CyberPeace Institute

2024

ACTIVITY REPORT

The CyberPeace Institute stands guard over the most vulnerable in cyberspace. We deliver critical cybersecurity assistance, revealing the real human costs of cyberattacks and information manipulation, while holding perpetrators who disrupt peace in cyperspace accountable for their actions. We advocate against the unacceptable use of Artificial Intelligence which threatens international peace and security, while promoting the responsible development and ethical use of AI for the common good.

Our mission to build a secure and inclusive cyberspace calls for a comprehensive, multi-faceted approach, and that's exactly what drives our theory of change. We **assist** civil society organizations and underserved communities to strengthen their **resilience**. We **analyze** the harms caused by cyberattacks and information manipulation, and **advance** responsible state behavior through evidence-based campaigns and public advocacy that promote **accountability**. Finally, we **anticipate** and **address** emerging risks from AI, such as the potential for autonomous cyberattacks, to safeguard global **cyberspace**.

"There's still a misconception that cybersecurity is a technical problem; it is a human security issue."

— Stéphane Duguin, Chief Executive Officer, CyberPeace Institute



CyberPeace Builders at an event



Mohamad Zivdar/ICRC, taken from: https://www.icrc.org/en/article/iranian-red-crescent-response-humanitarian-needs-recent-hostilities

Resilience

We **ASSIST** civil society organizations and underserved communities, including through leveraging AI for cybersecurity, to achieve **RESILIENCE.**



CyberPeace Builders at an event



Tabletop exercise at The Hague Humanity Hub

Answering the Call of NGO Leaders

Civil society delivers humanitarian aid, defends human rights, protects vulnerable populations, reports and documents abuses, advocates for international law and accountability, and builds resilience and capacity. However, they face rising cyberattacks. These disrupt missions, compromise data, and silence voices, yet as digital threats grow, resources for defense remain limited.

In August 2024, with the International Civil Society Centre, we issued an open letter urging governments, companies, and philanthropies to fund nonprofit cybersecurity, hold malicious actors accountable, and protect civil society from digital harm. The letter was signed by over 60 organizations, including WaterAid International, Doctors Without Borders, Transparency International and Reporter Without Borders.



“Access to sustainable funding”

“Commitment and expertise to identify and pursue malicious actors”

“Commitment to not attack nor disseminate disinformation”

“Public documentation on the human, societal and environmental impacts of cyberattacks”

“Recognition of civil society as a global critical infrastructure”

International Civil Society Centre

On September 30, this call was heard by leaders from NGOs, governments, philanthropy, and cybersecurity who united in The Hague to launch the BEYOND 125 action plan. This global initiative aims to protect justice in the digital era by strengthening the cybersecurity of nonprofits.

Setting an inspiring tone, Nobel Peace Prize Laureate Tawakkol Karman opened the event inspiring collective action and urgency. Co-organized by the City of The Hague, the Global Cyber Alliance, and the CyberPeace Institute, in partnership with Common Good Cyber, the Paris Peace Forum, the Global Forum on Cyber Expertise, and The Hague Humanity Hub, the gathering sought to establish a dedicated Common Good Cyber fund that supports the tools, services, and platforms nonprofits need to operate safely.







Launch of Beyond 125 Action Plan at the Peace Palace, The Hague

Opening a CyberPeace Chapter in The Hague

In 2024, the CyberPeace Institute established a chapter in The Hague with the support of the City of The Hague, to strengthen its operational presence in the Netherlands. Based at the Humanity Hub, this chapter supports the Institute's mission to assist vulnerable communities, promote accountability for cyber harm, and advocate for responsible digital technologies. It has also led local initiatives like Cybersecure The Hague, which offered free cybersecurity support to humanitarian NGOs.



Organizations at The Hague Humanity Hub



Launch of Cyber Resilience for NGOs Report??????

Den Haag

VREDE EN RECHT

2024 Journey to Resilience

Achieving Resilience Through Workforce

Achieving Resilience Through Data

From Local Resilience to Global Impact



CyberPeace Institute at an event



Islam Mardini/Oxfam. Taken from: https://www.oxfam.org/en/what-we-do/emergencies/crisis-syria

Achieving Resilience Through Workforce

Implementing such a plan requires workforce for civil society to safeguard them. In 2024, the CyberPeace Builders initiative delivered over 1,000 cybersecurity missions to NGOs worldwide, logging 2,442 volunteer hours and directly protecting 409 nonprofit organizations through the work of more than 1,200 corporate volunteers as our yearly CPB report shows.



