

ACTIVITY REPORT



2022

More impact, together

STHENZO

01.

*4 convictions, 4 strategic objectives,
3 priority populations
1 ambition: to make a difference*

02.

Who we are

03.

*The CyberPeace Institute around
the world*

04.

The CyberPeace Institute in 2022

05.

Our programs

06.

Our partners

NOTION OF CULTURE DIVERSITY PROTECTION

The story of the CyberPeace Institute began in December 2019, when a handful of actors from the tech and philanthropic sectors took the bold initiative of mapping out a path towards “digital peace”.

A necessary initiative, given the digital transformation of our societies and the proliferation of threats. Flexibility and agility were essential in order for us to anticipate the multinational frameworks in which the Institute is operating today.

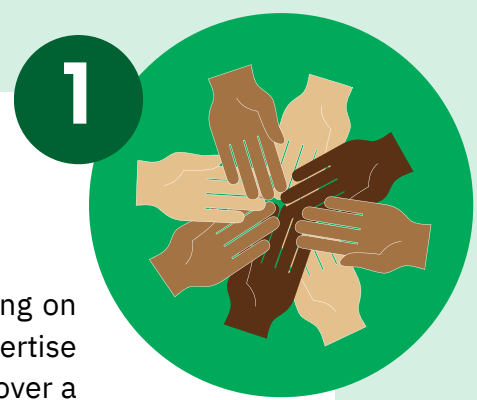


Our mission is based on **four convictions**. Those convictions guide our strategic objectives - **assistance, analysis, advancement and foresight**. Those objectives serve priority populations: the humanitarian world, the healthcare sector and the victims of armed conflict.

Assistance

We must unite to confront cyberthreats

Cyberthreats strike indiscriminately, but the harm they do varies, depending on the target and its vulnerability. Being united means mobilizing expertise wherever it is available. Many NGOs provide support of last resort, helping over a billion people a year to meet their most basic needs. What NGOs do for others, we do for NGOs.



2



Analysis

To deal with cyberthreats, we must know them and make them known

We must identify cyberthreats, trace them and analyze them from one single angle: their impact on people. Our research and analysis draw on our unique expertise and our worldwide links with academia. We describe cyberattackers' *modi operandi*, identify their motives and demonstrate societal impact.

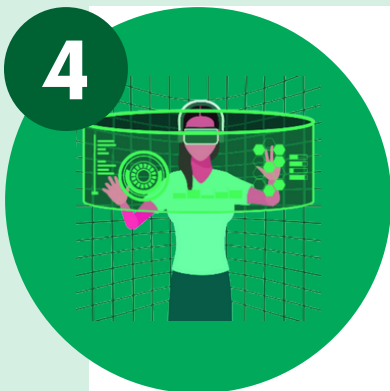
Advancement

All actors must account for greater responsibility - not just businesses but states as well.

We advocate for responsible behaviour in cyberspace to ensure the fundamental rights and freedoms of people are respected, whilst advancing the rule of law through a human-centric lens. We therefore document law violations, with the aim of fostering accountability and promoting dialogue, through our recommendations and our participation in international initiatives.



4



Foresight

It's imperative to analyse and raise awareness on security threats associated with emerging and disruptive technologies and their impact and harm on people.

We act as a platform to understand technology and policy disruption, develop innovative collaborative solutions and build capacity to strengthen the cyber resilient society of tomorrow.

We want to tell the story of the CyberPeace Institute through the eyes of the people who make up its teams, our Executive Board and our Advisory Board. And through the words of those who place their trust in us: our partners and everyone we support through our work.

Above all, we want to write this story with you—businesses, administrations, and foundations—whose donations and other types of support enable us to act.



“ Together, let us mobilize.

Together, let us continue to write the history of the CyberPeace Institute, as it serves the cause of digital peace.

Let us also prepare for the challenges that await us in 2023, as the Institute’s teams tackle the implications of artificial intelligence and disinformation.

”

Stéphane DUGUIN
CEO



OUR EXECUTIVE BOARD

The CyberPeace Institute was founded based on a clear goal - protecting vulnerable populations against the proliferation of cyberattacks and building trust in the digital ecosystem.

This means we **ASSIST** humanitarian NGOs and others are supported to prepare for and recover from cyberattacks, we **ANALYZE** threats and vulnerabilities affecting vulnerable communities to understand their threat landscape, provide advanced warning and reduce harm, and we **ADVOCATE** for responsible behavior in cyberspace to ensure the fundamental rights and freedoms of people are respected, whilst advancing the rule of law through a human-centric lens.

The skills, capabilities and programs we have put behind these missions, thanks to the support of our donors, have enabled us to address emerging needs, focusing on the proliferation of cyberattacks targeting the Humanitarian world, the Healthcare sector, and the cyber dimension of the Russia-Ukraine conflict.

