



CyberPeace
Institute



CYBERPEACE INSTITUTE ACTIVITY REPORT 2019-2021



CONTENTS

MESSAGE FROM THE CEO	04
MISSION, CORE PRINCIPLES AND STRATEGIC OBJECTIVES	06
OPERATIONALIZING CYBERPEACE	09
Evolution	09
From Theory to Impact: The Cyber4Healthcare Program	10
Key Achievements	
Strategic Objective 1: ASSISTANCE	13
Strategic Objective 2: ANALYSIS	15
Strategic Objective 3: ADVANCEMENT	16
Strategic Objective 4: FORESIGHT	18
WHO WE ARE: THE PEOPLE BEHIND THE NUMBERS	19
WHO WE WORK WITH: PARTNERS AND NETWORK	20
HOW WE COMMUNICATE	22
FINANCE AND FUNDING	23

MESSAGE FROM THE CEO



" The promise of technology increasingly infusing our lives can be met only if we can successfully counter the threats posed by those intent on leveraging that promise to harmful ends -- to surveil, attack, disrupt, misinform, and harm contrary to the norms, laws and security that civilized societies expect. "

The years 2020 and 2021 have been challenging for us all — the COVID-19 pandemic and the rapid changes imposed on the way we all interact, work and learn brought an unprecedented volume of cyberattacks and threats to cyberpeace.

At the core of the Institute is the firm belief that it is critical, and in some cases vital, to understand the impact of cyberattacks first and foremost in terms of societal harm: cyberattacks directly affect people and society. To this end, the Institute has developed, launched and implemented key programs to support the healthcare sector and Non-Governmental Organizations (NGOs). Systemic challenges need systemic answers, calling upon all actors to play their role.

The Institute has engaged in diplomatic efforts in a Call to All Governments to Stop Cyberattacks on the Healthcare Sector. This was coupled with practical operational support, through a Cyber4Healthcare platform to scale up assistance to victims of cyberattacks, and the publication of a Strategic Analysis Report, Playing with Lives: Cyberattacks on Healthcare are Attacks on People, to raise awareness and provide recommendations for concrete actions to increase the resilience of such a critical sector.

Recognizing the importance of documenting cyberattacks, the Institute launched the Cyber Incident Tracer (CIT) #HEALTH to help increase public awareness of the scale and impact of attacks against the healthcare sector, and to support evidence-led policy-making and redress for victims.

As a response to attacks on NGOs, the Institute launched the CyberPeace Builders, the first global network of corporate cybersecurity volunteers dedicated to cyber capacity building and support for humanitarian NGOs.

The expert staff at the CyberPeace Institute collaborated with relevant actors from industry, civil society, NGOs and international organizations to raise awareness of cyberthreats and advance concrete solutions to respond to these threats. Evidence-led response is a hallmark of the Institute's efforts to support those affected by cyberattacks, to propose and advocate effective measures to prevent cyberattacks. The Institute has built the capabilities to carry out forensic analyses of cyberattacks and provide reporting to their victims.

The expert staff at the CyberPeace Institute collaborated with relevant actors from industry, civil society, NGOs and international organizations to raise awareness of cyberthreats and advance concrete solutions to respond to these threats. Evidence-led response is a hallmark of the Institute's efforts to support those affected by cyberattacks, to propose and advocate effective measures to prevent cyberattacks. The Institute has built the capabilities to carry out forensic analyses of cyberattacks and provide reporting to their victims.

Diplomatic and advocacy efforts have also been key to raising awareness and advocating for responsible behavior in cyberspace to ensure respect of the international laws and norms, to limit conduct considered unacceptable and to hold accountable those who violate these rules. The Institute followed closely relevant negotiations at the United Nations, submitting recommendations and insights based on its expertise.

The support provided by donors and partners has been essential to the impact that the Institute has been able to achieve in such a short time. This Activity Report outlines many of the key achievements of the Institute in 2020 and 2021, and is testament to the tremendous support for which we are deeply grateful.