In addition, the CyberPeace Builders project was selected for the 2024–2025 Paris Peace Forum Scale Up Program, receiving tailored support to expand its global impact. This milestone boosts its mission to protect NGOs by connecting them with expert cybersecurity volunteers and fostering resilience through regional partnerships and sustainable digital defense.



Paris Peace Forum, 2024



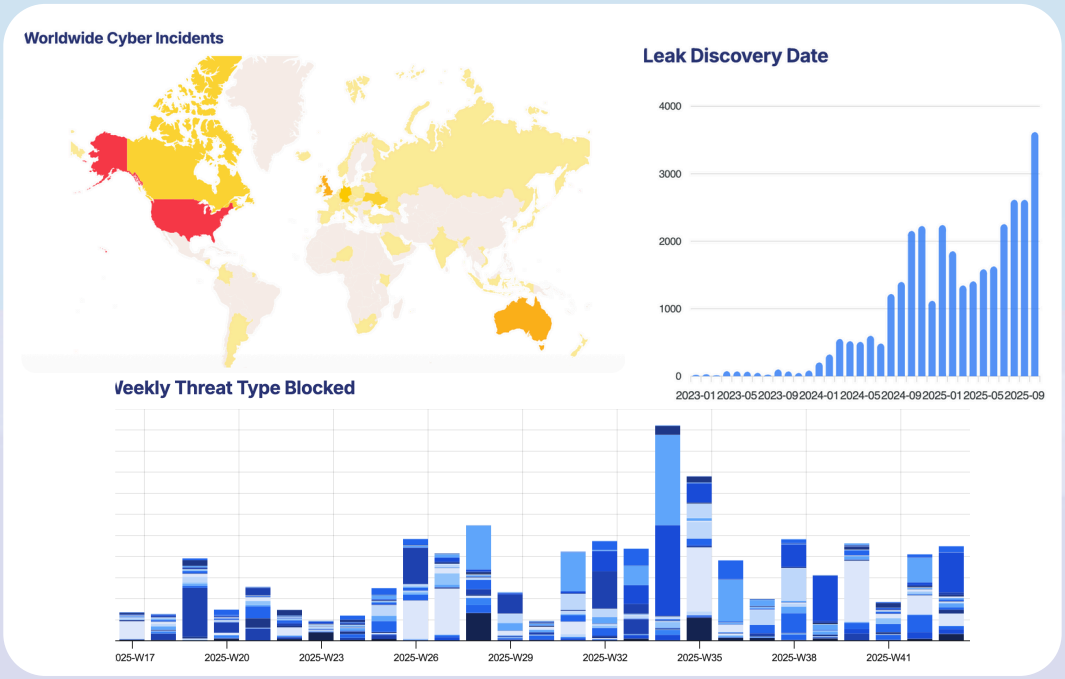
Paris Peace Forum, 2024

Achieving Resilience Through Data

Announcing the CyberPeace Tracer

After having launched Cyber Incident Tracer #Health in 2022 and Cyber Attacks in Times of Conflict Platform #Ukraine in 2023, we officially announced the launch of the CyberPeace Tracer, an AI-powered platform that monitors and analyzes threats against civil society. It's a powerful step toward transparency, accountability, and digital peace.

Threats at a Glance



From Local Resilience to Global Impact

Cybersecurity for the Underserved Population in the United States

Nonprofits, schools, local governments, and hospitals rely on digital tools but lack resources to secure them. These “target-rich, resource-poor” organizations face growing cyber threats that can disrupt or shut down vital community services without proper cybersecurity support.



Cyber Resilience Corps platform

In 2024, the Cyber Resilience Corps, co-founded by the CyberPeace Institute and UC Berkeley Center for Long-Term Cybersecurity, mobilized expert volunteers to support at-risk organizations with the support of Craig Newmark Philantropies. Through cybervolunteers.us, CyberPeace Institute provided CyberPeace Builders expertise, helped shape scalable volunteer models, and promoted equity-focused collective defense.

Key numbers:

- 1,200+ volunteers registered on cybervolunteers.us
- Hundreds of nonprofits, hospitals, and schools engaged
- Nationwide outreach to “target-rich, resource-poor” sectors

Building Cyber Resilience for Democracy and Communities Across the U.S.

