verschillende theoretische invalshoeken en professionele aannames (IO2). Ten eerste is HackShield op (het eerder genoemde) 'adversarial thinking' en 'representational fluency' gebaseerd. Representational fluency verwijst naar de manier waarop mensen leren. Om een mindset te veranderen, moeten hersenen worden geherprogrammeerd door verschillende delen van de hersenen aan te worden gesproken. Bij HackShield wordt daarom geprobeerd om elk onderwerp in tekst, met concrete voorbeelden en in beeld bij een kind aan te bieden (IO2). Ten tweede verwijst de respondent naar het eerder genoemde 'Hero Centred Design', waarin iemand een rol krijgt die diegene in de maatschappij niet heeft, maar wel heeft in die fictieve wereld. Het 'hero-centered-design' heeft de ontwikkelaar bedacht aan de hand van literatuur op het gebied van de kruising tussen 'storytelling' en 'gamification' (Figuur 1). Er is volgens de respondent veel geschreven over hoe gaming en storytelling ingezet kunnen worden om gedragsverandering teweeg te brengen, maar in het midden stond een vraagteken. Daarvan heeft de respondent gezegd: 'de held - het publiek dat de hoofdrol speelt, de eindgebruiker - staat centraal'.



Figuur 1: Hero Centred Design (Collegia, 2020)

De ontwikkelaar zou het 'Hero Centred Design' graag verder willen onderbouwen. Ook zou de respondent de vorm van cross-sectoraal samenwerken graag verder willen onderbouwen, omdat er veel aannames in allerlei sectoren zitten waardoor ze niet samenwerken. Ten slotte zou de respondent uiteindelijk graag precies willen weten wat een kind heeft geleerd nadat hij of zij uit de spel komt (IO2).

Bijhouden werking

Uit de documentanalyse en interviews blijkt dat de werking van het project op dit moment nog niet met behulp van effectevaluaties wordt bijgehouden. Wel houdt men op kwalitatieve wijze de werking op bepaalde punten in de gaten en heeft men ambities om in de toekomst effectevaluaties uit te voeren. In de projectaanvraag (z.d.) wordt namelijk aangegeven dat het niet realistisch is om een effectevaluatie uit te voeren gezien de doorlooptijd en het budget van het project. De interviews geven meer inzicht op welke punten de werking van het initiatief wel wordt bijgehouden. Zo geeft de ontwikkelaar vanuit Noord-Holland Samen Veilig aan dat er periodieke overleggen zijn waar de respondent inzicht krijgt in waar iedereen mee bezig is, of dat nog steeds bijdraagt aan de afspraken en doelen die zijn gemaakt en waar dit toe leidt (IO1). De respondent noemt als voorbeeld het doel 'de overheid slimmer laten functioneren', dat wordt gemonitord door met een werkgroep regelmatig bij elkaar te komen en te kijken wat er is bereikt. Of door HackShield daadwerkelijk cyberveiliger gedrag ontstaat wordt niet bijgehouden omdat er vanuit de overheid niet de capaciteit en expertise is om dit te onderzoeken. Flavour werkt volgens de respondent samen met TNO om effecten te onderzoeken (IO1). De ontwikkelaar vanuit Flavour noemt verschillende manieren waarop de werking van HackShield bij wordt gehouden in relatie tot de eerder genoemde ringen waar men impact op wilt maken.

Zo worden op het gebied van maatschappelijke beweging alle mediaberichten (in kranten en op radio/tv) verzameld om aantoonbaar te maken dat er gebeurtenissen plaatsvinden in de maatschappij. Aan ouders van 'testers'⁴ worden vragen gesteld met betrekking tot de mate waarin kinderen kennis met hen delen. Ten slotte wil men met betrekking tot de kinderen graag een nulmeting in het spel verwerken om te kijken of bepaalde competenties worden gehaald.

Uit de interviews blijkt verder dat HackShield continue wordt getest en geëvalueerd (IO1, IO2).

Onderdelen van het spel worden voordat ze openbaar worden gemaakt getest door mensen die betrokken zijn bij de ontwikkeling en een aantal kinderen (de meest fanatieke HackShield spelers). Ten slotte kijken ook externe partners mee: (security-) bedrijven doen suggesties of geven aan dat dingen niet kloppen en er zijn weleens ouders die bellen. De punten worden dan vaak meegenomen en aangepast. Aanpassingen vinden zowel inhoudelijk plaats, wanneer de uitleg niet klopt, als qua niveau, door ingewikkelde termen uit te leggen (IO2).

4.5 Inhoud project

Uit de documentanalyse en interviews met ontwikkelaars blijkt dat het initiatief 'HackShield in gemeenten Noord-Holland' uit grofweg drie verschillende onderdelen bestaat: een promotiecampagne, de spelperiode en een huldiging. Gemeenten die deelnemen aan het initiatief starten met een promotiecampagne waarin de doelgroep wordt opgeroepen om het spel HackShield te spelen. Vervolgens is er een spelperiode waarin de kinderen het spel spelen. De best presterende kinderen worden ten slotte gehuldigd door hun gemeente. Zoals eerder opgemerkt door een van de ontwikkelaars bestaat HackShield als bredere beweging echter niet alleen uit een spel of deze statische vorm van een promotiecampagne en huldiging. Desondanks worden in het kader van het onderzoek de drie eerder genoemde onderdelen verder toegelicht.

De promotiecampagne

Uit de projectaanvraag blijkt dat kinderen eerst door de burgemeester en/of de politie van de desbetreffende gemeente worden opgeroepen om het spel HackShield te spelen (Projectaanvraag, z.d.). De oproep vindt plaats via een digitaal filmpje dat online wordt verspreid. De campagne wordt verder ondersteund met een 'communicatietoolkit' die beschikbaar is voor gemeenten en bestaat uit communicatiemiddelen zoals posters, flyers en persberichten. Wanneer kinderen beginnen

met het spelen van het spel kunnen ze hun gemeente opgeven en aangeven of ze 'Junior Cyber Agent' willen worden (IO2).

Het spel

Het spel 'HackShield Future Cyber Heroes' wordt omschreven als een 'cross platform' spel dat kan worden gespeeld op drie verschillende platformen: een mobiele telefoon, een tablet en een computer/laptop (Collegia, 2020). Het spel bestaat uit 3 uur spel materiaal waarin kinderen door fictieve karakters worden meegenomen in een avontuur waarin ze een gezamenlijke vijand moeten verslaan (IO2). De fictieve karakters vertegenwoordigen allemaal een ander thema en helpen de kinderen bij een specifiek onderwerp. Tijdens het spel kunnen de kinderen Shields verdienen die een stuk kennis of een vaardigheid vertegenwoordigen die de speler heeft verworven (Collegia, 2020). Het spel bestaat uit drie onderdelen: levels, quests en een levelmaker (Collegia, 2020; IO2).

Levels – Kinderen die het spel spelen kunnen levels voltooien door vragen te beantwoorden en beveiligingspuzzels op te lossen (Collegia, 2020). De levels zijn onderverdeeld in verschillende 'episodes' over bijvoorbeeld data, hoe hackers data gebruiken en digitaal geld. Tijdens de levels leren kinderen vooruitdenken en te denken als de 'bad-guy'. Voor ieder level dat kinderen uitspelen verdienen zij punten.

'Quests' – 'Quests' worden omschreven als kleine lessen waarin karakters kinderen meenemen in een nieuw thema omtrent online veiligheid (Collegia, 2020). De ontwikkelaar vertelt dat deze opdrachten zijn gemaakt om kinderen interactie aan te laten gaan met hun omgeving (IO2). Er is bijvoorbeeld een 'wachtwoorden-quest' waarbij kinderen zelf een wachtwoord invoeren en hen wordt verteld hoe lang het ongeveer duurt om dit wachtwoord te hacken, zodat een kind leert wat veilig is en wat niet. Vervolgens wordt ook gevraagd aan de kinderen om naar hun ouders te gaan en hun ouders hetzelfde te laten doen.

Levelmaker – In de levelmaker kunnen kinderen zelf levels maken met behulp van bouwstenen die zij verdienen tijdens de eerdergenoemde 'levels' en 'quests' (Collegia, 2020). Doordat kinderen zelf levels kunnen maken is er altijd nieuwe content voor de kinderen (IO2). Ook kunnen de kinderen met de levelmaker punten en 'Shields' verdienen. Ten tijde van het interview met de ontwikkelaar was de levelmaker nog niet actief.

De ontwikkelaars benadrukken dat het spel continue wordt aangepast en dat er steeds nieuwe opdrachten, levels en onderdelen aan het spel worden toegevoegd (IO1, IO2).

⁴ Test-spelers zijn kinderen die alle levels van het spel uitgespeeld hebben en aangeven dat ze tester willen worden om het spel te verbeteren.

De huldiging

De lokale 'topspelers' van het spel komen in een scorelijst terecht (Collegia, 2020). Op het moment dat de gemeente deze topspelers positieve aandacht wil geven door middel van een huldiging, dan wordt er vanuit het 'back-end' systeem in het spel een bericht opgesteld en verstuurd naar alle kinderen die in de top-5 of top-10 staan van een bepaalde gemeente (IO2). Hierin staat dat de speler geselecteerd is voor een huldiging. Hetzelfde bericht wordt ook verstuurd naar alle ouders (via een geverifieerde e-mailaccount) van de kinderen voor toestemming voor de huldiging. Een van de ontwikkelaars geeft aan dat de borging en uitvoering van de huldiging per gemeente uiteindelijk kan verschillen (IO2).

Instructies voor gemeenten

Vanuit HackShield worden alle deelnemende gemeenten enerzijds ondersteund door middel van een nieuwsbrief met updates die twee a drie wekelijks wordt verspreid en anderzijds met instructies en tips op het platform 'Collegia' (Collegia, 2020). Op dit platform is specifieke informatie weergegeven die gemeenten nodig hebben om HackShield te kunnen implementeren. Het volgende 7-stappenplan wordt hierbij aan de gemeenten aangereikt:

1. *Een projectgroep samenstellen* - Gemeenten wordt geadviseerd om een projectgroep samen te stellen met verschillende partijen die een bijdrage kunnen leveren aan HackShield.
2. *Kaders en opbouw* - In een eerste overleg worden kaders van het project neergezet en tips gegeven omtrent de promotie, planning en interne communicatie van het project binnen de gemeente.
3. *Monitoring kick-off, start communicatie* - Deze stap betreft het opstarten van de externe communicatie campagne.
4. *Kick-off* - Tijdens deze stap gaat de externe communicatie campagne van start en wordt informatie gegeven omtrent de huldiging.
5. *Monitoring en planning huldiging* - Op basis van informatie die men verzameld over het aantal spelers wordt in deze stap eventueel bijgestuurd op de externe communicatie campagne. Daarnaast wordt de huldiging gepland.
6. *Huldiging* - De rollen van de gemeenten en HackShield tijdens de huldiging worden in deze stap beschreven.
7. *Eindevaluatie* - De laatste stap bestaat uit een evaluatie met de gemeenten en HackShield om van het project te leren.

