

2025 ACTIVITY REPORT



CyberPeace
Institute

A Theory of Change for Global Stability

In an era defined by the weaponization of digital vulnerabilities, the CyberPeace Institute serves as a critical guardian for the most vulnerable actors in cyberspace. We do not merely observe digital conflict; we actively shift the global paradigm from reactive assistance to systemic deterrence. This "Theory of Change" is the strategic foundation for 2025 and beyond, moving toward a future where peace is defined not just by the absence of attacks, but by the presence of a resilient, accountable, and anticipated digital environment.

The Institute's mandate is a comprehensive response to the erosion of digital trust. By assisting civil society organizations, analyzing the tangible harms of cyber-attacks, and advancing responsible state behavior through evidence-based advocacy, we bridge the gap between technical defense and international peace. Our operations seek to ensure that those who disrupt the digital commons are held accountable, while those who provide essential humanitarian services are shielded from the fallout of transnational crime.



HOW WE CREATE IMPACT

Our Theory of Change is operationalized through three strategic pillars:

RESILIENCE

Empowering civil society and underserved communities to achieve lasting resilience through scalable support and practical tools.

ANTICIPATION

Safeguarding the future by identifying emerging risks in the AI frontier and leveraging new technologies to empower the underserved.

ACCOUNTABILITY

Analyzing the harms caused by cyberattacks and information manipulation, and advancing responsible state behavior through evidence-based campaigns and public advocacy that promote accountability.

This mission converts raw data of the frontlines into the strategic evidence required for global policy. By treating every resilience mission as a sensor for the broader threat landscape, we transition from the immediate defense of a single NGO to the systemic protection of the global digital commons.

RESILIENCE

Resilience is not a static state but a repeatable mechanism for sustainable defense. For civil society, who delivers healthcare, defends human rights, and facilitates aid, a digital disruption creates humanitarian issues. Our 2025 strategy focused on building scalable systems that moved beyond one-off interventions, creating a permanent defensive posture for those who protect others.



RESILIENCE

RESILIENCE BY THE NUMBERS

This year our The CyberPeace Builders (CPB), program achieved:

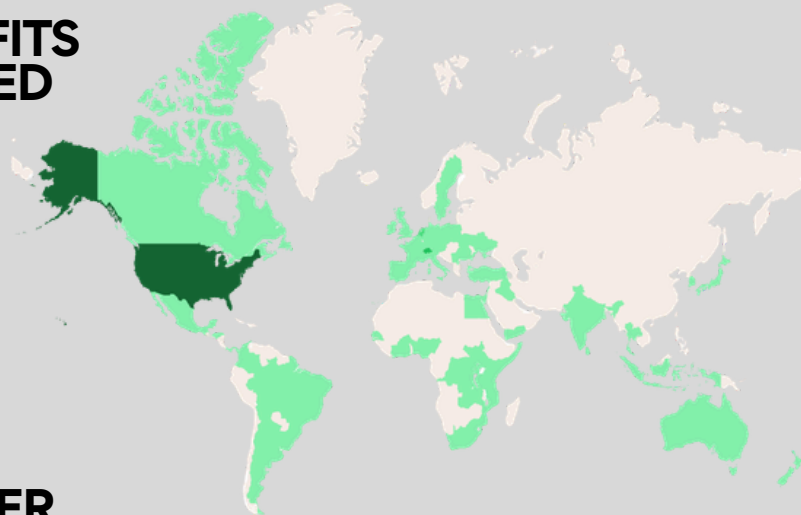
- 645 Nonprofits Protected
- 1426 CyberPeace Builders (Volunteers)
- 3521 Volunteer Hours Logged
- 1488 Cybersecurity Missions Delivered
- 97% Satisfaction Rate from Beneficiaries

645
NONPROFITS
PROTECTED

1488
MISSIONS

1426
BUILDERS

3521
VOLUNTEER
HOURS



We proudly celebrated the 4th anniversary of the CPB program, acknowledging a growing global movement of volunteers, corporate partners, and nonprofits coming together to secure civil society.



RESILIENCE

HOW WE BUILT RESILIENCE

CPB Chapters

To localize impact, we launched CyberPeace Builders local chapters in New York City, Geneva, and Dublin, creating regional hubs where cyber volunteers and nonprofits connect, collaborate, and execute regular missions.



