

## Persbericht

# Non-profit consortium lanceert pilot Cyber Resilience op nationale schaal om het cyberdreigingslandschap voor de NGO-sector in Nederland in kaart te brengen.

Den Haag, 1 april 2024

Een non-profit consortium - bestaande uit [The Hague Humanity Hub](#), het [CyberPeace Institute](#), [Connect2Trust Foundation](#) en [The Shadowserver Foundation](#), medegefinancierd door Rijksdienst voor Ondernemend Nederland (RVO), gaat op nationaal niveau een beoordeling van het cyberdreigingslandschap voor Ngo's uitvoeren, waarbij de impact en schade van cyberdreigingen op de sector wordt gemeten.

Een van de ontvangers van het [Digital Trust Center \(DTC\) Subsidieregeling Cyberweerbaarheid](#), Cyber Resilience for NGOs: A Collective Intelligence Effort, zal een vlaggenschipproject uitvoeren om Ngo's, een van de meest kwetsbare sectoren van de Nederlandse economie, te ondersteunen. Ngo's worden vaak geconfronteerd met cyberdreigingen zonder de ondersteunende middelen om zich effectief te verdedigen. Daarom kunnen ze profiteren van een ondersteunende gemeenschap om te leren, expertise en trends te delen om hun cybercapaciteit te versterken.

In 2023 ontving het Digital Trust Center 23 aanvragen van partners van publiek-private organisaties voor de subsidieregeling Cyberweerbaarheid. Zes projecten kregen een startsubsidie toegekend van een onafhankelijke adviescommissie. Het vergroten van de cyberweerbaarheid in verschillende economische sectoren was een gemeenschappelijk aandachtspunt bij verschillende projectaanvragen.

*"Met het programma Cyber Secure The Hague hebben we de eerste stappen gezet om de cyberweerbaarheid van het Ngo-ecosysteem te verbeteren. Veel van de Ngo's die hier gevestigd zijn, zijn cruciaal voor de internationale infrastructuur van vrede, recht en veiligheid en lopen risico op cyberaanvallen. Ik ben daarom erg blij dat het Rijksoverheid heeft besloten om dit non-profit consortium te steunen en hen te helpen om hun fundamentele werk op te schalen van Den Haag naar de rest van Nederland. Het is erg belangrijk om de cybercrisisvoorbereiding van Ngo's te verbeteren en meer inzicht te krijgen in de cyberdreigingen waarmee Ngo's geconfronteerd worden. Niet alleen in het belang van onszelf in Nederland, maar voor iedereen die wereldwijd door die door Ngo's gediend worden."*

- De Haagse burgemeester Saskia Bruines (verantwoordelijk voor Cyber Secure The Hague)

## Het probleem

Vanwege de gevoelige aard van hun werk nemen cyberaanvallen op Ngo's zowel in frequentie als in impact toe. Recente cyberaanvallen hebben grote internationale organisaties getroffen, zoals het [Internationale Comité van het Rode Kruis](#) en VN-agentschappen, maar ook [kleine Ngo's](#) zoals Roots of Peace en Insecurity Insights. Volgens een [rapport](#) dat Microsoft in oktober 2021 publiceerde, werden ngo's tussen juli 2020 en juni 2021 de op één na meest bedreigde sector door dreigingsfactoren uit natiestaten, vlak na de overheidssector.

Nader onderzoek heeft 500 bevestigde aanvallen op Ngo's sinds 2016 getraceerd, wat resulteerde in miljoenen euro's aan gestolen fondsen en meer dan een miljard gestolen gegevensrecords. In de meeste gevallen hebben Ngo's niet de middelen en capaciteit om zich goed te beveiligen tegen dergelijke bedreigingen.

Het Cyber Resilience for NGOs: A Collective Intelligence Effort project zal de basis leggen voor het beoordelen van het cyberdreigingslandschap voor Ngo's in Nederland en een beter begrip geven van de impact die deze dreigingen en aanvallen kunnen hebben op non-profitorganisaties. Daarnaast zal dit project de cybercapaciteit om gegevens te beveiligen van kleine en grote Ngo's vergroten.

## Het project - beter inzicht in het dreigingslandschap in heel Nederland

Dit project richt zich op een sector die kwetsbaar is voor cyberaanvallen, maar niet over de middelen beschikt om deze effectief te bestrijden. Hoewel de Ngo-sector niet onder de financieringsprioriteiten van de Europese Unie (EU) of vitale infrastructuur van Nederland valt, blijft deze sector essentiële diensten leveren aan kwetsbare delen van de samenleving in Nederland en daarbuiten.

Dit voorstel bouwt voort op het lopende project [CyberSecure the Hague](#), dat medegefinancierd wordt door gemeente Den Haag. Het wordt uitgevoerd in samenwerking met het CyberPeace Institute, het [Dutch Institute for Vulnerability Disclosure](#) (DIVD) en de Hague Humanity Hub. Bovendien vormt het een aanvulling op het Connect2Peace-programma, een initiatief uitgevoerd door CyberPeace Institute en Connect2Trust, en tevens gesteund door Gemeente Den Haag. Hiermee wordt een speciale hub voor het delen van informatie over bedreigingen gecreëerd waar Ngo's gratis beveiligingsadvies en waarschuwingen over hun kwetsbaarheden kunnen ontvangen van nationale cyberbeveiligingscentra en onderzoekers van de overheid, zoals Shadowserver en DIVD.