Stéphane Duguin
Chief Executive Officer
CyberPeace Institute

December 2021

MISSION, CORE PRINCIPLES AND STRATEGIC OBJECTIVES

Mission

Billions of people around the world depend on the power of the internet to engage, learn and educate, work, trade and share knowledge. Cyberspace has also become a growing risk factor in people's lives. When cyberattacks occur, people suffer.

The main aim for cyberpeace is to create the conditions in which people everywhere can fully benefit from cyberspace and access the full potential of technology without concern or fear for their safety, security and privacy.

To address the growing escalation of attacks and to contribute to creating the conditions for cyberpeace the Institute is an independent and neutral NGO with the mission to ensure the rights of people to security, dignity and equity in cyberspace.

The Institute works in close collaboration with partners to reduce the harms caused by cyberattacks on people's lives worldwide, and to provide them with assistance. By analyzing cyberattacks, the Institute exposes their societal impact, how international laws and norms are being violated, and advances responsible behavior to enforce cyberpeace.

The Institute advocates an evidence-based and human-centric approach to the analysis of cyberattacks as essential to the process of redress, repair and/or justice for victims.



Core principles

The Institute is guided in its work and collaborative approach by the following core principles:

INTEGRITY

The Institute's work and interactions with the cybersecurity community and victims of cyberattacks seek to ensure the highest ethical and analytical standards at all times.

IMPACT

The Institute reduces the frequency, harm and scale of cyberattacks by advocating for their restraint, by increasing accountability and by enhancing capabilities to prevent and recover from attacks.

INDEPENDENCE

The Institute operates in sole pursuit of its mission, free from the direction, control or interference of any actors, including states, industry or other organizations.

NEUTRALITY

The Institute supports the stability and security of cyberspace, not the interests of any individual actors. As such it complies with applicable legal frameworks in defence of cyberattack victims without discrimination in terms of their geographic location, philosophical, political or religious beliefs, nationality, race, social status, gender, sexual identity or disability.

INCLUSIVENESS

The Institute is inclusive and collaborative in its work, cooperates and seeks synergies with others.

TRANSPARENCY

The Institute is transparent about its own operations and the methodologies applied to fulfil its mission.

Strategic Objectives

To achieve this mission and to deliver practical support, the CyberPeace Institute pursues four strategic objectives:



Strategic Objective 1: ASSISTANCE

To increase and accelerate assistance efforts towards the most vulnerable, globally.



Strategic Objective 2: ANALYSIS

To close the accountability gap through collaborative analyses of cyberattacks.



Strategic Objective 3: ADVANCEMENT

To advance international law and norms in order to promote responsible behavior in cyberspace.



Strategic Objective 4: FORESIGHT

To forecast and analyze security threats associated with emerging and disruptive technologies, to innovate breakthrough solutions and to close the skills gap to address global cyber challenges.

OPERATIONALIZING CYBERPEACE

EVOLUTION

Confronted by the realities of the COVID-19 pandemic, the Institute started to map and scope how the impact of the virus affected cyberspace and cyberpeace. COVID-19 impacted societies at all levels and notably the cyber-related dimension by accelerating the uptake of digitization and digitalization in the economic and societal sphere, creating a rapidly growing digital dependency and thereby, the proliferation of cyberthreats and increased vulnerability for all users.

Criminal and state-sponsored threat actors are particularly savvy at exploiting the ambiguity of crisis situations such as the pandemic to further their malicious activities and gains through cyberattacks (malspam and phishing in particular).

An onslaught of mis- and disinformation – or "infodemic", combined with the amplification of conspiracy theories, have been used by malicious actors to erode trust in the healthcare sector, in vaccines and even to question the very validity of the virus. Escalating cyberattacks targeting hospitals and other services of the sector have hampered their ability to provide quality care and allocate resources effectively.

The Institute launched a series of operational initiatives tailored for the healthcare sector to provide assistance, promote accountability and advance responsible behavior in cyberspace. Activities focused on supporting the resilience of critical civilian infrastructure and protecting the most vulnerable communities.