4.6 Samenwerkingspartners

Het blijkt dat er verschillende publieke en private partijen betrokken zijn bij HackShield. Eerder is gebleken dat er onderscheid gemaakt kan worden tussen samenwerkingspartners die betrokken zijn bij het initiatief 'HackShield in de gemeenten' en partners die betrokken zijn bij HackShield als spel of beweging (zie paragraaf 4.3). Gezien de focus van het huidige onderzoek staat in deze paragraaf de samenwerking

omtrent het initiatief 'HackShield in de gemeenten' centraal. Op basis van de documenten en interviews kunnen de volgende belangrijkste partijen worden aangemerkt:

- Gemeenten
- Politie
- Flavour/HackShield & NHSV

De gemeenten en politie pelen een rol bij de promotie van HackShield en huldiging van deelnemers, zoals eerder benoemd in paragraaf 4.5. Vanuit de gemeenten zijn verschillende afdelingen en directies betrokken zoals openbare orde en veiligheid, communicatie, onderwijs en jeugd. Vanuit de politie is de politie-eenheid Noord Holland betrokken met aangesloten basisteams. Flavour/HackShield is betrokken bij de ontwikkeling van het spel dat door de deelnemers wordt gespeeld en NHSV bij de ontwikkeling van de pilots met gemeenten. Andere partijen die worden genoemd zijn betrokken bij de promotie van HackShield binnen gemeenten, zoals bibliotheken, scholen, sportclubs en kinderdagverblijven. Ten slotte worden ook partijen genoemd die betrokken zijn bij subsidieaanvragen, zoals het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), de Vereniging van Nederlandse Gemeenten (VNG) en andere regionale samenwerkingspartners.

Uit de interviews blijkt dat er met de samenwerkingspartners schriftelijk afspraken zijn vastgelegd in een subsidieaanvraag van het CCV, die loopt tot en met het eerste kwartaal van 2021. Met gemeenten die meedoen zijn concrete afspraken gemaakt dat zij capaciteit leveren, soms financiële middelen leveren op kleine onderdelen en dat zij bestuurlijk/ambtelijk commitment tonen. Verder zijn er weinig tot geen schriftelijke afspraken en zijn er geen afspraken op papier over de invulling van HackShield en de rol die samenwerkingspartners hebben.

De kwaliteit van de samenwerking met de partners wordt door de ontwikkelaar vanuit NHSV als goed, kritisch en 'scherp op elkaar' omschreven (IO1). Een eerste genoemde verklaring hiervoor is het enthousiasme en intrinsiek geloven in het concept. Waar de overheid volgens de respondent nogal eens enthousiasme en power mist bij het aanpakken van maatschappelijke veiligheidspunten, ziet de respondent dit enthousiasme juist wel bij de gemeenten die aan de HackShield pilots meedoen. Een tweede verklaring die wordt gegeven is het lef dat de partijen zoals de gemeenten durven te hebben op tonen. Ten slotte heeft de ontwikkelaar vanuit HackShield een belangrijke rol in de goede samenwerking:

“ Hij zorgt ervoor dat mensen gaan geloven, energie voelen, echtheid voelen, waardoor men zegt: dit zou wel eens wat kunnen zijn. Dat zorgt ervoor dat iets gaat werken. ” (IO1)

De kracht van het samenwerken tussen HackShield en de overheid ligt volgens de respondent in HackShield niet teveel te beperken door dingen op papier te zetten en teveel afspraken te maken. Dit gaat volgens de respondent ten koste van de snelheid, het enthousiasme en het effect:

“ En ik heb gedacht: jongens, we pakken dit gewoon op als overheid. En laat dit maar gaan bloeien. Natuurlijk stuur ik wel in de zijlijnen bij, en dat zit hem vooral in de gesprekken en het wijzen op de afspraken die we formeel hebben in het kader van de subsidieaanvraag met het CCV. Maar ik denk dat het voor elk innovatief traject de dood in de pot is om daarin alles te gaan zitten beschrijven. ” [IO1]

De samenwerking zou volgens de respondent verbeterd kunnen worden door nog meer commitment, ook formeel op papier. Dat veel vanuit innovatie gaat en niet alles wordt vastgelegd is volgens de respondent een kracht, maar om concepten die innovatief getest zijn uiteindelijk duurzaam te kunnen verankeren binnen een overheid moeten uiteindelijk formele afspraken op papier komen (IO1).

4.7 Resumé

Op basis van documenten en interviews met ontwikkelaars is duidelijk geworden wat het initiatief 'HackShield in gemeenten Noord-Holland' is en hoe dit initiatief is onderbouwd. De aanleiding voor het initiatief is dat er vanuit zowel de publieke sector (regionaal samenwerkingsverband Noord-Holland Samen Veilig) als private sector (de initiatiefnemer van Flavour) de behoefte is om bij te dragen aan digitale weerbaarheid. In de betekenis van HackShield lijkt er een onderscheid gemaakt te kunnen worden in HackShield als 'cybersecurity'-spel, HackShield als project met gemeenten en HackShield als een grotere beweging die ook bestaat uit andere onderdelen zoals een kaartspel en een digitale omgeving voor gemeenten. De doelgroep van HackShield zijn kinderen tussen de 8 en 12 jaar en het doel is om deze kinderen en Nederland als geheel cyberveiliger en cyberweerbaar te maken.

De ontwikkelaars verwachten met het project impact te maken op drie doelgroepen (1) kinderen, (2) de volwassenen eromheen en (3) de maatschappij als geheel. Verwacht wordt dat het project werkt omdat men in staat is om de hele maatschappij rondom het onderwerp in beweging te krijgen. Inhoudelijk wordt verwacht dat publieksactivatie, spel-mechanismen, immersiviteit en het 'Hero-centred-design' bijdragen aan de cyberweerbaarheid. Het 'Hero-centred-design' is de filosofie van de makers van het spel waarin de eindgebruiker centraal wordt gesteld en een (fictieve) rol krijgt die de gebruiker niet heeft in de echte wereld. Deze filosofie is gebaseerd op literatuur over 'storytelling', 'gamification' en 'problem solving'. De daadwerkelijke werking en effecten van het spel op de cyberweerbaarheid worden op dit moment niet bijgehouden. Wel probeert men op kwalitatieve wijze bij te houden hoe impact wordt gemaakt op de maatschappij door media-momenten te verzamelen en hoe impact wordt gemaakt op ouders door vragen aan ouders van testers te stellen. Het spel HackShield wordt steeds getest en geëvalueerd met behulp van de feedback van kinderen die het spel testen en andere betrokkenen.

Het initiatief 'HackShield in gemeenten Noord-Holland' bestaat uit grofweg drie onderdelen: een promotiecampagne, een spelperiode en een huldiging. Tijdens de promotiecampagne roepen burgemeesters en politiemedewerkers van eenheden binnen gemeenten kinderen op om HackShield te spelen en zich als 'cyber-agent' aan te sluiten bij de desbetreffende gemeente. Vervolgens spelen de kinderen het spel dat bestaat uit verschillende levels, opdrachten en een levelmaker. De spelers die de meeste punten hebben verzameld tijdens een bepaalde periode worden uiteindelijk gehuldigd door hun gemeente.

De belangrijkste partners die betrokken zijn bij de uitvoering van het initiatief zijn de deelnemende gemeenten, politie en HackShield/NHSV als ontwikkelaars van de pilot. Schriftelijke afspraken zijn vastgelegd in een subsidieaanvraag van het Centrum voor Criminaliteitspreventie en Veiligheid (CCV), welke loopt tot het eerste kwartaal van 2021. Verder zijn er weinig tot geen schriftelijke afspraken over de invulling van HackShield en de rol die samenwerkingspartners hebben.

5 De uitvoering van HackShield

5.1 Inleiding

In dit hoofdstuk staat de wijze waarop HackShield is uitgevoerd binnen de vier geselecteerde gemeenten centraal. Zo wordt duidelijk wat verschillen en overeenkomsten zijn tussen de deelnemende gemeenten. In de opeenvolgende paragrafen wordt de uitvoering binnen gemeente A (paragraaf 5.1), gemeente B (paragraaf 5.2), gemeente C (paragraaf 5.3) en gemeente D (paragraaf 5.4) besproken. Onderwerpen die aan bod komen zijn het tijdsverloop, de invulling van het project en de samenwerking met interne en externe actoren. De resultaten zijn gebaseerd op de interviews met medewerkers van de gemeenten en de politie. In paragraaf 5.5 wordt ten slotte ingegaan op de selectie en het bereik van de doelgroep in de geselecteerde gemeenten. Deze resultaten zijn gebaseerd op basis van interviews met medewerkers van de gemeenten, een interview met de communicatie-manager van HackShield en cijfers vanuit HackShield.

5.2 Casus 1: gemeente A

Tijdsverloop

De projectperiode is september 2020 begonnen en eindigde met de huldiging begin december 2020. De medewerker vanuit de gemeente is tevreden met deze duur, omdat het zo enerzijds voor kinderen nog te overzien was wanneer de huldiging zou plaatsvinden en zij dus punten moesten hebben en anderzijds de respondent voldoende tijd had om de kinderen te bereiken (GM1).

Invulling project

Voor de promotie van HackShield is er in gemeente A een promotiefilmpje gemaakt met de burgemeester en wijkagent om kinderen op te roepen HackShield te spelen. De volgende communicatiekanalen heeft de respondent tijdens het project ingezet:

- Sociale media kanalen van de gemeente (Facebook, Instagram en Twitter) zijn gebruikt om het opgenomen filmpje te verspreiden en kinderen op te roepen om HackShield te spelen.
- De wijkagent, politie en jongerenwerk is verzocht om oproepen te delen. Dit is niet bij ieder bericht gebeurt maar wel bij een aantal berichten.
- Scholen zijn gemaïld en gevraagd of ze flyers en posters over HackShield wilden verspreiden.

Met betrekking tot de huldiging zijn buitengewoon opsporingsambtenaren (BOA's) langsgegaan bij de nummers 2 tot en met 5 om hen te feliciteren en 'gadgets' en een certificaat te geven. De nummer 1 is gehuldigd via een digitale huldiging met de burgemeester en wijkagent. De digitale huldiging heeft ongeveer 20 minuten geduurd.

Uitvoering zoals beoogd?

De respondent geeft aan vooraf duidelijke informatie en instructies te hebben gehad. Enerzijds heeft de respondent via Collegia toegang gekregen tot alle communicatie informatie en ervaringen en werkwijzen van andere gemeenten, anderzijds was er om de drie weken een overleg met alle gemeenten die waren aangesloten waarin de planning en vragen werden besproken. In gemeente A heeft men volgens de respondent het project redelijk uitgevoerd zoals was aangegeven. De respondent denkt dat het project wel is uitgevoerd zoals van te voren bedacht, maar heeft niet vooraf helemaal bedacht hoe het zou lopen. Vanuit HackShield en NHSV stond men open voor andere ideeën en suggesties. Er werd niet gezegd 'dit is wat het is en zo moet het', zoals blijkt uit het volgende citaat over hoe men communiceerde over het vormgeven van persberichten:

“Joh, dit is een voorbeeld, doe er je voordeel mee. Als je je eigen bericht wil schrijven, dat kan ook.” (GM1)

Samenwerking

Bij de uitvoering van het project zijn verschillende interne en externe partijen betrokken geweest bij de uitvoering van het project door gemeente A:

- Team openbare orde en veiligheid (intern)
- Afdeling communicatie (intern)
- Een collega voor contact met scholen (intern)
- Politie (extern)
- HackShield (extern)
- Scholen (extern)
- Jongerenwerk (extern)

De samenwerking met deze partijen is niet schriftelijk vastgelegd en er zijn geen afspraken geweest omtrent het aantal uren aan mankracht. De respondent geeft aan dat dergelijke projecten 'gewoon samen worden opgepakt'. De samenwerking met HackShield en de politie ging volgens de respondent erg gemakkelijk omdat er korte lijntjes waren. Bij de scholen ging dit moeizamer omdat de respondent normaal geen contact heeft met de scholen (GM1).

