Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC Onderzoeksagenda 2019 - 2022

NCSC

Inleiding

Het NCSC richt zich op het *begrijpen* van kwetsbaarheden en dreigingen in het digitale domein, het *verbinden* van partijen, kennis en informatie en het *voorkomen* van maatschappelijke schade en beperken van dreigingen. Het onderzoekscluster van het NCSC draagt bij aan deze taken door wetenschappelijke ontwikkelingen op deze gebieden te duiden en relevante onderzoeksvragen uit te zetten.

De NCSC Onderzoeksagenda 2019-2022 geeft uitvoering aan de Onderzoeksambitie 2019.[1] Deze agenda wordt gebruikt om onderzoeksvragen uit te zetten, deel te nemen aan onderzoeken of zelf onderzoeken te starten. We zoeken daarbij een balans tussen fundamenteel onderzoek, onderzoek dat bijdraagt aan de taakuitvoering van het NCSC en onderzoek dat helpt om Nederland digitaal veiliger te maken.

Thema's

De NCSC Onderzoeksagenda 2019-2022 is opgedeeld in vier thema's:
- Crisismanagement (warme fase)
- Risicomanagement (koude fase)
- Strategische en sociale aspecten van cybersecurity (brede blik)
- Technologie en cybersecurity (technologische innovaties)

Op elk van de thema's is het idee van begrijpen, verbinden en voorkomen toe te passen, maar elk thema raakt verschillende vlakken van deze strategische opgave. De thema's worden in het document verder beschreven en worden uitgewerkt in een aantal verschillende subthema's. Per subthema worden ter illustratie ook een aantal mogelijke onderzoeksvragen genoemd.

Deze thema's zijn tot stand gekomen door de scope van de agenda te definiëren, deskresearch uit te voeren en na analyse een eerste versie te ontwikkelen. Daaropvolgend zijn interviews met interne en externe experts afgenomen om de eerste versie te verfijnen (zie bijlage 1).

Vervolgstappen

Ieder jaar bepalen we welke (sub)thema's prioriteit krijgen en verder worden uitgewerkt in onderzoeksvoorstellen. Dit doen we op basis van eerdere (onderzoeks)resultaten en aan de hand van actuele ontwikkelingen zoals die voortvloeien uit het dreigingsbeeld in het CSBN.

Na selectie van een subthema worden de genoemde onderzoeksvragen als uitgangspunt en inspiratiebron gebruikt. Deze worden dan in overleg met collega's en doelgroepen verder uitgewerkt tot definitieve onderzoeksvragen. Vervolgens voeren we deze onderzoeken zelf uit of we besteden ze uit.

De agenda zal ieder jaar worden aangepast aan de inzichten uit het voorgaande jaar. We kunnen besluiten een onderzoekslijn te stoppen of een onderwerp juist verder uit te diepen of te verlengen. Resultaten worden gedeeld met de doelgroepen waarvoor het onderzoek relevant is, in (wetenschappelijke) publicaties, en tijdens conferenties.

Achtergrond

De NCSC Onderzoeksagenda 2019-2022 geeft uitvoering aan de Onderzoeksambitie 2019,[1] waarmee we invulling geven aan de kennisontwikkelingsopdracht uit de Nederlandse Cyber Security Agenda (NCSA).[2] Ook past het onderzoek binnen de vijf pijlers van de Nationale Cyber Security Research Agenda (NCSRA).[3]

Hiermee geeft het onderzoekscluster ook opvolging aan kernbevindingen uit de jaarlijkse rapportage in het Cybersecuritybeeld Nederland (CSBN). Dit leidt tot de volgende activiteiten van het onderzoekscluster van het NCSC:

- Relevante onderzoeksvragen genereren voor het opstarten van projecten met ondersteunende organisaties, zoals TNO en het WODC.
- Deelnemen aan relevante onderzoeksprojecten met (inter)nationale academische partners.
- Richting geven aan onze eigen onderzoeksactiviteiten, met mogelijk gerelateerde detacherings- of promotiemogelijkheden.
- Kennis delen via begeleiding van afstudeerders en promovendi, inhoudelijke gastcolleges, etc.
- Beoordelen van onderzoeksvoorstellen, die zijn ingediend naar aanleiding van een *call* voor projecten waarbij het NCSC betrokken is.

Structuur van de NCSC Onderzoeksagenda 2019-2022

De vier thema's benaderen we vanuit relevantie voor de missie van het NCSC en vallen uiteen in een aantal subthema's. Bij ieder subthema hebben we mogelijke onderzoeksvragen geformuleerd. Hoewel sommige thema's en onderzoeksvragen overlappen, vormen ze verschillende invalshoeken op dezelfde onderwerpen.

