Routekaart

Automated Vulnerability Research

versie 3.0

3 februari 2021

1 Management samenvatting 4
2 Inleiding en context 8
3 Wat is Automated Vulnerability Research 12
3.1 Automatisering in cybersecurity 12
3.2 Automated vulnerability research 13
3.3 Processtappen in AVR 14
4 Ambitie Routekaart AVR 16
5 De Routekaart AVR 19
5.1 De innovatieketen 19
5.2 Waar staan we op dit moment? 20
5.3 Stakeholders 21
5.4 Waar liggen de behoeften? 22
5.4.1 Toepassingen 22
5.4.2 Behoeftematrix 24
5.5 De Routekaart 24
5.5.1 Spoor 1: Onderwijs en opleiding 25
5.5.2 Spoor 2: Versterking fundamenteel onderzoek 27
5.5.3 Spoor 3: Toepassing AVR 28
5.5.4 Fieldlab 32
5.5.5 Activiteiten en fasering 33
5.5.6 Internationalisering en aansluiting bij andere initiatieven 33
6 Organisatie en financiering 35
6.1 Organisatie 35
6.2 Financiering 37
7 Vervolgstappen Routekaart 38
8 Realisatie en risico’s 39
9 Bijlage 1. Overzicht betrokkenen 40

1 Management samenvatting

Reeds enige tijd wordt er op initiatief van de Ministeries van Defensie, Economische Zaken en Klimaat en Justitie & Veiligheid gewerkt aan het onderwerp Automated Vulnerability Research (AVR)[1]. AVR is binnen cybersecurity een relatief nieuw en onbekend onderwerp. Het onderwerp is verankerd in de KIA veiligheid, missie cyberveiligheid[2].

De betrokken ministeries willen nu overgaan tot een volgende stap en een Routekaart ontwikkelen voor het werken aan AVR. Hierbij is de hele cybersecurity keten van belang: van onderzoek en onderwijs tot toepassing (valorisatie). De Routekaart is hiermee een voorbeeld van 'programmering' van het Samenwerkingsplatform Cybersecurity.

Financiële middelen worden beschikbaar gemaakt om een start te maken de Routekaart te realiseren. Voor het volledig realiseren van de Routekaart zullen in de komende jaren aanvullende middelen moeten worden gevonden. De Routekaart draagt hieraan bij. In deze Routekaart wordt ook een eerste indicatie gegeven waar de beschikbare middelen aan zouden kunnen worden besteed, en hoe besluitvorming hierover zou kunnen plaatsvinden.

Doelen Routekaart AVR
De algemene doelen van de Routekaart AVR zijn:

- Duidelijk maken hoe er in Nederland de komende 6 jaar aan AVR kan worden gewerkt.
- Een gecoördineerde start maken met activiteiten op het gebied van AVR in een drietal sporen. En daarmee een impuls geven aan kennisontwikkeling en -toepassing van AVR.
- Aan partners uit de keten duidelijk maken waar en hoe deze mee kunnen doen om AVR in Nederland verder te brengen.
- Ketenpartners inspireren om nieuwe impulsen aan AVR te geven.
- Een levende 'community' op het gebied van AVR op te starten.
- Inzicht geven wat er op korte en middellange termijn kan worden gerealiseerd: en daarmee de zowel de mogelijkheden als beperkingen verduidelijken.
- Bijdragen aan de digitale autonomie van Nederland.

Ambitie Routekaart AVR
AVR versterkt het preventieve deel van de cybersecurityketen door automatisering van het vinden van bekende en onbekende kwetsbaarheden in software, ontwikkelen van exploits en het patchen van die kwetsbaarheden. De Routekaart AVR heeft een grote ambitie. Een 'stip op de horizon'.

De ambitie is om over zes jaar:

[1] **Zie hoofdstuk 3 voor toelichting op wat AVR is**
[2] **Zie hoofdtsuk 2 voor toelichting op de KIA Veiligheid**

- Als Nederland een *leidende positie* in Europa te hebben op het gebied van Automated Vulnerability Research (AVR). Dit blijkt uit onder meer de combinatie van publicaties (thought leadership), PhD's, aantal studenten, patenten (of open source gemaakte technologie) en de omvang van commerciële dienstverlening
- *Technologie te hebben ontwikkeld* om op bedrijfsmatige wijze succesvol geautomatiseerd kwetsbaarheden te kunnen vinden.
    - In minimaal één substantiële IT ontwikkel- of beheeractiviteit (TRL 8+).
    - Voor automatisch patchen een goede uitgangspositie te hebben bereikt voor valorisatie en industrialisatie (TRL6+ demonstrators).
- Sector specifieke toepassingen te hebben ontwikkeld. Zoals de capaciteit om geautomatiseerd kwetsbaarheden te vinden en/of deze te patchen, in door banken gebruikte software

Achterliggende beleidsdoelstellingen zijn bevordering van digitale veiligheid, ook van het MKB, versterken economisch verdienvermogen en strategische autonomie in het digitaal domein.

Stand van zaken, behoeften en toepassingsgebieden
In de routekaart is samengevat wat de stand van zaken op het gebied van AVR in Nederland nu is en wat de behoeften van betrokken partijen zijn. Hierbij gaat het om alle partners in de innovatieketen: hoger onderwijs (universiteiten en hogescholen), toegepaste onderzoeksinstellingen, security technologieleveranciers, security service providers, ontwikkelaars van software en IT eindgebruikers (vooral ook uit de vitale sectoren).
Bij alle betrokken partijen is behoefte om stappen te maken op het gebied van AVR

Inhoudelijk is er vooral belangstelling voor toepassing van AVR in de volgende vier deelgebieden[3].:

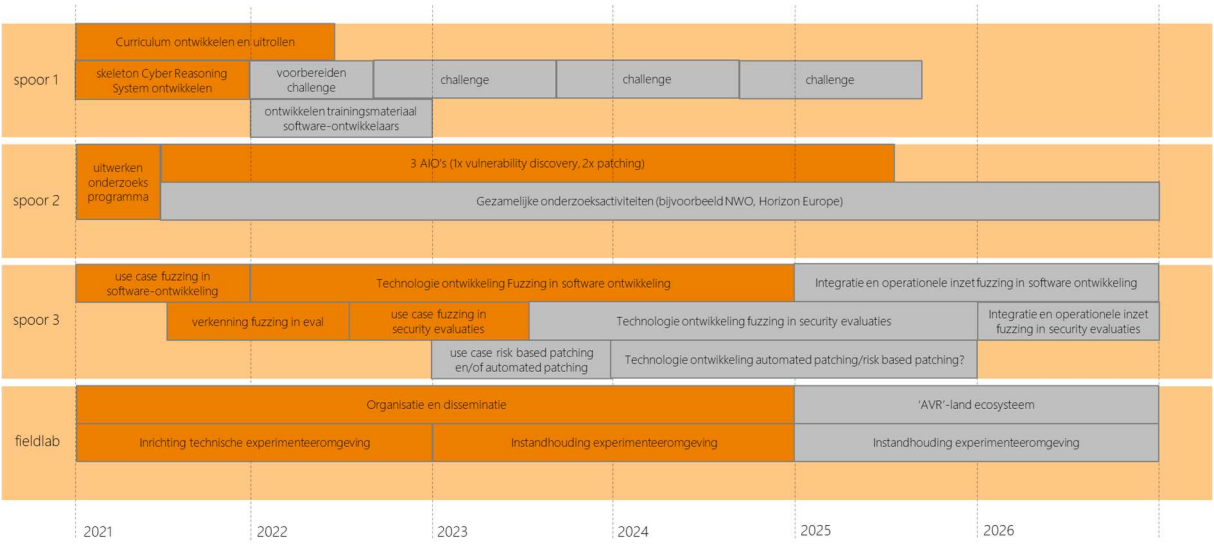
1. *Secure software development.* Door AVR toe te passen binnen het softwareontwikkelproces kunnen kwetsbaarheden in een vroegtijdig stadium, voordat de software wordt ingezet, worden verholpen. Dit past binnen de beweging om security al vroeg in de levenscyclus van systemen aandacht te geven ("shift security left").
2. *Security assessments/evaluaties.* Bij deze evaluaties wordt de security diepgravend onderzocht, o.a. door analyse van sourcecode, hardware, side channel analyses etc. AVR kan er aan bijdragen om deze evaluaties verder te automatiseren, aanvullende typen analyse uit te voeren, en daarmee het proces (kosten-)effectiever te maken.
3. *Patching van systemen zonder support*. Voor veel IT-systemen worden geen patches uitgebracht, ofwel doordat de supporttermijn verlopen is, ofwel (bijvoorbeeld in het geval van veel open source software) omdat er geen verantwoordelijke partij is voor het uitbrengen van patches. Het betreft zowel 'oude systemen' als nieuwe applicaties, bijvoorbeeld open source applicaties of zelf ontwikkelde applicaties. Automated patch generation, een van de onderzoeksgebieden binnen AVR, kan hiervoor een oplossing bieden.
4. *Risk based patching.* In sommige omgevingen brengt het doorvoeren van patches risico met zich mee. Een patch die onbedoelde neveneffecten heeft kan de stabiliteit van zulke omgevingen in gevaar brengen. Met AVR kunnen de (neven-)effecten van een patch worden geanalyseerd, zodat op basis van een onderbouwde risicoafweging kan worden gekozen om de patch wel of niet door te voeren.

[3] **Zie hoofdstuk 5 voor verdere uitwerking van de behoeften en toepassingsgebieden**

Routekaart AVR
De routekaart AVR kent 4 sporen.

1. *Onderwijs en opleiding*. Het spoor onderwijs en opleiding richt zich hoofdzakelijk op Uitbreiding van curricula en training en het geschikt maken van een basis cyber reasoning systeem (CRS) voor toepassing bij onderwijsdoeleinden en eventueel bij een cyberchallenge.
2. *Onderzoek*. Doel van dit spoor is versterking van het fundamentele AVR-onderzoek. Binnen het onderzoeksspoor is voorzien om in 2021 drie AIO's aan te stellen. De intentie is om de scope van de promotie-onderzoeken zo te kiezen dat academische relevantie zo goed mogelijk oplijnt met het adresseren van vraagstukken die praktische toepassing van AVR dichterbij brengen. Gekozen is voor de onderzoeksgebieden Automated patch generation / risk based patching en Automated vulnerability discovery. Van belang is dat de betrokken onderzoeksinstellingen in 2021 met elkaar een nadere onderzoeksagenda definiëren.
3. *Toepassing AVR*. Bij het toepasbaar maken van fundamentele (AVR) kennis tot aan validatie/demonstratie worden drie fasen doorlopen: Verkennen beschikbare kennis, technologie en toepassing, vervolgens het toepassen in (een) usecase(s) en tenslotte het consolideren in generieke technieken of tools. Er wordt gefocust op specifieke toepassingsgebieden. Met betrokken partners worden in 2021 specifieke projecten gedefinieerd en opgestart. TNO speelt hierbij een leidende rol.
4. *Fieldlab.* Het fieldlab is ondersteunend voor de andere sporen. Primair is het fieldlab hierbij verantwoordelijk voor informatieoverdracht en samenwerking tussen en binnen de sporen. Het is een virtuele ruimte waarbinnen experimenten en data kunnen worden uitgewisseld. Verder organiseert het fieldlab de samenwerking in alle sporen en faciliteert het actieve communicatie en het ontstaan van een AVR community.

In onderstaande figuur is de Routekaart (stand van zaken december 2020) samengevat. De routekaart zal jaarlijks worden geactualiseerd.



Organisatie en financiering

Het uitvoeren en door-ontwikkelen van de Routekaart kan worden gezien als een programma. Het programma moet worden bestuurd en worden gemanaged. Dit doen we middels de inrichting van een stuurgroep en het aanstellen van programmamanagers en projectleiders.

De stuurgroep wordt breed samengesteld (vergelijkbaar met het bestuur van het Samenwerkingsplatform cybersecurity), met vertegenwoordigers van bijvoorbeeld de Ministeries van EZK en Defensie, het hoger onderwijs, TNO als belangrijkste (toegepaste) kennisinstelling, cybersecurity bedrijven en eindgebruikers.

De programmamanager is primair verantwoordelijk voor het bewaken van de voortgang en het behalen van de resultaten in de gedefinieerde (en gefinancierde) stromen en projecten van de Routekaart AVR.

De programmamanager werkt samen met het Samenwerkingsplatform AVR. In dat platform werken immers 'innovatiemakelaars' aan het opzetten van programma's. Deze innovatiemakelaars hebben de verantwoordelijkheid ervoor te zorgen dat de Routekaart wordt uitgebreid. Ze jagen aan en ondersteunen bij het ontwikkelen van bijvoorbeeld nieuwe onderzoeksprogramma's en nieuwe samenwerkingsprojecten.

Van groot belang is de ontwikkeling van een AVR community. Het Virtueel Fieldlab speelt hier een belangrijke rol in.

In de Routekaart zullen op verschillende momenten belangrijke inhoudelijke besluiten moeten worden genomen. Van belang is dat deze besluiten pragmatisch, objectief en transparant worden genomen. De publicatie van deze Routekaart is een eerste stap in deze transparantie.

Voor realisatie van de ambities is voor 6 jaar een bedrag nodig van naar schatting 10 tot 15 miljoen euro. Op dit moment is een bedrag van €2.000.000 beschikbaar als start om de doelen van de Routekaart cybersecurity te realiseren. Op hoofdlijnen is de besteding van de beschikbare middelen weergegeven in deze routekaart[4].