5.3 Casus 2: gemeente B

Tijdsverloop

Het project heeft voor gemeente B ruim 3 maanden geduurd: in september 2020 was de start van het project en de huldiging was begin december 2020. De duur was voor de respondent precies goed, omdat de respondent merkte dat gedurende het project het aantal deelnemers omhoog ging.

Invulling project

De promotie van HackShield heeft binnen gemeente B op verschillende manieren plaatsgevonden:

- Sociale media kanalen van de gemeente zijn gebruikt om oproepen te verspreiden om deel te nemen.
- In een 'krantje' van de gemeente is een oproep geplaatst.
- Scholen zijn gebeld en gemaaild of zij bij wilden dragen aan het project door een video te laten zien, flyers uit te delen en posters op te hangen.
- De politie heeft via een mobiel media lab⁵ HackShield gepromoot door in de vrachtauto een filmpje te laten zien met de oproep om het spel te spelen en flyers uit te delen.
- Jongerenwerkers zijn benaderd en hebben wekelijks met de doelgroep het spel gespeeld in klasjes.

Voor de huldiging is de respondent samen met de burgemeester en politie langsgesegaan bij de kinderen op hun school zodat de kinderen in de klas werden gehuldigd. Tijdens de huldiging heeft de burgemeester de kinderen gehuldigd, zijn spullen zoals cakejes, certificaten en badges uitgedeeld en konden kinderen vragen stellen aan de politie en burgemeester. Twee scholen zijn bezocht, waardoor de nummers 1 tot en met 4 konden worden gehuldigd. De huldiging heeft in totaal ongeveer 30 minuten geduurd.

Uitvoering zoals beoogd?

De respondent van de gemeente geeft aan dat er vooraf informatie en instructies waren. Tijdens overleggen werd aangegeven dat er verschillende opties waren voor bijvoorbeeld communicatiemateriaal, de manier waarop mensen benaderd konden worden en de wijze waarop de huldiging kon worden georganiseerd. Er werden vaak verschillende 'smaken' aangeboden en dan kon de gemeente zelf kiezen. De respondent geeft aan twee keer heel iets anders te hebben gekozen, wat ook prima was. De uitvoering is verder verlopen zoals gepland, alleen de huldiging werd bij de scholen uitgevoerd in plaats van bij de burgemeester op het stadshuis.

Samenwerking

Tijdens de uitvoering van het project in gemeente B zijn verschillende interne en externe partijen betrokken geweest:

- Afdeling communicatie (intern)
- Afdeling jeugd (intern)
- Burgemeester (intern)
- Politie (extern)
- Scholen (extern)

De samenwerking met deze partijen is niet schriftelijk vastgelegd, wel worden er informele afspraken gemaakt. Voorbeelden zijn dat de politie het filmpje laat zien in het mobiele media lab en dat jongerenwerkers oproepen uitzetten bij jeugdgroepen die zij begeleiden. De samenwerking met de verschillende partners wordt door de respondent als 'heel goed' en 'heel soepel' omschreven. Dit komt volgens de respondent omdat de partners het een leuk project vonden en omdat er niet heel veel van hen wordt gevraagd.

5.4 Casus 3: gemeente C

Tijdsverloop

Voor gemeente C begon de samenwerking met het opzoeken van partners in juli 2020 en duurde de projectperiode net als in de andere gemeenten van september 2020 tot en met begin december 2020. De duur was voor de respondent precies goed, ook omdat er speciale themaweken bij waren zoals de Week van de Veiligheid en de Week van de Mediawijsheid waar het project aan werd opgehangen. Het had niet langer moeten duren volgens de respondent omdat er op een gegeven moment een verzadigingspunt wordt bereikt in het aantal kinderen dat zich aanmeldt.

Invulling project

De communicatie heeft in gemeente C via de volgende kanalen plaatsgevonden:

- Op het Facebook-account van de gemeente zijn oproepen geplaatst en een oproep-video waarin de burgemeester en een hoofdagent van de politie wat hadden ingesproken.
- Naar alle scholen in gemeente C (iets meer dan 50) zijn posters gestuurd met een begeleidende brief van de locoburgemeester. Ook kregen de scholen een e-mail waarin het project was aangekondigd.
- Bij jongerencentra bij de wijkteams zijn posters bezorgd.
- Vanuit de politie heeft men op social media oproepen gedeeld en heeft het mobiel media lab HackShield onder de aandacht gebracht door in een gedeelte van de wijk bij een basisschool te gaan staan en kinderen HackShield te laten spelen.
- De respondent en hoofdagent van de politie zijn beiden een keer op de lokale radio geweest.

5 Het Mobiel Media Lab is een vrachtauto die door Nederland rijdt en waarmee de politie op een laagdrempelige manier communicatiemiddelen test (Politie, 2021).

De huldiging in gemeente C heeft digitaal plaatsgevonden. Hierbij waren de burgemeester en twee personen vanuit de politie aanwezig. Tijdens de huldiging werd eerst het oproep-filmpje nogmaals laten zien en vervolgens sprak de burgemeester de kinderen toe en gingen ze nog in gesprek over wat ze hebben geleerd. Op de dag van de huldiging is ook de politie fysiek langs de kinderen gegaan met een 'goodie-pakket' met een shirt, pet, bol.com kaart etc. In totaal zijn 5 'cyber-agents' gehuldigd en de huldiging duurde maximaal 30 minuten.

Uitvoering zoals beoogd?

De medewerker van gemeente C heeft informatie en instructies gehad. Er zijn bijeenkomsten geweest met de regionale projectleider waarin uitleg werd gegeven over bijvoorbeeld activiteiten die uitgevoerd moesten worden en deadlines. Hierin kon iedereen volgens de respondent in principe zijn of haar eigen pad volgen. Een voorbeeld is dat er bij de Week van de Mediawijsheid op de start en aan het eind van de week een bericht zou worden geplaatst. De respondent heeft het laatste bericht niet geplaatst omdat de mensen die de pagina volgen er dan mee overspoeld zouden worden. Er was van te voren een planning vanuit HackShield en daar is aan voldaan, er waren geen onverwachte afwijkingen volgens de respondent. Wel werd gehoopt dat er misschien fysiek gehuldigd kon worden, maar dat was niet het geval door de corona-maatregelen.

Samenwerking

De volgende interne en externe partijen zijn bij gemeente C betrokken geweest bij de uitvoering van het project:

- Een collega van de afdeling communicatie (intern)
- De woordvoerder van de burgemeester (intern)
- Collega's bij de afdeling openbare orde en veiligheid (intern)
- Politie (extern)
- Scholen (extern)
- De lokale Rabobank (extern)

De samenwerking en afspraken met de verschillende samenwerkingspartners zijn niet op papier gezet maar informeel geweest. De samenwerking is volgens de respondent zowel intern als extern 'zeer goed verlopen', mede door het enthousiasme voor het project en omdat er vanuit de communicatie afdeling goed werd meegedacht. Alhoewel het bij de start van het project de bedoeling was om een samenwerking met de lokale Rabobank aan te gaan, blijkt dat in de praktijk alleen een bijdrage is geweest in de vorm van 'gadgets' voor de kinderen tijdens de huldiging. Volgens de respondent komt dit doorat niet helemaal duidelijk was hoe de samenwerking vorm had moeten krijgen.

5.5 Casus 4: gemeente D

Tijdsverloop

Het project heeft voor gemeente D een paar maanden geduurd: het begon in september 2020 en de huldiging was in december 2020. De projectperiode vond de respondent precies goed, omdat er dan tijd is om dingen te regelen en plannen.

Invulling project

Voor de communicatie van HackShield zijn de volgende kanalen gebruikt binnen gemeente D:

- Sociale media zoals de Facebook van de gemeente om oproepen te delen.
- Op een website van de gemeente is het project gepromoot.
- De blog van de burgemeester is gebruikt om over het project te communiceren.
- De politie is benaderd om oproepen te delen.
- Scholen (tussen de 50 en 70) zijn aangeschreven middels een mail en brief met het verzoek om flyers en posters op te hangen.
- Jongerencentra zijn gemaïld en hebben flyers en posters gekregen om op te hangen.

Er heeft een digitale huldiging plaatsgevonden vanuit gemeente D. Tijdens de huldiging waren de burgemeester, de teamchef van de politie en een gespreksleider aanwezig. Zij sloten net als de respondent digitaal aan bij de huldiging. De burgemeester heeft certificaten digitaal uitgereikt en die zijn later bij de kinderen thuisgebracht. Gadgets en spullen heeft de respondent zelf een dag van tevoren bij de kinderen langsgebracht. De digitale huldiging heeft ongeveer 20 minuten geduurd.

Uitvoering zoals beoogd?

De respondent heeft vooraf informatie en instructies gekregen. Zo was er toegang tot Collegia, daar stond in principe alles op en waar de respondent er zelf niet uit kwam konden projectleiders worden benaderd. Ook waren er bijeenkomsten met een projectgroep. Verder heeft de respondent altijd de ruimte gevoeld om eigen initiatieven te nemen en lokale invullingen en ideeën op te brengen. Er zijn geen grote aanpassingen geweest ten opzichte van het 'draaiboek'. Wel waren er ideeën zoals de handhaving langs de deur laten gaan maar dat ging dan niet door. Veel van de ideeën kwamen uiteindelijk niet van de grond omdat de respondent zelf de tijd niet had of omdat er elders geen capaciteit was.

Samenwerking

Vanuit gemeente D is er met de volgende interne en externe partners samengewerkt:

- Afdeling communicatie (intern)
- Afdeling jeugd (intern)
- Burgemeester (intern)
- Politie (extern)
- Scholen (extern)
- Jongerenwerk (extern)

De samenwerking met partners is niet schriftelijk vastgelegd. De respondent begreep wel dat er vanuit de regio bepaalde afspraken zijn gemaakt met de politie in de regio over dat zij zich zouden committeren aan het project en hun bijdrage zouden leveren. De samenwerking met de politie wordt door de respondent als matig omschreven, omdat zij moeilijk betrokken te krijgen waren. Uiteindelijk heeft men gedaan wat was afgesproken, maar de respondent merkte weinig initiatief en betrokkenheid. De kwaliteit van de samenwerking met overige partners is niet besproken tijdens het interview.

5.6 Selectie en bereik van deelnemers

Uit de interviews met uitvoerders en de communicatieadviseur van HackShield blijkt dat er op twee manieren een vorm van selectie van deelnemers plaatsvindt. Ten eerste zijn er de kinderen die HackShield gaan spelen en hun gemeente hierbij opgeven. Dit worden de 'cyber-agents' van de gemeente genoemd. Een tweede vorm van selectie vindt plaats doordat de beste 'cyber-agents' per gemeente worden gehuldigd. De wijze waarop de twee vormen van selectie hebben plaatsgevonden en hoeveelheid deelnemers die zijn bereikt worden nu besproken op basis van het interview met de communicatieadviseur van HackShield en cijfers over het aantal 'cyber-agents'.⁶

Selectie cyber-agents

Op het moment dat kinderen HackShield gaan spelen en hun gemeente invullen worden zij 'cyber-agent' van de desbetreffende gemeente. Het kan zijn dat spelers die in de gemeente het spel hebben gespeeld geen gemeente hebben ingevuld (COM1). Het daadwerkelijke aantal kinderen dat het spel heeft gespeeld kan daardoor hoger liggen. Het aantal 'cyber-agents' dat de geselecteerde gemeenten hebben bereikt tijdens de projectperiode is weergegeven in tabel 3.