1. Crisismanagement

Crisismanagement raakt het hart van het NCSC. Het NCSC is primair een crisisorganisatie. Als aanvulling op het werkveld crisismanagement bij de NCTV kijkt het NCSC naar specifieke cybersecurity-aspecten in crisismanagement. De huidige inventarisatie van communicatie door Computer Emergency Response Teams (CERTs) en Computer Security Incident Response Teams (CSIRTs) laat zien dat er nog veel te winnen is, vooral op het gebied van het verhogen van het herstelvermogen van organisaties. Maar ook de impact van de GDPR op CERT-communicatie, CERT-maturity modellen en het stimuleren van internationale samenwerking zijn onderwerpen die sterk in ontwikkeling zijn.

Dit onderwerp sluit primair aan bij het *voorkomen* van maatschappelijke schade en het verhogen van weerbaarheid door bij te dragen aan de (interne) ontwikkeling op het gebied van crisismanagement. Daarbij is het van belang ook zo goed mogelijk de verbinding te zoeken met andere partijen en doelgroepen.

1.1 Communicatie door CERTs en CSIRTs / Maturity Modellen

Om het NCSC te helpen haar taak beter uit te voeren is meer inzicht in de communicatie tussen en binnen CSIRTs noodzakelijk. Binnen de doelgroepen van het NCSC zijn er meerdere communicatiekanalen die cruciaal zijn voor de weerbaarheid van Nederland. Voorbeelden hiervan zijn: EGC, MISP, o-irt-o, de ISAC's en uiteraard het Nationaal Detectie Netwerk. De ontwikkelingen binnen deze gremia zijn belangrijk. Uit de praktijk blijkt een behoefte aan meer kennis over best practices, de impact van ontwikkelingen zoals de GDPR en het toepassen van modellen. Een voorbeeld hiervan is het CTI-capabiliteitsmodel. Het NCSC heeft voor dit onderwerp een unieke positie om workshops met stakeholders te organiseren, ervaringen te delen of toegang te bieden tot het netwerk van het NCSC.

Mogelijke onderzoeksvragen

- Wat zijn best practices met betrekking op CSIRT-communicatie?
- Wat zijn succesfactoren voor sectorale of ketensamenwerking?
- Hoe kan de kloof tussen academisch onderzoek en de sociale werkelijkheid van CSIRT-communicatie verkleind worden?
- Hoe kunnen capabiliteitsmodellen zoals het CTI-capabiliteitsmodel toegepast worden bij CSIRTs in Nederland?

1.2 Herstelvermogen

In het cybersecuritywerkveld is het over het algemeen niet de vraag óf je kwetsbaar bent, maar wannéér je geraakt wordt door een aanval. Daarom is het belangrijk om niet alleen na te denken over beveiligingsmaatregelen, maar ook over (aanvullende) maatregelen voor het herstelvermogen en incidentafhandeling van een organisatie. Er zou verkennend onderzoek uitgevoerd kunnen worden naar de factoren en omstandigheden die een rol spelen in het herstelvermogen van organisaties na een cyber-gerelateerd incident. Daarbij kan ook gekeken worden naar de mogelijke overeenkomsten tussen, of de verschillen met, traditioneel herstelvermogen.

Mogelijke onderzoeksvragen

- In hoeverre is herstelvermogen meetbaar?
- Hoe kan het herstelvermogen van organisaties verhoogd worden?
- Wat voor maatregelen (in brede zin) dragen bij aan het herstelvermogen of het lerend vermogen van organisaties?
- Hoe kunnen organisaties samenwerken om herstelvermogen te verhogen?

2. Risicomanagement

Risicomanagement van bedrijfsprocessen door ICT-beveiliging is een belangrijke factor voor het veilig houden van de Nederlandse vitale infrastructuur. Wat zijn effectieve manieren om in beheerprocessen beveiliging te stroomlijnen en verbeteren? Bijvoorbeeld door onderzoek dat leidt tot inzicht in ketenafhankelijkheid die worden veroorzaakt door het uitbesteden van ondersteunende ICT-diensten. Daarnaast is er behoefte aan onderzoek naar verbindende factoren van cyberrisicomanagement en risicomanagement van andere bedrijfsprocessen zoals financieel risicomanagement.

Risicomanagement sluit aan bij *begrijpen* en *voorkomen*: door risico's te identificeren en daarbij passende maatregelen te nemen, kan schade en impact worden voorkomen. Daarbij is het van belang dat dit zo effectief mogelijk gebeurt, zowel intern bij het NCSC als extern bij doelgroeporganisaties.