Er is dus nog veel meer geld nodig om de ambitie van de Routekaart AVR te realiseren. Een juiste besteding van de nu beschikbare middelen, het actief aanhaken van de hele keten en het ontwikkelen van een AVR community en een groter focus op het onderwerp AVR zal moeten leiden tot het beschikbaar komen van meer middelen: het vliegwiel komt op gang.

[4] **Zie figuur 13**

2 Inleiding en context

Reeds enige tijd wordt er op initiatief van de Ministeries van Defensie, Economische Zaken en Klimaat en Justitie & Veiligheid gewerkt aan het onderwerp Automated Vulnerability Research (AVR).

Vooruitgang gaat zeer geleidelijk. Dit komt vooral doordat er nog relatief weinig mensen en organisaties zijn die aan dit onderwerp werken en er ook nog weinig contact tussen deze mensen en organisaties is. Ook potentiële gebruikersorganisaties van AVR zijn hier nog niet veel mee bezig. Dit is nogmaals gebleken na een serie interviews met allerlei personen en partijen vóór en kort na de zomer van 2020[5].

AVR, en in brede zin, security automation, worden gezien als logische en noodzakelijke middelen om cybersecurity te waarborgen. Er komt steeds meer cybersecurity werk en er zullen nooit voldoende gekwalificeerde resources beschikbaar zijn. Dus ligt voor de hand om (onderdelen) van de cybersecurity keten te automatiseren. Bij AVR gaat het hier primair om het automatisch vinden en duiden van onbekende kwetsbaarheden in software.

De betrokken ministeries willen nu overgaan tot een volgende stap en een Routekaart ontwikkelen voor het werken aan AVR. Hierbij is de hele cybersecurity keten van belang: van onderzoek en onderwijs tot toepassing (valorisatie). Financiële middelen worden beschikbaar gemaakt om een start te maken de Routekaart te realiseren. Voor het volledig realiseren van de Routekaart zullen in de komende jaren aanvullende middelen moeten worden gevonden. De Routekaart draagt hieraan bij. In deze Routekaart wordt ook een eerste indicatie gegeven waar de beschikbare middelen aan zouden kunnen worden besteed, en hoe besluitvorming hierover zou kunnen plaatsvinden.

Doelen Routekaart AVR
De algemene doelen van de Routekaart AVR zijn:

- Duidelijk maken hoe er in Nederland de komende 6 jaar aan AVR kan worden gewerkt.
- Een gecoördineerde start maken met activiteiten op het gebied van AVR in een drietal sporen. En daarmee een impuls geven aan kennisontwikkeling en -toepassing van AVR.
- Aan partners uit de keten duidelijk maken waar en hoe deze mee kunnen doen om AVR in Nederland verder te brengen.
- Ketenpartners inspireren om nieuwe impulsen aan AVR te geven.
- Een levende ‘community’ op het gebied van AVR op te starten.
- Inzicht geven wat er op korte en middellange termijn kan worden gerealiseerd: en daarmee de zowel de mogelijkheden als beperkingen verduidelijken.
- Bijdragen aan de digitale autonomie van Nederland.

[5] De gesprekken richtten zich primair op het opzetten van een cyberchallenge op het gebied van AVR.

Verankering AVR in de KIA Veiligheid en Missie Cybersecurity

Het belang van AVR en security automation wordt breed onderkend. De verankering van het belang van het onderwerp AVR kan worden gevonden in de KIA Veiligheid en de Missie cybersecurity. Zie figuur 1 voor een uitgebreider toelichting.

KIA Veiligheid

De Kennis- en innovatieagenda (KIA) Veiligheid is een verdere uitwerking van het maatschappelijke thema veiligheid zoals beschreven in het missiegedreven topsectoren- en innovatiebeleid. De missies uit de KIA zijn opgesteld door vakdepartementen in consultatie met vele partijen en topsectoren en vervolgens goedgekeurd door het kabinet. De uitwerking van deze missies heeft geleid tot een aantal Meerjarige Missiegedreven Innovatie Programma's (MMIP's), en moet leiden tot vele vormen van publiek-private samenwerking en het benutten van economische kansen voor grotere en kleinere bedrijven. De KIA's zijn 'first and foremost' een inventarisatie van de kennis en innovatiebehoeften bij bedrijven, departementen, de brede wetenschap, kennisinstellingen, NWO en regionale overheden. [6]

Missie Cyberveiligheid

De KIA Veiligheid is opgesteld door betrokken topsectoren High Tech Systemen en Materialen, Creatieve Industrie, Logistiek, Water & Maritiem en Team Dutch Digital Delta. De missie cyberveiligheid stelt zichzelf ten doel dat Nederland in staat moet zijn "om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren." Kennisontwikkeling en innovatie op het gebied van cybersecurity zijn noodzakelijk om dreigingen in het digitale domein tegen te gaan. Het doel van deze missie is cyberkennis en - kunde in Nederland te versterken, onderzoek en innovatie te faciliteren en een ecosysteem van experts en organisaties te bouwen. Om de Nederlandse cybersecurity kennisbasis te kunnen versterken is actieve, effectieve en meerjarige samenwerking over de gehele keten een randvoorwaarde.

Automated Vulnerability Research (AVR)

Ondanks toenemende investeringen in cybersecurity, kunnen de meeste organisaties de snelheid en ontwikkelingen van digitale dreigingen nauwelijks bijhouden. In de KIA Veiligheid wordt het automatiseren van cybersecurity werkzaamheden genoemd als een belangrijke oplossing om met beperkte capaciteit alsnog weerbaar te blijven. Onder deze noemer neemt AVR een centrale plaats in, met kennis- en innovatievragen betreffende "het ontwikkelen van manieren om geautomatiseerd kwetsbaarheden te signaleren in broncode", alsmede "het automatisch patchen op applicatie-niveau". De capaciteit om kwetsbaarheden op te sporen en te patchen voordat kwaadwillenden er misbruik van kunnen maken is ook essentieel voor digitale soevereiniteit wanneer andere statelijke actoren ook gebruik maken van geautomatiseerde aanvalstechnieken. AVR speelt verder een sleutelrol binnen het deelprogramma "Offensieve technologie". Om te komen tot innovatie op het gebied van AVR is intensieve samenwerking nodig tussen stakeholders vanuit de gehele cybersecurity keten.

Figuur 1: Verankering AVR als prioriteitsonderwerp in KIA en Missie cyberveiligheid

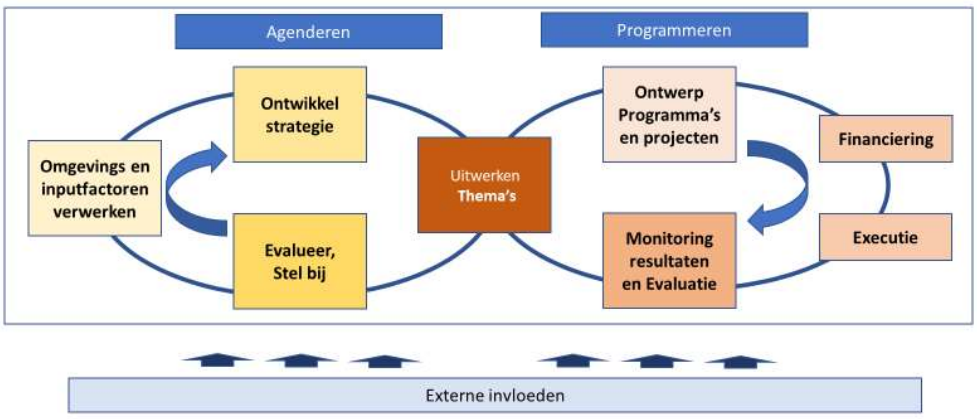
Agenderen en programmeren

Het uitwerken van een Routekaart past zeer goed bij de thematische aanpak en het proces van programmeren zoals beschreven in het Advies van de kwartiermakers voor het

[6] Referentie KIA

Samenwerkingsplatform cybersecurity.[7] In figuur 2 staat meer in detail wat in het advies staat over het proces van programmeren.

De thematische aanpak kent twee cycli: agenderen & programmeren



Programmeren betreft het uitwerken van de thema's (uit de agendering) in concrete programma's en projecten. De ontwerpen dienen concreet genoeg te zijn om op basis daarvan ook financiering te zoeken. Het zal doorgaans om een meerjarige 'Routekaart' gaan. In verschillende fases spelen verschillende partners een rol. Vraag en aanbod komen bij elkaar.

Het ontwerp van de programma's en projecten vraagt specifieke kennis en deskundigheid. Kennis van het thema: deze komt van de diverse partners in de keten. Kennis van de partners: wie zijn met het onderwerp bezig? Ook internationaal. En kennis van de mogelijkheden voor financiering. Hierbij gaat het om nationale en internationale subsidie mogelijkheden voor kennis en innovatie.

Een meerjarige Routekaart kan weliswaar worden ontwikkeld, maar de ervaring laat zien dat de echte beweging (realisatie) altijd start met kleinere projecten. Het zetten van de eerste stap is cruciaal voor later succes. De rol van de verschillende overheden zal hierbij essentieel zijn. Maar de overheden zijn zeker niet de enige initiatiefnemers. (Klein) Beginnen kan ook door bedrijven. Experimenteren kan worden gestimuleerd.

Programma's komen alleen van de grond indien er sprake is van echte behoeften bij één of meerdere partners. Des te beter programma's zijn uitgewerkt en des te meer betrokken partners zijn, des te groter is de kans dat voor programma's en projecten ook financiering wordt gevonden. Dat zegt de theorie, en er zijn voldoende voorbeelden uit de praktijk die de theorie staven. …

Indien er financiering is start de executie van de programma's en projecten. Gefaseerd. En op basis van resultaten zal worden geëvalueerd en zullen vervolgfasen al dan niet doorgang vinden. De cyclus van programmering eindigt dan ook met monitoring en evaluatie.

Figuur 2: Agenderen en programmeren8

[7] Zie. Samenwerkingsplatform cybersecurity. Advies kwartiermakers, 12 augustus 2020.
[8] Zie. Samenwerkingsplatform cybersecurity. Advies kwartiermakers, 12 augustus 2020, p. 18-19.

Concept Routekaart

Deze concept Routekaart is in de maanden september-november 2020 ontwikkeld. Op basis van de reeds verkregen inzichten en met steun van diverse partijen. En in de geest van het Advies van de kwartiermakers.[9]

Deze concept Routekaart is geenszins in beton gegoten:

- Op de eerste plaats doordat deze in een korte tijdsspanne tot stand is gekomen en er verschillende iteraties zijn voorzien om tot definitieve keuzes voor eerste projecten te komen
- Op de tweede plaats, en belangrijker, is dat het onderwerp zelf zich snel ontwikkelt. 6 jaar vooruit kijken is utopisch: we zullen door de ontwikkelingen worden ingehaald. Voorgesteld wordt de Routekaart tenminste jaarlijks te evalueren en te herijken.
- En op de derde plaats, omdat er naast de beschreven sporen en initiatieven hopelijk meer middelen en initiatieven komen om de Routekaart verder aan te vullen en succesvol uit te voeren.

De Routekaart is zo geschreven dat deze ook voor mensen met een niet technische achtergrond begrijpelijk zou moeten zijn. De Routekaart AVR bestaat uit de navolgende hoofdstukken.

In hoofdstuk 3 leggen we kort uit wat AVR eigenlijk is. Waarom het belangrijk is en waarom het zo'n lastig onderwerp is.

In hoofdstuk 4 zoomen we in op de resultaten die we willen behalen. Hierbij gaat het om een vergezicht over 6 jaar (de 'stip op de horizon') en over meer concrete doelen voor de kortere termijn.

Hoofdstuk 5 is de kern van het document en bevat de Routekaart AVR zelf.

Hoofdstuk 6 beschrijft de organisatie en financiering.

In hoofdstuk 7 zijn de vervolgstappen op hoofdlijnen weergegeven.

Hoofdstuk 8 vat tenslotte de belangrijkste risico's en mogelijke mitigerende maatregelen samen.

9 Op 30 september met vertegenwoordigers van de financiële sector (banken) en op 6 oktober met vertegenwoordigers van universiteiten, hogescholen en de cybersecurity sector. Waarbij organisaties en mensen zijn benaderd waarvan bekend is dat deze met het onderwerp AVR bezig zijn. Deze concept Routekaart zal opnieuw met deze partijen worden besproken

3 Wat is Automated Vulnerability Research

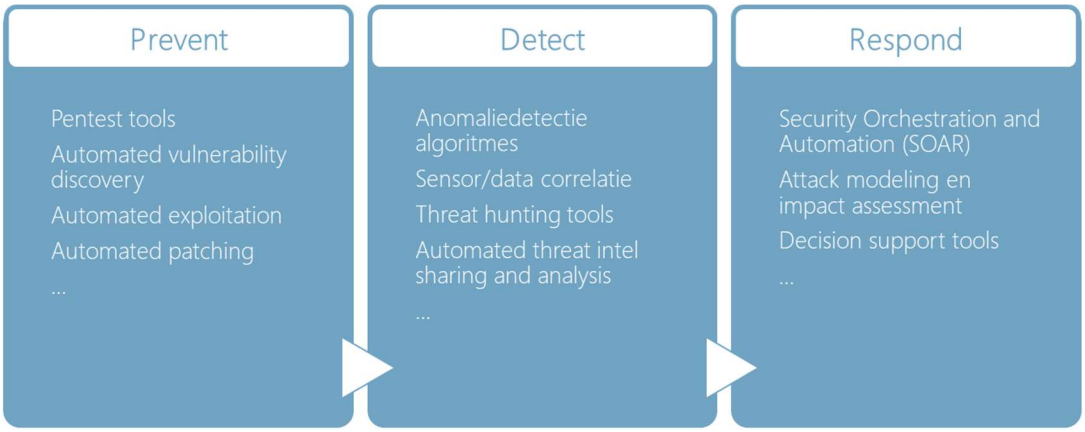
3.1 Automatisering in cybersecurity

Met de steeds toenemende digitalisering, en daarmee de afhankelijkheid van digitale devices en de data die deze verwerken, wordt ook het belang van cybersecurity breed herkend. Dit belang zal nog verder toenemen met de uitrol van het internet-of-things, ook in onze vitale infrastructuren.