It is an honor to be a founding board member of the **CyberPeace Institute** and now serve as the Chair of the Executive Board. The Executive Board has an international composition and its members, appointed by the members in office by co-optation, are individuals with expertise in digital and cyber. As a board, we are committed to supporting, whenever possible, the Institute's experts in their projects, in the service of those who need it most.

The CyberPeace Institute is powerful because it not only imagines a safer cyberspace, but delivers concrete tools and resources to deliver on that objective.

Alexander Niejelow
Chair of the Executive Board

The Executive Board is the governing body of the CyberPeace Institute. The Board has an international composition and its members are individuals with expertise in digital and cyber. Board members are appointed by the members in office by co-optation. A Board member serves a 3 year term and can be re-elected for two further terms of 3 years. The Board meets on a quarterly basis and its decision-making is by consensus.



**Alejandro
BECERRA GONZALEZ**

Global Information Security
Director, Telefonica



Andrew MCCRAKEN

Global Director of Wateraid
International



Maya BUNDT

Chair of the Cyber Resilience
Chapter of the Swiss Risk
Association



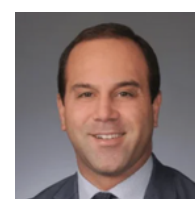
Hoo MING NG

Strategic Business & Operations
Advisor, Former Deputy CEO,
Security Agency of Singapore



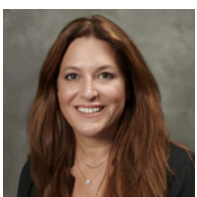
Amy HOGAN-BURNEY

General manager and Associate
General Counsel for Cybersecurity
Policy & Protection, Microsoft



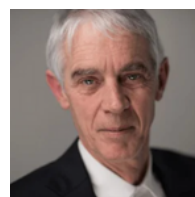
Alexander NIEJELOW

Cybersecurity & Technology
Executive



Bonnie LEFF

Senior vice President, Corporate
Security, Mastercard



Martin VETTERLI

President, EPFL



OUR ADVISORY BOARD

It is incredible how technology can fast-forward our lives through digital innovation. It is also scary how the very same technology can be used to harm all of humanity very rapidly. Without cybersecurity, there can be no human security.

Without digital rights, there can be no human rights. Without digital dignity, there can be no human dignity.

The aim of the CyberPeace Institute is to protect the right to security, dignity and equity in cyberspace.

Last year, I accepted the invitation to join its **Advisory Board**, a diverse team with expertise and insights on cybersecurity, human rights, peace and security.

On a personal level, I am keen to see how we balance innovation and abuse of innovation, how we regulate and how we monitor compliance with regulation, how we agree on the responsibility of stakeholders and how we promote that responsibility.

I am expecting the CyberPeace Institute to provide leadership, conduct research and analysis, generate evidence and defend the rights of all.

Open and inclusive working methods in a multi-stakeholder setting are the recipe for success.

In my small way, I hope to play a part in that. Because we need peacebuilding more than ever, and cyberpeace is critical to peace.

Nnenna Nwakanma

ICT4D Strategist, Expert in EParticipation & Citizen Engagement

The Advisory Board is selected and appointed by the Executive Board, based on the advice of the CEO. It has an international composition with a diversity of expertise and insights on cybersecurity, human rights, peace and security. The Advisory Board meets two times a year with the CEO and leadership team of the Institute.



Sunil ABRAHAM

Former Executive Director, Centre for Internet & Society



Eric MEERKAMPER

Fellow, Montreal Institute for Genocide & Human Rights Studies



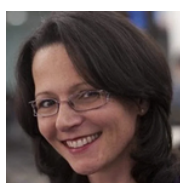
Khoo BOON HUI

Former Président, Interpol



Nnenna NAWAKANMA

ICT4D Strategist, Expert in Eparticipation & Citizen Engagement



Frédéricick DOUZET

Director Geopolitics of the du Datasphere Center (GEODE)



Luisa PARRAGUEZ KOBEC

Global Affairs & International Security Professor, Tecnológico de Monterrey



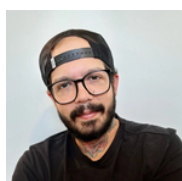
Jen ELLIS

Cybersecurity Advocate



Alejandro ROMERO

Chief Operations Officer, Constella Intelligence



Melanio ESCOBAR

Activist, Journalist, Author



Marietje SCHAAKE

International Policy Director, Stanford University Cyber Policy Center



Camille FRANÇOIS

Global Director of Safety at Niantic, INC.



Vincent SUBILIA

General Director, the Geneva Chamber of Commerce, Services & Industry (CCIG)



Vasu GOUNDEN

Executive Director, African Centre for the Constructive Resolution of Disputes



Eli SUGARMAN

Content Director at Oversightboard; Former Director, Cyber Initiative at William & Flora Hewlett Foundation

OUR TEAMS

The CyberPeace Institute has recruited specialists from the business world, the humanitarian sector and diplomacy. They have joined the organization with a clear ambition: to make a difference and have an impact on a subject of vital importance that will determine the future of the digital sphere.