New York City Chapter Gathering

Global participation

We actively supported civil society resilience at major 2025 events, including RightsCon 25 in Taipei, the RSA Conference in San Francisco, and DEFCON in Las Vegas.



RSA 2025



DEFCON 2025

RESILIENCE

UnderServed

As part of the EU-funded UnderServed project, we assisted in developing a threat intelligence exchange platform connecting NGOs, law enforcement agencies, and CSIRTs to enhance cross-border cybersecurity resilience.



Co-funded by
the European Union

Asia Foundation x Google

Through the APAC Cybersecurity Fund, supported by Google.org, we partnered with The Asia Foundation and the Global Cyber Alliance to empower 300,000 underserved MSMEs and nonprofits across 12 countries with tailored tools and training.



The Asia Foundation

Google.org



GLOBAL
CYBER
ALLIANCE.

APAC Financial Inclusion Metrics

Our 2025 Cyber Resilience for Financial Inclusion: Threat Landscape Report, supported by Mastercard Center for Inclusive Growth, assessed 95 APAC organizations and uncovered critical gaps. We found that 89% of these organizations had leaked credentials (exposing over 294,803 records) primarily due to infostealer malware. 64 organizations exhibited known vulnerabilities, and TLS (Transport Layer Security) misconfigurations affected roughly 50% of the assessed group.



Center for
Inclusive Growth

RESILIENCE

Cyber Resilience Corps (USA)

Co-created with UC Berkeley's Center for Long-Term Cybersecurity and supported by Craig Newmark Philanthropies (with a \$1.2M initial investment and a \$1M renewal), we mobilized the first national U.S. cyber volunteer platform at cybervolunteers.us. This initiative deployed over 1,200 volunteers to protect critical community infrastructure, from rural hospitals to K-12 schools.



2025 Cyber Volunteering Day

RESILIENCE

LOCAL AND COMMUNITY RESILIENCE

Resilience is not delivered through one-off interventions. It is built through repeatable mechanisms that help organizations assess risk, receive support, and continuously improve.

Éclaire initiative

Supported by the City and Canton of Geneva, the Éclaire initiative deployed mobile digital counters at markets and stations to provide accessible, on-the-spot advice about digital safety and AI to the public in Geneva, Switzerland.



Éclaire project in Geneva

éclaire



REPUBLIQUE
ET CANTON
DE GENEVE

POST TENEBRAS LUX



Éclaire project in Geneva



Éclaire project in Geneva

RESILIENCE

CyberPeace Builders Local Workshops

In November 2025, we hosted a highly successful cyber crisis simulation in Geneva for 23 participants from 20 nonprofits, earning a 4.7/5 rating for its immersive and confidence-building approach.



CPB crisis exercise in Geneva



CPB crisis exercise in Geneva

RESILIENCE

Geneva Cyber Week 2025

The event served as a key platform for us to advance discussions on digital resilience and artificial intelligence.

During the week, we led and participated in several critical sessions:

- "From Summits to Solutions: Advancing Multilateral Action on AI-driven Cyber Risks": A luncheon roundtable focused on anticipating and mitigating cyber risks fueled by AI.
- "CyberPeace Builders: Cafe & Croissants": A community-building event held to support and connect the local cyber resilience network.
- "Stronger Together: Harnessing AI for Collective Digital Resilience in International Geneva": An open discussion exploring how artificial intelligence can be safely leveraged to protect and strengthen civil society.



Panel at Geneva Cyber Week 2025



CyberPeace Builders: Cafe & Croissants

RESILIENCE

Looking ahead

Building on the momentum from these 2025 engagements, the Institute is integrating these themes into its future initiatives. Looking ahead, the Institute will host Protect.ngo'26, an exclusive, invitation-based event scheduled for May 6, 2026, during the 2026 Geneva Cyber Week. This upcoming gathering will convene foundations, municipal leaders, Fortune 500 companies, and cybersecurity experts to move beyond dialogue and forge concrete commitments for protecting the global nonprofit sector



RESILIENCE

FROM RESILIENCE TO DATA

H-ARMOR

A collective project involving multiple organizations in the cybersecurity and Foreign Information Manipulation and Interference (FIMI) sectors. The initiative is designed to strengthen global accountability by shifting the focus from merely diagnosing digital threats to facilitating concrete disruption. We held two events discussing the initiative with industry professionals and presented H-ARMOR initiative at the EU Cyber Agora 2025 in Brussels, prototyping joint investigation workflows for hybrid threats



RESILIENCE

1

Collect & standardise EU-based, machine-readable

We ingest public reporting and partner-safe indicators, then normalise them into a tool-agnostic, machine-readable format (entities + relationships across domains, hosting, registrars, IP space, payment rails).