Through a partnership with NGO-ISAC on the "Protecting Democracy" project, we extended the Cyber Carwash initiative into 2025—helping at-risk organizations take a closer look at vulnerabilities and boost their defenses. The results speak for themselves: 100% of participating organizations improved their cyber resilience.

NGO-ISAC
BETTER TOGETHER

Cybersecurity in Switzerland from General Population to Swiss Foundation

The CyberPeace Institute, supported by the City and Canton of Geneva, lunched the Éclaire initiative, mobile digital counters placed in public locations like markets, stations, university areas, and festivals, to spark open conversations about cybersecurity, AI, and digital safety. These pop-up stands will allow passersbyers to ask questions freely and share their digital concerns, helping the Institute tailor accessible support networks. Through Éclaire, the Institute fostered stronger partnerships among local associations and institutions, ensuring Geneva's community knows where to turn for practical cybersecurity assistance

éclaire
le phare numérique

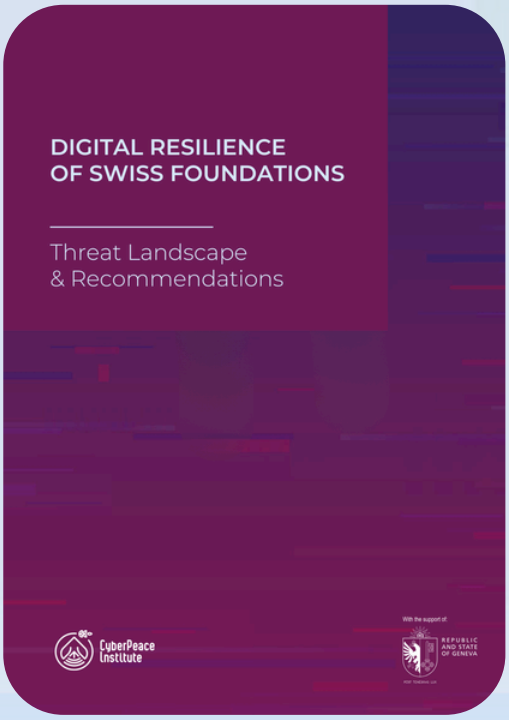
REPUBLIQUE
ET CANTON
DE GENEVE
POST TENEBRAS LUX

AVEC · LE · SOUTIEN
· · · · · · · · · · · DE · LA
VILLE · DE · GENÈVE



Cyber awareness campaign at Gare Cornavin, Geneva with the Éclaire project

Swiss foundations face rising cyber threats, yet many lack the resources to respond. The CyberPeace Institute, supported by the Republic and State of Geneva, had researched their digital resilience.
Publishing in 2025, the report offers insights and recommendations to help foundations strengthen cybersecurity and protect their critical philanthropic missions.



With support of:

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

Cybersecurity for Civil Society In The Netherlands

Cyber threats have no border. Humanitarian NGOs in the Hague also face face rising cyber threats with limited resources to defend themselves. These vulnerabilities put vital humanitarian aid and sensitive data at risk amid an increasingly hostile digital environment.



CyberPeace Builders table top excercise at the Hague Humanity Hub



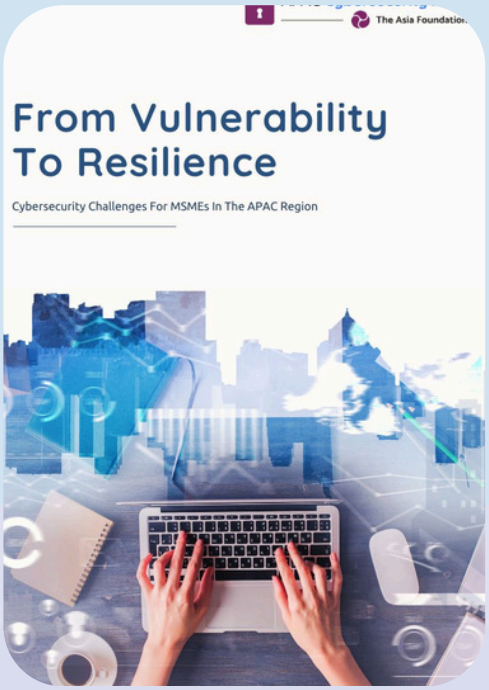
ONE Conference in the Hague
Source: The Hague Humanity Hub (THHH) website

Since launching Cyber Secure The Hague in 2023 alongside The Hague Humanity Hub, DIVD, and CSIRT.global, we provide free cybersecurity support to NGOs of the Hague to strengthen their digital defenses. In 2024, we actively led and contributed to key initiatives like the Cyber Resilience for NGOs report and the Beyond 125 initiative, driving awareness and collaboration around NGO cybersecurity at local and global levels.