Adaptability is our teams' greatest asset. The Institute was born during the Covid crisis. As a result, it operated remotely before meeting in Geneva, using the assets offered by the diversity of its members.

They come from **19 different countries**, and each of them acts as a local hub for the work of the Institute. Diversity is one of our core values: we have achieved almost perfect gender parity (**52%** women and **48%** men at the end of 2022) and have one colleague with a disability.

We started to welcome interns and young professionals in 2022. Applications are welcome all year round and contracts last for at least **3 months**, with interns and young professionals working onsite in Geneva and/or remotely.

Our interns are university students for whom an internship is part of their academic program, and a tripartite internship agreement is drawn up between the university, the student and the Institute. In 2022, **88%** of our interns were masters-level students in fields that included law, international relations, geopolitics and information technology.

Young professionals are recent postgraduate degree holders looking for initial professional experience. They are contracted to carry out specific projects for the Institute.

In 2022, the Institute also set up a fellowship program, to give experienced, specialized individuals the opportunity to immerse themselves in the humanitarian cybersecurity community. The program is for experts with a passion, who want to develop their talents and use their skillsets on projects that directly benefit those in need of assistance and support.

AT THE END OF 2022, THE INSTITUTE HAD SIX TEAMS, CONSISTING OF:



27.6

FTEs

4

“YOUNG PROFESSIONALS”

8

TRAINEES

MANAGEMENT TEAM

Cyberspace knows no borders. Neither do we. We're professionals from different backgrounds, with a wide range of skills from inside and outside the cyber industry. Diversity, equality and inclusion are integral to our collective vision of cyber peace.



Stéphane DUGUIN

Chief Executive Officer



Charlotte LINDSEY

Chief Public Policy Officer



Khristine BENEDICTO

Head of Human Resources



Fabien LEIMGRUBER

Senior Program Manager



Florent BITSCHY

Chief Information Security Officer



Adrien OGÉE

Chief Operations Officer



Francesca BOSCO

Senior Advisor - Strategy & Partnerships



Coralie PÉGAT-TOQUET

Head of Governance



Vincent de CRAYENCOUR

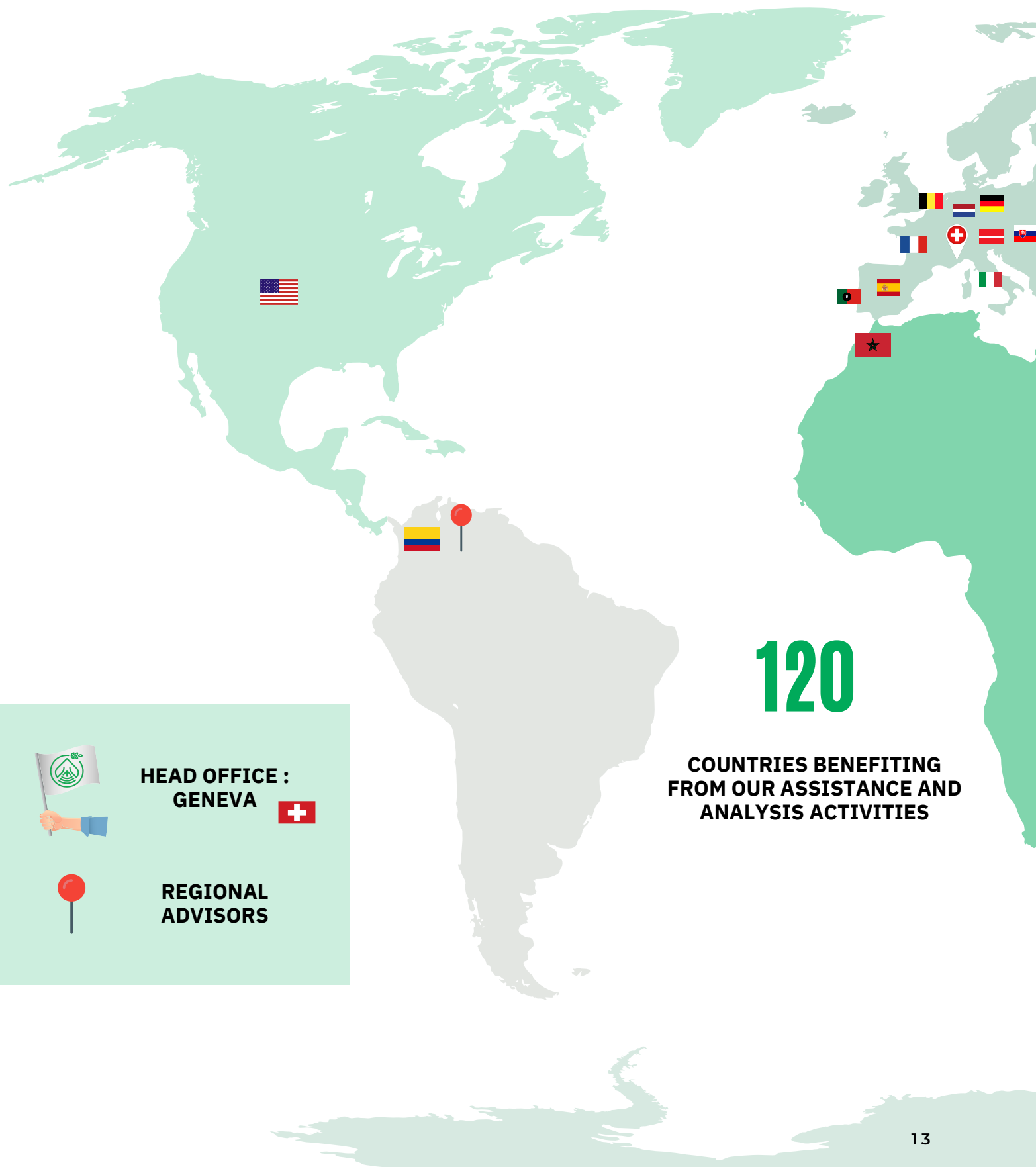
Chief Business Development & Strategy Officer