Tabel 3: aantal cyber-agents per geselecteerde gemeente

	Aantal cyber-agents ⁷	Aantal kinderen 8 t/m 12 jaar ⁸	% bereikt
Gemeente A	44	2644	1,66%
Gemeente B	74	796	9,30%
Gemeente C	201	8670	2,32%
Gemeente D	306	9807	3,12%

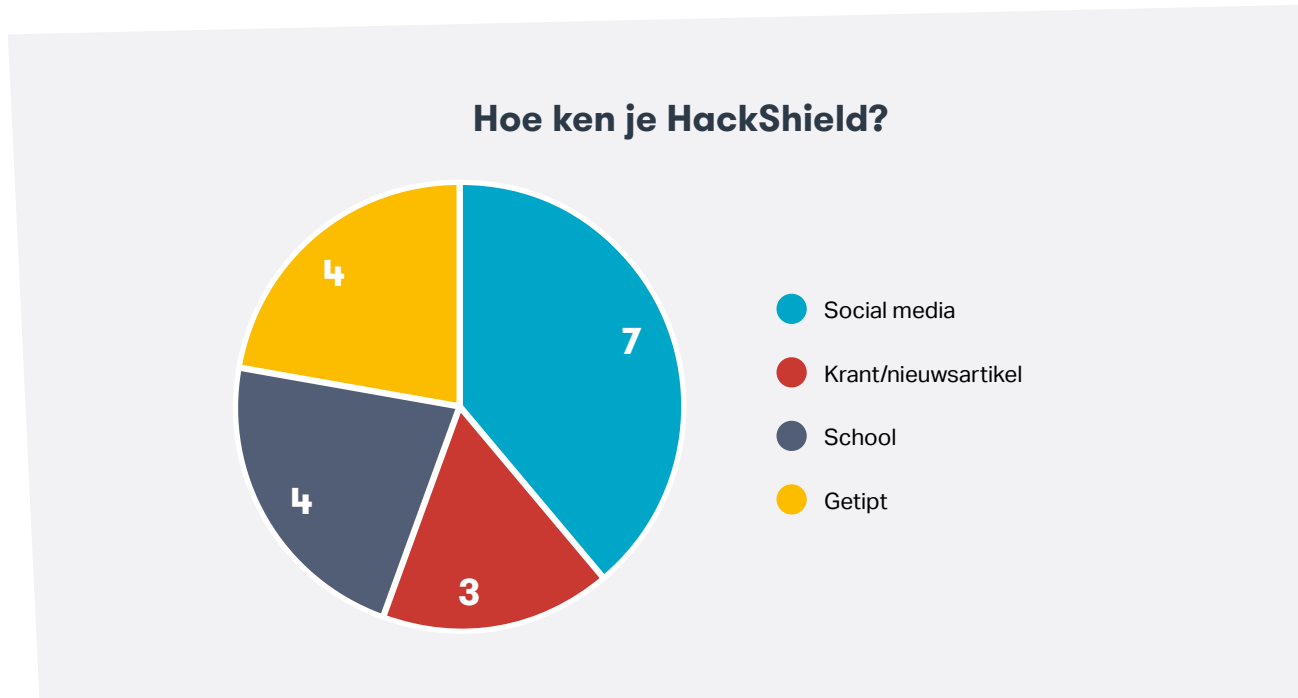
Aan uitvoerders in de desbetreffende gemeenten is gevraagd wat zij vinden van het aantal 'cyber-agents' dat is bereikt. In gemeente A vindt de respondent het aantal 'op zich redelijk weinig', maar vergeleken met andere kleine gemeenten noemt de respondent het 'gemiddeld' (GM1). Het aantal had volgens de respondent hoger kunnen zijn als er meer aandacht bij scholen was besteed aan HackShield. In gemeente B vindt de medewerker van de gemeente het aantal 'cyber-agents' een succes, omdat het een klein dorp betreft met een groot bereik (GM2). Een verklaring voor het hoge aantal ligt volgens de respondent in de inzet die op het project is gepleegd en de verschillende kanalen die zijn gebruikt voor de promotie. Vanuit gemeente C is de medewerker van de gemeente tevreden met het aantal kinderen dat is bereikt, omdat de respondent de cijfers heeft bekeken en vergeleken met andere gemeenten (GM3). Een verklaring voor het goede bereik vindt de respondent lastig om te geven. Ten slotte vindt de medewerker vanuit gemeente D dat gezien de grootte van de gemeente en het aantal kinderen dat de gemeente heeft er 'heel weinig kinderen' zijn die de game hebben gespeeld (GM4). Een verklaring voor het lage aantal 'cyber-agents' ligt volgens de respondent mogelijk in de samenwerking, omdat niet iedereen het project als een even grote prioriteit heeft gezien.

Aan de deelnemers die zijn geïnterviewd is gevraagd hoe zij erop kwamen om HackShield te gaan spelen (figuur 3). Uit de antwoorden blijkt dat zij HackShield hebben leren kennen door een bericht op social media (n=7), via iemand die het al speelde (n=4), via school (n=4) of door een nieuwsartikel in de (lokale) krant (n=3). Wanneer het gaat over de promotie van HackShield geven twee respondenten aan dat er weinig ruchtbaarheid aan het spel wordt gegeven. Meer kinderen kunnen worden bereikt door het spel te promoten op basisscholen.

6 Vanuit HackShield is een overzicht aangeleverd van het aantal cyber-agents dat zich heeft geregistreerd tijdens de projectperiode.

7 Aantal cyber-agents geregistreerd door HackShield op 30 november 2020.

8 Op basis van data over inwoneraantallen op 1 januari 2020 (CBS, 2020b).



Figuur 1: wijze waarop deelnemers van HackShield hebben vernomen (n=18)

De kinderen zelf spreken ook regelmatig over HackShield (n=17). Ze hebben het er vooral over op school (n=12), met familie (n=10), met vrienden (n=9) en thuis (n=6). Ook geven negen respondenten aan dat er andere kinderen HackShield zijn gaan spelen omdat zij het spelen van HackShield hebben aanbevolen.

Selectie huldigen

De selectie van de spelers die vervolgens worden gehuldigd is gebaseerd op het aantal punten dat is behaald tijdens het spelen van het spel (zie paragraaf 4.5). Met de gemeenten is een einddatum afgesproken waarop de competitie "op slot" gaat en de huldigen worden voorbereid. Een week voordat de competitie sluit wordt er een 'inbox-bericht' gestuurd naar de spelers van gemeenten dat er nog een week is om punten te verzamelen en dat er een geverifieerd e-mailadres in het profiel moet zijn toegevoegd. Een geverifieerd e-mailadres door een ouder is een voorwaarde om gehuldigd te worden, omdat ouders toestemming moeten geven voor de huldiging. Als spelers geen geverifieerd e-mailadres hebben en er geen contact kan worden opgenomen met ouders, dan kunnen spelers niet gehuldigd worden en wordt de volgende speler op de ranglijst gehuldigd (COM1). De respondent geeft aan dat er

een aantal spelers was met niet-geverifieerde e-mailaccounts, waardoor de spelers niet konden worden bereikt voor de huldiging. Mogelijke verklaringen die de respondent hiervoor kan bedenken zijn dat veel accounts wellicht zijn aangemaakt in de klas en dat juffen of meesters hebben geadviseerd om geen e-mailadres op te geven of dat ouders zich niet voor iets dergelijks willen inschrijven.

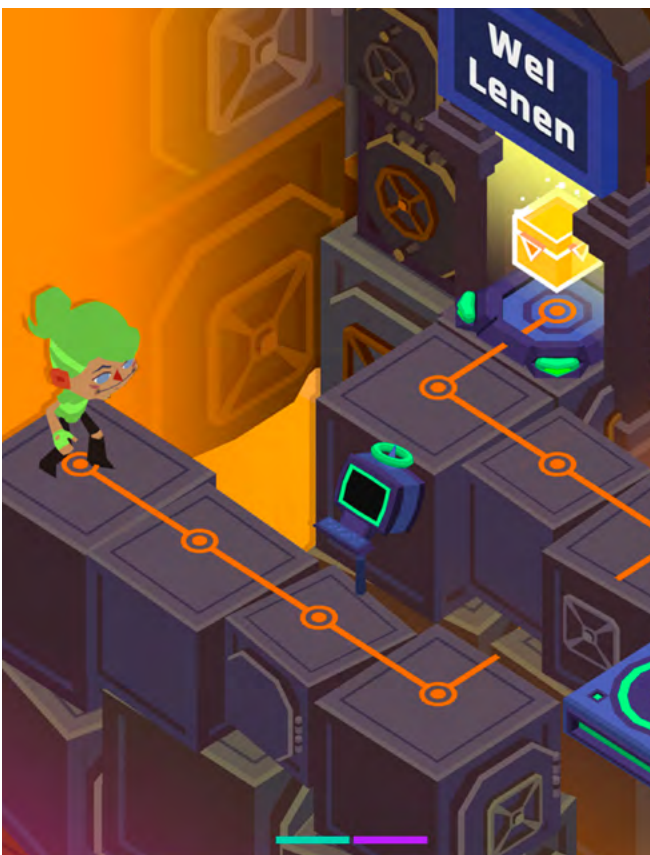
Het aantal kinderen dat uiteindelijk wordt gehuldigd door de gemeente bepalen gemeenten zelf (COM1). HackShield adviseert om 3 kinderen te huldigen, zodat er genoeg aandacht gegeven kan worden aan iedere speler en iedereen voldoende aan het woord komt. Sommige gemeenten vonden het leuk om meer spelers te huldigen of extra prijzenpakketten weg te geven, maar dat is aan de gemeente zelf (COM1). Gemeente A heeft 5 'cyber-agents' gehuldigd, waarvan 1 kind virtueel en 4 kinderen die een prijzenpakket hebben gekregen. In gemeente B zijn uiteindelijk 6 'cyber-agents' gehuldigd, waarvan 4 kinderen op school en 2 kinderen die achteraf een prijzenpakket hebben gekregen. Verder zijn in gemeente C in totaal 5 'cyber-agents' gehuldigd. Ten slotte zijn er door gemeente D in totaal 3 kinderen gehuldigd.

5.7 Resumé

In dit hoofdstuk is de uitvoering van het project binnen vier geselecteerde gemeenten beschreven. Het blijkt dat de projectperiode ruim 3 maanden heeft geduurd. Alle respondenten waren tevreden met deze duur omdat het genoeg tijd geeft om de deelnemers te bereiken terwijl het ook weer niet te lang duurde waardoor spelers misschien afhaken. De uitvoering bestond voor de gemeenten uit twee onderdelen: de promotie van HackShield en de huldiging van de kinderen met de meeste punten. Voor de promotie hebben alle gemeenten op eigen sociale media berichten gedeeld, de politie benaderd om oproepen te delen en scholen en jongerenwerkers of -centra benaderd om aandacht te besteden aan het spel. De meeste gemeenten hebben de scholen een mail en brief gestuurd met het verzoek om posters en flyers op te hangen, één gemeente heeft hiervoor ook telefonisch contact gehad met scholen. In twee gemeenten is verder het mobiel media lab van de politie ingezet om meer aandacht voor HackShield te genereren. De wijze waarop de huldiging van deelnemers heeft plaatsgevonden verschilt per gemeente. Zo hebben drie gemeenten een digitale huldiging gehad en heeft een gemeente een fysieke huldiging gehad op basisscholen waar de kinderen op zaten. Bij alle huldigingen zijn de burgemeester van de gemeente en politieagenten

betrokken geweest. De huldigingen duurden tussen de 20 en 30 minuten. Als onderdeel van de huldiging zijn in enkele gemeenten ook fysiek 'goodies' (zoals certificaten, petten en 'badges') langsgebracht bij de kinderen door een medewerker van de gemeente, politieagenten of buitengewoon opsporingsambtenaren. Er is tijdens het project door gemeenten samengewerkt met diverse interne partners (zoals collega's van de afdelingen communicatie, jeugd en openbare orde en veiligheid) en externe partners (zoals de politie, scholen en jongerenwerk). Medewerkers van gemeenten geven aan dat zij informatie en instructies hebben gehad over het uitvoeren van het project, door het online platform 'Collegia' en bijeenkomsten die zijn georganiseerd met andere gemeenten vanuit NHSV. Er was echter ruimte om hiervan af te wijken en eigen (lokale) initiatieven te nemen. De uitvoering is volgens alle respondenten grotendeels verlopen zoals gepland. Aanpassingen zijn bijvoorbeeld gemaakt in de wijze van huldigen.