The Cyber Resilience for NGOs study revealed that the average cybersecurity maturity among participating NGOs was 49.9%, with only 32% using multi-factor authentication. Based on those numbers, the report offers targeted recommendations to help NGOs strengthen their cybersecurity posture

Cybersecurity for Micro, Small, and Medium Sized Enterprises in the APAC Region

The APAC Cybersecurity Fund, launched by The Asia Foundation, CyberPeace Institute, and Global Cyber Alliance, responds to rising cyber risks facing MSMEs and nonprofits post-pandemic. With support from Google.org, it empowers 300,000 underserved organizations across 12 countries through tailored tools, training, and awareness to build lasting digital resilience.

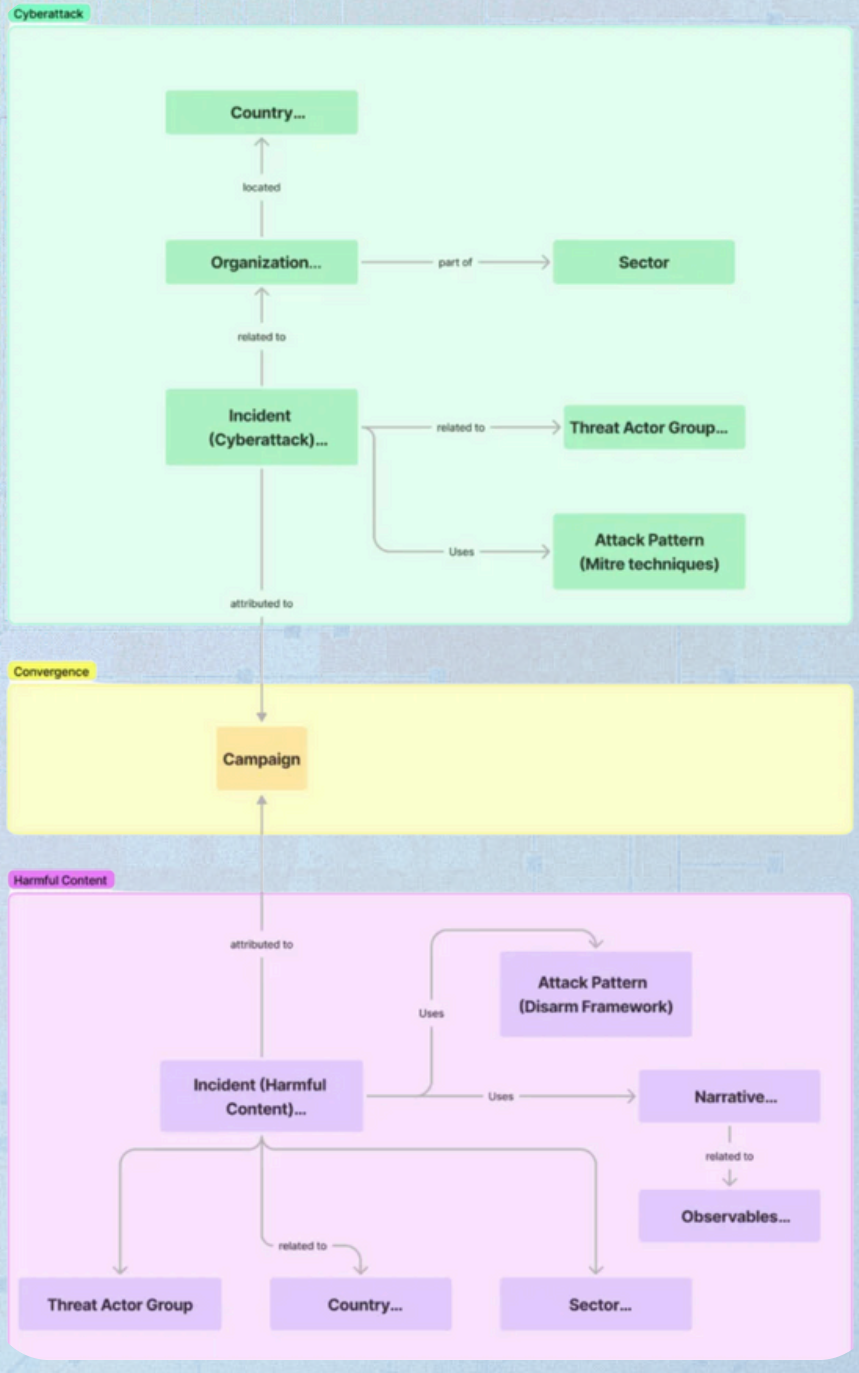


Accountability

We **ANALYZE** harm of cyberattacks and information manipulation, and ADVANCE State-responsible behavior through collaborative evidence-based campaigns and public positions to enforce **ACCOUNTABILITY**

