



## Press Release

# Non-profit consortium launches national scale Cyber Resilience pilot to assess the cyber threat landscape for the NGO sector in The Netherlands.

The Hague, 1<sup>st</sup> April 2024

A non-profit consortium – consisting of [The Hague Humanity Hub](#), the [CyberPeace Institute](#), [Connect2Trust Foundation](#) and [The Shadowserver Foundation](#), co-funded by Rijksoverheid (RVO), will produce a national level assessment of the cyber threat landscape for NGOs, while measuring the impact and harm of cyber threats on the sector.

One of the awarded projects of the [Digital Trust Center \(DTC\) Cyber Resilience Subsidy Scheme](#), Cyber Resilience for NGOs: A Collective Intelligence Effort will implement a flagship project to support NGOs, one of the most vulnerable sectors of the Dutch economy. NGOs often face cyber threats without the resources to defend themselves effectively and therefore can benefit from a supporting community to learn, share expertise and trends to strengthen their cyber capacity.

In 2023, the Digital Trust Center received 23 applications by partnerships of public-private organisations for the Cyber Resilience Subsidy Scheme. Six projects were awarded an initial grant by an independent advisory committee. Increasing cyber resilience across different economic sectors was a common focus across several project applications.

*“With the Cyber Secure The Hague program we have taken the first steps to improve the cyber resilience of the NGO ecosystem. Many of the NGOs that are based here are crucial for the international infrastructure of peace, justice and security and are at risk of cyberattacks. I am therefore delighted that the national government has decided to support this non-profit consortium to help them scale their foundational work from The Hague to the rest of the Netherlands. It’s very important to help improve the cyber crisis preparation of NGO’s and to gain more insight into the cyber threats that NGOs face. Not only in the interest of ourselves in the Netherlands, but for everybody that is served by those NGOs worldwide.”*

- The Hague’s Deputy Mayor Saskia Bruines (responsible for Cyber Secure The Hague):

## The problem

Due to the sensitive nature of their work, cyberattacks on NGOs are increasing both in frequency and impact. Recent cyberattacks have affected large international organisations such as the [International Committee of the Red Cross](#) and UN agencies as well as [small NGOs](#) such as Roots of Peace and Insecurity Insights. According to a [report](#) published by Microsoft in October 2021, NGOs became the second most targeted sector by nation-state threat actors between July 2020 and June 2021, right after the governmental sector.

Further research has tracked 500 confirmed attacks on NGOs since 2016, determining that several millions of euros were in stolen funds and more than a billion data records have been stolen. In most cases, NGOs do not have the resources and capacity to properly secure themselves against such threats.

The Cyber Resilience for NGOs: A Collective Intelligence Effort project will set the baseline for assessing the cyber threat landscape for NGOs in The Netherlands and to better understand the impact that these threats and attacks can have on not-for-profit organisations. In addition, this project will build the cyber capacity of small and large NGO operations to secure data.

The project – better understanding of the threat landscape across The Netherlands

This project targets a sector that is vulnerable to cyberattacks yet lacks the resources to mitigate them effectively. While the NGO sector does not fall under European Union (EU) or Dutch critical infrastructure funding priorities, it continues to provide critical services to vulnerable sections of society in the Netherlands and abroad.

This proposal builds on the ongoing project [CyberSecure the Hague](#), co-funded by the Municipality of The Hague and implemented in partnership with CyberPeace Institute, the [Dutch Institute for Vulnerability Disclosure](#) (DIVD) and the Hague Humanity Hub. Moreover, it complements the Connect2Peace programme, another initiative supported by the Municipality of The Hague, implemented by CyberPeace Institute and Connect2Trust. The initiative creates a dedicated threat intelligence sharing hub for NGOs to receive, free-of-charge, security advice and warnings on their vulnerabilities from governmental national cyber security centres and researchers such as Shadowserver, and DIVD.

Cyber Resilience for NGOs: A Collective Intelligence Effort aims to lay the foundation for more research and activities at the national level by establishing a well-rounded understanding of the entire cyber threat landscape in the Netherlands.

The specific objectives of this new project are to:

1. Assess the cyberthreat landscape and cybersecurity maturity level of the target organisations in the long term by providing an in-depth analysis via a threat intelligence report.
2. Provide appropriate cyber threat intelligence based on their cybersecurity maturity, to build trust and help the NGO community act on it.

3. Develop a crisis response simulation for NGOs to better prepare them should an attack occur and to turn the information generated by the research analysis into concrete action.
4. Raise awareness about cyber resilience within the wider ecosystem of NGOs in the Netherlands and by extension, among policy makers and donors, informing them about the critical role of cybersecurity for NGOs.

### The ambition

The project's ambition is to continue building on this initiative by supporting capacity-building in the coming year and – in collaboration with other partners – build a long-term support infrastructure for the NGO sector throughout the country. The project aims to create a scalable model for assessing the threat landscape across the country for Dutch NGOs' cybersecurity and to improve the awareness of the main gaps and weaknesses and identify opportunities for strengthening NGOs' cyber resilience.

This project also seeks to lobby and involve policymakers and donors since its inception and brainstorm on the impact of their active involvement in support of building cyber resilient NGOs ecosystems. Through the activities listed in the project, the consortium seeks to further create and consolidate an NGO-Industry-Academia-Philanthropy community, joining forces to ensure the sustainability of the approach.

### The Call to Action

For NGOs interested in enrolling in the project, to receive support and learn about their own cyber resilience and threat landscape.

For policymakers, governments, networks and other groups of stakeholders interested in supporting and joining the community, to share expertise and learn, working together towards a more resilient cyber landscape in the Netherlands.

- End of Press Release -

## About the Project Partners

### *About The Hague Humanity Hub*

The Hague Humanity Hub was founded in 2018 and is a not-for-profit foundation in The Hague that supports and strengthens the NGOs ecosystem working towards a more peaceful and just world. The Hague Humanity Hub facilitates connections and innovation by offering the necessary ingredients for chance encounters, new alliances, inspirational collaborations, and the exchange of knowledge.

### *About CyberPeace Institute*

The CyberPeace Institute was founded in 2019 and is an independent and neutral non-governmental organisation (NGO) based in Geneva, Switzerland. The mission of the Institute is to ensure the rights of people to security, dignity, and equity in cyberspace. The CyberPeace Institute works in close collaboration with relevant partners to reduce the harm of cyberattacks on people's lives worldwide. By analysing cyberattacks, the Institute exposes their societal impact, how international laws and norms are being violated, and advances responsible behaviour to enforce cyber peace. Amongst others the CyberPeace Institute has launched the CyberPeace Builders (CPB) Program and the Humanitarian Cybersecurity Center.

### *About Stichting the Shadowserver Foundation Europe*

Shadowserver (Dutch Stichting and US 501c3 non-profit) is the world's largest provider of free public benefit cyber threat intelligence, active for nearly 20 years. Shadowserver investigates malicious Internet activity, collecting large volumes of malware and related analysis and meta data, and shares infection and malicious data with appropriate network owners, National and Sectoral CSIRTs.

### *About Connect2Trust Foundation*

Connect2Trust is a cross-sector partnership between (inter)national companies active in the Netherlands. Connect2 Trust provides a safe and trusted environment within which private parties who are part of Connect2 Trust can analyse and exchange sensitive and confidential information about cyberthreats and best practices, together with (cyber)security-challenged government parties.