Tijdens het project heeft er op twee verschillende manieren een selectie van deelnemers plaatsgevonden. Enerzijds is er een selectie van kinderen die HackShield gaat spelen en daarbij hun gemeente opgeven, anderzijds is er een selectie van kinderen die uiteindelijk wordt gehuldigd. Kinderen die tijdens het spelen van HackShield hun gemeente opgeven worden 'cyber-agents' van de gemeente genoemd en komen in aanmerking om gehuldigd te worden als zij een geverifieerd e-mailadres van hun ouders hebben opgegeven. De kinderen die de meeste punten hebben verzameld met het spelen van het spel tijdens de projectperiode zijn gehuldigd. Het aantal 'cyber-agents' verschilt van 44 tot 306 per gemeente en lijkt deels afhankelijk van het aantal kinderen dat in de gemeente woont. Desondanks is er ook een verschil in de verhouding tussen het aantal 'cyber-agents' en de totale populatie kinderen tussen de 8 en 12 jaar in de gemeente van 1,66% tot 9,30%. Uitvoerders van de gemeente verschillen over de mate waarin zij tevreden zijn met dit bereik. Enerzijds zijn er respondenten die tevreden zijn wanneer zij de cijfers vergelijken met anderen gemeenten, anderzijds is er een respondent die vindt dat – gezien het totale aantal kinderen in de gemeente – weinig kinderen het spel hebben gespeeld. Uit de interviews met 'cyber-agents' blijkt dat zij HackShield voornamelijk zijn gaan spelen door een bericht op sociale media, via vrienden of door school. Het aantal deelnemers dat uiteindelijk is gehuldigd per gemeente varieert van 3 tot 6 'cyber-agents'. Onduidelijk blijft in hoeverre de doelgroep wordt bereikt, aangezien er geen informatie is over de leeftijden van deelnemers die HackShield spelen.



6 De ervaringen rondom HackShield

6.1 Inleiding

In dit hoofdstuk staan ervaringen centraal van personen die betrokken zijn geweest bij de uitvoering van 'HackShield in de gemeenten Noord-Holland' of hebben deelgenomen aan het initiatief. Eerst bespreekt paragraaf 6.1 hoe betrokkenen het initiatief waarden. Vervolgens laat paragraaf 6.2 zien in hoeverre het initiatief volgens betrokkenen bijdraagt aan cyberweerbaarheid. Het hoofdstuk sluit af met factoren die volgens respondenten het initiatief bevorderen of belemmeren. Per paragraaf wordt steeds eerst het perspectief van uitvoerders besproken en vervolgens het perspectief van deelnemers en ouders.

6.2 Waardering betrokkenen

Uitvoerders

De medewerkers van de gemeente en politie uit de geselecteerde gemeenten zijn over het algemeen tevreden over het verloop van het initiatief (n=8). Respondenten die tevreden zijn geven aan dat het project 'heel soepel', 'soepel', 'positief', 'goed' of 'over het algemeen goed' is verlopen. Verklaringen voor de positieve waardering van het project zijn de goede begeleiding en duidelijke instructies vanuit de initiatiefnemers (n=2), de extra aandacht die het project geeft aan cybercriminaliteit (n=2), dat kinderen fanatiek bezig zijn geweest (n=1), het aantal kinderen dat is bereikt (n=1) en de goede afstemming en het contact met partners (n=1). Een van de respondenten vindt dat het initiatief 'redelijk goed' is verlopen, maar dat er wel punten zijn die anders of beter gedaan hadden kunnen worden (POL2). In paragraaf 6.3 worden de bevorderende en belemmerende factoren die respondenten aanmerken verder besproken.

De meeste respondenten geven aan dat zij bij een volgende ronde weer mee zouden doen (n=5). Redenen hiervoor zijn dat het bijvoorbeeld een project is waarmee men met een kleine inspanning kan inspelen op digitale veiligheid (n=3) en omdat het een leuk project is om te doen waarmee men weer in contact komt met jeugd (n=1). Een andere respondent geeft aan niet direct met HackShield in een volgende ronde mee te doen (GM3). De reden hiervoor is dat een dergelijk project eerst moet wegzakken en vervolgens weer opgepakt moet worden. In 2022 zou men wel weer mee willen doen aan HackShield. Ten slotte vindt een respondent het lastig om te zeggen of men bij een vervolgronde opnieuw zou deelnemen (POL2). De respondent denkt wel dat men weer mee zou doen, maar zou liever met een frisse blik kijken naar wat er nog meer mogelijk is aangezien het project niet helemaal het resultaat had wat de respondent voor ogen had. Er waren volgens de respondent beperkingen door corona in de uitvoering en ook verbeterpunten voor het project (zie paragraaf 6.3 voor een uitgebreidere toelichting). Eén respondent heeft niet gereageerd op een vraag via e-mail of de gemeente bij een volgende ronde opnieuw mee zou doen.

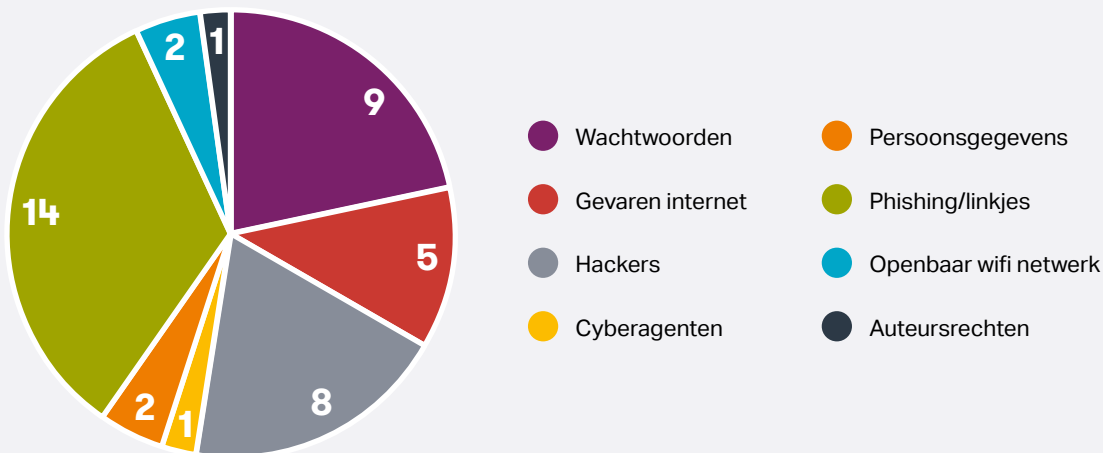
Deelnemers en ouders

Alle deelnemers die zijn gesproken waren erg enthousiast over HackShield. Alle kinderen noemen de woorden 'leuk' (n=16) of 'leerzaam' (n=3) als eerste reactie op het spel. Varianten daarop waren 'super leuk' (n=2) of 'heel leuk' (n=3). Een aantal deelnemers waren iets uitgebreider en vulden (super of heel) 'leuk' aan met 'leerzaam' (n=4), 'spannend' (n=1), 'uitdagend' (n=1) of 'grappig' (n=1). De intensiteit waarin de kinderen HackShield spelen, verschilt aanzienlijk. Sommige kinderen spelen 1 tot 2 uur per dag (n=2), terwijl anderen juist maar 1 tot 2 uur per week (n=2) het spel spelen. De meeste kinderen vonden het overigens lastig om in te schatten hoeveel uur per week ze daadwerkelijk aan het spel besteden (n=7). Een groot deel van de deelnemers gaf ook aan dat ze eerst heel intensief speelden, maar daarna (bijna) niet meer omdat ze alle levels uitgespeeld hadden (n=11). Er zijn een paar deelnemers die dagelijks kijken of er iets nieuws gedaan kan worden (n=2) of die af en toe HackShield spelen om zelf levels te maken (n=2).

De ouders van de deelnemers delen het beeld met hun kinderen en geven aan dat ze zien dat hun kind plezier heeft tijdens het spelen van HackShield en/of er heel enthousiast over is (n=11). De overige ouders (n=5) geven aan geen zicht op hun kind te hebben als het aan het spelen is. In totaal geven 12 ouders aan dat er ook thuis gesproken wordt over de dingen die hun kind leert van het spel. De overige ouders geven aan dat er thuis niet gesproken wordt over de dingen die hun kinderen leren van HackShield (n=4). Tot slot zouden alle ouders het spel aanraden aan andere ouders en kinderen (n=16). Redenen die hiervoor genoemd worden zijn: het is een leuk spel (n=4), leerzaam (n=2) en goed initiatief dat kinderen er op deze manier ook achter kunnen komen of ze ICT interessant vinden (n=1). Een aantal ouders heeft informatie over HackShield gedeeld op social media (n=3) om zo ook andere ouders en kinderen aan te sporen om het spel te gaan spelen.

Ouders vinden verder dat zij voorafgaand aan het traject voldoende informatie hebben ontvangen (n = 13). Zij zijn hier dan ook zeer over te spreken. Eén respondent geeft aan dat het spelen van HackShield werd aanbevolen door de school van hun kind waardoor zij weinig betrokken zijn geweest bij het traject. Zij hadden het dan ook gewaardeerd als er een 'factsheet' met de belangrijkste informatie over HackShield was uitgedeeld aan ouders. Verder is het voor kinderen duidelijk waar zij problemen kunnen melden of hun vragen kunnen stellen. Volgens hen kunnen ze "tante Shelley" altijd mailen. Hiervoor dient het eigen mailadres gebruikt te worden. Contact via de mailbox in HackShield is niet mogelijk, terwijl dit het contact wel makkelijker zou maken en het tot een prettiger en veiliger gevoel zou leiden bij de ouders (n=1).

Wat heb jij geleerd?



Figuur 2: onderwerpen waar deelnemers wat over hebben geleerd (n=18)

6.3 Bijdrage cyberweerbaarheid

Uitvoerders

Aan medewerkers van de gemeenten en politie is gevraagd in hoeverre de doelen van het project zijn behaald. Voor de meeste respondenten is het onbekend of de benoemde doelen zijn behaald (n=6). Het is voor de uitvoerders niet bekend omdat het onduidelijk is of er gedragsverandering heeft plaatsgevonden in het internetgedrag van de kinderen (G1, G3), omdat dit nog onderzocht moet worden (G4) of omdat er geen heldere, meetbare doelen zijn vastgesteld of gecommuniceerd (POL2, POL3, POL4). Een andere respondent geeft aan dat het project heeft bijgedragen aan de eerder genoemde doelen, omdat kinderen bij de huldinging veel van cybercrime wisten en veel hadden geleerd van het spel (G2). Kinderen beginnen dan over hackers, een goed wachtwoord en hoe ze mailtjes kunnen onderscheiden bij phishing. Een laatste respondent geeft aan dat aan winnaars is gevraagd of zij de kennis hebben gedeeld met anderen, maar dat bleek dat zij de kennis met name voor zichzelf hebben gehouden en het spel wel erg leuk vonden (POL1).