Analyzing the Convergence of Cyberattacks and Information Manipulation

From hacked data leaks to defaced websites pushing propaganda, the convergence of cyberattacks and information manipulation poses a growing threat. To counter it, we combine the MITRE ATT&CK and DISARM frameworks with OpenCTI, enabling collaborative analysis of tactics and narratives, because tackling digital harm requires both technical insight and shared understanding.

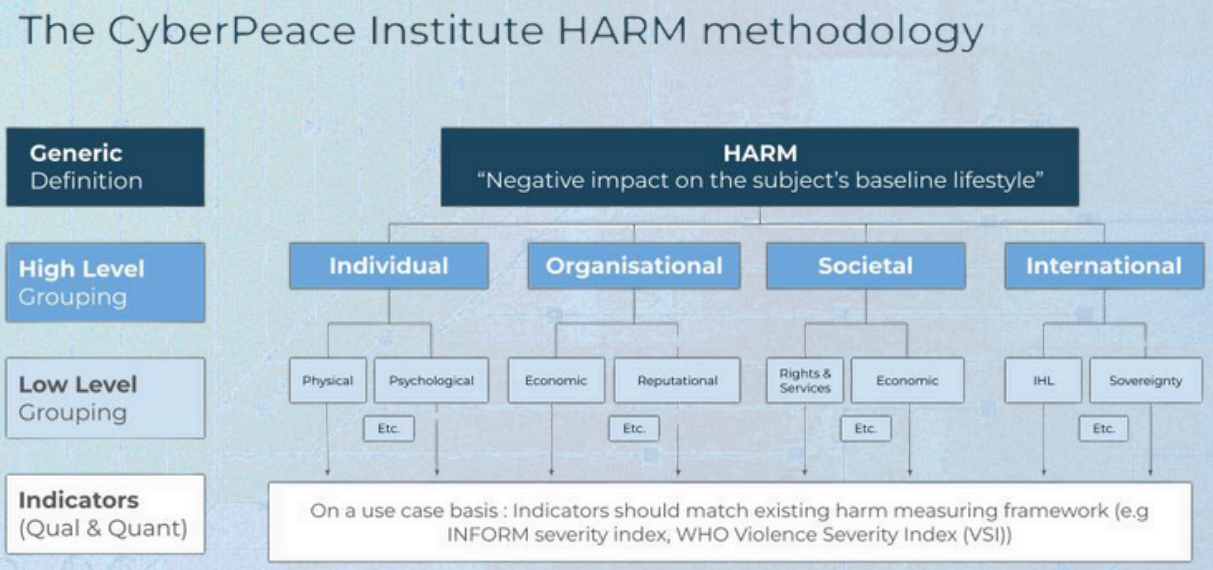


CyberPeace Institute framework to analyze cyberattacks

Measuring Harm to Enforce Accountability

Harms Methodology

Cyberattacks are increasing and continue to escalate, yet their impacts are often measured only in technical terms, downtime, financial loss, breached data. Our CyberTransparency Value Chain report shows how this misses the wider harm inflicted on people and societies. That's why we're developing a framework to assess the human impact, strengthening resilience, informing policy, and driving accountability in cyberspace.







Experts Meeting for the development of a Harms Methodology

Calling for Accountability on a Global Level

Intervention at UN Security Council

At the UN Security Council on June 24, 2024, our CEO, Stéphane Duguin called for urgent action on evolving cyber threats. In his intervention, he stressed the need for transparent attribution, enforcement of norms, and preparedness for AI and quantum risks, underscoring that de-escalation is impossible without accountability and harm-focused impact measurements.

United Nations
Security Council



Calling for human rights safeguard within the UN Cybercrime Convention

In October 2024, we joined a global call urging the EU and its member states to reject the draft UN Cybercrime Convention, citing its failure to include strong human rights safeguards. We warned about the treaty's overbroad scope and that the vague provisions could enable surveillance abuses, threaten civil liberties, and jeopardize cybersecurity research. We instead called for rights to be respected and transparent alternatives backed by international law.