Emma RAFFRAY

Chief Research & Analysis Officer

THE CYBERPEACE INSTITUTE



**HEAD OFFICE :
GENEVA**



**REGIONAL
ADVISORS**

AROUND THE WORLD



2022

**Was the third full year in the life of the Institute.
A pivotal year, for several reasons.**

01

NEW PARTNERS

We opened up to new partners and entered into a new form of cooperation with states.

In addition to raising awareness, making our work available and communicating in multilateral settings, we now invite states to contribute to our work, both technically and financially. In the same spirit, we have successfully responded to European Union calls for projects.



BRIDGES TO THE WORLD

Finally, 2022 was the year we began to build bridges from Geneva to other major cities.

We now also have a presence in the Cyber Campus, a unique Paris-based ecosystem bringing together all the players in cybersecurity.

02

03

CONSOLIDATION

In the healthcare field, we developed the **Cyber Incident Tracer #HEALTH** and launched the **Compendium of Multistakeholder Perspectives** in September, working alongside the United Nations.

That followed on from our **Cyber 4 Healthcare** program, which supports health professionals, analyzes the cyberattacks they suffer and promotes policies to protect the sector.

In the humanitarian sphere, the **CyberPeace Builders** program - the world's first cyber assistance platform for NGOs - became the driving force behind an ambitious project announced in December: the **Humanitarian Cybersecurity Center**, which will offer NGOs a full range of cyber protection services.



04

COMMITMENT

We committed ourselves to the promotion of responsible behavior. The Institute took this message to **80 countries** and major diplomatic forums, including the United Nations, the OECD, the G77 and the Paris Peace Forum, striving to combat the abuse of information and communication technologies for criminal purposes and to build the digital capacity of developing countries.



05

CREATION

We launched the **Cyberattacks in Times of Conflict Platform #Ukraine**, a unique initiative that tracks all cyberattacks in the Russian-Ukrainian conflict and provides a sectoral impact assessment, to better evaluate damage to civilian populations. The Institute began looking at new topics, including spyware, alongside the World Economic Forum.



OUR PROGRAMS IN 2022, WHAT OTHERS ARE SAYING ABOUT US...

"With their experience and professionalism, the CyberPeace Builders have convinced our organization about the importance of cybersecurity. We feel supported, and confident that we are taking the right steps to greater digital resilience and protection."

Nonviolent Peaceforce

"As field, assistance and emergency workers, we particularly appreciate the approach of the CyberPeace Institute, which focuses on vulnerable populations and makes every effort to better anticipate crisis situations."

Alliance Urgences

"[The CyberPeace Institute] is helping build staff capacity, both locally and in Switzerland, thus preventing major crises."

**Centre écologique
Albert Schweizer**

"To me, one of the best steps of the past 18 months or so has been the creation of the CyberPeace Institute."

Brad Smith, Chair,
Microsoft

"I must congratulate the CyberPeace Institute on having come up with the first technological report on this very important subject. Governments, industry, technology experts, civil society, media and academia will need to cooperate to combat these threats."

Latha REDDY, co-chair of the Global Commission on the Stability of Cyberspace

"We received precise, detailed advice on what needs to be done from an accomplished IT security professional at very short notice. Following a basic general security assessment, FSD is now aware of the areas that most urgently need attention."

**Fondation Suisse de
Démontage (FSD)**

"Together, let us commit ourselves to the CyberPeace Institute and its partners, so healthcare professionals can work under the best possible cyber conditions."

ASEAN, Chief Information Officer
Association (ACIOA)

"The CyberPeace Institute was able to help [Christina] Wille, the Insecurity Insight director, assess the hacking attempts aimed at her organization, she said."

CNN

"An eye-opening experience. We look forward to implementing the measures proposed in the security assessment."