Cybersecurity heeft echter te maken met een aantal uitdagingen, zoals:

- Het brede palet en het grote aantal cyberaanvallen waartegen we ons moeten verdedigen.
- De steeds grotere hoeveelheid informatie die snel moet worden verwerkt om aanvallen het hoofd te bieden.
- De substantiële schaarste aan cybersecurity-experts ten opzichte van een stijgende behoefte. Naar verwachting zal dit tekort aan personeel de komende jaren alleen maar toenemen.

Een belangrijke oplossingsrichting voor deze uitdagingen is het waar mogelijk automatiseren van cybersecurityhandelingen en -functies die nu nog door schaarse experts worden uitgevoerd.



Figuur 3: Positionering automated vulnerability research in de cybersecurity-keten

Automatisering kan worden toegepast in alle fasen van de cybersecurity-keten. Het NIST cyber security framework onderscheidt de functies 'protect', 'detect' en 'respond'[10], zie figuur 3. Binnen elk van deze functies wordt automatisering al toegepast en wordt onderzoek gedaan naar mogelijkheden tot verdere automatisering. Een voorbeeld is het consortium Automated Security Operations (ASOP) dat in september 2020 is gestart[11] met steun van het ministerie van EZK. Dit consortium heeft tot doel om in de komende jaren een platform te ontwikkelen waarmee organisaties cyberaanvallen geautomatiseerd, en daardoor sneller, kunnen ontdekken en beantwoorden. Het richt zich dus primair op de detect- en respond-functies in het NIST-model. ASOP

[10] Naast deze zijn ook de 'identify' en 'recover' onderdeel van het framework, echter deze zijn meer ondersteunend aan de andere. Het NIST framework is beschikbaar via https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

[11] https://cyberveilignederland.nl/consortium-automated-security-operations-asop-van-start/

is een voorbeeld van meerjarige programmering en publiek-private samenwerking tussen kennisorganisaties, overheid en de cybersecurity-industrie.

Maar ook in de “prevent” stap kan automatisering een belangrijke rol spelen. In de volgende paragrafen wordt uitgewerkt wat AVR is en hoe het bijdraagt aan de preventie van cybersecurity-incidenten.

3.2 Automated vulnerability research

AVR heeft als doel het (semi-)geautomatiseerd vinden van kwetsbaarheden. Hiermee is AVR onderdeel van het ‘prevent’ deel van de cybersecurity keten. (zie figuur 3)

De ‘prevent’ functie heeft betrekking op het voorkomen van cyberaanvallen. Een belangrijk aandachtspunt daarbij is het veilig houden van netwerken, computers en applicaties, o.a. door kwetsbaarheden tijdig te herkennen en op te lossen. In de huidige praktijk wordt dit ingevuld door patching (het systematisch doorvoeren van software updates die door leveranciers worden aangeboden), vulnerability scanning (het zoeken naar oude, onveilige softwareversies op eigen systemen) en pentesting/red teaming (technisch security-experts vragen om de security van eigen systemen te onderzoeken of zelfs te breken). Al deze activiteiten richten zich bijna uitsluitend op het vinden en herstellen van *bekende* kwetsbaarheden: kwetsbaarheden die bij de softwareleverancier en/of de security community bekend zijn.

Van alle software-kwetsbaarheden kennen we het grootste deel niet. Dat geldt voor vrijwel alle typen software. Het (onder-)zoeken van *nieuwe, onbekende* kwetsbaarheden in software gebeurt mondjesmaat door een kleine groep cybersecurity onderzoekers. Dit vakgebied, *vulnerability research*, vraagt zeer specialistische vaardigheden die zelfs binnen het bredere cybersecurity vakgebied schaars zijn. Is een kwetsbaarheid eenmaal gevonden, dan kan er een patch voor worden ontwikkeld waarna de kwetsbaarheid een plek krijgt in de reguliere processen van security patching.

Uiteraard hebben nieuwe, ‘zero-day’ kwetsbaarheden voor cyberaanvallers grote waarde. Voor een ‘zero-day’ kwetsbaarheid zijn nog geen patches beschikbaar, waardoor het voor een gebruiker praktisch onmogelijk is om zich ertegen te beschermen. Daarom is het belangrijk dat wanneer er een kwetsbaarheid gevonden wordt die actief misbruikt wordt, om deze snel mogelijk te patchen en openbaar te maken. Zoals onlangs gedaan is met een kwetsbaarheid die door het Google Project Zero gevonden is[12].

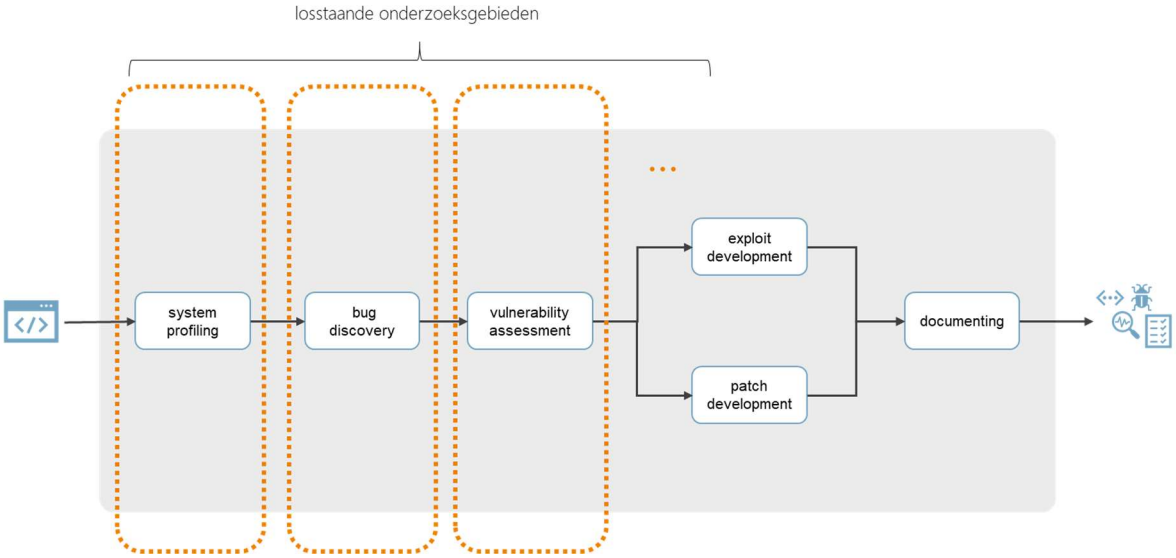
[12] **https://arstechnica.com/information-technology/2020/10/googles-project-zero-discloses-windows-0day-thats-been-under-active-exploit/#:~:text=Google's%20Project%20Zero%20says%20that,almost%20two%20weeks%20from%20now.&text=Attackers%20were%20combining%20an%20exploit,recently%20fixed%20flaw%20in%20Chrome**

In de V.S. investeert het instituut voor Defensie-onderzoek DARPA al jarenlang in onderzoek naar AVR. AVR-kennis en capaciteiten hebben dus een strategisch karakter, en zullen niet zonder meer tussen landen worden gedeeld.

Door zelf tijdig AVR-capaciteit op te bouwen kan Nederland de eigen vitale IT-systemen blijven beschermen, ook tegen aanvallers die geautomatiseerd en grootschalig onze kwetsbaarheden kunnen blootleggen.

3.3 Processtappen in AVR

AVR omvat verschillende onderzoeksgebieden, die op zichzelf staan maar onderling raakvlakken en afhankelijkheden hebben. Gezamenlijk werken deze onderzoeksgebieden toe naar een procesflow voor (semi-)automatische analyse van software-targets. In figuur 4 wordt een overzicht van deze procesflow gegeven.



Figuur 4: de verschillende processtappen binnen AVR

Processtappen die worden doorlopen zijn:

- Analyse van het software-target of beschikbare informatie daarover (profiling);
- Identificeren van ontwerp- of programmeerfouten die mogelijk een kwetsbaarheid hebben geïntroduceerd (bug discovery);
- Beoordelen of daadwerkelijk sprake is van een kwetsbaarheid, het type kwetsbaarheid, en hoe deze kan worden geëxploiteerd (vulnerability assessment);
- Ontwikkelen van een exploit voor de gevonden kwetsbaarheid (exploit development);
- Ontwikkelen van een patch die de kwetsbaarheid wegneemt (patch development).

Het onderzoek naar automated bug discovery ontwikkelt zich in recente jaren snel. Er is een groot aantal (open source) tools beschikbaar voor broncode analyse[13] en fuzzing[14]. Het effectief inzetten van deze tools en technieken brengt nog diverse (onderzoeks-)uitdagingen met zich mee. Automatisering van de latere processtappen staat nog in de kinderschoenen.

[13] https://owasp.org/www-community/Source_Code_Analysis_Tools
[14] https://arxiv.org/pdf/1812.00140.pdf

4 Ambitie Routekaart AVR

AVR versterkt het preventieve deel van de cybersecurityketen door automatisering van het vinden van bekende en onbekende kwetsbaarheden in software, ontwikkelen van exploits en het patchen van die kwetsbaarheden. De Routekaart AVR heeft een grote ambitie. Een 'stip op de horizon'.

De ambitie is om over zes jaar:

- Als Nederland een *leidende positie* in Europa te hebben op het gebied van Automated Vulnerability Research (AVR). Dit blijkt uit onder meer de combinatie van publicaties (thought leadership), PhD's, aantal studenten, patenten (of open source gemaakte technologie) en de omvang van commerciële dienstverlening
- *Technologie te hebben ontwikkeld* om op bedrijfsmatige wijze succesvol geautomatiseerd kwetsbaarheden te kunnen vinden.
    - In minimaal één substantiële IT ontwikkel- of beheeractiviteit (TRL 8+).
    - Voor automatisch patchen een goede uitgangspositie te hebben bereikt voor valorisatie en industrialisatie (TRL6+ demonstrators).
- Sector-specifieke toepassingen te hebben ontwikkeld. Zoals de capaciteit om geautomatiseerd kwetsbaarheden te vinden en/of deze te patchen, in door banken gebruikte software

Achterliggende beleidsdoelstellingen zijn bevordering van digitale veiligheid, ook van het MKB, versterken economisch verdienvermogen en strategische autonomie in het digitaal domein.

Om de ambitie te kunnen bereiken zijn meer mensen nodig, meer expertise en meer diensten.
Als procesdoelstellingen gelden:

- De hele valorisatieketen is betrokken;
- Onderzoek en ontwikkeling vinden plaats in samenwerking met meerdere maatschappelijke sectoren;
- Kennis en technologie worden door minimaal twee Nederlandse bedrijven (liever meer) geadopteerd voor commerciële doorontwikkeling. Als er onverhoopt geen bedrijf op wil treden als technology provider, wordt oprichting van één of meer start-ups gestimuleerd.

Voor het bereiken van de ambities is naar eerste schatting een bedrag van 10-15m€ nodig. Bij de uitvoering van de Routekaart zal de vraag blijven of en hoe we *Nederland* en het Nederlandse belang voorop kunnen blijven zetten, bij een onderwerp dat ook sterk internationaal is (denk aan o.a. export control). In hoofdstuk 7 wordt nader ingegaan op de financiering van de Routekaart.

De doelen van de Routekaart AVR sluiten aan bij de doelen van het Samenwerkingsplatform cybersecurity en zijn daarvan ook afgeleid. De doelen van het samenwerkingsplatform staan in figuur 5 weergegeven.

Samenwerkingsplatform cybersecurity
Het platform kiest voor een doel- en resultaatgerichte aanpak op basis van een missie, visie en doelen. De gekozen werkwijze draagt steeds aantoonbaar bij aan het behalen daarvan.

- **Missie**: Bijdragen aan een veiliger, slimmer, digitaal autonoom en economisch sterker Nederland
- **Visie**: Het samenwerkingsplatform cybersecurity brengt vraag, aanbod en financiering voor cybersecurity onderwijs, onderzoek, innovatie en toepassing effectief bij elkaar.
- **Doelen**:
    - Er zijn voldoende goed opgeleide cybersecurity mensen in Nederland, én
    - We genereren internationaal leidende expertise in cybersecurity in Nederland, én
    - Deze expertise leidt tot effectieve toepassing in Nederlandse producten en diensten: er is valorisatie.