EU Disinfo Lab Conference 2024

Pall Mall Process - Commercial Intrusion Tools

The CyberPeace Institute contributed to the Pall Mall Process in 2024, advocating for stronger oversight of commercial cyber intrusion tools. At the November 12 meeting in Paris, co-hosted by France, the United Kingdom, and the Paris Peace Forum, we emphasized the need for transparency, accountability, and harm-focused regulation. This dialogue informed a report that will guide the 2025 conference on countering cyber intrusion proliferation.

Pall Mall Process



Anticipation

We **ANTICIPATE** and **ADDRESS** unacceptable risks of AI, such as the risk for autonomous cyberattacks, to protect **CYBERPEACE**

Supporting EU Research & Development to combat AI Augmented Cybercrime and Information Manipulation

Enhancing Cross-Border Cybercrime Investigation

In December 2024, we joined the launch of the EU-funded ENSEMBLE project that aimed to enhance cross-border cybercrime investigations. As part of a consortium led by the Centre for Research & Technology Hellas, we support the development of an AI-based investigation toolbox, public awareness efforts, and training for law enforcement to strengthen Europe's collective response to complex cyber threats.

Developing European Threat Intel Platform

As part of the project, Underserved, the CyberPeace Institute contributed to the EU-funded project by assisting in the development of a threat intelligence exchange platform. This platform connects NGOs, law enforcement agencies, and Computer Security Incident Response Teams (CSIRTs) to enhance cybersecurity resilience. Additionally, the Institute supported the creation of a report detailing the cybersecurity landscape of EU-based NGOs, highlighting vulnerabilities and the urgent need for targeted interventions.

Addressing the Risk of AI in Cyberspace

Engaging the Community for European Research and Innovation for Security (CERIS)

Regulated research and innovation is critical to empower EU judiciary and law enforcement to combat cybercrime. At the CERIS 2024, we joined the EU research Community to debate on how the AI Act provide safeguards while allowing for innovation.



CERIS 2024



CERIS 2024

Promoting Responsible and Human Rights-Respecting AI at Freedom Online Coalition (FOC)

On the sidelines of the FOC in Geneva, we participated in a session exploring how AI systems can be harnessed for the benefit of society. The discussion explored how existing international human rights laws can guide the responsible design, development, deployment, and use of AI, and how to embed these safeguards throughout the AI life cycle.

FREEDOM ONLINE COALITION

Delivering AI Skills Training in Switzerland

In partnership with Microsoft, the CyberPeace Institute held a workshop in Zurich, Switzerland to demystify AI tools, explore their use by nonprofits, share insights from the Institute's experience developing a responsible AI policy, and examine AI-enabled cybersecurity threats such as deepfakes and phishing and their impact on nonprofit organizations.



Microsoft

Hosting a workshop at GESDA Summit 2024

In collaboration with GESDA, the CyberPeace Institute organized the workshop "AI, autonomy and the future of peace and security – ideating safeguards". It aimed to identify potential safeguards, which would be further researched to inform international discussions and support the development of robust strategies to prevent and mitigate autonomous cyberattack risks.



GESDA Summit, 2024

Engaging at Rhodes Forum on Technology and Society 2024

At the session “Data Defenders — Keeping Cyber Threats at Bay”, we explored the critical need for advanced data protection strategies and proactive defense against evolving threats.



Panel at Rhodes Forum on Technology and Society 2024

Exploring “AI in Humanitarian Aid: Boosting Impact, Navigating Risks” at AIdEx 2024

We took part in a session to discuss how artificial intelligence can enhance humanitarian operations while managing its risks, and highlighted the need to balance innovation with responsibility in an increasingly digital sector.