2.1 Beschermen van energie-netwerken / keren & beheren

Het doel van dit subthema is om beter grip te krijgen op de brede vraag naar de status van de bescherming van de kritieke infrastructuren en deelonderwerpen binnen deze sector. Energienetwerken hebben reeds internationaal de aandacht. Systemen rondom keren & beheren zijn in Nederland veel belangrijker voor de nationale veiligheid dan in de meeste andere landen. Naar deze laatste systemen heeft het NCSC al eerder onderzoek begeleid. Ons onderzoek naar risicomanagement zal zich dan ook vooral op deze twee sectoren toespitsen.

De Algemene Rekenkamer constateert dat de minister van Infrastructuur en Waterstaat nog stappen moet zetten om aan de eigen doelstellingen voor cybersecurity te voldoen.[4] Het NCSC wil beter inzicht naar specifieke kwetsbaarheden in ICS/SCADA-systemen en de kenmerkende aspecten van de beveiliging van de netwerken waar deze systemen in voorkomen. Verder willen we weten wat in de weerbaarheid de succesfactoren voor OT-security zijn en hoe de kritieke infrastructuur de beheerprocessen voor ICS /SCADA-systemen kan verbeteren. Dit levert inzichten op over de bescherming, maar levert het NCSC ook kennisopbouw over ICS/ SCADA-systemen.

Mogelijke onderzoeksvragen

- Welke rol spelen menselijke factoren in het behandelen en beoordelen van cyberrisico's?
- Hoe kan de complexe informatievoorziening toegankelijk gemaakt worden voor beleidsmakers?
- Wat zijn de bepalende succesfactoren voor OT-security volwassenheid in organisaties?
- Hoe kan per sector, in zowel de vitale als niet-vitale infrastructuur, de scheiding en overlap in security in beheerprocessen tussen IT en OT beter benut worden?
- Hoe kan patchmanagement beter ingezet worden bij bestaande systemen zodat deze systemen minder kwetsbaar worden?
- Hoe kunnen de verschillende vormen van 'testen' beter ingezet worden door organisaties?
- Hoe kan risicomanagement binnen ICS/SCADA-omgevingen effectief ingezet worden?
- In hoeverre zijn bestaande risk-managementmodellen toepasbaar op ICS/SCADA-omgevingen?

2.2 Kwantificering van cyberrisico's en schade

Er is niet altijd draagvlak voor het investeren in digitale beveiliging bij organisaties. Het kunnen kwantificeren van de mogelijke risico's en daarbij behorende schade is een middel om draagvlak te creëren. Informatie over de kwantificering van cyberrisico's kan ook een hulpmiddel zijn bij de totstandkoming van het CSBN. De informatie over cyberrisico's is de afgelopen jaren exponentieel gegroeid en vergelijkend onderzoek naar andere (lid)staten zou interessant zijn. Er ligt dan ook een behoefte om de complexiteit en onderlinge verbanden op een begrijpelijke manier te verwerken en toe te passen in organisaties. Cyberrisico's werken door in diverse domeinen, maar cybersecurityrisicomanagement is momenteel vaak niet verbonden met risicomanagement in andere domeinen. Tegelijkertijd staat de grote afhankelijkheid van ICT-producten uit andere landen steeds vaker ter discussie.

Mogelijke onderzoeksvragen

- Hoe ziet een goede systematische kwantitatieve risicoanalyse eruit?
- Hoe kan cybersecurityrisicomanagement binnen integraal risicomanagement geïntegreerd worden?
- Wat zijn de verschillen en overeenkomsten tussen lidstaten in de regulering van cyberrisico's en schade?
- Hoe kan historische data over cyberrisico's systematisch geanalyseerd en onderbouwd gekwantificeerd worden?
- In hoeverre kunnen bedrijven en verzekeraars bijdragen aan het systematisch analyseren en het onderbouwd kwantificeren van historische data?
- In hoeverre is klassieke schade verschoven naar cybersecurity-schade?

2.3 Supply-chainrisico

Welke organisaties en processen zijn van elkaar afhankelijk in ICT-dienstverlening? Organisaties nemen ICT als dienst af of zijn voor hun kritieke dienstverlening afhankelijk van anderen. Organisaties zijn voor de continuïteit en veiligheid steeds meer afhankelijk van een netwerk van aanbieders waar ze soms wel en soms niet een contract mee hebben. (Risico)management op al die afhankelijkheden in de gehele keten wordt steeds belangrijker.