Union for International Cancer Control

"At DNDi we value our relationship of trust with the CyberPeace Institute and their commitment to helping us find appropriate solutions to our cybersecurity challenges, in particular that of protecting our beneficiaries' data. The new CyberPeace Builders program will bring great added value to NGOs based in Geneva and around the world, helping them face today's digital challenges."

Pascal Carpentier, Head of Information Systems and
Technology at the Drugs for Neglected Diseases
initiative (DNDi)

"Companies are encouraging their cyber employees to volunteer at nonprofits, a nudge that managers say can help businesses retain in-demand technical experts despite high turnover in security roles. The CyberPeace Institute, a Geneva-based group that helps nonprofits, humanitarian and healthcare organizations address cybersecurity, set up a program last year to enlist professionals from the corporate world to explain things like email phishing to nonprofits that might lack the budget to hire their own experts."

Catherine Stupp,
The Wall Street Journal

"[Thanks to the CyberPeace Institute] we learned to be constantly aware of cyberthreats."

World Medical Association

"I'm extremely proud that Logitech is contributing to the CyberPeace Builders program. Everyone at Logitech who participated in that fantastic program loved the experience."

Tana Dubel, CISO,
Logitech

WHAT WE CARE ABOUT

We develop programs to support communities vulnerable to threats in cyberspace. By monitoring, assessing and communicating on the cyber threats to these communities, we can work together with partners to better protect them.



HUMANITARIAN

More than one billion people depend on NGOs for food, water, shelter or healthcare. The current economic, geopolitical and social tensions impact them directly.

Because they hold key data, NGOs are subject to an increasing number of cyberattacks; the humanitarian world is the second most targeted sector after the tech industry. But NGOs are struggling to implement even the most basic cybersecurity solutions, for a number of reasons: their recent and often hasty digital transformation, the budgetary restrictions inherent to the sector and the impossibility of competing with the private sector for cyber experts.

We are an NGO with a mission to protect other NGOs online. Our solution? Connecting NGOs with corporate cybersecurity volunteers. More impact, together.

THE CYBERPEACE BUILDERS PROGRAM: A BENEFICIARY'S VIEW

TESTIMONY OF HANSJÖRG EBERLE | FSD

Hansjörg Eberle, director and co-founder of FSD (**Fondation suisse de déminage**), shares the impact cybersecurity has on the daily activities of his organization, which deals with mines and explosive remnants of war, clears mines in areas polluted by toxic waste and supports peace and development in countries affected by armed conflict.



“As a demining organization, we clear landmines and unexploded ordnance. We have about 400 staff, most of whom use computers regularly. Cybersecurity is essential for us and is becoming increasingly important. Unfortunately, we’ve been the target of cyberattacks and we’ve recently noticed a dramatic increase in the number of phishing emails and scam messages sent to our staff.

We contacted the CyberPeace Institute in 2021. At the time, I told them that we didn’t really have a strong IT department, but that we certainly did want an improved situation. It was hard to find a reliable source of guidance on ways to improve our cybersecurity and how to implement the necessary changes effectively.

The CyberPeace Institute helped us approach some really top-notch IT security professionals, and they started to help us in specific areas, through the **CyberPeace Builders** program. We were able to access a network of experts who volunteered their skills for free and improved our response to security problems.

We’ve made a lot of progress since then. Having updated security assessments of our systems is not only reassuring but proves that our cybersecurity skills are growing long-term. For instance, we’re hardening our Microsoft Office 365 systems, managing our passwords better, making sure all devices have anti-virus software, using a VPN for certain important functions and encrypting our data.

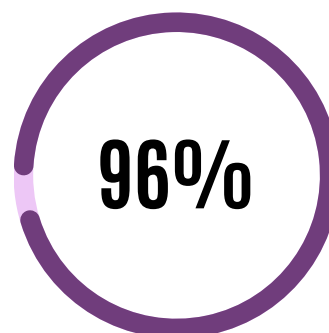
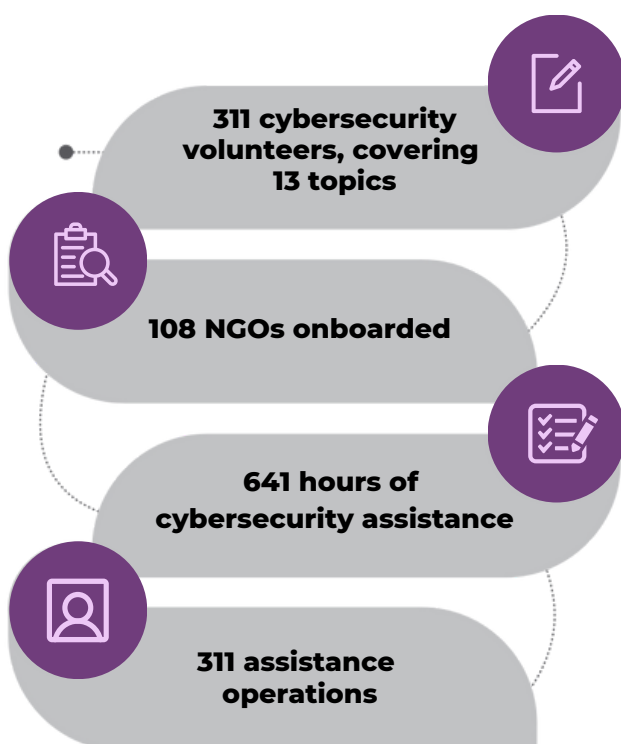
We’ve also started to roll out cybersecurity awareness training to all our staff. There’s a lot of work ahead, but I’m delighted to be receiving the support of competent and motivated IT security specialists through the CyberPeace Builders initiative.”