2

LLM-assisted entity extraction
Speed without losing traceability

LLMs help extract and structure entities (domains, orgs, services, wallets, aliases, infrastructure providers) from large volumes of with provenance preserved so every claim can be traced back to sources.

3

Federated overlap detection
Hit / No-Hit, data stays "at home"

Participants keep sensitive data locally, but can answer a simple question: "Do we see this entity-yes or no?" This reveals infrastructure reuse and blind spots without centralising datasets.

4

Disruption pathway design
Disruption is the KPI

Because the KPI is disruption-not publication-the workflow is built to produce actionable, structured evidence: registrar/hosting interventions, takedown waves, sanctions enforcement pathways, and LEA-ready referrals where appropriate.

EVIDENCE AND TOOLS FOR ACCOUNTABILITY

Infinity project

CyberPeace Institute continues its participation in the EU-funded INFINITY (Innovative Fighting in Forensics) project. This project uses immersive data visualization, AI, and virtual reality (VR) to transform criminal investigations, analyzing cyber threats across European jurisdictions.



Co-funded by
the European Union

CyberPeace Tracer Launch

We officially launched the AI-powered CyberPeace Tracer to monitor threats against civil society. In 2025, the platform recorded 560,597 phishing emails targeting NGOs, highlighting phishing as a persistent vector for credential theft and fraud.



KADUU

 **Dataminr**[®]

 **CLOUDFLARE**

BIT SIGHT[™]

ACCOUNTABILITY

Ransomware Report (2025)

We published "Ransomware: Follow the Threat Actor", a report mapping 290 threat actors and analyzing 2,753 global incidents from 2020-2025. Of the 168 actors with sufficient data, 112 were connected to the Russian Federation, followed by Iran (13) and China (8). The report identified the U.S. as the most targeted country (1,488 incidents) and Healthcare as the most targeted sector (818 incidents). We also mapped 1,157 IP addresses to demonstrate critical shared infrastructure vulnerabilities.

Swiss Foundations Digital Resilience Report

Drafted with the support of the Republic and Canton of Geneva, this report provides insights and recommendations to help Swiss philanthropic foundations strengthen their cybersecurity and protect their critical missions.



Harms Methodology Update

We moved beyond technical metrics to measure the human, societal, and environmental impacts of cyberattacks, using these insights to foster transparency and support legal accountability processes.

ACCOUNTABILITY

EDRN Blueprint

Co-created the European Democracy Resilience Network (EDRN), pilot (Aug 2025–Jan 2026) with EU DisinfoLab and 30+ Civil Society Organizations to defend democratic spaces from hybrid threats. The project's dashboard blueprint features EDRN Trends, including a Narrative Radar and Impersonation Trends, and Resources (First 24h Checklist, Crisis Communications Kit).



Ensemble

In May, the CyberPeace Institute attended the General Assembly of the ENSEMBLE consortium, funded by Horizon Europe. By uniting law enforcement, researchers, industry, and civil society, ENSEMBLE is a reminder that resilience is not built alone.



ACCOUNTABILITY

FROM EVIDENCE TO JUSTICE AND POLICY

UN Open-Ended Working Group

We hosted a session at the United Nations Open-Ended Working Group in New York examining whether international norms support a victim-centric response to cyberattacks against NGOs.



Side-event at the UN's 10th OEWG session

NATO EEAS Informal Joint Analytical Conference

In September our CEO, Stéphane Duguin, represented the CyberPeace Institute at the EEAS Analytical Conference organized with NATO in Brussels. As EU and NATO leadership increasingly prioritize practical collaboration to confront contemporary security challenges, this high-level forum focused on critical convergence areas, including digital transformation, cyber defence, capability development, and ongoing support for Ukraine.