In het verleden is in specifieke omgevingen gekeken naar keten-afhankelijkheden, bijvoorbeeld binnen de Rotterdamse haven en bij Schiphol. Ervaringen uit deze trajecten kunnen helpen om hier op een algemener niveau over na te denken of om nieuwe onderzoeksvragen op te leveren, om op deze manier tot generieke adviezen voor onze doelgroep te komen. Andere ontwikkelingen, zoals Software Bill of Materials (SBOM), dragen bij aan het beter in kaart brengen van deze afhankelijkheden.

Mogelijke onderzoeksvragen

- Welke methoden zijn beschikbaar om supply-chainrisico's (devices, applications, platforms, networks, services) binnen de vitale infrastructuur in kaart te brengen en wat leveren die methoden op?
- Hoe kan SBOM ingezet worden om kwetsbaarheden in de vitale infrastructuur inzichtelijk te maken?
- Hoe kunnen cyberrisico's rond de afhankelijkheden van dienstenleveranciers inzichtelijk gemaakt worden?

3. Strategische en sociale aspecten van cybersecurity

Cybersecurity is een complex domein waarbij de verhoging van de weerbaarheid van Nederland onder andere afhankelijk is van sociale, economische, politieke en bestuurlijke processen. Door de aspecten van cybersecurity binnen deze processen te onderzoeken kan het NCSC haar rol als crisisorganisatie en haar netwerk verbeteren. De laatste jaren is het besef gegroeid dat cybersecurity niet alleen maar technische oplossingen betreft, maar dat het een multidisciplinair werkveld is. Zo is het vergroten van de weerbaarheid afhankelijk van verbeterde organisatieprocessen en internationale samenwerking. De onderstaande subthema's gaan over governancevraagstukken, veilig handelen door eindgebruikers, capaciteitsopbouw van het NCSC en de rol van ethiek binnen cybersecurity.

Door op de juiste manier te *verbinden* kan het NCSC effectief bijdragen aan de digitale veiligheid. Tegelijkertijd is het belangrijk te *begrijpen* hoe sociale processen kunnen bijdragen aan kwetsbaarheden en dreigingen. Daarnaast kunnen sociale processen ook een middel zijn om dreigingen te beperken of schade te *voorkomen*.

3.1 Governance van cybersecurity

Governance van cybersecurity gaat over het besturen en managen van cybersecurity op staatsniveau en organisatieniveau, maar behelst ook nationale en internationale cybersecuritynetwerken, samenwerkingsverbanden en allianties. Een belangrijk aspect hiervan is (inter)nationale wet- en regelgeving. In verschillende hoeken van de organisatie groeit de behoefte om inzicht te krijgen in de processen die het werk van het NCSC beïnvloeden. Het is cruciaal om effectief samen te werken binnen multilaterale organisaties zoals ICANN, RIPE of IETF. Relevante onderwerpen die hieraan bijdragen zijn onderzoek naar (inter)nationale samenwerkingen tussen CERTs, de wettelijke beperkingen van het verzamelen en delen van incidentdata en de rol van economische veiligheid in het cybersecurity speelveld.

Mogelijke onderzoeksvragen

- Hoe kan de internationale samenwerking tussen CERTs verder verbeterd worden?
- Welke rol spelen niet-technische invloeden het cyberdomein, zoals economische veiligheid?
- Hoe kan vertrouwen tussen nationale en internationale actoren in het cyberdomein verder verbeterd worden?
- Wat zijn belangrijke elementen in een normenkader voor cybersecurity?
- Wat zijn de wettelijke beperkingen en mogelijkheden om data te delen zodat een effectief cybersecuritybeleid verwezenlijkt kan worden?
- Wat zijn verschillende rollen binnen een organisatie die relevant zijn voor het effectief op orde krijgen van cybersecurity en waar liggen knelpunten bij het effectief vervullen van deze rollen?

3.2 Eindgebruikers in staat stellen om veiliger te handelen

Al jaren is ingezet op awareness-training. Inmiddels is in de praktijk gebleken dat bewustwording mogelijk helpt, maar het probleem niet volledig oplost. Binnen dit subthema wordt gekeken naar aanvullende oplossingen, bijvoorbeeld onderzoek naar alternatieve incentives of verbeterd user- interface-design.