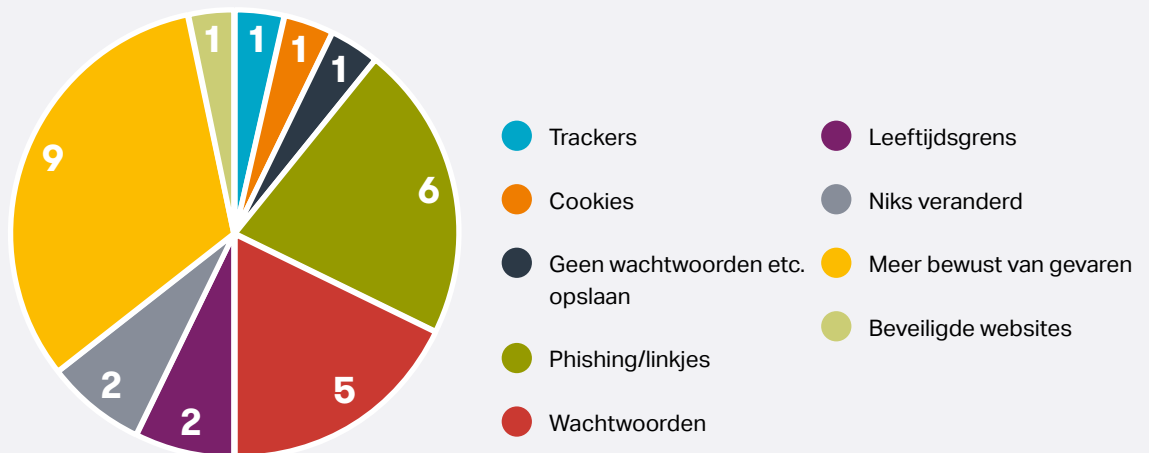
Verder blijkt uit de antwoorden van verschillende respondenten dat zij het gevoel hebben dat het initiatief heeft bijgedragen aan cyberweerbaarheid (n=4). Zo ervaren respondenten tijdens de huldinging dat kinderen kennis hadden over cybercriminaliteit (n=2), denkt een andere respondent dat het helpt omdat dingen bespreekbaar worden gemaakt (n=1) en geeft weer een andere respondent aan dat 'als je maar een zaadje plant, dan ooit, komt het van pas' (n=1). Ten slotte blijft het voor een andere respondent onduidelijk of het initiatief bijdraagt aan cyberweerbaarheid omdat hij niet goed op de hoogte is van de inhoud van het spel (n=1).

Deelnemers en ouders

Over het lerend effect van HackShield zijn de kinderen het eens. Iedereen geeft aan dingen geleerd te hebben van het spel. De kinderen zijn zich het meest bewust geworden van het belang van sterke wachtwoorden die regelmatig worden veranderd (n=9). Daarnaast hebben zij geleerd dat er phishingmails bestaan en dat zij niet zomaar op linkjes moeten klikken (n=8). Ook weten de kinderen nu veel beter wat hacken is en hoe je kan voorkomen dat je computer gehackt wordt (n=8). Verder geven vier kinderen aan dat zij zich voor het spelen van HackShield niet bewust waren van de gevaren van het internet en dit nu wel zijn. Ten slotte geeft iemand aan nu te weten wat cyberagenten precies doen om (internet)gebruikers te beschermen (n=1).

Het merendeel van de kinderen geeft aan dat zij de opgedane kennis ook daadwerkelijk gebruiken tijdens het internetten (n=16). De deelnemers zijn zich over het algemeen bewuster van gevaren waardoor ze kritischer zijn op het internet (n=9). Er worden sterkere wachtwoorden gebruikt die af en toe ook veranderd worden (n=5). Eén deelnemer geeft aan dat hij ook geen wachtwoorden opslaat, omdat het voor hackers dan erg gemakkelijk wordt om in te loggen. Verder kijken deelnemers kritischer naar mails om op deze manier phishingmails te herkennen (n=6) en letten deelnemers op of websites wel beveiligd zijn (n=1). Daarnaast hebben sommige ouders of deelnemers de instellingen van de computer of telefoon aangepast zodat er een leeftijdsgrens is ingesteld en niet alle handelingen uitgevoerd kunnen worden (n=2). Ten slotte let één deelnemer op het aantal 'trackers' dat aanwezig is op een site. Dit leidt niet tot verdere gedragsverandering, maar draagt wel bij aan het vergroten van het bewustzijn over de informatie die je achterlaat op het internet. Ten slotte worden niet alle cookies meer klakkeloos geaccepteerd, maar wordt de informatie gelezen en daarna besloten om de cookies wel of niet te accepteren (n=1).

Gedragsverandering door HackShield



Figuur 4: gedragsverandering door HackShield volgens deelnemers (n=18)

Van alle ouders geven tien van de zestien geïnterviewden aan dat het gedrag van hun zoon of dochter op internet zichtbaar veranderd is. Ouders vinden over het algemeen dat hun kinderen zich bewuster zijn van gevaren (n=6). Naast de positieve effecten van het spel die ouders bij kinderen zien, geeft het ouders het vertrouwen dat ze hun kind(eren) wat meer los kunnen laten (n=2). De ouders die geen verschil in gedrag zien geven hiervoor twee redenen: (1) voor het spelen van HackShield was er al toezicht vanuit ouders waardoor er niet veel ruimte voor verandering aanwezig is (n=2) en (2) het spel heeft niet genoeg impact of het is niet vaak genoeg gespeeld om impact te kunnen hebben (n=1).

Naast de gedragsverandering die voor sommige ouders zichtbaar is, spreken kinderen actief over HackShield in hun omgeving (n=9). Kinderen waarschuwen anderen voor de gevaren op het internet en geven tips hoe mensen zich hiertegen kunnen beschermen (n=8). Ook spreken de spelers over bijvoorbeeld de huldiging (n=1).

6.4 Bevorderende en belemmerende factoren

Uitvoerders

Er worden door uitvoerders van de geselecteerde gemeenten verschillende factoren genoemd die bijdragen aan een goed verloop van het initiatief. Een veelgenoemde factor is de energie, inzet en betrokkenheid van verschillende betrokken partners (n=4). Specifiek wordt de inzet van burgemeesters en politie genoemd (G1, G2, POL1), maar ook de betrokkenheid en passie van betrokken uitvoerders vanuit de gemeenten wordt door de politie gezien als een belangrijke bevorderende factor (POL1, POL2). Een andere veelgenoemde factor is de goede ondersteuning die uitvoerders hebben gehad vanuit HackShield en NHSV (n=5). Zo was er veel toegang tot

informatie over hoe het project kon worden opgepakt, goed promotiemateriaal, veel voorwerk gedaan en kon men altijd bij iemand terecht voor vragen. In aansluiting op de goede ondersteuning benoemen respondenten dat het voor de gemeente en politie slechts een kleine inspanning vereist om mee te doen aan het initiatief (n=4). Het volgende citaat illustreert dit:

“Ook door de begeleiding vanuit NHSV, dat was echt top moet ik zeggen. Daardoor werd je echt op sleeptouw genomen en was het eigenlijk best wel makkelijk om het ook binnen [gemeente X] uit te zetten. Want er was gewoon een duidelijke planning, deadlines en ook bijna om de twee weken volgens mij overleg.” [G3]

Andere bevorderende factoren die worden genoemd zijn persoonlijk contact en korte lijntjes met partners (n=1), langsgaan bij basisscholen tijdens de huldiging (n=1), enthousiasme binnen en buiten de gemeente (n=1), duidelijke afspraken (n=1) en de link die tijdens de promotie bijvoorbeeld werd gemaakt met de week van de mediawijsheid (n=1).

Respondenten is ook gevraagd naar factoren die een goed verloop van het project belemmeren. Bijna alle uitvoerders noemen de maatregelen rondom het COVID-19 virus als belemmerend (n=6). Hierdoor waren bijvoorbeeld geen fysieke huldigingen mogelijk, konden respondenten niet fysiek langsgaan bij scholen om het project te promoten of les te geven en was er een gebrek aan fysieke afstemmingsmomenten. Een tweede punt dat wordt genoemd is het contact met scholen (n=3). Zo geeft een van de respondenten aan dat er mails gestuurd zijn naar scholen met de vraag of zij toegestuurde flyers en posters wilden verspreiden op de school, maar is er verder geen aandacht besteed in de les en hoopte te respondent op meer respons, enthousiasme en samenwerking (G1). Een andere respondent geeft aan dat in de gemeente meer dan 50 basisscholen zijn, waardoor het niet haalbaar is om naar alle basisscholen zelf toe te gaan (G3). Een van de respondenten geeft aan op de hoogte te zijn van scholen waar de posters niet zijn opgehangen (POL2). Een andere factor die wordt genoemd is de beperkte capaciteit binnen en buiten de gemeente (n=1). Zo geeft de respondent aan dat er bij de afdeling communicatie van de gemeente veel concurrentie was van andere onderwerpen die aandacht vroegen en was de politie lastig betrokken te krijgen (G4). Eén van de respondenten geeft aan dat er geen belemmerende factoren waren.

In aansluiting op de genoemde belemmerende factoren dragen de uitvoerders verbeterpunten aan voor het initiatief. Ten eerste worden er verbeterpunten genoemd rondom de promotie op scholen (n=4). Zo zou het helpen om meer persoonlijk contact te hebben met scholen door zelf directieleden te bellen en te vertellen over het project in plaats van e-mails versturen met het verzoek om posters en flyers op te hangen (n=2). Ook geeft een respondent aan dat vanuit de gemeente eerder lijntjes hadden moeten worden gelegd richting de scholen (G4). Een tweede verbeterpunt dat wordt genoemd is de rol van de politie (n=3). Respondenten vanuit gemeenten geven aan dat meer betrokkenheid en aansluiting van de politie meer winst op kan leveren (n=2). Ook een medewerker van de politie geeft aan dat men vanuit de politie meer 'exposure' had kunnen geven aan het project (n=1). Overige mogelijkheden voor verbetering die worden genoemd zijn om uitvoerders het spel te laten spelen zodat ze beter vragen van kinderen kunnen beantwoorden (n=2), het breder trekken van HackShield naar onderwerpen zoals cyberpesten en sexting zodat het project aantrekkelijker wordt voor partners (n=1), goede afspraken maken met partners over hun capaciteit (n=1), een social-media kit voor de politie (n=1), de kwaliteit van de filmpjes en certificaten verbeteren (n=1) en het project 'lokaler' maken door lokale gezichten in de promotiefilmpjes in te zetten en lokale ondernemers te betrekken bij het project (n=1). Andere respondenten geven aan dat men meer kanalen zou kunnen aangrijpen voor de promotie van het initiatief (n=2), zoals bijvoorbeeld TikTok, online fora of spelcomputerplatformen als PlayStation en Xbox. Ook benoemt een van de respondenten

van de politie dat de tutorial van het spel maar één keer gespeeld kon worden op een apparaat, waardoor men in het mobiele media lab niet alle kinderen de tutorial kon laten spelen.

Ten slotte is aan uitvoerders gevraagd wat cruciaal is voor de implementatie van het project binnen andere gemeenten. De meest cruciale factor is volgens de respondenten een goede samenwerking en communicatie tussen gemeente, politie en andere betrokken partijen (n=4). Verder worden enthousiasme en durf om het project te promoten ook door meerdere respondenten genoemd (n=3). Overige factoren die worden benoemd zijn inzet (n=1) en bestuurlijke prioriteit (n=1).