Figuur 5: Overzicht missie, visie en doelen van het samenwerkingsplatform cybersecurity

De ambitie kan worden uitgewerkt in meer concrete doelen. Bijvoorbeeld::

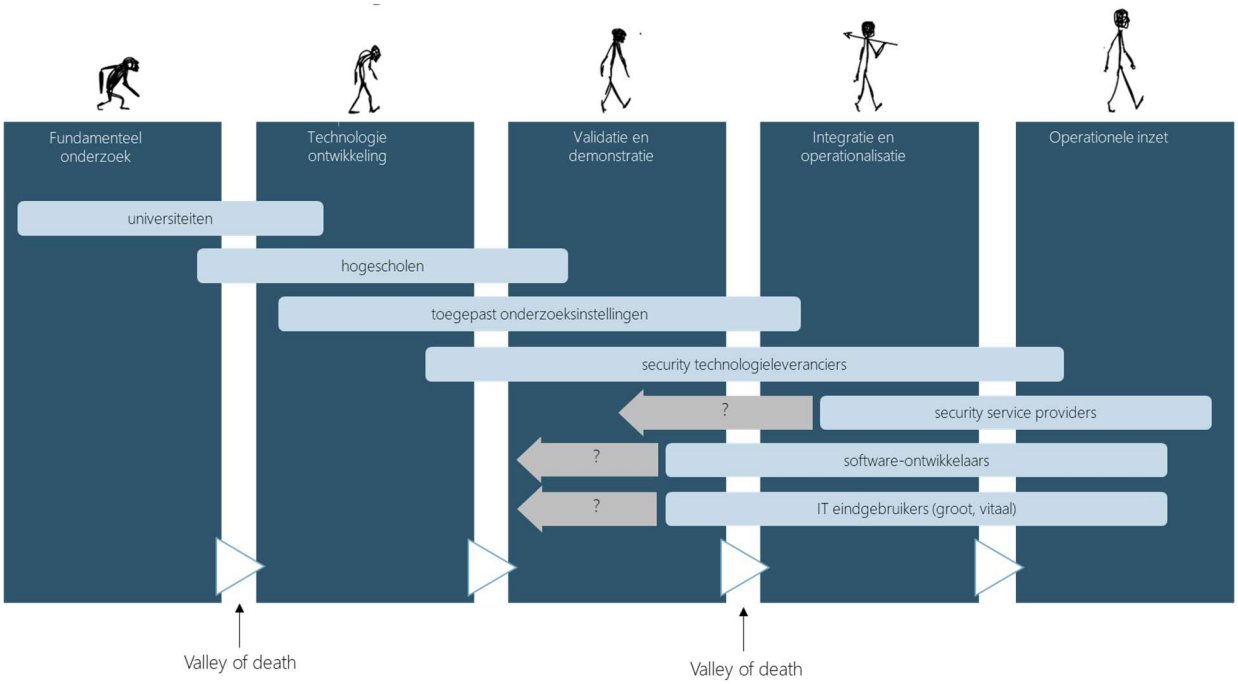
- *Cybersecurity mensen*
    - Lesmateriaal op het gebied van AVR is beschikbaar voor het hoger onderwijs en voor cybersecurity specialisten in het bedrijfsleven. Het lesmateriaal wordt tenminste gebruikt bij alle relevante Masteropleidingen.
    - Er is een technische omgeving waarin door studenten op het gebied van AVR kan worden geëxperimenteerd, gebaseerd op een Cyber Reasoning Systeem.
    - Er is een jaarlijkse challenge op het gebied van AVR waar teams van diverse universiteiten en hogescholen aan deelnemen.
    - Er is een constante stroom van vraag en aanbod van relevante stageplaatsen voor cybersecurity studenten
    - Over 6 jaar is er een significante toename van AVR specialisten onder master studenten, promovendi, vaste medewerkers in het hoger onderwijs, en specialisten bij cybersecurity dienstverleners en bij eindgebruikers
- *Cybersecurity expertise*
    - Er is een actieve community van AVR experts in Nederland die elkaar kent en regelmatig contact heeft. Hierbij gaat het om experts uit de hele cybersecurity keten
    - Jaarlijks starten er promovendi met research projecten op het gebied van AVR
    - Er zijn helder gedefinieerde (gezamenlijke) onderzoeksprogramma's op het gebied van AVR
    - Betrokken onderzoeksgroepen staan in Europa en de wereld bekend om hun AVR expertise
    - Deze expertise komt tot uitdrukking in zowel wetenschappelijke publicaties als in nationaal ontwikkelde tools en producten op het gebied van AVR.
- *Cybersecurity toepassing*
    - Het (academische) onderzoek aan AVR leidt tot (een bruikbare basis voor) tools en producten, die bekend zijn bij kennisinstellingen, cybersecurity dienstverleners en eindgebruikers

- Sector specifieke toepassingen. Bijvoorbeeld voor de banken, en/of voor de cybersecurity dienstverleners
- Er is een stroom van projecten om de tools en producten toepassingsgeschikt te maken. Hierin wordt door diverse partners in de keten samengewerkt.
- Verschillende tools worden door cybersecurity dienstverleners en eindgebruikers (commercieel) ingezet
- Nationale partijen dragen zorg voor onderhoud, doorontwikkeling en ondersteuning van tools en producten.

5 De Routekaart AVR

5.1 De innovatieketen

Onderstaande figuur 6 geeft een overzicht van de innovatieketen, waarbij het fundament wordt gelegd met academisch onderzoek, verschillende fasen worden doorlopen om deze kennis toepasbaar te maken, met als uiteindelijk resultaat inzet bij eindgebruikers in operationele omgevingen.



Figuur 6: De routekaart AVR in relatie tot de innovatieketen

De figuur benoemt ook de typen organisaties die voor AVR een rol kunnen spelen in de innovatieketen. Bekende uitdagingen zijn de “valleys of death”:

- Van basic research naar technologieontwikkeling
- Van demonstratie naar operationalisering

De eerste valley of death kan worden overbrugd door nauwe samenwerking tussen universiteiten en toegepast onderzoek. Daarnaast is belangrijk dat de eindgebruikers van AVR technologie in een vroegtijdig stadium worden betrokken om zo de tweede valley of death te omzeilen.

In AVR kunnen we twee typen eindgebruikers onderscheiden:

- Organisaties die hun eigen systemen en software willen beschermen. Hieronder vallen IT-eindgebruikers die voor hun bedrijfsvoering leunen op IT en data. Maar ook softwareontwikkelaars die de kwaliteit en security van hun producten willen bewaken.
- Cybersecurity-bedrijven die de daadwerkelijke eindgebruikers bedienen. Hierbij onderscheiden we bedrijven die security-technologie ontwikkelen, en bedrijven die security services aanbieden.

Uiteraard betreft het hier rollen en zijn er organisaties die meerdere rollen combineren.

We richten ons met de Routekaart AVR in eerste instantie op Nederlandse partijen die een rol kunnen spelen in de ontwikkeling van AVR. Er kunnen ook buitenlandse partijen worden betrokken, bijvoorbeeld als zij (security-)producten leveren die door Nederlandse organisaties breed worden gebruikt. Voorbeelden zijn antivirus-leveranciers en de ontwikkelaars van operating system kernels.

5.2 Waar staan we op dit moment?

Om technologie te kunnen ontwikkelen voor automated vulnerability research, zijn allereerst ervaren vulnerability researchers nodig. Experts die de technieken kennen, begrijpen hoe automatisering daarin een plaats kan krijgen en bijdragen aan de ontwikkeling daarvan. In Nederland is het aantal experts dat zich daadwerkelijk bezighoudt met vulnerability research zeer beperkt. Slechts een handvol organisaties houdt zich er (min of meer) structureel mee bezig.

Aan de Nederlandse universiteiten wordt AVR als belangrijk onderzoeksveld herkend. Kwetsbaarheden bestaan in vele vormen maar wanneer de focus ligt op kwetsbaarheden in software/firmware binaries (zoals bij de DARPA cyber grand challenge), is diepgaande kennis van software en systemen een noodzakelijk voorwaarde. De cybersecurity groep van de VU is hierin gespecialiseerd en heeft van de Nederlandse universiteiten de sterkste kennispositie.
Ook andere universiteiten en hogescholen besteden in hun curriculum aandacht aan softwarekwetsbaarheden en exploitatie daarvan. Ook vindt aan verschillende universiteiten onderzoek plaats dat meer of minder nauw gerelateerd is aan AVR. Toch is de totale omvang van het academische AVR-onderzoek in Nederland gering, zeker ten opzichte van belangrijke andere landen, en is een substantiële extra impuls nodig om te zorgen dat de kennisachterstand niet groeit. .

Naast de onderwijsinstellingen heeft ook de cybersecurity-onderzoeksgroep van TNO zich enkele jaren geleden toegelegd op onderzoek naar AVR. Daarbij richt TNO zich op het toepasbaar maken van de huidige AVR technologie en het scheppen van voorwaarden om deze verder te brengen richting praktische toepassing.

In de eerder genoemde serie interviews die dit jaar is uitgevoerd onder Nederlandse cybersecurity bedrijven, gaven de meesten aan zich nu niet met vulnerability research bezig te houden. Zij richten zich vooral op bekende kwetsbaarheden. Die oplossen blijkt in de praktijk al een grote opgave. En zolang reguliere patching niet op orde is, heeft dat de hoogste prioriteit. Wel wordt AVR door deze bedrijven als een belangrijk onderzoeksthema gezien. Ook geeft een deel van de organisaties aan dat AVR technologie, eenmaal volwassen, mogelijk kan worden toegevoegd aan hun dienstenportfolio.

Tenslotte kent Nederland veel hackers, sommige heel capabel, die zich professioneel of in vrije tijd bezig houden met cybersecurity. Dit is een waardevolle kennispoel. Op dit moment verdienen talentvolle hackers die vulnerability research zouden kunnen doen, in de praktijk hun geld met andere cybersecurity-activiteiten omdat dat is waar de markt in 2020 om vraagt. Enkele gedreven vulnerability researchers verdienen zogenaamde. ‘bug bounties’ door kwetsbaarheden te melden bij

de softwareleverancier. Het bekendste platform hiervoor is HackerOne[15], een online platform waar softwareleveranciers hun producten aanbieden aan de hackercommunity om er tegen beloning kwetsbaarheden in te vinden. HackerOne heeft zijn hoofdkwartier in Silicon Valley en een bedrijfswaarde van bijna een miljard dollar. HackerOne is in 2012 opgericht door twee Groningse hackers, uit frustratie dat zij de softwarekwetsbaarheden die ze zelf vonden niet konden rapporteren.

5.3 Stakeholders

In 2020 is in opdracht van de ministeries van EZK, Defensie en J&V een inventarisatie gedaan van partijen die een belang hebben bij en/of actief zij op het gebied van AVR. In onderstaande figuur 7 worden deze partijen en hun (mogelijke) rollen aangegeven. Ook is aangegeven welke partijen al actief zijn op het gebied van onderzoek/toepassing van AVR, en welke geïnteresseerd zijn en/of concrete plannen hebben om actief te worden op het gebied van AVR.

		Fundamenteel onderzoek	Technologieontwikkeling	Demonstratie en validatie	Integratie en operationalisatie	Operationele inzet
Onderzoek						
	Vrije Universiteit	√	√			
	Universiteit Twente	√				
	TU Delft	√				
	Radboud Universiteit	√				
	Rijksuniversiteit Groningen	√				
	Open Universiteit	√				
	Hogeschool van Amsterdam		√			
	Hogeschool Leiden		√			
	TNO		√	√	√	
Cybersecurity-bedrijven						
	KPN			√	√	√
	Deloitte			√	√	√
	CapGemini			√	√	
	Riscure		√	√	√	√

[15] https://www.hackerone.com/company

	Secura				√	√
	QBit				√	√
	Cybersprint				√	√
	Zerocopter				√	√
	Tesorion				√	√
	SIG en CIP overheid				√	√
	NBV (Min. van BZK)				√	√
IT-eindgebruikers en softwareontwikkelaars						
	ING				√	√
	Rabobank				√	√
	ABN AMRO				√	√
	Ministerie van Defensie			√	√	√

groen: al actief in AVR
oranje: interesse in AVR aangegeven

Figuur 7: AVR-interesse en -activiteit bij organisaties (stand 2020).

Er zijn meer partijen die in de komende jaren kunnen worden betrokken. Deze tabel geeft slechts de huidige gecontacteerde organisaties weer.

5.4 Waar liggen de behoeften?

In de maanden september en oktober zijn sessies gehouden met een deel van de hierboven genoemde stakeholders om de interesse voor, en de mogelijke toepassingen van AVR te bespreken. In de verschillende gesprekken zijn specifieke toepassingen besproken, met daarnaast de specifieke behoeften en bijdragen die partijen kunnen leveren. Beide worden in de komende paragrafen besproken.

5.4.1 Toepassingen

In de gevoerde gesprekken zijn de volgende toepassingen als het meest waardevol benoemd:

Toepassing 1: secure software development
Door AVR toe te passen binnen het softwareontwikkelproces kunnen kwetsbaarheden in een vroegtijdig stadium, voordat de software wordt ingezet, worden verholpen. Dit past binnen de beweging om security al vroeg in de levenscyclus van systemen aandacht te geven ("shift security left").
Met name grote softwareontwikkelaars gebruiken al statische en dynamische security testing, en ook wordt dit toegepast op populaire open source libraries. En GitLab, een van de leidende aanbieders van CI/CD (softwareontwikkeling) toolchains, heeft recent twee securitybedrijven opgekocht die gespecialiseerd zijn in fuzzing, met als doel om dit in hun portfolio te integreren.