Mogelijke onderzoeksvragen

- Wat zijn organisatorische en economische incentives voor organisaties om veiligheid te verhogen?
- Wat zijn de middelen die de grootste dreiging vormen voor eindgebruikers (smartphone, e-mail, applicaties) en hoe kunnen deze weerbaarder gemaakt worden?
- Hoe kunnen cybersecurityrisico's effectief gecommuniceerd worden door de systemen zelf?
- Waar gaat het mis in het begrip van informatie en hoe kan communicatie over cyberrisico's aangepast worden aan het kennisniveau van de gebruiker?
- Welke maatregelen kunnen genomen worden om desinformatie over ICT-beveiliging bij eindgebruikers tegen te gaan?

3.3 Capaciteitsopbouw

Er is al geruime tijd een tekort aan cybersecurity experts op de arbeidsmarkt, iets wat ook merkbaar is binnen het NCSC. Met multidisciplinair verkennend onderzoek kan worden gekeken naar het vergroten van het aantal cybersecurity experts in Nederland, bijvoorbeeld door succesfactoren te onderzoeken en het inventariseren van potentiele (om)scholingstrajecten zoals Life Long Learning. Andere mogelijke onderwerpen zijn vergelijkend onderzoek naar andere (lid)staten met betrekking tot capaciteitsopbouw, maar ook welke competenties nodig zijn in het cybersecurity vakgebied in 2025.

Onderzoek toont aan dat hogere diversiteit leidt tot effectievere samenwerking in teams en organisaties. De diversiteit binnen de cybersecurityarbeidsmarkt blijft echter achter of neemt zelfs af. Welk effect heeft dit op de digitale weerbaarheid van Nederland, zowel binnen het NCSC als bij doelgroep-organisaties?

Mogelijke onderzoeksvragen

- Welke rol spelen soortgelijke organisaties als het NCSC in andere (lid)staten bij capaciteitsopbouw?
- Welke rollen en taken in het cyberdomein zullen (kunnen) verdwijnen door toekomstige innovaties zoals artificial intelligence?
- Hoe organiseren andere (lid)staten capaciteitsopbouw en wat zijn de waardevolle lessen voor het NCSC/Nederland?
- Van welke organisaties kan het NCSC leren (best practices) en hoe vertaalt dit zich naar het NCSC?
- In hoeverre sluiten rollen en functies van het NCSC aan bij andere cyber-gerelateerde departementen binnen het Rijk?
- Hoe kan het NCSC bijdragen aan een inclusieve en meer diverse gemeenschap van cybersecurityspecialisten?
- Hoe behoud je mensen en hoe zet je ze effectiever in?
- Welke barrières voor toetreding tot het vakgebied spelen in Nederland? En hoe zijn deze weg te nemen?
- Welke competenties worden nu aangeleerd in het onderwijs en welke competenties zijn noodzakelijk voor cybersecurity-experts in 2025?

3.4 Ethiek binnen cybersecurity

Binnen het NCSC is er een groeiend besef van mogelijke waardenspanning tussen ethiek en handelingsvermogen binnen het incident response werk. Het publieke debat richt zich meer en meer op ethische aspecten van AI, social media en andere informatica-toepassingen. Hoe kunnen organisaties met dilemma's omgaan? Hoe wordt daar in de wetenschap mee omgegaan?

Mogelijke onderzoeksvragen

- Wat zijn de ethische dilemma's waar het NCSC nu en in de toekomst mee te maken zal krijgen?
- Welke oplossingen kunnen worden voorgedragen voor het omgaan met ethische dilemma's?
- Wat zijn ethische richtlijnen van beveiligingsonderzoek zoals worden gehanteerd binnen ethische commissies? In hoeverre kan het NCSC deze adopteren?
- Wat zijn de ethische grenzen van vulnerability disclosure?
- Hoe verandert vulnerability disclosure in het geval van multi vendor coördinatie trajecten?

4. Technologie en cybersecurity

Technologische ontwikkelingen binnen het cybersecurity-speelveld volgen elkaar snel op. Zowel in de academische wereld als in het bedrijfsleven wordt op dit moment fors geïnvesteerd in onderzoek en ontwikkeling van artificial intelligence (AI) en de beveiliging van Internet of Things (IoT). Tegelijkertijd vraagt het verhogen van weerbaarheid dat het ontwikkelproces van producten moet worden herzien om veiligheid in de gehele proces te verweven. Deze ontwikkelingen kunnen het dagelijks functioneren van het NCSC verbeteren, maar tegelijkertijd ook zowel kansen als bedreigingen vormen voor onze doelgroepen.

Het bijhouden van de technische ontwikkelingen is onontbeerlijk voor het *begrijpen* van digitale kwetsbaarheden. Andere ontwikkelingen kunnen partijen, kennis en informatie op een effectievere manier *verbinden*. Ten slotte bieden technische ontwikkelingen ook nieuwe manieren om schade te *voorkomen*.