ACCOUNTABILITY

Forum INCYBER 2025

We spoke at Forum INCYBER Europe in Lille on the convergence of cyberattacks and information manipulation targeting EU Trusted Flaggers, expert organizations officially designated under the Digital Services Act to identify and report illegal online content, with their reports given priority by platforms.



Discussion at Forum INCYBER Europe 2025

Pall Mall Process

We advocated for stronger oversight of commercial cyber intrusion tools at the Paris Peace Forum, emphasizing the need for transparency and harm-focused regulation. We spoke about information manipulation and fact-checking tools to combat false information and applying scalable cybersecurity measures to defend nonprofits.

Our CyberPeace Builders volunteer program, selected as a Scale-Up project at the 2024 Forum, returned this year to showcase its progress in helping nonprofits around the world strengthen their cyber resilience.



Paris Peace Forum 2025

Common Good Cyber

Our Institute took part in a roundtable at Paris Peace Forum discussing the launch of the Common Good Cyber Fund. We also plan to attend the 1-year anniversary of the Common Good Cyber conference, an event supported by the UK FCDO. The partners gathered for a dedicated strategic discussion in London to advance the Common Good Cyber Fund, where the Institute represented the Ecosystem Committee.

The core message is clear: cybersecurity is no longer just a national concern, but a global public-interest challenge that directly impacts democracy, human rights, and the resilience of civil society.

This ongoing advocacy builds heavily upon the momentum of the "BEYOND 125" action plan, which originally brought leaders together at the Peace Palace in The Hague to champion this exact cause in 2024.



ACCOUNTABILITY



GLOBAL ADVOCACY AND NORM SHAPING

Geneva Peace Week 2025

At the Geneva Peace Week we led a dedicated session on "Drafting a Shared Compass: Co-Creating a Code of Conduct for the Responsible Use of AI in Peacebuilding". By actively participating in Geneva Peace Week to co-create a Code of Conduct, the Institute is driving multilateral action to anticipate the risks of artificial intelligence (AI), while promoting its responsible and ethical use for the common good. This ensures that emerging AI technologies are harnessed safely to support peacebuilding and civil society, rather than being weaponized to disrupt global stability.



Geneva Peace Week 2025

ACCOUNTABILITY

Munich Cyber Security Conference 2025

At the 2025 Munich Cyber Security Conference in Germany, our team engaged global leaders to discuss practical solutions to manifold challenges in information and cybersecurity. We strategically leveraged this premier forum and its associated side events to spotlight the launch of the CyberPeace Tracer (CPT). By showcasing this AI-powered platform, which actively monitors and analyzes cyber threats against civil society, we bridged high-level multilateral security dialogues with frontline, data-driven evidence, showing powerful, concrete steps toward transparency, digital peace, and state accountability.



Side event at MCSC 2025



#Disinfo2025

Engaged cross-sector leaders at the #Disinfo2025 conference in Slovenia to address the convergence of AI, information manipulation, and cyber threats.



ACCOUNTABILITY

AI FOR RESILIENCE

AI Skills Training

We partnered with Microsoft to provide free AI Skills Training for nonprofit professionals. A dedicated hands-on workshop in Zurich helped NGO staff safely adopt AI tools, master prompt creation, and understand AI-enabled threats like deepfakes and phishing.



AI Skills Training in Zurich



AI Skills Training in Zurich



We continued the effort by developing a free online AI Skills training in collaboration with Microsoft Elevate. The training aims to help nonprofit staff, volunteers, teachers, students, and public sector professionals build practical and ethical AI skills.

Patrick J. McGovern Foundation AI Fund

We received vital funding (US\$ 540 000) to integrate AI capabilities into our operational and data pipelines, accelerating our ability to analyze and protect civil society.