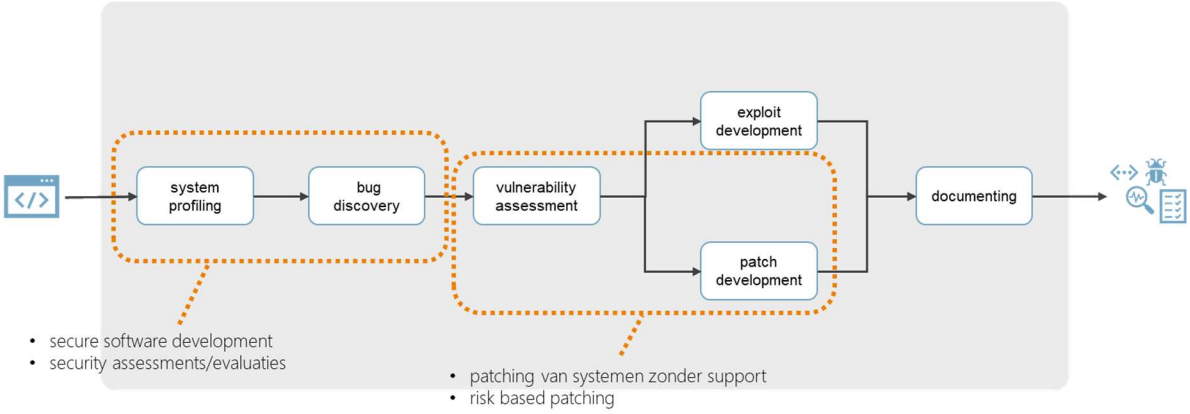
Toepassing 2: security assessments/evaluaties

In Nederland zijn enkele bedrijven gespecialiseerd in het uitvoeren van security-evaluaties van IT-componenten waarvan de security cruciaal is. Bijvoorbeeld omdat deze worden ingezet in gerubriceerde netwerken, of omdat ze het fundament vormen waarop andere securitymaatregelen zijn gebouwd. Bij deze evaluaties wordt de security diepgravend onderzocht, o.a. door analyse van sourcecode, hardware, side channel analyses etc.
AVR kan er aan bijdragen om deze evaluaties verder te automatiseren, aanvullende typen analyse uit te voeren, en daarmee het proces (kosten-)effectiever te maken.

Toepassing 3: patching van systemen zonder support
Patching is een regulier proces waarbij sofware-updates door leveranciers beschikbaar worden gesteld aan hun klanten. Zo kunnen kwetsbaarheden worden verholpen, kort nadat ze gevonden of gemeld zijn.
Voor veel IT-systemen worden echter geen patches uitgebracht, ofwel doordat de supporttermijn verlopen is, ofwel (bijvoorbeeld in het geval van veel open source software) omdat er geen verantwoordelijke partij is voor het uitbrengen van patches. Het betreft zowel 'oude systemen' als nieuwe applicaties, bijvoorbeeld open source applicaties of zelf ontwikkelde applicaties.
Automated patch generation, een van de onderzoeksgebieden binnen AVR, kan hiervoor een oplossing bieden. Dit onderwerp heeft veel interesse uit de financiële sector.

Toepassing 4: risk based patching
In sommige omgevingen brengt het doorvoeren van patches risico met zich mee. Een voorbeeld is de operationele technologie die veel in industrie en vitale infrastructuren wordt toegepast. Een patch die onbedoelde neveneffecten heeft kan de stabiliteit van zulke omgevingen in gevaar brengen.
Met AVR kan enerzijds het effect van een patch worden geanalyseerd. Anderzijds kan AVR worden gebruikt om de kwetsbaarheid te beoordelen waarvoor de patch bedoeld is.
Zo kan een onderbouwde risicoafweging worden gemaakt voor het al dan niet doorvoeren van de patch.

De eerste twee toepassingen maken gebruik van de stappen voorin het AVR-proces: het automatisch analyseren van een softwarecomponent om daar fouten/bugs in te vinden. De laatste twee toepassingen zitten juist achterin het AVR-proces: automatiseren van het patching-proces, nadat de kwetsbaarheid al gevonden is. Dit is in figuur 8 visueel weergegeven.

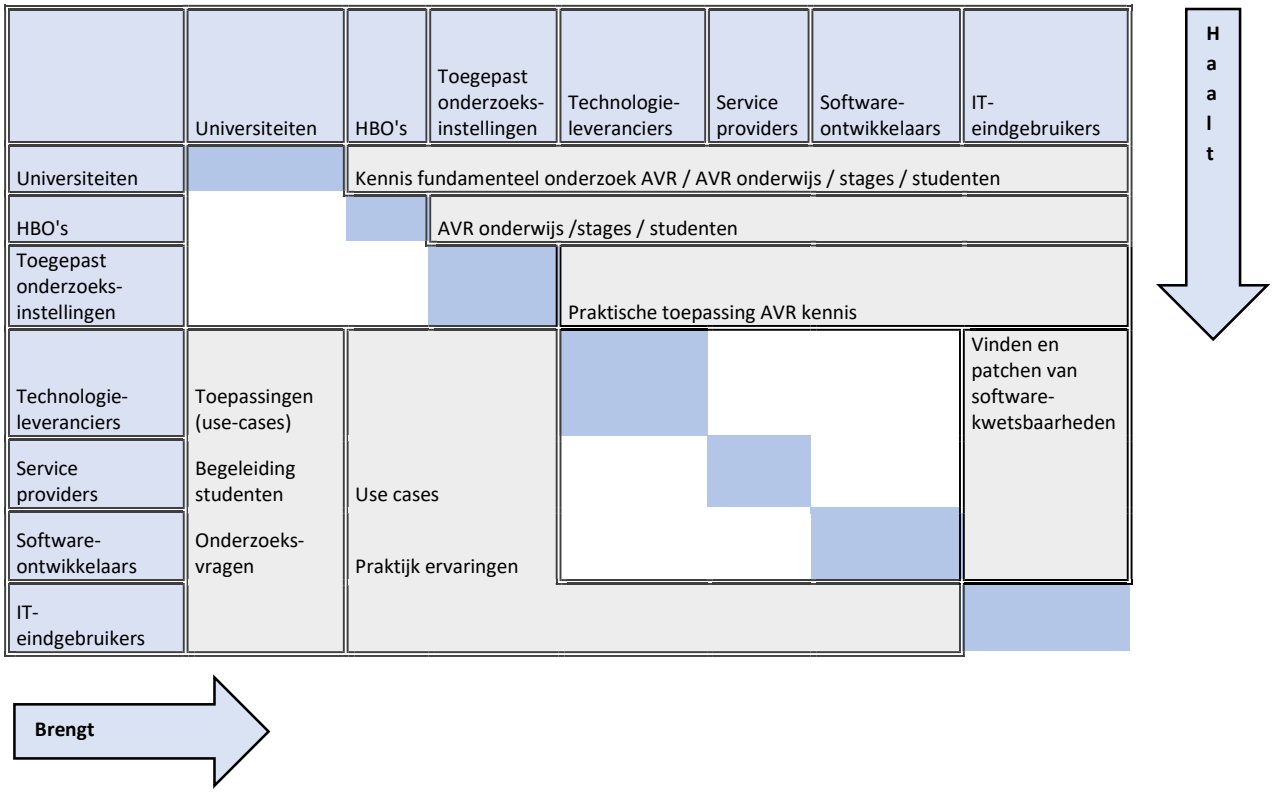


Figuur 8: Mogelijke toepassingen in relatie tot de processtappen AVR

Een ander onderscheid is, dat al veel onderzoeksresultaten en tools beschikbaar zijn die zijn gericht op het vinden van kwetsbaarheden. Weliswaar is nog veel onderzoek nodig om de effectiviteit van deze technieken en tools te verbeteren, maar het is al wel mogelijk om op basis van de huidige stand der techniek resultaten te bereiken. Het automatiseren van patching is nog minder ver gevorderd in de innovatieketen. Hier is primair fundamenteel onderzoek nodig om methoden en haalbaarheid te bestuderen.

5.4.2 Behoeftematrix

In de gesprekken met de verschillende partijen is door alle partijen aangegeven welke specifieke behoeften er zijn, en welke specifieke bijdragen er kunnen worden geleverd. Deze input is samengevat in de behoeftematrix in figuur 9.



Figuur 9: De behoeftematrix AVR

5.5 De Routekaart

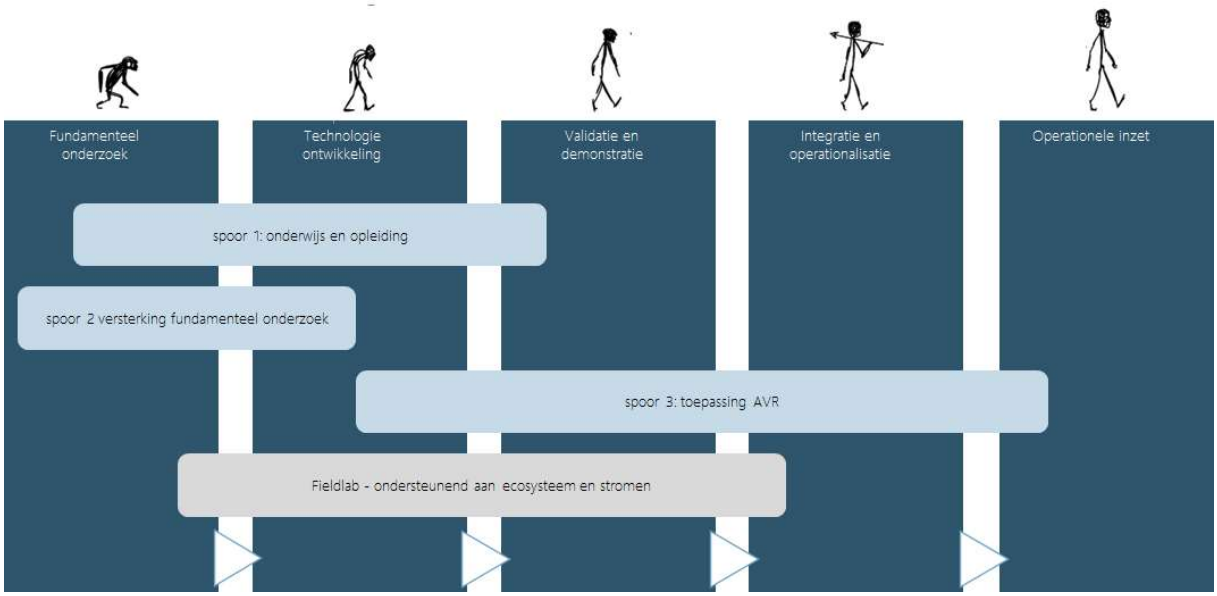
Doel van de routekaart is om de nationale capaciteiten op het gebied van AVR te versterken en uit te bouwen, en de achterstandspositie die Nederland ten opzichte van andere landen heeft te beperken of zelfs in te lopen (zie hoofdstuk 4 voor meer detail). Dit vraagt een meerjarige investering in kennis en technologieontwikkeling.

De routekaart richt zich op de periode 2021 tot en met 2026, omdat in zes jaar een substantiële impuls kan worden gegeven en concrete resultaten kunnen worden bereikt.

Binnen de routekaart zijn nu drie sporen gedefinieerd:

1. Onderwijs en opleiding
2. Versterking fundamenteel onderzoek
3. Toepassing

Ondersteunend aan deze sporen, en aan de kruisbestuiving tussen de sporen, is een 'field lab' voorzien. In figuur 10 zijn de drie sporen en het fieldlab in de innovatieketen gepositioneerd.



Figuur 10: de sporen van de routekaart AVR over de valorisatieketen heen

5.5.1 Spoor 1: Onderwijs en opleiding

Het spoor onderwijs en opleiding richt zich hoofdzakelijk op:

- Uitbreiding van curricula en training
- Geschikt maken van een basis cyber reasoning systeem (CRS) voor toepassing bij onderwijsdoeleinden **en eventueel bij een** cyberchallenge

Uitbreiding curricula

Om het onderwijs op het onderwerp AVR te verstevigen en te verbreden, zal een lespakket worden samengesteld dat kan worden gebruikt binnen de verschillende cybersecurity opleidingen. Er is reeds materiaal beschikbaar op verschillende universiteiten en hogescholen. Er wordt niet vanaf nul gestart. Doel is om gebruik te maken van het lesmateriaal dat nu al aan de verschillende universiteiten wordt gebruikt en dit te integreren, consolideren en breder beschikbaar te maken. Van belang is hierbij dat deze module op verschillende niveaus toegepast moet kunnen worden, zodat deze zowel door universiteiten als hogescholen zal worden gebruikt. Doel is ook om het onderwerp AVR attractiever te maken waardoor het voor meer (cybersecurity) studenten interessant wordt. Het

Cyber Reasoning Systeem zal hier ook aan bijdragen (zie de navolgende paragraaf). Het in de toekomst organiseren van een challenge zal ook naar verwachting een positieve aantrekkingskracht hebben op studenten.
Tenslotte zal trainingsmateriaal worden ontwikkeld gericht op de toepassing van AVR bij bedrijven. Dit draagt bij aan de integratie en acceptatie van AVR-technologie bij eindgebruikers. Bedrijven geven aan behoefte te hebben aan goed opgeleide mensen op dit terrein.
Qua werkwijze ligt voor de hand te starten met lesmateriaal voor WO en het materiaal voor HBO en bedrijven daar van af te leiden. Van belang is ook te waarborgen dat de opleiding niet alleen theoretisch is maar juist ook mogelijkheden biedt voor het opdoen van 'hands on' ervaring (zie hiervoor ook de CRS ontwikkeling).

Voor de ontwikkeling van de lespakketten is geld niet zozeer de beperkende factor, maar de benodigde tijd van de (schaarse) experts. Gezocht moet worden naar een pragmatische manier om tot bundeling van kennis en materialen te komen. Het strekt ook tot aanbeveling om de lespakketten modulair op te bouwen, gericht op de verschillende processtappen in AVR. Tenslotte moet er ook aandacht zijn voor het up-to-date houden van het lesmateriaal: de AVR wereld verandert zeer snel.

Uitvoering:

- VU, TU Delft, UT (master curriculum)
- Hogescholen
- TNO (trainingsmateriaal bedrijven)

Start: 2021

Cyber reasoning systeem
In het voorgaande traject heeft TNO een eerste versie van een Cyber reasoning systeem gebouwd. Dit CRS bestaat uit modules die gezamenlijk alle stappen om kwetsbaarheden te vinden, exploiten en te patchen. Het CRS bevat dus veel 'basistechnologie'.