4.1 Privacy-by-design

Vanuit het privacy denkkader "Wat je niet hebt, kan je ook niet verliezen" kijkt het NCSC ook naar preventieve maatregelen. Een opkomend onderwerp op dit gebied is privacy-by-design, waarbij onze aandacht vooral uitgaat naar big data-analyse, machine-learning en AI-toepassingen met een grote vraag naar data. Daarnaast wordt er ook gekeken naar privacyaspecten bij het delen van data, door het NCSC of door anderen, waarbij de focus in eerste instantie ligt op technische maatregelen maar ook organisatorische maatregelen in beeld komen.

Mogelijke onderzoeksvragen

- Hoe kunnen big data-analyse en privacy-by-design met elkaar verenigd worden?
- Welke privacymodellen en -methoden zijn beschikbaar om incidentdata en informatie binnen het NDN te delen?
- Hoe ziet de marktontwikkeling van privacyvriendelijke producten er uit? Hebben ze een concurrentievoordeel?
- Welke ontwikkelingen in Privacy Enhancing Technologies (PETs) verhogen de veiligheid van het delen van data?
- Hoe ziet het businessmodel van software (als dienst) in de toekomst eruit en welke impact heeft dit op datazeggenschap?
- Welke standaardprotocollen of middleware zijn er of kunnen er ontwikkeld worden om privacy-by-design te realiseren voor bestaande legacy-systemen, zoals e-mail, agenda's en dergelijke? (Het is een technische uitdaging om bijvoorbeeld IMAP, CALDAV, CARDDAV etc. met 'clientside' encryptie te krijgen).

4.2 Internet of Things

Binnen IoT wordt specifiek gekeken naar standaardisering/certificering en het in kaart brengen van de status in Nederland. IoT-security krijgt van het NCSC de aandacht vanuit de weerbaarheid van Nederland tegen digitale aanvallen. Er is onderzoek gedaan naar de veiligheidsrisico's van IoT voor de vitale infrastructuur, maar er is behoefte aan meer en breder onderzoek naar het zichtbaar en meetbaar maken van de veiligheidsrisico's van IoT in de vitale infrastructuur.

Mogelijke onderzoeksvragen

- Hoe kunnen cyberrisico's van IoT zichtbaar en meetbaar gemaakt worden?
- Wat zijn veelbelovende vormen van certificering en standaarden, zoals SBOM of MUD, en hoe kunnen ze ingezet worden voor de vitale infrastructuur?
- In hoeverre zijn verschillende certificeringsniveaus nodig bij vitale en niet-vitale infrastructuur? Wat betekent dit voor de kosten?
- Wat zijn de IoT-cybersecurityrisico's voor de vitale infrastructuur?

4.3 Fundament van het internet

Het internet is een duidelijk voorbeeld waar security-by-design niet is toegepast. Een van de gevolgen daarvan is dat DDoS-aanvallen een grote dreiging vormen voor de Nederlandse infrastructuur die voorlopig niet zal verdwijnen. Zijn er maatregelen te nemen om dit soort aanvallen te ondervangen, of kan er ingezet worden op een ander ontwerp?

Mogelijke onderzoeksvragen

- Wat zijn effectieve en haalbare maatregelen aan het fundament van het internet om DDoS tegen te gaan?
- Wat voor andere dreigingen vloeien voort uit de huidige standaarden binnen het internet?
- Hoe kan het toekomstige internet bijdragen aan een digitaal veiliger Nederland?
- Hoe kunnen partijen gestimuleerd worden om het fundament van het internet te verbeteren op het gebied van ICT-veiligheid (denk hierbij aan de open source-gemeenschap, internetproviders, internetexchanges, overheden, multilaterale organisaties)?

4.4 Artificial intelligence voor cybersecurity

Er wordt fors geïnvesteerd in artificial intelligence (AI), bijvoorbeeld met onderzoek naar slimme auto's, beeldherkenning en het automatiseren van probleemanalyse. Op dit moment wordt er veel gesproken over de inzet van AI voor cybersecurity. Ook is er nationaal en internationaal aandacht naar de gevolgen van artificial intelligence voor de arbeidsmarkt en de rol van ethiek binnen AI. Wat is de toegevoegde waarde van AI voor cybersecurity? Kunnen we dit als NCSC ook inzetten? Er is nog veel onbekend, dus inventariserend en verkennend onderzoek naar de mogelijkheden en dreigingen van artificial intelligence is op zijn plaats.