FROM THEORY TO IMPACT: THE CYBER4HEALTHCARE PROGRAM

The COVID-19 pandemic created a new reality for the healthcare sector, testing its limits around the world. Taking advantage of pandemic conditions, malicious actors launched a series of phishing campaigns and ransomware attacks on healthcare organizations. Hospitals simply cannot afford to cease operations in order to counter cyberattacks, and they are more likely than other organizations to pay a ransom to protect their patients.

As a critical and often vital service provider, healthcare should be off-limits to any malicious intent or action, safeguarded for and by all, at all times.

The Cyber4Healthcare Program (C4H), launched by the Institute in May 2020, demonstrated the Institute's unique ability to bring industry and civil society together to achieve an ambitious goal: stop cyberattacks on the healthcare sector and increase its resilience.

CYBER4HEALTHCARE PROGRAM (C4H)

Frame the issue: a global [Call to governments](#), with high level engagement to call upon States to commit to stop attacks on the healthcare sector.

More than 50 international leaders from government, industry, international organizations, NGOs and academia endorsed the appeal to governments to take immediate and decisive action to prevent and stop cyberattacks against the healthcare sector.

Provide direct help: the [Cyber4Healthcare](#) platform, with direct support from corporations provided concrete support to vulnerable communities.

Cyber4Healthcare scaled up assistance to vulnerable communities in the healthcare sector who were victims of cyberattacks by connecting them with corporate partners willing to offer free cybersecurity assistance to healthcare organizations anywhere in the world. Via the Cyber4Healthcare partners, the Institute provided services to 18 beneficiary organizations in seven countries - Cameroun, France, Haiti, India, Kenya, Nigeria, Switzerland.

“... we’ve actually been saved from a breach that could have been disruptive... Thank you to the CyberPeace Institute for helping healthcare startups like OneHealth be safer and secure on the internet. So now, we can focus on taking care of people in a very timely manner and safely as well.”

Adeola Alli, CEO, OneHealth, Kenya, February 2021

Formulate and issue practical guidance and recommendations: “[Playing with Lives: Cyberattacks on Healthcare are Attacks on People](#)”. A Strategic Analysis Report, with practical recommendations to states, industry and NGOs.



The Report aggregates, for the first time, information on cyberattacks perpetrated against the healthcare sector, demonstrating the complexity, magnitude and scope of the cyber threat to healthcare, in the form of ransomware, disinformation and COVID-19-related cyberespionage.

The key findings of the Report link the numbers of cyberattacks with the impact on people, and show that while healthcare professionals and patients are facing a significant threat, collective action is necessary and possible.

Main findings:

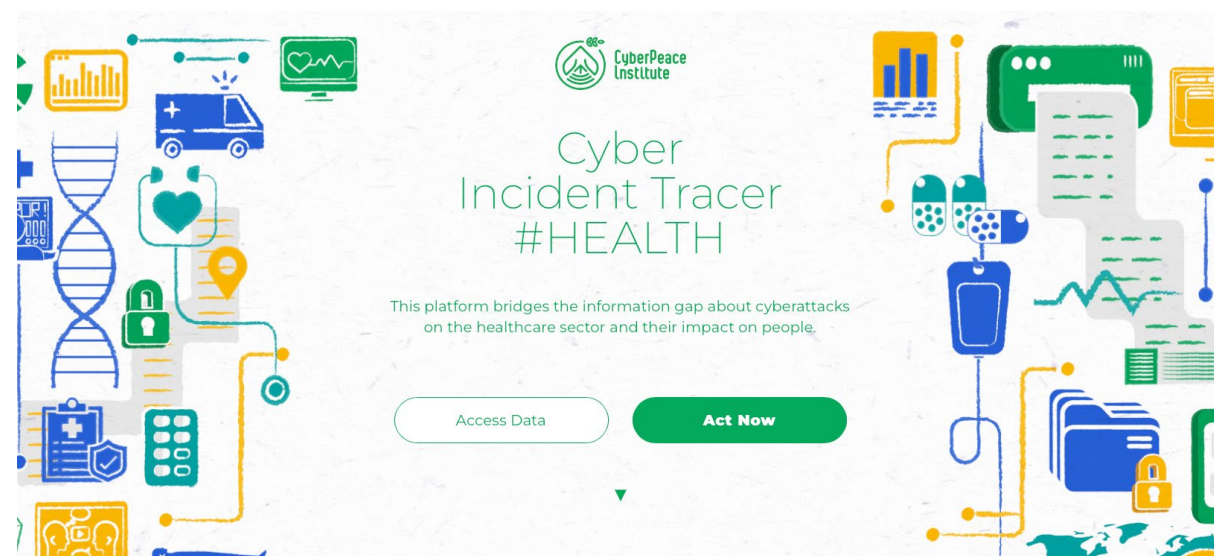
- Attacks on healthcare are causing direct harm to people and are a threat to public health, globally.
- Attacks are increasing and evolving as they continue to exploit vulnerabilities in the healthcare sector’s fragile digital infrastructure and weaknesses in its cybersecurity posture.
- Attacks on healthcare are low-risk, high-reward crimes.
- Healthcare professionals and patients do not benefit fully from legal instruments and existing initiatives designed to protect them.
- Governments should lead the way to protect healthcare, apply and enforce national and international norms and laws, commit to do no harm and declare cyberespionage and intelligence-gathering against healthcare as unlawful.
- Healthcare needs investment to protect and defend itself.
- The private sector has a responsibility given its role in building the technologies used across the sector.