Cyber Resilience for NGO's: A Collective Intelligence Effort heeft als doel de basis leggen voor meer onderzoek en activiteiten op nationaal niveau door een goed afgerond begrip te creëren van het gehele cyberdreigingslandschap in Nederland.

De specifieke doelstellingen van dit nieuwe project zijn:

- Het cyberbedreigingslandschap en het cyberbeveiligingsvolwassenheidsniveau van de doelorganisaties op de lange termijn beoordelen door een diepgaande analyse te bieden via een bedreigingsintelligentieverslag.
- Gepaste informatie over cyberbedreigingen verstrekken op basis van hun cyberbeveiligingsvolwassenheid, om vertrouwen op te bouwen en om de Ngo-gemeenschap de middelen te geven om erop te reageren.

- Een crisisrespons simulatie ontwikkelen voor Ngo's om hen beter voor te bereiden op een eventuele aanval en om de informatie die het onderzoek analyse oplevert om te zetten in concrete actie.
- Bewustwording creëren over cyberweerbaarheid binnen het bredere ecosysteem van Ngo's in Nederland en, in het verlengde daarvan, onder beleidsmakers en donoren, door hen te informeren over de kritieke rol van cyberbeveiliging voor Ngo's.

## De ambitie

De ambitie van het project is om voort te bouwen op dit initiatief door het ondersteunen van capaciteitsopbouw in het komende jaar en - in samenwerking met andere partners - een ondersteunende infrastructuur voor de lange termijn op te bouwen voor de Ngo-sector in het hele land. Het project is gericht op het creëren van een schaalbaar model voor het beoordelen van het dreigingslandschap in het hele land voor de cyberveiligheid van Nederlandse Ngo's en op het verbeteren van het bewustzijn van de grootste hiaten en zwakke punten, en het identificeren van mogelijkheden voor het versterken van de cyberweerbaarheid van Ngo's.

Dit project is er ook op gericht om beleidsmakers en donoren vanaf het begin bij het project te betrekken en te brainstormen over de impact van hun actieve betrokkenheid bij de ondersteuning van het opbouwen van cyberbestendige Ngo-ecosystemen. Door middel van de in het project genoemde activiteiten, wil het consortium de gemeenschap van Ngo's, industrie, academische wereld en filantropie verder groeien en consolideren, waarbij de krachten worden gebundeld om de duurzaamheid van de aanpak te garanderen.

## De Oproep Tot Actie

Voor Ngo's die geïnteresseerd zijn in deelname aan het project, om ondersteuning te ontvangen en te leren over hun eigen cyberweerbaarheid en dreigingslandschap.

Voor beleidsmakers, overheden, netwerken en andere groepen belanghebbenden die geïnteresseerd zijn in het ondersteunen van en aansluiten bij de community, om expertise te delen en te leren en samen te werken aan een veerkrachtiger cyberlandschap in Nederland.

- Einde persbericht -

## Over de projectpartners

### *Over The Hague Humanity Hub*

The Hague Humanity Hub is opgericht in 2018 en is een not-for-profit stichting in Den Haag die het ecosysteem van Ngo's met doel doet een vreedzamere en rechtvaardigere wereld, ondersteunt en versterkt. The Hague Humanity Hub faciliteert verbindingen en innovatie door de nodige ingrediënten te bieden voor toevallige ontmoetingen, nieuwe allianties, inspirerende samenwerkingen en het uitwisselen van kennis.

### *Over het CyberPeace Instituut*

Het CyberPeace Institute is opgericht in 2019 en is een onafhankelijke en neutrale niet-gouvernementele organisatie (NGO) gevestigd in Genève, Zwitserland. De missie van het instituut is om de rechten van mensen op veiligheid, waardigheid en gelijkheid in cyberspace te waarborgen. Het CyberPeace Institute werkt nauw samen met relevante partners om de schade van cyberaanvallen op het leven van mensen wereldwijd te beperken. Door cyberaanvallen te analyseren, onthult het instituut de maatschappelijke impact ervan, hoe internationale wetten en normen worden geschonden en bevordert het verantwoordelijk gedrag om cyberpeace af te dwingen. Het CyberPeace Institute heeft onder andere het CyberPeace Builders (CPB) programma en het Humanitarian Cybersecurity Center gelanceerd.

### *Over Stichting Shadowserver Europa*

Shadowserver (Nederlandse Stichting en Amerikaanse 501c3 non-profit) is 's werelds grootste leverancier van gratis informatie over cyberbedreigingen van algemeen nut, al bijna 20 jaar actief. Shadowserver onderzoekt schadelijke internetactiviteiten, verzamelt grote hoeveelheden malware en gerelateerde analyse- en metagegevens en deelt infectie- en schadelijke gegevens met de betreffende netwerkeigenaren en nationale en sectorale CSIRT's.

### *Over Connect2Trust Foundation*

Connect2Trust is een sector overstijgend samenwerkingsverband tussen (inter)nationale bedrijven die actief zijn in Nederland. Connect2Trust biedt een veilige en vertrouwde omgeving waarbinnen private partijen die deel uitmaken van Connect2 Trust gevoelige en vertrouwelijke informatie over cyberbedreigingen en best practices kunnen analyseren en uitwisselen, samen met (cyber)beveiligde overheidspartijen.