Deelnemers en ouders

Deelnemers zijn zoals in paragraaf 6.1 besproken erg positief over HackShield en noemen het in eerste instantie een 'leuk' (n=16) of 'leerzaam' (n=3) spel. Ze vinden het een leuk spel omdat je zelf levels kunt maken (n=7), je goed moet nadenken over de vragen (n=7), levels moet behalen om verder te komen in het spel (n=3), maar ook de afwisseling tussen opdrachten en vragen vinden deelnemers leuk (n=4). Tevens vinden een aantal deelnemers het contact met HackShield erg fijn verlopen (n=3). Je kunt zelf makkelijk contact met HackShield opnemen als je bijvoorbeeld een foutje in het spel ontdekt (n=2), een deelnemer kreeg zelfs een handgeschreven kaart op zijn verjaardag (n=1), de huldiging is heel indrukwekkend en leuk (n=2) en je kunt veel dingen winnen (n=1).

Toch zijn er volgens de deelnemers enkele punten te benoemen die minder leuk of moeilijk zijn aan HackShield en verbeterd kunnen worden om het spel leuker en leerzamer te maken. De levels zijn namelijk snel uit te spelen (n=3), (veel) herhaling in de levels (n=1), je kunt maar 10 levels zelf maken (n=1), er wordt niks met feedback gedaan (n=1) en shields verdienen is tijdsgebonden en dat is jammer (n=1). Daarnaast gaat de besturing niet altijd goed in het spel (n=2), lukt het niet altijd om zonder hulp een level uit te spelen (n=6) of zit er juist te weinig uitdaging in het spel (n=1).

HackShield kan volgens de deelnemers beter gemaakt worden door het toevoegen van meer levels (n=5), meer uitleg over het zelf maken van de levels (n=1), meer levels zonder QR-code want die werken niet goed (n=1), testversie eenvoudiger maken qua indeling/layout (n=1), meer opties in de levelmaker zodat je zelf mooiere en grotere levels kunt maken (n=1), meer shields bij uitdagingen kunnen verdienen (n=1) en een optie voor 'multiplayer' (n=1). Er werden ook dingen genoemd als 'een foto van jezelf kiezen voor het poppetje in het spel' (n=1), het spel op pauze kunnen zetten (n=1), score tijdens het level zien zodat je weet hoe ver je bent (n=1), via de persoonlijke mail op de hoogte gehouden worden van updates of nieuwe versies (n=1) en het zou leuk zijn als er een krantje of nieuwsbrief komt met informatie over hacken of mediawijsheid (n=1).

Ook was er een aantal kinderen die geen verbeterpunten hadden voor het spel (n=5). Tot slot bleek uit de interviews dat een aantal deelnemers testers waren en als eersten op de hoogte worden gebracht van updates om deze te testen en te evalueren (n=8). Zij krijgen tussendoor vragenlijsten om deze updates te beoordelen. Sommige kinderen vullen deze vragenlijsten ook in (n=4) maar geven daarbij wel aan dat ze de vragenlijsten alleen invullen als ze deze voorbij zien komen (n=2) of dat ze de laatste tijd minder of geen tijd hebben om deze in te vullen (n=2). Sommige testers vullen de vragenlijsten niet in (n=2), waarbij één deelnemer toelicht dat hij de inbox niet zo interessant vindt maar het wel heel cool vindt om tester te zijn om op die manier één van de eersten te zijn die een level gaat testen. Een andere deelnemer geeft nog aan dat het heel erg leuk is om tester te zijn omdat er ook één keer afgesproken is met de testers en makers van het spel.

6.5 Resumé

Uit het onderzoek naar de ervaringen van uitvoerders en deelnemers blijkt dat uitvoerders, deelnemers en ouders bijna allemaal tevreden zijn over HackShield. Uitvoerders zijn tevreden over het project omdat er duidelijke instructies en goede begeleiding was gedurende het project vanuit HackShield en NHSV en omdat het project extra aandacht creëert voor cybercriminaliteit. De tevredenheid zorgt ervoor dat bijna alle uitvoerders bij een volgende of latere projectronde weer willen meedoen. Een respondent vindt het lastig om te zeggen of hij opnieuw mee zou doen omdat het project niet helemaal het beoogde resultaat heeft gehad. Deelnemers zijn enthousiast omdat zij het spel leuk en leerzaam vinden. De intensiteit waarmee kinderen spelen verschilt wel sterk: van 1 à 2 uur per dag tot 1 à 2 uur per week. Een mogelijke verklaring is dat kinderen minder zijn gaan spelen omdat zij de levels van het spel hadden uitgespeeld. Een enkele deelnemer maakt zelf levels. Ouders zijn veelal positief over HackShield omdat kinderen plezier hebben tijdens het spelen en er enthousiast over zijn. Andere ouders hebben er geen zicht op als hun kind HackShield speelt. Alle ouders zouden het spel aan andere ouders en kinderen aanraden. Ten slotte hebben ouders voldoende informatie ontvangen voorafgaand aan het traject. Ook voor kinderen is het duidelijk waar zij met vragen of problemen terecht kunnen.

In hoeverre de doelen van het initiatief worden behaald is voor de meeste uitvoerders onbekend, omdat dit lastig te meten is of omdat er geen concrete doelen zijn gesteld. Wel hebben enkele uitvoerders het gevoel dat het project heeft bijgedragen aan de cyberweerbaarheid, omdat zij signalen hebben gekregen tijdens huldigingen dat kinderen kennis hebben opgedaan en omdat alleen het onderwerp bespreekbaar maken volgens respondenten al bijdraagt. Alle kinderen geven aan iets van het spel geleerd te hebben, voornamelijk over het belang van sterke wachtwoorden, hoe phishing mails te

herkennen zijn en wat hacken is en hoe je dit kunt voorkomen. Ook een meerderheid van de ouders geeft aan dat het gedrag van hun kind is veranderd. Kinderen zijn zich volgens hen vooral bewuster geworden van de gevaren. Een kleiner deel van de ouders ziet geen verschil omdat er hiervoor al toezicht was van de ouders of omdat het spel niet vaak genoeg is gespeeld om impact te hebben.

Uitvoerders en deelnemers benoemen verschillende succesvolle factoren van HackShield. Zo noemen uitvoerders de energie, inzet en betrokkenheid van partners, de ondersteuning van HackShield en NHSV en de kleine inspanning om mee te doen als bevorderende factoren voor een goed verloop van het project. De belangrijkste factoren die deelnemers noemen waarom het spel leuk is, zijn dat je zelf levels kunt maken en dat je goed moet nadenken over de vragen. Factoren die een goed verloop van het project in de weg staan hebben volgens uitvoerders voornamelijk te maken met de maatregelen rondom COVID-19, waardoor fysieke activiteiten zoals langsgaan bij scholen en fysieke huldigingen niet mogelijk waren. Ook het contact met scholen wordt als belemmerende factor genoemd, omdat er veel scholen waren, niet alle scholen reageerden op e-mails en flyers en posters niet overal zijn opgehangen. Voor deelnemers waren belemmerende factoren dat het niet altijd lukt om zonder hulp levels uit te spelen en dat de levels snel uit zijn te spelen. Het project zou kunnen worden verbeterd door meer persoonlijk contact te hebben met scholen door te bellen of langs te gaan in plaats van mailen, door meer betrokkenheid vanuit de politie te creëren en door ook uitvoerders het spel te laten spelen. Deelnemers zouden graag willen dat er meer levels aan het spel worden toegevoegd.

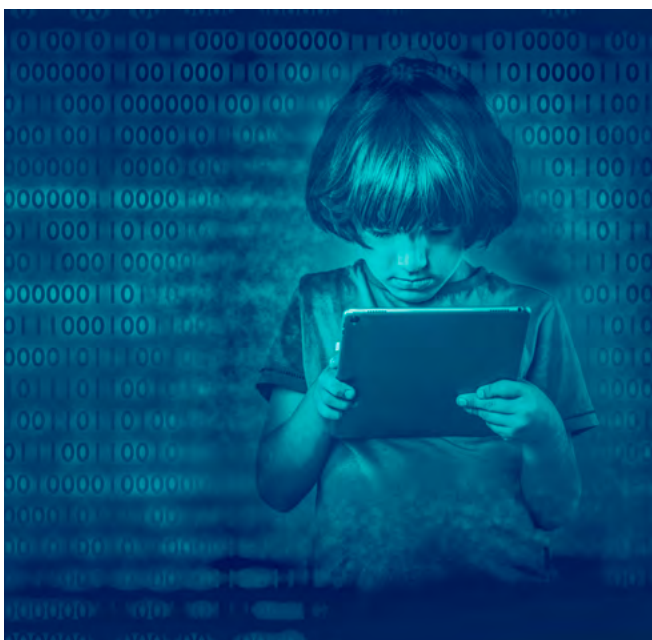


7 Conclusie en discussie

7.1 Conclusies

Het doel van dit onderzoek was om het initiatief 'HackShield in gemeenten Noord-Holland' te evalueren aan de hand van een beknopte plan- en procesevaluatie. Op basis van de documentanalyse en interviews met ontwikkelaars, uitvoerders en deelnemers kunnen de volgende conclusies worden getrokken:

- HackShield is een project, spel en maatschappelijke beweging.** Een onderscheid kan worden gemaakt tussen HackShield als een project in de gemeenten, een 'cybersecurity'-spel en een grotere beweging die bestaat uit verschillende projecten. Het project van de gemeenten bestaat uit een promotiecampagne waarin deelnemers worden opgeroepen om het spel HackShield te spelen en een huldiging van de best presterende spelers. De doelgroep van HackShield betreft kinderen van 8 tot 12 jaar en het doel is om deze kinderen en Nederland als geheel cyberveilig te maken. Ontwikkelaars verwachten dit doel te bereiken door aan de ene kant een maatschappelijke beweging op gang te brengen rondom het onderwerp cyberweerbaarheid. Aan de andere kant wordt inhoudelijk verwacht dat publieksactivatie, spel-mechanismen, immersiviteit en het 'Hero-centred-design' bijdragen aan cyberweerbaarheid. Het 'Hero-centred-design' is de filosofie van de makers van het spel waarin de eindgebruiker centraal wordt gesteld en een (fictieve) rol krijgt die de gebruiker niet heeft in de echte wereld. Deze filosofie is gebaseerd op literatuur over 'storytelling', 'gamification' en 'problem solving'.
- De uitvoering van HackShield is gestandaardiseerd met ruimte voor eigen invulling.** Het HackShield project heeft voor de gemeenten ruim drie maanden geduurd en alle respondenten zijn tevreden met deze duur. Het project bestond uit de promotiecampagne om kinderen 'cyber-agent' te laten worden van hun eigen gemeente. Om 'cyber-agent' te worden moeten kinderen het spel spelen en daarbij hun gemeente opgeven. Verschillende communicatiekanalen zijn hiervoor aangewend: oproepen zijn gedeeld via sociale media van gemeenten en politie, en flyers en posters zijn uitgedeeld aan scholen en jongerenwerkorganisaties met het verzoek om deze te verspreiden. De gemeenten hebben vergelijkbare communicatiekanalen gebruikt, al is in twee gemeenten bijvoorbeeld het mobiel media lab van de politie ingezet om meer aandacht te genereren. Geïnterviewde deelnemers geven aan HackShield te zijn gaan spelen door een bericht op sociale media, via vrienden of door school. In totaal hebben de geselecteerde gemeenten 41 tot 306 'cyber-agents' bereikt aan het einde van de projectperiode. De beste spelers zijn in alle gemeenten digitaal of fysiek gehuldigd door burgemeesters en politieagenten. Sommige gemeenten hebben ook fysiek nog een medewerker van de gemeente, politie of handhaving langs de kinderen laten gaan om een certificaat en andere 'gadgets' te overhandigen. Het aantal gehuldigde deelnemers varieert van 3 tot 6. Medewerkers van gemeenten geven aan dat zij informatie en instructies hebben gehad over de uitvoering van het project via het online platform 'Collegia' en bijeenkomsten georganiseerd vanuit NHSV. Er was echter ruimte om hiervan af te wijken en eigen (lokale) initiatieven te nemen. De uitvoering is volgens alle respondenten grotendeels verlopen zoals gepland, enkele aanpassingen zijn bijvoorbeeld gemaakt in de huldigingen vanwege COVID-19 maatregelen.
- Deelnemers en uitvoerders zijn erg tevreden.** Zowel uitvoerders als deelnemers zijn erg tevreden over het project en spel. Uitvoerders zijn tevreden over het project omdat er duidelijke instructies en goede begeleiding was en omdat er door het project extra aandacht is voor cybercriminaliteit. Op een respondent na zouden alle uitvoerders een volgende of latere projectronde opnieuw meedoen. De deelnemers zijn vooral enthousiast omdat zij het spel leuk en leerzaam vinden. Wel zit er een groot verschil in het aantal uur dat zij spelen: van 1 à 2 uur per dag tot 1 à 2 uur per week. Ouders zijn tevreden omdat kinderen enthousiast zijn en plezier hebben tijdens het spelen. Bovendien zouden alle ouders het spel aanraden aan andere ouders en kinderen.