ABOUT CYBERPEACE BUILDERS

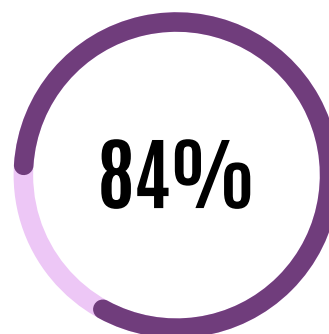
CyberPeace Builders - often shortened to “**Builders**” - is the first online cyber assistance platform for NGOs. It connects the most vulnerable entities with hundreds of volunteer cybersecurity experts, to solve the problems those entities encounter and protect them against cyberattack. By the end of 2022, 100 NGOs were benefiting from this free tool, thanks to the Institute’s first 30 partner companies. Our objective is to be supporting 1000 NGOs by the end of 2024.

55 Documented cyberattacks or other incidents involving non-profit or non-governmental organizations, in **12 countries**.

Incident types included account takeover, ransomware and denial of service.



Of NGOs satisfied with our services



Of volunteers satisfied with the program

IN 2022

The Builders program became part of a global initiative serving the humanitarian world: the **Humanitarian Cybersecurity Center**.

WHY DID WE DECIDE TO CREATE THE HUMANITARIAN CYBERSECURITY CENTER?

In 2022, we decided to gather all our activities related to humanitarian and development NGOs into a single initiative with global impact: the **Humanitarian Cybersecurity Center** (HCC).

The HCC aims to protect humanitarian actors in cyberspace worldwide. Each action will involve launching dedicated programs and activities.

THROUGH 4 MAIN MISSIONS

COMMUNICATE

ON THE CYBERTHREATS, VULNERABILITIES AND INCIDENTS THAT HUMANITARIAN ORGANIZATIONS FACE

HELP

HUMANITARIAN ORGANIZATIONS DETECT CYBER INCIDENTS AND PREVENT THEM FROM CAUSING HARM

RESPOND

TO CYBER INCIDENTS INVOLVING HUMANITARIAN ORGANIZATIONS SO THEY RECOVER FASTER

CREATE

A RESILIENT DIGITAL ECOSYSTEM FOR HUMANITARIAN ORGANIZATIONS

We announced the creation of the HCC on December 8, at the end of a design phase during which we identified all Institute activities dedicated to the humanitarian sector and those that were missing. The aim was to extend our catalogue of services by developing new partnerships. The December 8 announcement was therefore a *call for partnerships*, which yielded over 70 new partners and supporters for the Institute. This brought us new tools, services and expertise dedicated to the humanitarian and development sectors. **Together we are stronger!**

Guided by the CyberPeace Institute's mission of supporting the most vulnerable in cyberspace, we launched the **Cyber 4 Healthcare** program in 2021, to assist healthcare professionals, analyze cyberattacks and promote policies to protect the health sector. Following our call to governments for the protection of medical and healthcare facilities, our report **Playing with Lives: Cyberattacks on Healthcare are Attacks on People** (March 2021) and its **Addendum** (November 2021), we launched two further important initiatives in 2022:

The Cyber Incident Tracer #Health (CIT)

The Compendium of Multistakeholder Perspectives

REACTION FROM THE PARIS PEACE FORUM

“

In a recent report, the CyberPeace Institute identified a significant knowledge gap regarding global cyber incidents and their impact on people and society. Based on this analysis, the Institute is developing a public platform that serves as a repository of information on cyberattacks that disrupt the delivery of healthcare. The goal is to provide information about the impact of these attacks on patients, healthcare professionals and facilities.

Through the tracing of healthcare cyberattacks across the globe, the Cyber Incident Tracer (CIT) #HEALTH seeks to bring greater visibility to the scale of the problem and how such attacks impact people and the provision of care. The aim is to boost human security, dignity and equity in cyberspace. The vision for the CIT is to develop the platform in cooperation with global partners across sectors and it will be part of a larger platform that provides a holistic view of the impact that cyber incidents have on people, highlights the instruments available to protect/empower them and exposes the gaps that allow these incidents to exist.