Mogelijke onderzoeksvragen

- Op welke wijze en met welke vormen van AI kunnen wij de huidige technieken van aanval en verdediging verbeteren?
- Welke nieuwe vormen van aanvallen maakt AI mogelijk?
- Wat zijn de kwetsbaarheden van AI?
- Wat zijn factoren waardoor het vertrouwen in het gebruik van AI verhoogd kan worden?
- Hoe transparant moet de werking van het algoritme zijn (*algorithmic accountability*) voor verantwoord gebruik van AI door niet-technische personen?
- Wat zijn de maatregelen die nodig zijn om inclusieve en niet-discriminerende AI te ontwikkelen en *bias* tegen te gaan?

4.5 Forecasting

Forecasting betreft de mate waarin organisaties effectief kunnen anticiperen op de toekomst. Door kennis van het heden met ervaringen uit het verleden te vergelijken kun je tijdig trendbreuken zien en de koers bijsturen. Zowel bij het NCSC als haar doelgroep zitten veel inhoudelijk experts en specialisten. Effectieve forecasting is echter gebaat bij een brede blik door kennis te bundelen uit veel verschillende disciplines. Hoe kunnen we specialisten en experts de tools meegeven om die brede blik te ontwikkelen?

Forecasting verhoogt het reactie- en herstelvermogen van organisaties en werkt kostenbesparend. Het NCSC maakt nu al producten waarin verwachtingen voor de toekomst inzichtelijk gemaakt worden zoals de Cyber Security Radar, recentelijk omgedoopt tot het Cyber Kompas. Ook participeert het NCSC in het lopende Cyberforecastingtoernooi, waarin forecasters leren om actief te anticiperen op toekomstige ontwikkelingen. Via onderzoek kunnen trendanalyses worden verbeterd en praktische forecastingtechnieken worden gekozen. Trendanalyses worden verdiept door sociaalwetenschappelijk onderzoek naar de menselijke factoren van cyberaanvallen, bijvoorbeeld door criminologische profielen van daders en hun organisaties op te stellen.

Mogelijke onderzoeksvragen

- Hoe kan een forecasting-methodiek ontwikkeld worden aan de hand van inzichten uit producten zoals de Cyberradar/ Cyberkompas en het Cyberforecastingtoernooi?
- Welke forecastingtechnieken en -tools zijn van belang voor het NCSC en hoe kunnen we deze verder ontwikkelen?
- Hoe kunnen forecastingtechnieken en –tools verbeterd worden door inzichten uit cruciale afwegingen in selectie, ontwikkeling, delivery en effect van criminele activiteiten?
- Wat zijn de verwachte trends voor menselijke factoren die een rol kunnen spelen in toekomstige cyberaanvallen?
- Hoe kunnen historische en forensische data bijdragen aan trendanalyses?

Referenties

1 Nationaal Cyber Security Centrum. *Onderzoeksambitie 2019* [intern document]. Den Haag, 2018.

2. Nationaal Coördinator Terrorismebestrijding en Veiligheid. *Nederlandse Cybersecurity Agenda*. Den Haag, 2018. Geraadpleegd op 27 november 2018: https://www.rijksoverheid.nl/documenten/rapporten/2018/04/21/nederlandse-cybersecurity-agenda-nederland-digitaal-veilig.

3. Dcypher. National Cyber Security Research Agenda III. Dcypher. Den Haag, 2018. Geraadpleegd op 6 mei 2019: https://www.dcypher.nl/national-cyber-security-research-agenda-iii-ncsra-iii-2018.

4. Algemene Rekenkamer. *Digitale dijkverzwaring: cybersecurity en vitale waterwerken*. Den Haag, 2019. Geraadpleegd op 2 mei 2019: https://www.rekenkamer.nl/publicaties/rapporten/2019/03/28/digitale-dijkverzwaring-cybersecurity-en-vitale-waterwerken.

Bijlage 1: Methode

De NCSC Onderzoeksagenda 2019-2022 is tot stand gekomen door de scope van de agenda te definiëren, deskresearch uit te voeren en na analyse een eerste versie te ontwikkelen. Daaropvolgend zijn interviews met interne en externe experts afgenomen om de eerste versie te verfijnen.