- **Onduidelijk in hoeverre doelen worden behaald, wel positieve signalen.** Voor de meeste uitvoerders is het onduidelijk in hoeverre het project heeft bijgedragen aan cyberweerbaarheid. Enkele respondenten benoemen wel dat zij signalen hebben gekregen tijdens huldingingen dat kinderen meer kennis hebben. Deelnemers geven zelf allemaal aan iets geleerd te hebben van het spel. Het gaat dan om het belang van sterke wachtwoorden, hoe phishing mails zijn te herkennen en wat hacken is en hoe dit voorkomen kan worden. Een deel van de ouders geeft aan dat het gedrag van hun kinderen veranderd is doordat kinderen zich bewuster zijn van gevaren, een ander deel geeft aan dat zij geen verschil zien in gedrag.
- **Er zijn bevorderende factoren en mogelijkheden voor verbetering.** De factoren die het project tot een succes maken zijn volgens uitvoerders de inzet van betrokken partners, de goede ondersteuning vanuit HackShield en NHSV en de kleine inspanning die het vergt om mee te doen als partner. Deelnemers vinden het spel leuk omdat je goed moet nadenken over de vragen en omdat je zelf levels kunt maken. Factoren die een succes in de weg hebben gestaan zijn voornamelijk te herleiden tot de maatregelen rondom COVID-19, waardoor fysieke activiteiten en fysieke huldingingen niet altijd mogelijk waren. Daarnaast wordt ook de rol van scholen belicht, die niet altijd reageerden op verzoeken en niet allemaal posters en flyers hebben verspreid. Verbetering is dan ook mogelijk door scholen beter te betrekken bij het initiatief, door bijvoorbeeld te bellen of langs te gaan in plaats van te mailen. Deelnemers zouden graag willen dat er meer levels worden toegevoegd aan het spel.

7.2 Discussie

Maatschappelijke beweging & veiligheid

Uit het onderzoek blijkt dat de ontwikkelaars van het initiatief 'HackShield in Noord-Holland' verwachten dat zij een maatschappelijke beweging op gang krijgen met HackShield. Deze verwachting wordt deels bevestigd door respondenten van de gemeenten en politie die tevreden en enthousiast zijn over het project. Ook deelnemers en ouders geven aan dat zij HackShield positief waarderen en (zouden) aanraden aan andere kinderen en ouders. Verder blijkt dat steeds meer gemeenten zich aansluiten bij het initiatief binnen en buiten Noord-Holland (CCV, 2020; JoinHackShield, 2021). Een dergelijke maatschappelijke beweging lijkt aan te sluiten bij recente oproepen uit de literatuur om bij preventieve interventies de kracht van lokale bekendheid van professionals in te zetten (Leukfeldt, Spithoven & Misana-ter Huurne, 2020; Horgan et al., 2020; Collier, 2020). Bestaande contacten tussen bijvoorbeeld gemeente- en politiemedewerkers kunnen volgens de literatuur effectief worden ingezet om specifieke doelgroepen te benaderen. Op deze wijze kan via

risicocommunicatie een lokaal preventief antwoord op de dreiging van cybercriminaliteit worden gegeven (Leukfeldt, Spithoven & Misana-ter Huurne, 2020; Horgan et al., 2020; Collier, 2020). In het geval van HackShield worden organisaties zoals de gemeenten, politie en scholen ingezet om kinderen te bereiken en zodoende kinderen en hun omgeving cyberweerbaar te maken. De grote vraag blijft momenteel natuurlijk wel wat de daadwerkelijke effecten van HackShield zijn, zowel op de kinderen, hun directe (sociale) omgeving en de maatschappij.

Beperkingen

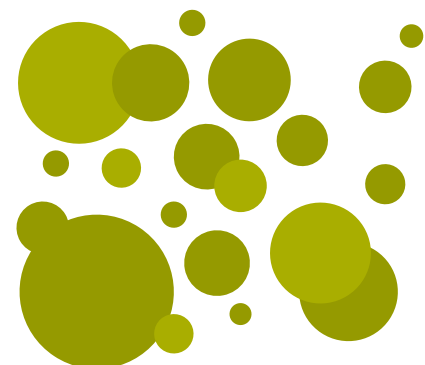
Het huidige onderzoek kent enkele beperkingen, die van belang zijn voor de interpretatie van de gevonden resultaten. Ten eerste zijn er beperkingen rondom de representativiteit van de geïnterviewde respondenten. Ouders en kinderen zijn vanuit HackShield gevraagd om deel te nemen aan het onderzoek. Enkel de ouders en deelnemers die hebben gereageerd en wilden meewerken zijn voor dit onderzoek geïnterviewd. Aangezien bijna de helft van de respondenten tester is, zijn de resultaten van dit onderzoek gebaseerd op de meest fanatieke spelers (testers zijn kinderen die alle levels van het spel uitgespeeld hebben en aangeven dat ze tester willen worden om het spel te verbeteren). Dit kan een vertekend beeld geven. Ten tweede is voor dit onderzoek een selectie gemaakt van vier Noord-Hollandse gemeenten. Ondanks dat er is geselecteerd op de grootte van de gemeente (een kleine en grote) en het bereik (een relatief goede en minder goede) van de gemeente, is maar een beperkt aantal gemeenten onderzocht. Daarnaast is het mogelijk dat respondenten sociaal wenselijke antwoorden hebben gegeven. Dit is geprobeerd te onder- vangen door open vragen te stellen en actief te vragen naar factoren die minder goed zijn verlopen. Ten slotte heeft de dataverzameling plaatsgevonden tussen september 2020 en februari 2021. Dit betekent dan ook dat de huidige evaluatie een momentopname betreft, aangezien projecten tussentijds kunnen worden aangepast.

Vervolgonderzoek

Omdat dit onderzoek een beknopte plan- en procesevaluatie betreft, blijft het onduidelijk wat de daadwerkelijke effecten zijn van HackShield op het gedrag van kinderen en hun omgeving. Toekomstig evaluatieonderzoek in de vorm van (kwantitatieve) effectevaluaties kan aantonen wat de daadwerkelijke effecten zijn van het initiatief. Zo kan er een voor- en nameting plaatsvinden met betrekking tot de kennis die deelnemers en ouders daadwerkelijk opdoen, door vragenlijsten op te stellen die deze kennis toetsen. Verder verdient het de aanbeveling om ook kwalitatief onderzoek te blijven uitvoeren, zodat zowel positieve effecten als mogelijke ongewenste consequenties van het initiatief in kaart kunnen worden gebracht. Interviews met deelnemers en ouders zijn hiervoor geschikt, mits de steekproeven representatief zijn voor alle deelnemers.

Referenties

- Brantingham, P. J., & Faust, F. L. (1976). A conceptual model of crime prevention. *Crime & Delinquency*, 22(3), 284-296.
- Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). *Cybercrime prevention: Theory and applications*. Cham, Switzerland: Palgrave Pivot, an imprint of Springer.
- Centraal Bureau voor de Statistiek. (2020a). Slachtofferschap criminaliteit; regio. Geraadpleegd van <https://opendata.cbs.nl/#/CBS/nl/dataset/82464NED/table?dl=3DCBD>.
- Centraal Bureau voor de Statistiek. (2020b). Bevolking op 1 januari en gemiddeld; geslacht, leeftijd en regio. Geraadpleegd van <https://opendata.cbs.nl/statline/#/CBS/nl/dataset/03759ned/table?fromstatweb>
- Centrum voor Criminaliteitspreventie en Veiligheid. (2020). Groeiend aantal gemeenten betreft kinderen in de strijd tegen cybercrime. Geraadpleegd van <https://hetccv.nl/nieuws/groeiend-aantal-gemeenten-betrekt-kinderen-in-de-strijd-tegen-cybercrime/>
- Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91-150.
- Collier, B., Horgan, S., Jones, R., & Shepherd, L. A. (2020). The implications of the covid-19 pandemic for cybercrime policing in scotland: a rapid review of the evidence and future considerations. Scottish Institute for Policing Research.
- Horgan, S., Collier, B., Jones, R., & Shepherd, L. (2021). Re-territorialising the policing of cybercrime in the post-COVID-19 era: towards a new vision of local democratic cyber policing. *Journal of Criminal Psychology*.
- JoinHackShield. (2021). Nederland zoekt nog meer Cyber Agents! Geraadpleegd van <https://www.joinhackshield.nl/nieuws/61>
- Leukfeldt, E. R., Notte, R. J., & Malsch, M. (2020). Exploring the Needs of Victims of Cyber-dependent and Cyber-enabled Crimes. *Victims & Offenders*, 15(1), 60-77.
- Leukfeldt, E. R., Spithoven, R. & Misana-ter Huurne, E.F.J. (2020). De lokale aanpak van cybercrime. Risicocommunicatie als antwoord op een grenzeloos vraagstuk. In: Lievens, E., Stol, W., & De Kimpe, L. (2020). *Politie en Cybercrime*. *Cahiers Politiestudies*, 2020, 56, 203-223.
- 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.
- Noord Holland Samen Veilig. (2018). *Integraal Meerjarenbeleidsplan Veiligheid 2019-2022*. Gemeenten, Openbaar Ministerie, Politie en hun partners.
- Noord Holland Samen Veilig. (2020). *Regionale aanpak cybercrime en gedigitaliseerde vormen van criminaliteit. Uitvoeringsplan 2020*.
- Oosterwijk, K. & Fischer, T. (2017). *Interventies jeugdige daders cybercrime*. Den Haag: WODC.
- Ooyen-Houben, M. M. J., & Leeuw, F. L. (2010). *Evaluatie van justitiële (beleids) interventies*. Den Haag: WODC.
- Politie. (2021). Mobiel Media Lab. Geraadpleegd van <https://www.politie.nl/themas/mobile-media-lab.html>
- Rossi, P. H., Lipsey, M. W., & Freeman, H. E. (2004). *Evaluation: a systematic approach*. Thousand Oaks: SAGE Publications.
- Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society*. Boom Criminologie.
- 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.





Adres- en contactgegevens



**Johanna Westerdijkplein 75
2521 EN Den Haag**



dehaagsehogeschool.nl