ANTICIPATION

AI FOR ACCOUNTABILITY AND GOVERNANCE

UN Commission on Science and Technology for Development

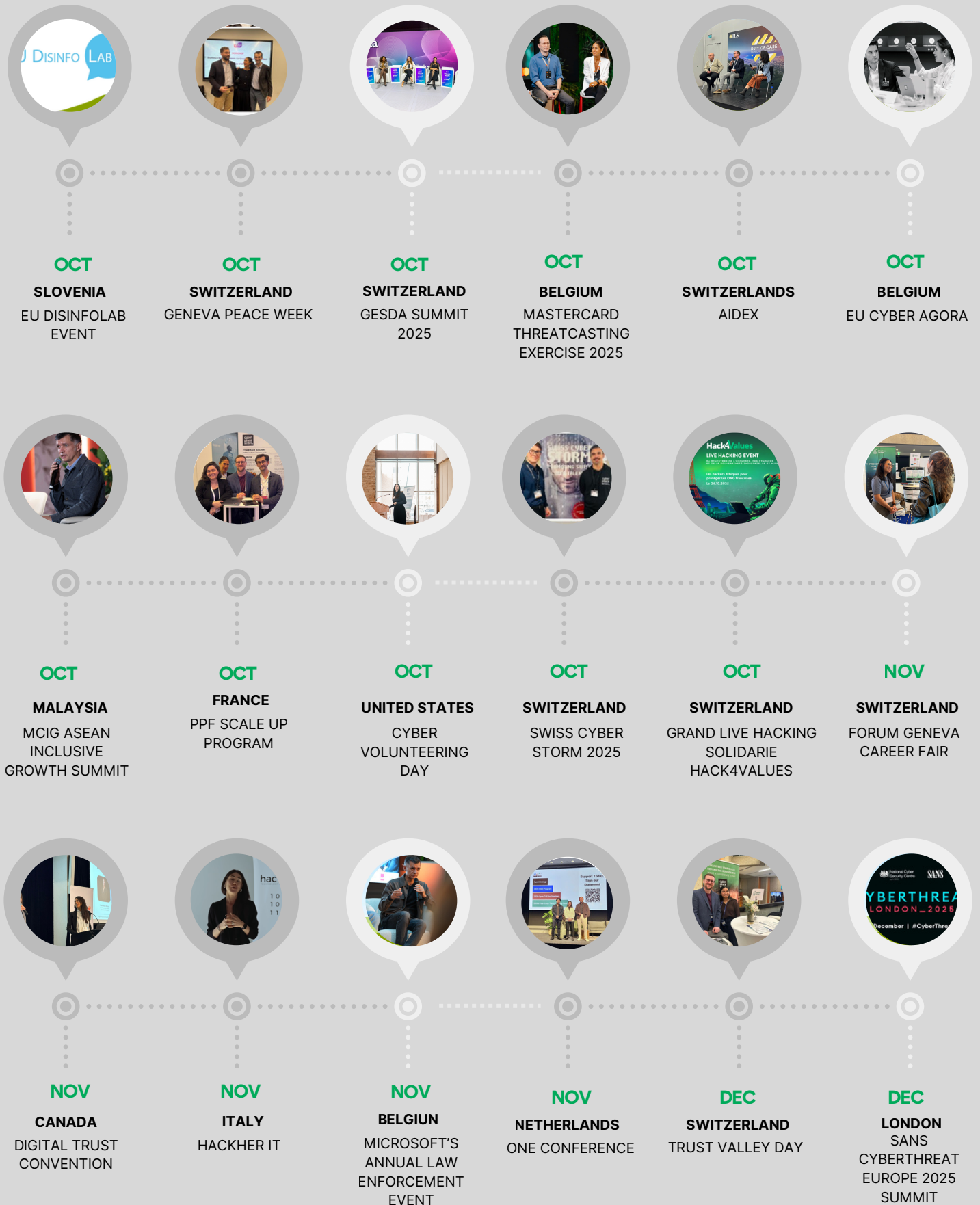
Institute took part in the Side Event organized by the United Nations Human Rights Office (OHCHR), at the UN Commission on Science and Technology for Development, where we highlighted the need for AI and data to be deployed responsibly and effectively to safeguard human rights.



ANTICIPATION

WHERE WE SHOWED UP





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 50% female and 50% male colleagues.

An integral part of our teams are our interns and young professionals. In 2025, we partnered with 10 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 Institute.

12

Interns

28

Employees

1

Fellow

6

Young
Professionals

2

Consultants

20

Nationalities

FUNDING AND FINANCING

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 2025 amounted to **CHF 4 647 824**, which was fully funded by donors.

CONTRIBUTE TO THE 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