1. **Scope definiëren en deskresearch:** De eerste stap was het definiëren van de scope van de Onderzoeksagenda. Het vertrekpunt voor de afbakening vormde de NCSC Onderzoeksambitie 2019 en Onderzoeksagenda (2018a), de Cyber Security Radar (NCSC 2018b) en ontwikkelingen zoals beschreven in de verschillende Cyber Security Beeld Nederland (CSBN) rapporten. Daarnaast vormt de wettelijke taak van het NCSC het uitgangspunt voor deze Onderzoeksagenda. Parallel hieraan is deskresearch uitgevoerd om de scope te vergelijken met andere EU-lidstaten (UK, DE, DK, BE), de Verenigde Staten, alsmede internationale organisaties (EU, ENISA, NAVO, OSVE, Interpol, OESO, VN).
2. **Analyse en ontwikkeling eerste versie:** De resultaten van het deskresearch zijn getoetst aan de missie van het NCSC. In een kwalitatieve analyse is gekeken naar overeenkomsten en verschillen in dossiers, doelen en prioritering. Rekening houdend met de nationale prioriteiten en focus van het NCSC is de scope van de onderzoeksagenda vastgesteld en op basis van bovenstaande analyse is de eerste versie geschreven.
3. **Verzamelen input interne en externe experts:** Na interne inventarisatie zijn drie interviews uitgevoerd met interne en externe cybersecurity experts. Het doel was om eerdere bevindingen te trianguleren en te valideren binnen het netwerk van NCSC. De interviews hebben bijgedragen aan de evaluatie van de onderzoeksthema's.
4. **Verfijning en ontwikkeling definitieve versie:** Op basis van alle bevindingen voortvloeiend uit de desk research en de interviews is de definitieve versie van de Onderzoeksagenda geschreven.

Documentatie deskresearch

Danish Ministry of Finance (2018) "Danish Cyber and Information Security Strategy." The Danish Government, Ministry of Finance. Copenhagen.

Danish Agency for Science and Higher Education (2018) "Research 2025." *Danish Government, Ministry of Education and Science*. Accessed 9 april 2019 from https://ufm.dk/en/publications/2018/research2025-catalogue.

Dcypher (2018) "National Cyber Security Research Agenda." Herbert Bos, Michel van Eeten, Sandro Etalle, Frank Fransen, Jaap Henk Hoepman, Erik Poll, Jan Piet Barthel (eds). *Dcypher*. Den Haag.

Di Franco, F (2018) "Analysis of the European R&D priorities in cybersecurity: Strategic priorities in cybersecurity for a safer Europe." *European Union Agency for Network and Information Security (ENISA)*, doi:10.2824/14357. Athens.

German Federal Ministry of Education and Research (2015) "Self-determined and secure in the digital world 2015-2020: The German government's research framework programme on IT security." Federal Ministry of Education and Research (BMBF) Division Communication Systems, IT Security. Bonn.

Kenneally, E Randazzese, L en Balenson, D (2018) "Cyber Risk Economics Capability Gaps Research Strategy". *United States Department of Homeland Security, Science and Technology Directorate*, doi: 10.23721/1460960.

National Coordinator for Security and Counterterrorism (2018) Cybersecuritybeeld Nederland 2018. *Ministerie van Justitie en Veiligheid – NCTV*, juni, Den Haag.

National Cyber Security Centre of the Netherlands (2018) *Cyber Security Radar.* Rapport van het Nationaal Cyber Security Centrum, juli, Den Haag.

National Cyber Security Centre United Kingdom (2018) NCSC Annual Review. Accessed 9 april 2019 from https://www.ncsc.gov.uk/annual-review-2018.

North Atlantic Treaty Organization (2019) NATO Cyber Defence factsheet. Accessed April 11 2019 from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

Organisation for Economic Cooperation and Development (2015), Digital Security Risk Management for Economic and Social Prosperity: OECD Recommendation and Companion Document, OECD Publishing, Paris. DOI: http://dx.doi.org/10.1787/9789264245471-en.

Organisation for Economic Cooperation and Development (2019) "Policies for the Protection of Critical Information Infrastructure: Ten Years Later." *OECD Digital Economy Papers*.

Organisation for Economic Cooperation and Development (2019) "Draft OECD Recommendation on Digital Security of Critical Activities" OECD Directorate for Science, Technology and Innovation / Division for Digital Economy Policy. Accessed 11 april 2019 http://www.oecd.org/sti/ieconomy/digital-security-of-critical-activities.htm.

Organization for Security and Co-operation in Europe (2016) "OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies", PC. DEC/1202, 10.

Rothenpieler, S (2017) "National Cyber Security Strategy 2016." *Federal Office for Information Security (BSI)* [presentation]. ENISA 26 april 2017, Athens.

United States Department of Homeland Security (2018) "Cybersecurity Strategy." United States Department of Homeland Security. NATO Public Diplomacy Division.

Uitgave
Nationaal Cyber
Security Centrum (NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
research@ncsc.nl
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

122464 | augustus 2019