In spoor 1 zal dit CRS verder geschikt gemaakt worden voor gebruik in de volgende toepassingen:

- Ondersteuning bij de curricula. Studenten kunnen tijdens het lespakket werken met en aan het CRS, om zo beter inzicht te krijgen in de verschillende stappen die vereist zijn in het kwetsbaarheden onderzoek.
- Afstudeeropdrachten. Er kunnen afstudeeropdrachten gedefinieerd worden waarbij studenten verbeteringen in het CRS ontwikkelen, of hier nieuwe modules voor ontwikkelen. Dit kan bij voorkeur in overleg met de (cybersecurity) bedrijven gebeuren.
- Cyberchallenge. Eventueel kan er een (jaarlijkse) cyberchallenge georganiseerd worden. In deze cyberchallenge kunnen studenten in een competitie werken aan nieuwe modules voor dit CRS.
- Datasets. Er is (dringend) behoefte aan geschikte datasets waar studenten mee kunnen werken. Onderzocht moet worden of deze, bv. als onderdeel van het CRS, beschikbaar kunnen komen.

Uitvoering:

- TNO, VU

5.5.2 Spoor 2: Versterking fundamenteel onderzoek

Doel van dit spoor is versterking van het fundamentele AVR-onderzoek. Hiervoor zal de kennispositie van de VU als leidende onderzoeksgroep verder worden versterkt. Daarnaast is een doel om het onderwerp bij de andere cybersecurity onderzoeksgroepen prominenter te maken en zo de basis te verbreden.

In dit spoor dient op de eerste plaats nog beter in kaart te worden gebracht welk onderzoek al plaatsvindt. Kennis hierover is nu nog fragmentarisch. Hierbij gaat het niet alleen om het onderzoek aan de universiteiten en hogescholen. Ook het Ministerie van Defensie, TNO en mogelijk andere overheidsinstellingen verrichten onderzoek op het gebied van AVR.
Doel is om eerst meer inzicht en overzicht te krijgen, en vervolgens (gezamenlijk) nieuwe onderzoeksprogramma's te definiëren.

Binnen het onderzoeksspoor is voorzien om in 2021 drie AIO's aan te stellen. De intentie is om de scope van de promotie-onderzoeken zo te kiezen dat academische relevantie zo goed mogelijk oplijnt met het adresseren van vraagstukken die praktische toepassing van AVR dichterbij brengen. Hiertoe wordt van AIO's verwacht dat zij actief bijgedragen aan het fieldlab, en waar mogelijk tussenresultaten overdragen aan de andere sporen.

Spoor 2 richt zich op de volgende onderzoeksgebieden:

- Automated patch generation / risk based patching
- Automated vulnerability discovery

Zoals aangegeven in **Error! Reference source not found.** liggen de eerste nog volledig in de fase van fundamenteel onderzoek. Ook automated vulnerability discovery kent echter nog fundamentele onderzoeksuitdagingen, en op dit thema is nauwe aansluiting mogelijk met de projecten in spoor 3. Het zwaartepunt voor de AIO's ligt dan bij de thema's die nog volledig in de fase van fundamenteel onderzoek zijn.

Voorstel is om in 2021 twee AIO's te laten starten op de onderzoeksthema's rond patching en één AIO op automated vulnerability discovery. Om de continuïteit van het onderzoek te waarborgen is het waarschijnlijk verstandig om ook in de jaren vanaf 2022 regelmatig AIO's aan te stellen (gemiddeld minstens één per jaar).

Belangrijker nog is om gezamenlijk nadere keuzes te maken voor nieuwe onderzoeksimpulsen voor specifieke deelthema's. En hiervoor onderzoeksvoorstellen te formuleren en funding te zoeken, bijvoorbeeld in het kader van een NWA-call of Europese onderzoeksprogramma's.

Automated/risk based patching
Binnen het spoor automated patch generation / risk based patching wordt fundamenteel onderzoek gedaan naar het automatisch ontwikkelen van patches voor gevonden kwetsbaarheden, het geautomatiseerd beoordelen van de ernst van een kwetsbaarheid, en het analyseren van de effecten van een patch (patch qualification).
Toepassingen van dit onderzoek zijn het kunnen prioriteren van kwetsbaarheden naar risico, beslissingsondersteuning over al dan niet patchen, en het verkorten van de kosten en doorlooptijd om patches te ontwikkelen.

Tussenresultaten van het onderzoek kunnen naar verwachting in de loop van 2023 worden gebruikt in spoor 3, mogelijk voor een eerste use case.

Start: in 2021, twee AIO's

Automated vulnerability discovery
Automated vulnerability discovery richt zich op het vinden van nog niet bekende kwetsbaarheden. Dit onderzoek bouwt voort op eerder onderzoek aan de VU. Doel van dit traject zal zijn om te verkennen hoe kwetsbaarheden zo vroeg mogelijk in het software ontwikkelproces gevonden kunnen worden, bijvoorbeeld door het combineren van fuzzing met andere analysetechnieken.

Deze kennis zal al in 2021 van belang zijn voor spoor 3, waar gestart wordt met het toepassen van automated vulnerability discovery in het software ontwikkelproces, op basis van de dan beschikbare technieken en tools.

Start: 2021 , één AIO

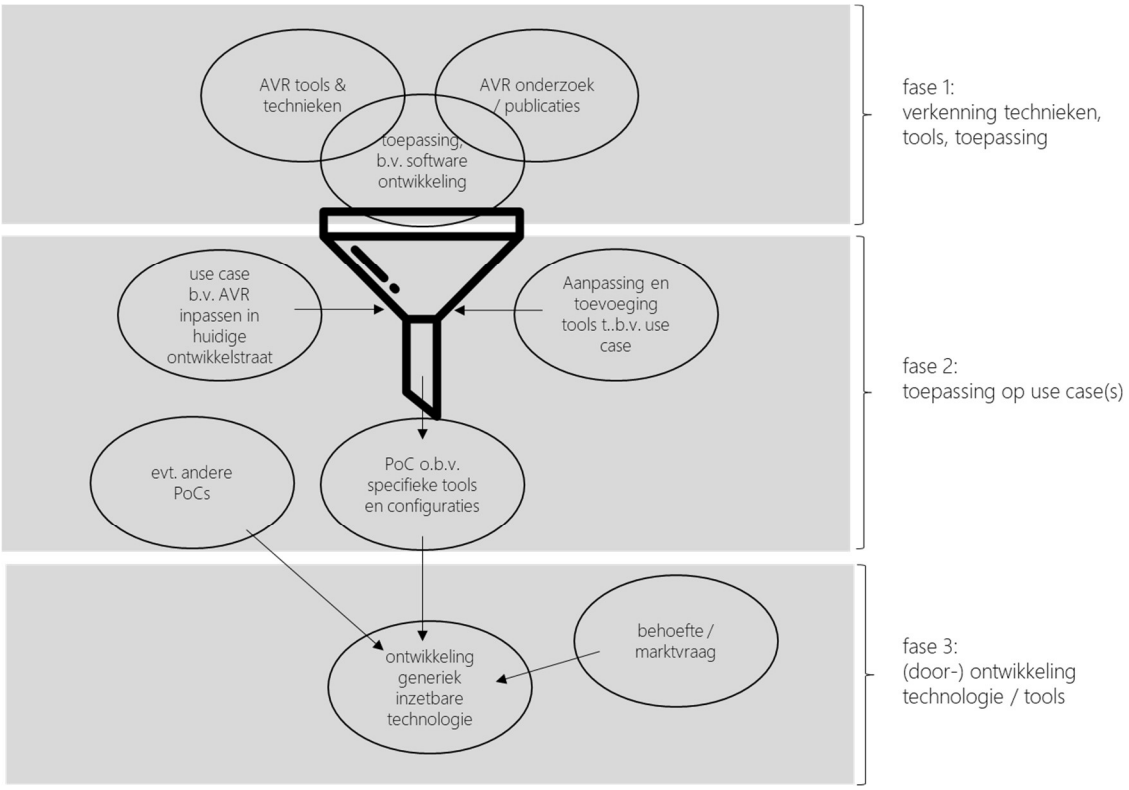
5.5.3 Spoor 3: Toepassing AVR

Bij het toepasbaar maken van fundamentele (AVR) kennis tot aan validatie/demonstratie worden drie fasen doorlopen:

- Verkennen beschikbare kennis, technologie en toepassing
- Toepassen in (een) usecase(s)
- Consolideren in generieke technieken of tools

Deze fasen vormen een zandlopermodel. In de verkenningsfase wordt kennis en experimentele ervaring opgedaan met een breed spectrum aan actuele AVR-technieken en tools, voor een specifieke toepassing (bijvoorbeeld: software-ontwikkeling). Dit geeft inzicht in mogelijkheden en beperkingen, configuratie-opties, combinatiemogelijkheden etc. In de tweede fase wordt een specifieke use case gekozen (bijvoorbeeld: het aantonen van kwetsbaarheden in een specifiek software-target). Hierbij worden alleen die kennis, technieken, configuraties etc. gecombineerd die aan de use case kunnen bijdragen, en worden waar nodig use-case specifieke aanpassingen gedaan. Nadat één of meer use cases succesvol zijn doorlopen kunnen de toegepaste technieken worden geconsolideerd en doorontwikkeld tot tools die generieker inzetbaar zijn. Dit proces in weergegeven in figuur 11.

In fasen 2 en 3 is inbreng van, en toetsing door, potentiële eindgebruikers noodzakelijk. Zij kunnen relevante use cases aandragen, evenals randvoorwaarden om technologie in hun bedrijfsproces te kunnen integreren. In zekere zin staan de use cases ook aan de basis van spoor 2 (onderzoek). Immers, het onderzoek zou zich zo mogelijk moeten richten op de voor het veld interessante toepassingen om de kans op valorisatie te verhogen. De relatie tussen de sporen 2 en 3 zal zich in de tijd moeten ontwikkelen. Bedrijven zijn vooral geïnteresseerd als er een duidelijke 'return on investment' mogelijk is. Projecten moeten voldoende vernieuwend zijn en/of potentieel hebben. Het moet vooral gaan over onderwerpen en technologieën die bedrijven zelf niet of heel moeilijk kunnen ontwikkelen. Of die nog niet 'off the shelf' te koop zijn.
Bedrijven kunnen ook mee willen doen vanwege de kennisontwikkeling. En om gezien te worden als een bedrijf dat vooroploopt bij vernieuwing en onderzoek.



Figuur 11: Toegepast onderzoek van verkenning tot technologie-ontwikkeling

De eerder benoemde AVR-toepassingen hebben niet dezelfde maturiteit: voor AVR in secure software development is een PoC op basis van de huidige stand der techniek mogelijk. Voor automated patch generation is nog geen bruikbare tooling beschikbaar.

De genoemde fasen kunnen dus voor alle AVR-toepassingen worden doorlopen, maar gefaseerd in de tijd:

- (2021) Fuzzing in software-ontwikkeling, use case
- (loop van 2021) Fuzzing in software assessments, start met verkenning

- (2023/24) Automated patch generation en/of risk based patching, afhankelijk van resultaten spoor 2

Fuzzing in software-ontwikkeling
Bij software-ontwikkeling wordt gebruik gemaakt van een software-ontwikkelstraat. Hierbij worden variërende niveaus van automatisering toegepast. In de meest vergaande versie wordt iedere 'commit' van een ontwikkelaar automatisch opgeslagen, gecompileerd en getest op een aantal vooraf gedefinieerde tests, op verschillende (vooraf gedefinieerde) platformen. Deze optimalisering van het ontwikkelproces (DevOps, continuous integration) krijgt veel aandacht in de markt en wordt ondersteund door softwarepakketten zoals Gitlab. Ook security testing krijgt toenemende aandacht, bijvoorbeeld door het toepassen van source code analyzers. Gitlab heeft recent voorzichtige stappen gezet om om fuzzing tests mee te nemen in de ontwikkelstraat[16].

In spoor 3 zullen beschikbare fuzzingtools worden gecombineerd met de laatste resultaten van academisch AVR-onderzoek. Een representatieve software-ontwikkelstraat zal worden ingericht om experimentele ervaring op te doen en use cases uit te voeren. Zowel bij het inrichten van de ontwikkelstraat als het formuleren van use cases zal samenwerking worden gezocht met routekaart-partners die zelf software-ontwikkeling doen. Gezien de maturiteit van deze toepassing, is een use case op korte termijn haalbaar.

Bij een positief resultaat van de use case is vanaf 2022 een vervolgfase voorzien waarin generiek inzetbare tooling wordt ontwikkeld. Dit kan gebeuren in samenwerking tussen TNO en een eindgebruiker van securitytechnologie. Wanneer een ontwikkelaar van security-technologie belangstelling toont zal deze ook betrokken worden.

Doel: aantoonbaar het software-ontwikkelingsproces verbeteren doordat bugs nog voor de release gevonden worden (shift security left).

Uitvoering: TNO
Partners: software-ontwikkelaars (bv. financiële sector)
Faciliteiten: experimentele ontwikkelstraat in fieldlab
Start: 2021

Fuzzing in security assessments/evaluaties
Het beoordelen van de security van software is een steeds complexere taak. In de huidige situatie kan dit gedaan worden op basis van source code (welke niet altijd beschikbaar is) of op basis van documentatie en certificering van het ontwikkelproces. Security-assessments worden uitgevoerd door gespecialiseerde partijen, en op systemen waarvoor een hoog niveau van assurance nodig is. In de interviewronde hebben Riscure (commerciële aanbieder van security assessments) en het NBV (overheidspartij belast met security-evaluaties voor o.a. Defensie) interesse getoond in AVR als mogelijke aanvulling op hun toolbox.