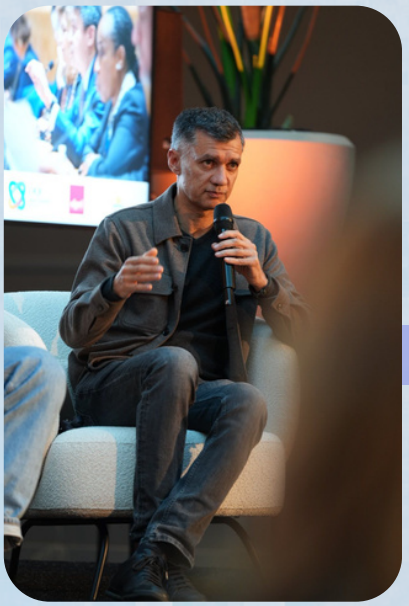


Panel at AidEx - The Global Humanitarian Aid Community

Contributing to the “Quantum for Good: Setting the Agenda for the International Year of Quantum” Conference 2024

We participated in the panel “Deep Dives: The Potential of Quantum for Good” at the two-day conference hosted by UNICC, ITU, and Quantum Delta NL. We explored opportunities for quantum innovation to advance sustainable development ahead of the International Year of Quantum Science and Technology 2025.





UNICC panel on promises and challenges of quantum computing for civil society.

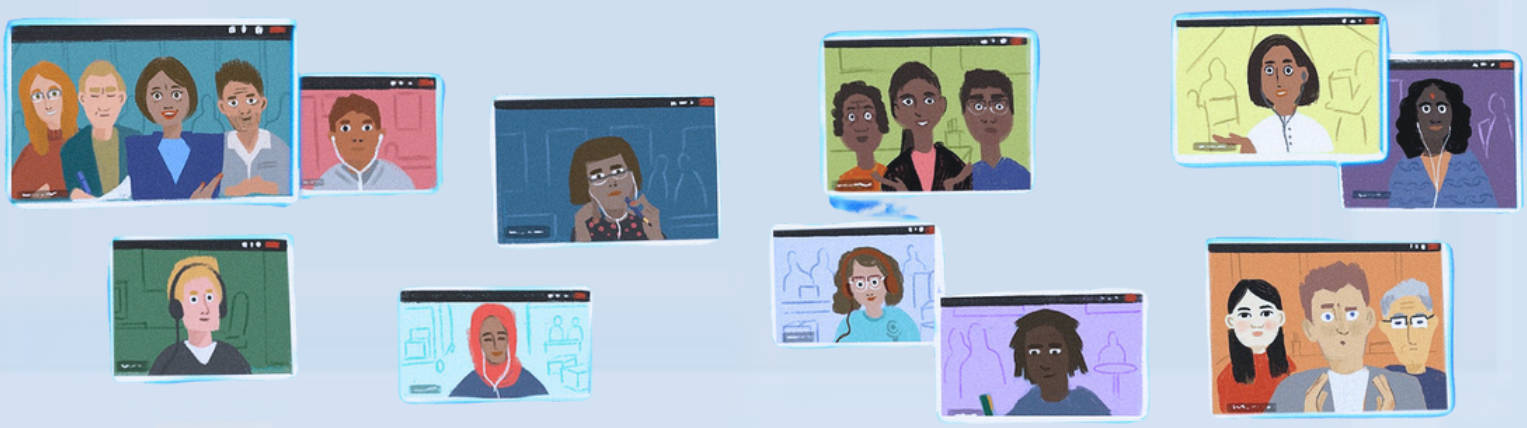
The People Behind the Institute

The CyberPeace Institute brings together a varied team—from cybercrime investigators and cybersecurity experts to policy specialists and communications professionals—united by a shared commitment to advancing cyberpeace.

Diversity is one of our core values and we continue to strive for gender parity among our employees. Currently, our full-time staff is composed of 48.4% female and 51.6% male colleagues.

An integral part of our teams are our interns and young professionals. In 2024, we partnered with 16 universities to welcome their students as interns. Young professionals are recent postgraduate degree holders looking for initial professional experience. They are contracted to carry out specific projects for the





Finance and Funding

In accordance with our core principle of independence, the Institute operates free from the direction, control or interference of any actor, including states, industry or other organization. The Institute relies on voluntary donations and independently fundraises to support its operations while ensuring that donations are in accordance with its mission, principles and standards of due diligence. The financial reports of the organization are published annually and analyze the preceding year of activity of the Institute.