From recommendations to action - Enabling accountability: the [Cyber Incident Tracer #HEALTH](#) & the [Addendum](#) to the Strategic Analysis Report, *Playing with Lives: Attacks on Healthcare are Attacks on People*



Following the Strategic Analysis Reports' first recommendation, which encourages the documentation of attacks and analysis of their human and societal impact, the Institute developed an online platform to enhance transparency and access to information about cyberattacks on the healthcare sector.

The Cyber Incident Tracer (CIT) #HEALTH is a publicly accessible platform that bridges the current information gap on cyberattacks on healthcare and their impact on people. Information on this platform has been analyzed in the Addendum to the Strategic Analysis Report, and is a valuable source of information for evidence-led operational, policy and legal decision-makers.



The high level of expertise of the Institute confirmed it as a reputable and trustworthy partner, collaborating with global health authorities like the World Health Organization on the interconnection between the COVID-19 infodemic and cyberattacks. Demonstrating its multistakeholder approach, the Institute collaborated with the Ministry of Foreign Affairs of the Czech Republic and Microsoft to champion a project on "[Protecting the healthcare sector from cyber harm](#)".

KEY ACHIEVEMENTS



Strategic Objective 1: ASSISTANCE

The Institute assists vulnerable communities and NGOs to prepare for and recover from cyberattacks by mobilizing expert supporters and volunteers and by amplifying the impact of existing assistance efforts.

- ◇ In the period under review, the Institute received 114 assistance requests from Europe, Latin America, Africa and Asia.

• *Training and Toolkits for Humanitarian NGOs:*

- ◇ The Institute developed 22 knowledge toolkits in English, French and Swahili providing public-facing actionable good practices for cyber resilience.
- ◇ The Institute supported capacity-building efforts of various civil society organizations and networks, notably The Global Fund and the International Civil Society Centre, for a total of 18 training sessions to over 400 participants.



FOCUS on

• *CyberPeace Builders*

- ◇ NGOs play a critical role in developing society, improving communities and promoting citizen participation, supporting the achievement of the UN Sustainable Development Goals. In many developing countries, NGOs ensure the delivery of critical services, such as provision of healthcare, access to food, micro-loans and information, and protection of human rights.
- ◇ Malicious actors are already targeting development and humanitarian NGOs in efforts to seek ransoms and exfiltrate data. Often these NGOs do not have the budget, know-how or time to effectively secure their infrastructures and develop robust incident response to manage and overcome sophisticated attacks.