”

THE COMPENDIUM: TESTIMONIAL

*“I was honored to moderate a discussion about the launch of the **Compendium** in parallel with the **Open-ended Working Group** meeting in December 2021. I was pleased to see the interest in this issue, which confirms that protecting the health sector from cyberattacks is extremely important and that there are a large number of people involved in thinking about how to do so. I am convinced that the Compendium can make a substantial contribution to finding solutions to specific dilemmas. For me, the Compendium is also clear evidence that a multi-stakeholder approach can work smoothly in practice.”*



Richard Kadlčák, Director of the Cyber Security Department, Special Envoy for Cyber Space, Ministry of Foreign Affairs of the Czech Republic

WHY DID WE LAUNCH THE COMPENDIUM?

In 2022, the Czech Government, Microsoft and the CyberPeace Institute brought healthcare and cybersecurity communities together through multi-stakeholder workshops, each addressing a critical topic related to the protection of the healthcare sector from cyber harm.

The workshops collected recommendations, lessons learned and good practices from a diverse group of experts, practitioners and stakeholders. This resulted in the **Compendium of Multistakeholder Perspectives on Protecting the Healthcare Sector from Cyber Harm**, which was launched in New York in connection with the UN General Assembly **Open-Ended Working Group on Information and Communication Technologies** in July 2022. The Compendium offers healthcare facilities, governments, international organizations and other stakeholders a useful resource to support their efforts to protect the healthcare sector against cyberthreats.

Not a month went by in 2022 without a cyberattack on a healthcare entity somewhere in the world. The reporting and documentation of these incidents are lagging behind. Without reporting and documentation, society cannot:

Understand the true scale and scope of the problem

Measure the harm these attacks cause to individuals, communities and society

Develop appropriate responses to reduce the threat

We designed the **Cyber Incident Tracer #Health** in 2021 and built it in 2022. CIT is a human-centric data-driven platform that documents cyberattacks, increases public awareness, supports evidence-led policymaking and promotes redress for victims.



WHY DID WE LAUNCH THE CYBER INCIDENT TRACER?

In the midst of a global pandemic, the healthcare sector has been under significant threat, not just from the increasing pressures on staff and organizations to maintain critical services at a time of increased demand, but from malicious actors targeting the sector for financial gain and information.

As the CyberPeace Institute sought to capture and evidence the harm of these attacks on the health sector, on people and on society, it noted a gap in the collection of cyber incidents across the world.

Without these data, we could only rely on anecdotal observations and reporting of isolated incidents to establish the who, what, when, why, where and how of the threat landscape.

This anecdotal research and the publication of "**Playing with Lives: Cyberattacks on Healthcare are Attacks on People**", prompted the idea of creating a public repository and visual representation of cyber incidents in this sector and the impact that they have on people and organizations - the **Cyber Incident Tracer**.



IN 2022, THE CYBER INCIDENT TRACER #HEALTH DOCUMENTED:

141   

DISRUPTIVE ATTACKS ON
HEALTHCARE FACILITIES:

34   

HOSPITALS

12   

12 PHARMACEUTICAL COMPANIES

7   

MENTAL HEALTH AND
SUBSTANCE ABUSE FACILITIES

3,8   



MILLION RECORDS BREACHED

3,7   

AN AVERAGE ATTACKS A WEEK

33   

COUNTRIES AFFECTED

250   

DAYS OF OPERATIONAL DISRUPTION

CIT REVEALED LOCKBIT, VICE SOCIETY AND HIVE TO BE THE MOST ACTIVE RANSOMWARE OPERATORS TARGETING THE SECTOR.



When the current phase of the Russian-Ukrainian conflict began in February 2022, civilians and civilian infrastructure immediately became the target of cyberattacks, of which several were clearly coordinated with kinetic military operations. How could the CyberPeace Institute mobilize its experts in this situation, while preserving its independence and neutrality? How could we use our analysts and public policy experts to highlight the human impact of those cyberattacks, which were part of the most major conflict of the 21st century so far?

IN THE MEDIA

“

Both sides are using hacking, network sabotage and other forms of cyber warfare as Russia's invasion of Ukraine grinds on, though the covert operations have not proved decisive on the battlefield—at least so far. Western allies initially feared a tsunami of cyberattacks against Ukraine's military command and critical infrastructure, hindering its ability to resist the Russian forces pouring across its borders. As of mid-September, the CyberPeace Institute, an NGO based in Switzerland, counted nearly 450 attacks - roughly 12 a week - carried out by 57 entities on either side since the invasion was launched in February.

AFP, Security Week, 28 septembre 2022

”



WHY DID WE LAUNCH THE CYBERATTACKS IN TIMES OF CONFLICT PLATFORM #UKRAINE?

Russia's February 2022 invasion prompted the Institute to begin aggregating and analyzing data on cyberattacks related to this international armed conflict, and to develop the **Cyberattacks in Times of Conflict Platform #Ukraine**. Documenting cyberattacks and operations targeting infrastructure essential for the survival of the civilian population aims to contribute to analysis of the use of cyber in armed conflict, and to inform law and policy discussions. It also provides an important repository of information for any future accountability measures.