[16] https://docs.gitlab.com/ee/user/application_security/coverage_fuzzing/

In spoor 3 zal reeds ontwikkelde fundamentele kennis rond fuzzing en automated vulnerability discovery toegepast worden binnen een omgeving waarbij het evalueren van software een primaire taak is. Hierbij is nauwe samenwerking gewenst tussen TNO (inbrengen AVR-kennis) en een organisatie gespecialiseerd in het uitvoeren van software security assessments. Omdat nog beperkt kennis beschikbaar is, zal onderzoek naar deze toepassing starten in de 1^{e} fase (verkenning van de toepassingsmogelijkheden)

Doel: aantoonbaar de kwaliteit van software security assessments verbeteren, door toepassing van nieuwe technieken om kwetsbaarheden te vinden.

Uitvoering: TNO
Partners: Riscure, andere security-evaluatie dienstverleners
Faciliteiten: IT-faciliteiten voor remote samenwerking tussen partners (fieldlab)
Start: loop van 2021

Automated patch development / risk based patching
Spoor 2 zal in 2021 starten met fundamenteel onderzoek op het gebied van patching. Vanaf 2023 worden de eerste resultaten van dit onderzoek verwacht. In spoor 3 zal deze kennis vervolgens worden toegepast.

De use case voor dit project, en de tijdlijnen daarvan, zullen in sterke mate afhangen van de resultaten van spoor 2. Binnen dit project zal een partner gezocht worden voor wie automated patch generation een waardevolle toepassing is, waarna een use case kan worden uitgevoerd. In de behoefte-inventarisatie toonden partijen uit de financiële sector interesse voor het patchen van systemen zonder support, waaronder open source.

Doel: aantoonbaar het patching proces verbeteren door patches beschikbaar te maken voor software zonder support, en beslissingsondersteuning over het al dan niet doorvoeren van patches.

Uitvoering: TNO
Partners: VU, financiële sector
Start: 2023/2024

Nadat academische AVR-kennis is gebracht tot technologie gevalideerd in use cases, volgen de laatste twee fasen in de valorisatieketen: integratie/operationalisering en daadwerkelijke toepassing. Tussen demonstratie en operationalisering ligt de tweede valley of death. Om deze succesvol te kunnen overbruggen moeten partijen die AVR-technologie willen toepassen al in de eerdere onderzoeksfasen nauw betrokken worden. Daarbij moet tijdig afspraken worden gemaakt/ingeregeld over:

- Eigendomsrecht; een mate van exclusiviteit kan voor bedrijven randvoorwaarde zijn om in de technologie te investeren. Dit kan bijten met de wens van universiteiten of andere partijen om kennis te delen en resultaten te open-sourcen.

- Maintenance; een partij moet bereid zijn om de technologie te onderhouden en daar moeten voordelen tegenover staan. Bij sterke voorkeur gebeurt dit door een Nederlandse partij om te voorkomen dat opgebouwde kennis naar het buitenland verdwijnt.

5.5.4 Fieldlab

Het fieldlab is ondersteunend voor de andere sporen. Primair is het fieldlab hierbij verantwoordelijk voor informatieoverdracht en samenwerking tussen en binnen de sporen. Het fieldlab is dus geen fysieke ruimte waarbinnen wordt geëxperimenteerd. Veel meer is het een virtuele ruimte waarbinnen experimenten en data kunnen worden uitgewisseld.

Voor het fieldlab is een verbindende rol voorzien, zowel in de samenwerking tussen partijen als (technisch) voor de integratie van resultaten. Het fieldlab bestaat uit de volgende onderdelen

- Virtuele/IT-omgeving voor opslag van code en uitvoeren van experimenten.
- Organisatie van samenwerking.

Virtuele/IT-omgeving voor opslag van code en uitvoeren van experimenten.
Om de overdracht tussen de verschillende sporen te bespoedigen zal ieder spoor de resultaten beschikbaar maken op een gezamenlijke omgeving. Doel hiervan is dat alle betrokkenen toegang tot deze data verkrijgen, en zelf de gedane onderzoeken kunnen herhalen. Een belangrijk onderdeel van deze virtuele omgeving is het CRS (zie 5.5.1). In het CRS kunnen de resultaten van onderzoek, use cases en challenges worden geïntegreerd, gedeeld en herbruikt.

Deze omgeving zal niet alleen gebruikt worden voor de opslag van code en data (bijvoorbeeld door middel van een Git omgeving) maar ook voor het uitvoeren van experimenten (bijvoorbeeld door het beschikbaar stellen van rekencapaciteit voor experimenten). De omgeving kan ook worden gebruikt voor het delen van alle lesmaterialen rond AVR

Delen van het fieldlab zullen worden opengesteld voor deelnemers aan stages of challenges, waaronder het skeleton-CRS. Van belang is om afspraken te maken over eventuele vertrouwelijkheid van data en kennis en dit ook te waarborgen.

Uitvoering: TNO, VU
Partners: use case partners spoor 3, overige partners, challenge-deelnemers
Start: 2021

Organisatie van samenwerking
Om de samenwerking tussen de sporen te bevorderen worden er bijeenkomsten georganiseerd. Reguliere meetings zijn voorzien tussen de betrokken personen binnen de routekaart. Hier zullen plannen en (deel-)resultaten gedeeld worden. Doelstelling is om de overdracht van kennis te bevorderen. Bijzondere aandacht gaat ernaar uit om fundamentele kennis uit spoor 2 toe te passen binnen concrete use cases in spoor 3, en praktijkervaringen uit spoor 3 terug te koppelen naar spoor 2.
Er zullen hierbij verschillende ontmoetingen worden georganiseerd:

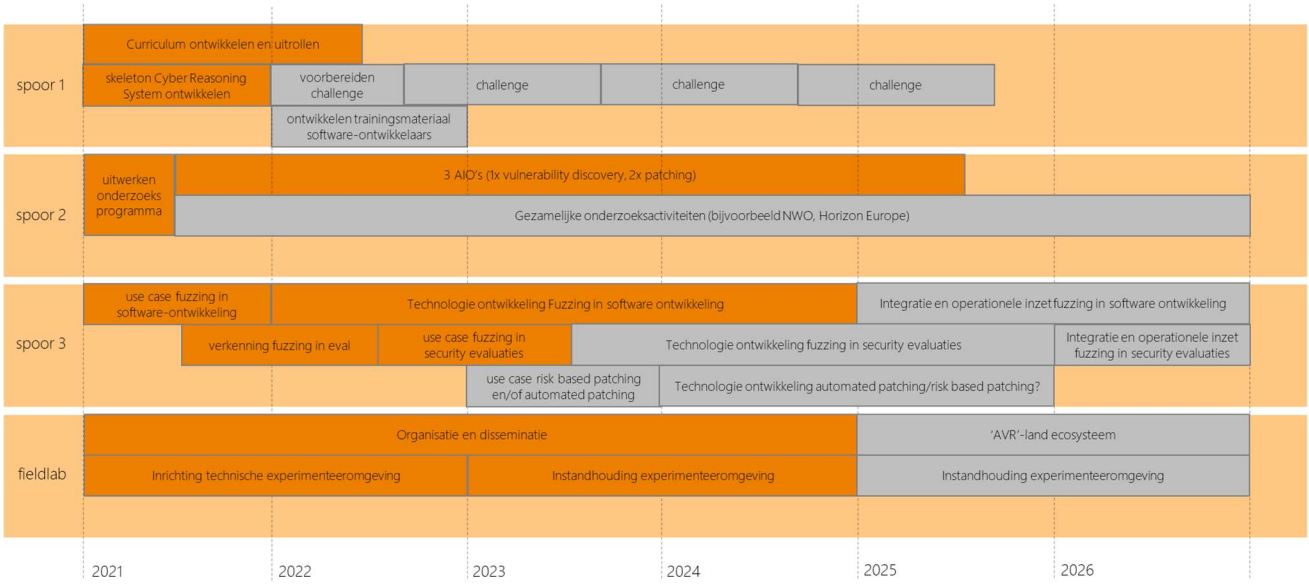
- Technische ontmoetingen waarin een focus is op het presenteren en bespreken van de technische resultaten. Deze ontmoetingen kunnen zowel per spoor als per onderwerp worden georganiseerd.
- Ontmoetingen met alle betrokken partijen, zodat een community ontstaat op het onderwerp AVR.

Van belang is om wanneer dit weer kan (corona) ook fysieke ontmoetingen te organiseren waar mensen echt met elkaar kunnen samenwerken. Daarnaast kunnen virtuele samenwerkingsomgevingen worden gecreëerd, bijvoorbeeld met slow-messaging en andere communiicatiefaciliteiten.

Uitvoering: programmamanagement, TNO, VU
Partners: partners uit alle sporen
Start: 2021

5.5.5 Activiteiten en fasering

In de voorgaande paragrafen is toegelicht welke activiteiten in de sporen van de routekaart zullen plaatsvinden. Figuur 12 geeft een overzicht met de initieel voorziene planning in de tijd. In donker oranje is aangegeven welke activiteiten worden uitgevoerd binnen het vanaf november 2020 beschikbare budget. In grijs staan activiteiten waarvoor in de komende periode (tijdig) budget zal moeten worden gevonden.



Figuur 12: activiteiten en initiële planning

5.5.6 Internationalisering en aansluiting bij andere initiatieven

Gezien de complexiteit van het onderzoeksgebied AVR, en de huidige nationale kennispositie zal de gewenste capaciteiten niet volledig zelfstandig kunnen realiseren. Tenminste heeft Nederland er belang bij om samenwerking te zoeken, bijvoorbeeld binnen Europa. In het academisch AVR-

onderzoek is al sprake van samenwerking tussen de VU en andere universiteiten binnen en buiten Europa.

De routekaart wil in eerste instantie een ecosysteem van Nederlandse partijen tot stand brengen. Dit creëert een goede uitgangspositie voor latere internationale samenwerking en maakt bovendien een snelle start mogelijk.

Er zijn in Nederland ook andere programma's op het gebied van (automatisering in) cybersecurity. Bijvoorbeeld het al eerder genoemde ASOC programma. Van belang is de onderscheidende positie van de Routekaart AVR scherp te houden en te bewaken dat in verschillende programma's niet dezelfde activiteiten plaatsvinden en dat programma's goed op elkaar aansluiten. Het samenwerkingsplatform cybersecurity zal hier een belangrijke rol in spelen.

De programmamanager verantwoordelijk voor uitvoering van de routekaart AVR zal onderzoeken waar aansluiting bij Europese/internationale partners en initiatieven zinvol is.

6 Organisatie en financiering

6.1 Organisatie

Het uitvoeren en door-ontwikkelen van de Routekaart kan worden gezien als een programma. Het programma moet worden bestuurd en worden gemanaged. We stellen voor dit te doen middels de inrichting van een stuurgroep en het aanstellen van programmamanagers en projectleiders.

Als de Routekaart zich goed ontwikkelt is het waarschijnlijk dat allerlei andere samenwerkingen en projecten ontstaan waarover zowel stuurgroep als programmamanager geen zeggenschap hebben. We zien dit als een teken van succes. Wel zou het goed zijn als er overzicht blijft van deze samenwerkingen en ontwikkelingen, zodat kan worden beoordeeld in welke mate de ambitie en de doelen van de Routekaart AVR worden behaald.

Onderstaand lichten we genoemde rollen nader toe.

Stuurgroep

De stuurgroep Routekaart AVR:

- Heeft passie voor het onderwerp AVR.
- Heeft direct belang bij het succes van de Routekaart. De leden stellen daarbij de algemene doelen die met de Routekaart moeten worden bereikt voorop.
- Bewaakt de voortgang in de werkstromen en de ontwikkeling van de Routekaart in het algemeen, via de rapportages van de programmamanager.
- Draagt het onderwerp AVR binnen en buiten de AVR community uit en versterkt daarmee het belang van AVR.
- Spant zich in om additionele middelen voor de Routekaart beschikbaar te krijgen.
- Stuurt de programmamanager aan en voorziet deze gevraagd en ongevraagd van advies.

De stuurgroep komt tenminste 4x per jaar bij elkaar. De volgende samenstelling wordt voorgesteld, zodat alle partners in de keten vertegenwoordigd zijn. Vertegenwoordigers van:

- Ministerie EZK (als belangrijkste financier en initiator)
- Ministerie Defensie (als initiator en aanjager)
- Hoger Onderwijs (voorgesteld: VU Sec, als initiator en erkend leider op het gebied van AVR)
- Kennisinstellingen (voorgesteld TNO, als budgethouder, initiator en leider op het gebied van AVR)
- Cybersecurity bedrijven (Voorgesteld worden twee vertegenwoordigers: 1 persoon vanuit een groot bedrijf en 1 persoon vanuit een MKB bedrijf)
- Eindgebruikers (voorgesteld wordt een vertegenwoordiger van een financiële instelling/bank)

De stuurgroep kiest een voorzitter en zorgt er zelf voor dat nieuwe leden indien nodig worden gezocht en gevonden om effectief te blijven, waarbij wordt bewaakt dat alle partners vertegenwoordigd blijven.