- ◇ With this in mind, the Institute launched its [CyberPeace Builders](#) program in 2021, a unique network of corporate volunteers providing pre- and post-incident assistance to NGOs supporting vulnerable populations.
- ◇ CyberPeace Builders help NGOs prepare for and recover from cyberattacks. This initiative brings support to NGOs in critical sectors at a level that is unequaled in terms of staff, tools and capabilities.
- ◇ In a few months the program enrolled 20 NGOs, with six corporations providing volunteers.
- ◇ Capabilities were activated in 2021 to offer the program in Africa and Latin America in 2022.

“At DNDi we value the trusted relationship with the CyberPeace Institute and their commitment to help us find adequate solutions to our cybersecurity challenges, in particular to protect the data of our beneficiaries. The new CyberPeace Builders program will bring great added value to NGOs based in Geneva, but also around the world, to help them face today's digital challenges.”

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

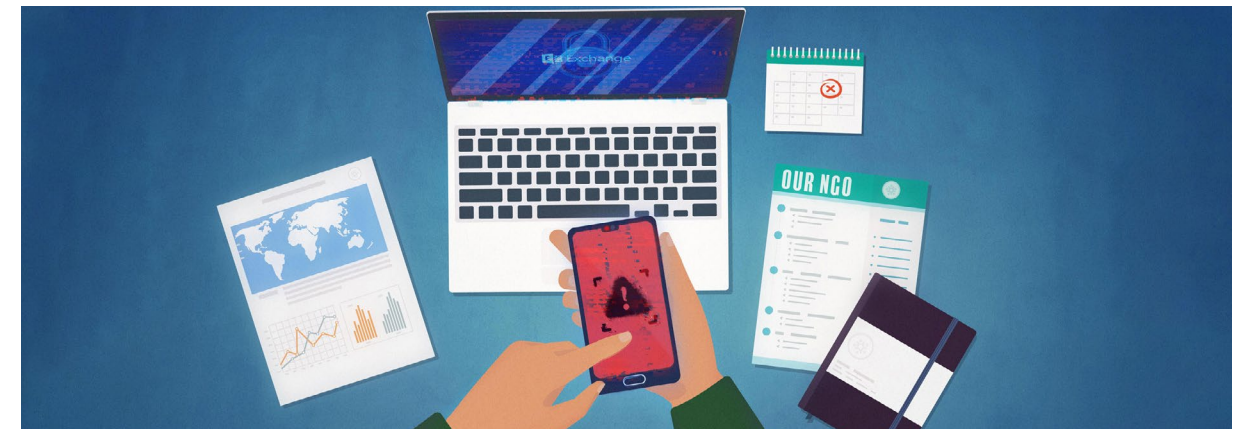


Strategic Objective 2: ANALYSIS

The Institute performs, facilitates and coordinates collective analysis, research and investigations of cyberattacks targeting vulnerable communities to ultimately support accountability of malicious actors.

• Case Analysis and Forensic Intelligence Reports

- ◇ The Institute has supported 5 cases with data analysis, serving as a Clearing House service to identify targets of attacks and warn victims.
- ◇ Forensic Intelligence reports were produced for partners and beneficiaries, and shared confidentially.



• Societal Impact of Ransomware

- ◇ The Institute led an ad hoc workstream within the [Ransomware Task Force](#), a multistakeholder group facilitated by the [Institute for Security and Technology](#), working towards a comprehensive set of actionable recommendations to combat the ransomware threat.
- ◇ The knowledge acquired led the Institute to facilitate a [workshop on ransomware](#) for journalists, to share knowledge and expertise strengthen human-centric reporting about cyberattacks. For the purposes of this workshop, the Institute joined forces with the [Global Cyber Alliance](#) and [Swissnex](#) in Boston and New York.

FOCUS on

• Offensive Cyber Capabilities (OCCs) and Surveillance Technology

To support a key international effort to respond and call out the use of highly intrusive offensive cyber capabilities (OCCs) to target dissidents, political opposition figures, journalists, lawyers, international investigators and other members of civil society, the Institute offered free forensic tools and support to detect spyware intrusion. The Institute supported the development of the Digital Violence Platform launched by Forensic Architecture and has expressed its concerns to key [experts](#) calling for a global [moratorium](#) on the sale and transfer of surveillance technology until such time as rigorous human rights safeguards are adopted.