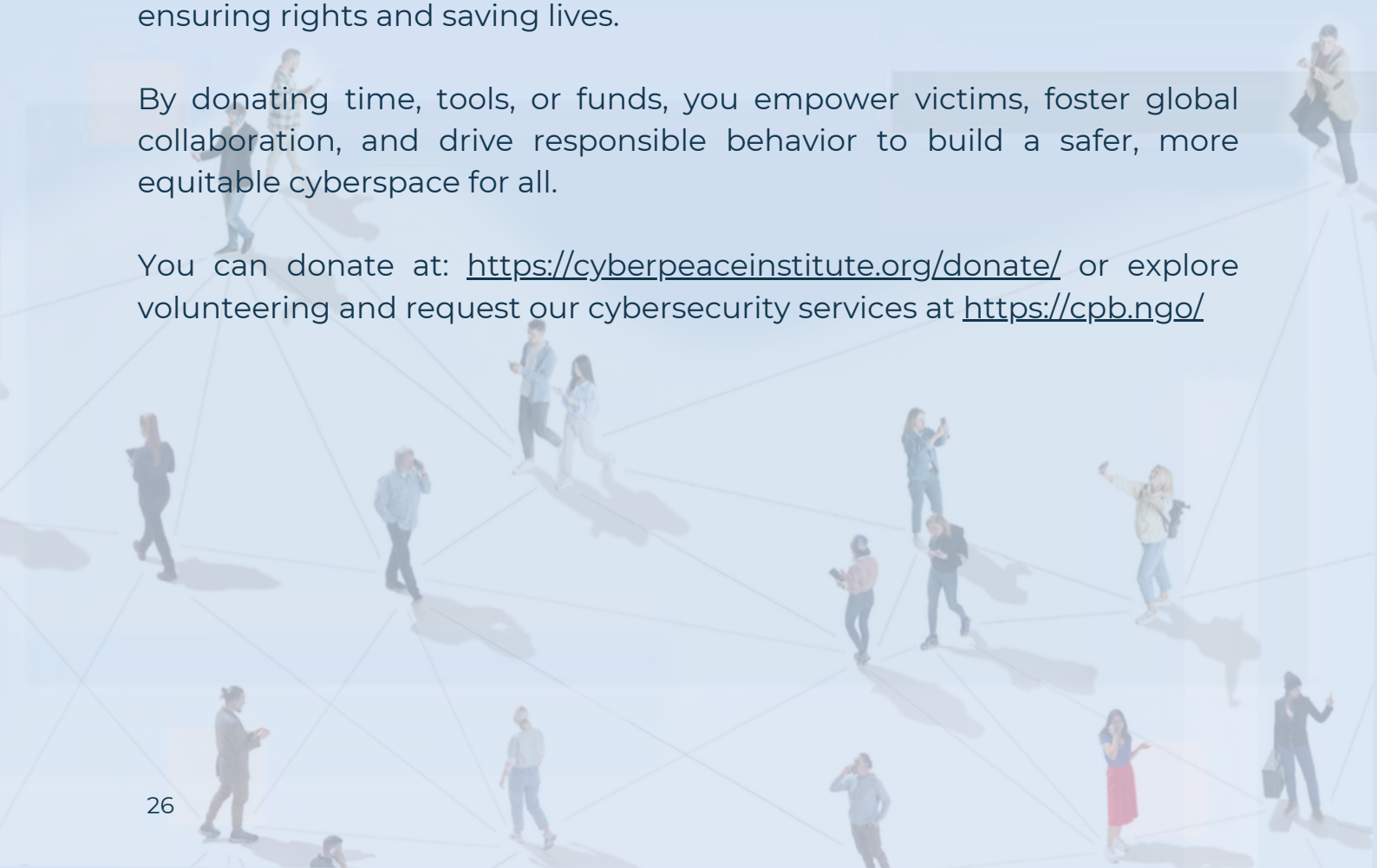
The **annual budget** of the Institute in 2024 amounted to **CHF 4 534 193**, which was fully funded by donors.

Contribute to CyberPeace Institute

We support essential service providers, such as Civil Society Organizations, whose vulnerability to cyber threats affects us all. Your contribution helps secure their resources and resilience to cyberattacks, ensuring rights and saving lives.

By donating time, tools, or funds, you empower victims, foster global collaboration, and drive responsible behavior to build a safer, more equitable cyberspace for all.

You can donate at: https://cyberpeaceinstitute.org/donate/ or explore volunteering and request our cybersecurity services at https://cpb.ngo/



We express our appreciation to those who read our publications, listen to us, follow our work, and participate in our programs.

Thank you.

CyberPeace Institute

Campus Biotech Innovation Park
Avenue de Sécheron 15
1202 Geneva, Switzerland

CyberPeace Institute Stichting

The Hague Humanity Hub
Fluwelen Burgwal 58
2511 CJ The Hague, The Netherlands

@CyberPeace Institute
@Cyberpeaceinstitute

cyberpeaceinstitute.org