Programmamanager

De programmamanager:

- Is primair verantwoordelijk voor het bewaken van de voortgang en het behalen van de resultaten in de gedefinieerde (en gefinancierde) stromen en projecten van de Routekaart AVR.
- Is direct verantwoordelijk voor het Virtuele Fieldlab.
- Fungeert als ‘spin in het web’, als centrale contactpersoon voor alle betrokkenen en stemt daarmee dus regelmatig af. Zoekt en betrekt actief partijen die een rol in de Routekaart kunnen gaan vervullen.
- Zoekt mogelijkheden en middelen om de Routekaart uit te kunnen blijven voeren.

- Onderhoudt contact met het samenwerkingsplatform cybersecurity.
- Rapporteert vanuit zijn/haar rol aan het bestuur

De programmamanager zal de rol vooralsnog part-time vervullen. Hoewel bovenstaande taken gemakkelijk tot full-time inzet kunnen leiden. Het programma zal zich primair richten op de activiteiten waarvoor budget beschikbaar is (zie figuur 12 en 13). Hiervoor zullen projecten worden gedefinieerd. Succes in het programma zal moeten leiden tot aanvullende middelen om de rol van programmamanager uit te breiden en te coördineren.

De programmamanager werkt samen met het Samenwerkingsplatform AVR. In dat platform werken immers 'innovatiemakelaars' aan het opzetten van programma's. Deze innovatiemakelaars hebben de verantwoordelijkheid ervoor te zorgen dat de Routekaart wordt uitgebreid. Ze jagen aan en ondersteunen bij het ontwikkelen van bijvoorbeeld nieuwe onderzoeksprogramma's en nieuwe samenwerkingsprojecten.

Projectleider

Projectleiders zullen waar nodig worden aangesteld voor de werkzaamheden in de stromen. Wij voorzien vooralsnog de volgende projecten waarvoor de rol van projectleider nodig is.

- Stroom 1: Onderwijs en opleiding
    - Ontwikkeling lesmateriaal. Projectleider vanuit een universiteit die de leiding heeft bij deze ontwikkeling.
    - Geschikt maken CRS voor toepassing bij onderwijs. (vanuit TNO).
- Stroom 2: Versterking onderzoek
    - Geen projectleider nodig
- Stroom 3:
    - Projectleiding voor het toegepast onderzoek (vanuit TNO).
    - Projectleiding voor ieder van de nader te definiëren samenwerkings- en cofinancieringsprojecten
- Fieldlab: Projectleiding vanuit TNO in de eerste programmafase. Doorontwikkeling onder de verantwoordelijkheid van de programmamanager.

De kosten van projectleiding maken onderdeel uit van het voor het project beschikbare budget.

AVR Community

Van groot belang is de ontwikkeling van een AVR community. Het Virtueel Fieldlab speelt hier een belangrijke rol in. De ontwikkeling van deze community valt onder de verantwoordelijkheid van de Programmanager. Vanuit het samenwerkingsplatform cybersecurity is te verwachten dat zich meerdere inhoudelijke cybersecurity communities zullen vormen. De programmamanager zal hierover direct contact houden met het samenwerkingsplatform om een en ander zo efficiënt en effectief mogelijk in te richten.

Besluitvorming

In de Routekaart zullen op verschillende momenten belangrijke inhoudelijke besluiten moeten worden genomen. Bijvoorbeeld: Aan welke universiteit worden AIO's aangesteld? Aan welke onderwerpen gaan de AIO's werken? Wie gaat het opleidingsmateriaal ontwikkelen? Etc. Van belang is dat deze besluiten pragmatisch, objectief en transparant worden genomen. Hiervoor zal een pragmatisch proces worden ontwikkeld.

6.2 Financiering

Voor realisatie van de ambities is voor 6 jaar een bedrag nodig van naar schatting 10 tot 15 miljoen euro. Op dit moment is een bedrag van €2.000.000 beschikbaar als start om de doelen van de Routekaart cybersecurity te realiseren. Over de verantwoording van de middelen zullen nadere afspraken worden gemaakt tussen het ministerie van EZK als financier en TNO als budgethouder.

Bovendien is nog een budget van €200.000 beschikbaar vanuit een project voor de ontwikkeling voor een CRS en het organiseren van een cyberchallenge AVR.

Dit is 'nieuw geld'. Daarnaast investeren diverse partijen al op het gebied van AVR (diverse universiteiten, Ministerie van defensie, enkele bedrijven). De omvang van deze middelen is onbekend.

Uit voorgaande hoofdstukken blijkt dat veel zaken nog verder moeten worden uitgewerkt. In hoofdstuk 7 staat beschreven hoe we tot deze uitwerking komen. Maar verdere detaillering en uitbreiding van de Routekaart zal nodig blijven. De routekaart zal tenminste jaarlijks worden bijgesteld en op ieder moment kunnen aanvullende projecten worden gestart. Financiering zal altijd een voorwaarde zijn.

Op hoofdlijnen is de besteding van de beschikbare middelen weergegeven in figuur 13. Opgenomen zijn ook verdere activiteiten waarvoor nog géén financiering beschikbaar is. Dit overzicht is de basis voor verdere detaillering.

Cofinancieringsopties zullen begin 2021 worden onderzocht op basis van meer uitgewerkte projectvoorstellen. Mogelijk is ook cofinanciering mogelijk voor start-ups die op het gebied van AVR zullen/kunnen ontstaan. Ook naar deze mogelijkheid zal worden gekeken.

Er is dus nog veel meer geld nodig om de ambitie van de Routekaart AVR te realiseren. Een juiste besteding van de nu beschikbare middelen, het actief aanhaken van de hele keten en het ontwikkelen van een AVR community en een groter focus op het onderwerp AVR zal moeten leiden tot het beschikbaar komen van meer middelen: het vliegwiel komt op gang.

Spoor	Activiteit	Budget (€) beschikbaar	Budget (€) benodigd	2021	2022	2023	2024	2025	2026
Spoor 1: Onderwijs en opleiding	Ontwikkelen en uitrollen lespakket	€ 100,000							
	Geschikt maken en skeleton CRS	€ 200,000							
	Lesmateriaal softwareontwikkelaars		p.m.						
	Cyberchallenge		p.m.						
	Subtotaal	€ 300,000							
Spoor 2: Versterking onderzoek	Nader analyse naar huidige en gewenst onderzoek	€ 20,000							
	Aanstellen 3 AIO's	€ 730,000							
	AVR Research programma, inclusief aanvullende AIO's		p.m.						
	Subtotaal	€ 730,000							
Spoor 3: Toepassing	Toegepast onderzoek	€ 650,000							
	Verdere projecten		p.m.						
	Cofinanciering projecten	€ 250,000							
	Verdere projecten		p.m.						
	Subtotaal	€ 900,000							
Spoor 4: Fieldlab en programma	Programmamanager (part time)	€ 150,000	p.m.						
	Fiedlab opzetten en aanjagen (part time & out of pocket)	€ 100,000	p.m.						
	Subtotaal	€ 250,000							
	Totaal	**€ 2,180,000**	**p.m.**						

Financiering beschikbaar
Financiering beschikbaar uit budget CRS/cyberchallenge
Financiering nog niet beschikbaar

Figuur 13: Overzicht activiteiten en financiering in de tijd.

7 Vervolgstappen Routekaart

Dit document is een tweede uitgewerkt concept van de Routekaart AVR. Voorgesteld wordt om in de komende maanden acties te starten op basis waarvan de eerste projecten van de Routekaart daadwerkelijk kunnen starten en de middelen daarvoor beschikbaar kunnen worden gesteld. Het aanstellen van een (part-time) programmamanager is daar onderdeel van.

In figuur 14 staan de voorgestelde vervolgstappen op hoofdlijnen uitgewerkt.

Spoor	Onderwerpen	Acties	Wanneer/wie
Spoor 1: Onderwijs en opleiding	Ontwikkelen lespakket	Ontwikkelen eerste voorstel voor: Pragmatische uitwisseling van beschikbaar materiaal Scope en diepgang te ontwikkelen materiaal	S. Verwer (TU Delft), E. Kok, jan/feb 2021
	Geschikt maken CRS	Uitwerken projectplan	TNO, jan/feb 2021
Spoor 2: Versterking onderzoek	Aanstellen 3 AIO's	1. Uitwerken proces, randvoorwaarden en criteria (feedback van alle betrokken universiteiten) 2. Indienen voorstellen 3. Beoordeling voorstellen en keuze (door twee	optimistisch tijdplan: stap 1: E. Kok, jan 2021 stap 2: feb 2021 stap 3: maart 2021
	AVR Research programma	1. Verkennen mogelijkheden en gedachten op hoofdlijnen. 2. Voorbereiden en organiseren bijeenkomst van WO/HBO vertegenwoordigers	E. Kok, TNO, ?. Q1 2021
Spoor 3: Toepassing	Toegepast onderzoek	Definitie concrete projecten/voorstellen. Individuele werksessies TNO-bedrijven. Verdieping van interessegebieden en doelstellingen.	TNO, start Q1 2021
		Uitwerking projectkalender door TNO, als leider van deze stroom	TNO, Q1 2021
	Cofinanciering projecten	Nader uitwerken regels/mogelijkheden van cofinanciering. Daarbij ook aandacht voor afspraken over IP en samenwerking.	TNO, Q1 2021
		Exploratie van financieringsmogelijkheden in de individuele werksessies	TNO, start Q1 2021
Spoor 4: Fieldlab en programma	Fiedlab opzetten	Uitwerken technische omgeving. Afstemmen met partijen. Realiseren omgeving	TNO, start Q1 2021
		Organiseren 'community'. Bekendmaken, openstellen. Opstellen concept activiteitenkalender	TNO, E. Kok start Q1 2021
Organisatie	Stuurgroep	Inrichting/uitbreiding stuurgroep	Huidige stuurgroep, E. Kok, jan 2021
	Programmamanager	Aanstellen programmamanager	Stuurgroep, jan 2021

.

8 Realisatie en risico's

In onderstaande tabel staan de belangrijkste risico's die we op dit moment voorzien opgenomen, en de mitigerende maatregelen die kunnen worden genomen.

Risico	Toelichting en mitigerende maatregelen
Onvoldoende draagvlak voor de Routekaart	Transparantie is en blijft van groot belang: Uitleggen van de Routekaart Betrekken van alle partijen Fieldlab openstellen Blijven communiceren
Onvoldoende cofinanciering	Is niet direct een probleem wegens de beschikbaarheid van middelen Realiseren doelen routekaart zal niet kunnen plaatsvinden. Programmamanager en stuurgroep moeten dit onderwerp structureel agenderen en actief in het netwerk naar additionele middelen zoeken
Lespakket wordt niet gebruikt	In het Nederlandse onderwijsmodel zijn veel regels over toepassing van lesmateriaal. Het lespakket zal zo veel mogelijk modulair moeten worden gemaakt om breed inpasbaar te zijn. Vanuit de community zal steeds aandacht moeten zijn voor toepassing van het materiaal
Europa haalt ons in	Dat zou wellicht niet erg zijn. Als er internationaal in Europa meer aandacht komt voor AVR dan kan daar vanuit deze Routekaart snel bij worden aangesloten: Nederland is dan al georganiseerd. Betrokkenen kennen elkaar en werken al meer samen.

9 Bijlage 1. Overzicht betrokkenen

De volgende personen zijn betrokken geweest bij het ontwikkelen van deze roadmap.

Stuurgroep

Ministerie van Defensie	LKol Ilse Verdiesen
	LTZ1 TD Jos van den Burg
Ministerie van EZK	Lars van Willigen
	Timon Domela Nieuwenhuis Nyegaard
TNO	Patrick de Graaf
Universiteiten	Herbert Bos (m.i.v. december 2020)

Projectteam

TNO	Bert-Jan te Paske
	Gerben Broenink
	Dana Tiggelman
Cocus Consult	Edwin Kok (onafhankelijk projectleider)

Onderwijs sector

Universiteit / Hogeschool	**Persoon**
VU (Amsterdam)	Herbert Bos
RUG (Groningen)	Fatih Turkmen
UT (Twente)	Andreas Peter
UT (Twente)	Andrea Continella
TU Delft	Sicco Verwer
Radboud Universiteit Nijmegen	Erik Poll
Radboud Universiteit Nijmegen	Ileana Buhan
Open Universiteit	Harald Franken
Hanze hogeschool Groningen	Arne Padmos
Hanze hogeschool Groningen	Ellen van Hegelsom

Bedrijfsleven (cybersecurity sector)

Bedrijf	**Persoon**
Cyberveilig NL	Liesbeth Holterman
Tesorion	Rogier van Agt
Tesorion	Rick Hofstede
Tesorion	Daniel Jansen
Zerocopter	Edwin van Andel

Cybersprint	Vincent van Thiele
Fox-IT	Michelle Postma
Fox-IT	Dennis de Hoog
KPN	Edwin Bron
KPN	Oscar Koeroo
Capgemini	Geert van der Linden
Capgemini	Sanne Kuijpers
Philips	Maarten Bodlaender
Riscure	Marc Witteman
Riscure	Erwin in't Veld
Deloitte	Jelle Niemantsverdriet
Deloitte	Cas van Cooten
Deloitte	Kevin Jonkers
Deloitte	Daan van Moorsel
Secura	Ralph van Moonen

Financiële sector

Bedrijf	**Persoon**
ING	Yehenew Gizaw
ING	Stefan Petrushevski
ABN AMRO	Olaf Streutker
ABN AMRO	Coen Klaver
ABN AMRO	Alexander den Engelsman
ABN AMRO	Robert van Lierop
ABN AMRO (clearing)	Jeroen Schilders
Rabobank	Johan Romkes

Overig

Organisatie	**Persoon**
FME werkgroep cybersecurity	Stijn Bouwhuis
RDW	Marc de Bruin
Enexis	Mauriche Kroos
NLNCSA	Jan Verschuren