The platform helps raise awareness of the effect that cyberattacks have on the civilian population and of the laws that apply to the use of cyber in armed conflict. It also facilitates the Institute's calls to respect civilians and international humanitarian law.

THE UKRAINE PLATFORM IN 2022:

3



REPORTS PUBLISHED

9



ARTICLES AND 2
FACTSHEETS PUBLISHED

77



ITEMS OF MEDIA COVERAGE

80



THREAT ACTORS IDENTIFIED

1.1K



CYBERATTACKS REPORTED,
AFFECTING 22 CRITICAL
INFRASTRUCTURE SECTORS

40

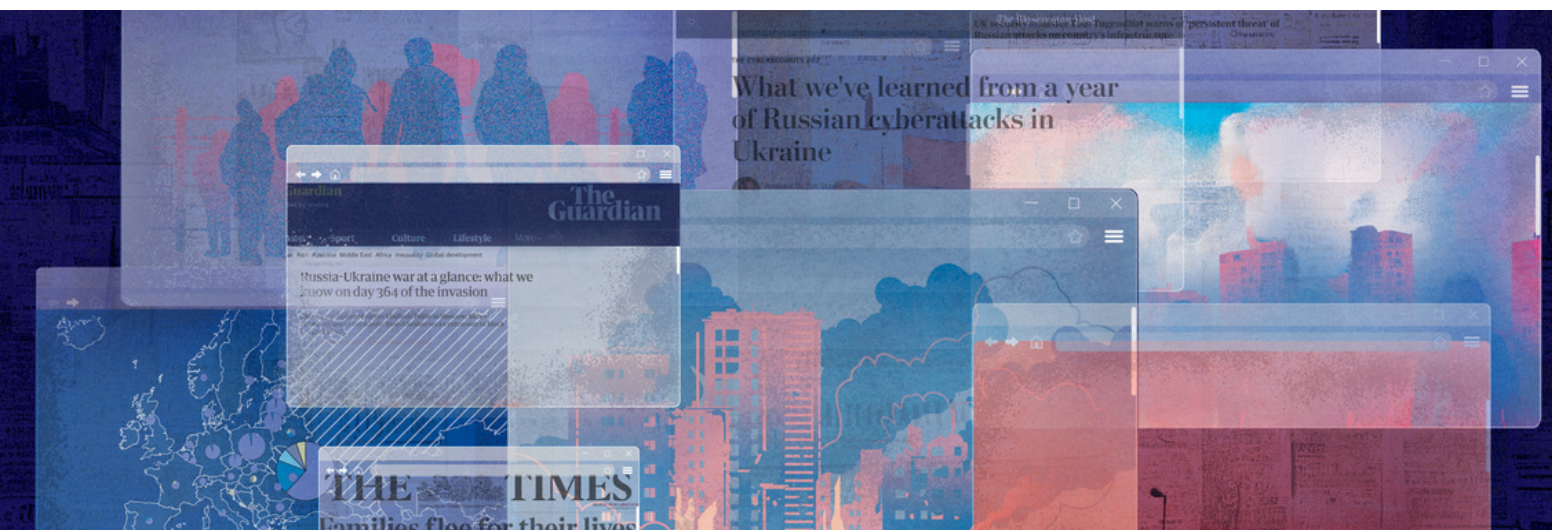


COUNTRIES IMPACTED

30K



VIEWS OF THE PLATFORM, WITH AN
AVERAGE TIME OF 3 MINUTES ON A PAGE



OUR QUARTERLY ANALYTICAL REPORTS

In 2022, we published three quarterly analysis reports providing insights into the cyber dimensions of the conflict in Ukraine. The reports combine analysis of data collected via the **Cyberattacks in Times of Conflict Platform #Ukraine** and information gathered through OSINT research. The CyberPeace Institute invites readers to discover the trends and emerging issues relating to cyber incidents in Ukraine, the Russian Federation and other countries impacted by cyberattacks in the context of the armed conflict.

By looking at the economic sectors affected, the types of cyberthreats they face and the most active threat actors, we provide a greater understanding of the Ukraine-related cyberthreat landscape during 2022. We also assess the impact of cyberattacks on civilians, look at key events and examine economic and geopolitical activities.

Quarterly Analysis Report
Q4 October to December 2022

Cyber Dimensions of the Armed Conflict in Ukraine



31

OUR PARTNERS



ACKNOWLEDGMENT

"Thank you to those who have supported the CyberPeace Institute since its inception, thank you to those who have enabled us to carry out all our projects in 2022, thank you to those who read us, listen to us, follow our work, participate in our programs. Finally thank you to all those who will choose to join us in the years to come..."

CONTACT

Avenue de Sécheron 15
1202 Geneva
Switzerland

www.cyberpeaceinstitute.org
media@cyberpeaceinstitute.org



@cyberpeaceinst



@cyberpeaceinst



CyberPeace Institute



CyberPeace Institute