Strategic Objective 3: ADVANCEMENT

The Institute reminds state and non-state actors of the international law and norms governing responsible behavior in cyberspace, and contributes to advancing the rule of law to reduce harm and ensure the respect of the rights of people.

• Contribution to UN Processes

◇ The Institute contributed to and commented on various United Nations-led processes (notably the *United Nations Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security (UN GGE)* and the *Working Group (WG) on the use of mercenaries as a means of violating human rights and impeding the exercise of the rights of peoples to self-determination*).

◇ The Institute has closely followed the work of the *United Nations Open Ended Working Group (UN OEKG)* on developments in the field of information and telecommunications in the context of international security, advocating recognition of the healthcare sector as a critical infrastructure and raising concerns about the lack of commitment towards an actionable and genuine human-centric approach.

• Participation in International Initiatives: the Paris Call Working Groups

◇ Group 5 of the Paris Call: Creating a cyberspace stability index was co-chaired by the CyberPeace Institute, Geopolitics of the Datasphere (GEODE) of the Paris 8 University, and the Hague Center for Strategic Studies.

◇ The work of this group led to the [Final Report](#) published during the Paris Peace Forum 2021. It presents a methodology to facilitate understanding of how the implementation of normative, legal, operational and technical measures, or the lack thereof, contribute to stability in cyberspace and ultimately to cyberpeace.

◇ The Institute contributed to Group 3: Advancing the UN negotiations with a strong multistakeholder approach, leading to the publication of the final report on “[Multistakeholder participation at the UN: The need for greater inclusivity in the UN dialogues on cybersecurity](#)”.



FOCUS on

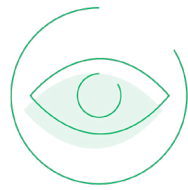
• Multistakeholder Manifesto

◇ Responding to the challenge presented by the proposal to negotiate a United Nations treaty on “Countering the use of information and communications technologies for criminal purposes (UN Cybercrime Convention)”, the CyberPeace Institute and the [Cybersecurity Tech Accord](#) brought together over 60 stakeholders to sign a [Multistakeholder Manifesto on Cybercrime](#). The signatories affirmed the need for the principles outlined in the Manifesto to be at the heart of any cybercrime legislation and to guide the negotiating process, bringing respect for human rights to the core.



“The participation of stakeholders from civil society, the private sector and academia in the process of this working group has raised awareness of the need for a multi-stakeholder cooperation approach in strengthening cybersecurity. Numerous written contributions from stakeholders on the working group's website, including contributions from the CyberPeace Institute, are evidence of the potential of such cooperation.”

Ambassador Jürg Lauber, Permanent Representative of Switzerland to the Office of the United Nations and other International Organizations in Geneva, March 2021



Strategic Objective 4: FORESIGHT

The Institute forecasts and investigates opportunities, risks and threats to people associated with emerging and disruptive technologies, and analyzes emerging global cyber challenges.

- **Disruptive Technologies and Cyberpeace**

- ◊ The Institute has developed a framework for foresight- related work by collecting expert considerations during the [CyberPeace Lab on Disruptive Technologies and Cyberpeace](#) and by framing the underlying narrative on both Disruptive Technologies and [Convergence of Technologies](#) in relation to cyberpeace.

FOCUS on

- **Artificial Intelligence and Vulnerable Communities**

- ◊ Peace mediators were identified as a vulnerable community in their interaction with emerging and existing technologies. The Institute explored the current and forthcoming use of artificial intelligence in peace mediation processes focusing not only on opportunities and risks, but also on their often overlooked societal impact.

WHO WE ARE: THE PEOPLE BEHIND THE NUMBERS

Governance and Staff

Executive Board

The Executive Board is the supreme governing body of the CyberPeace Institute and possesses the highest and most extensive authority over decision-making and administration. It comprises a diverse group of global thought leaders and individuals driving the digital peace agenda. Executive Board Members in this period:

- Alejandro Becerra Gonzalez, Global Information Security Director, Telefonica
- Kelly Born, Director, Cyber Initiative, The Hewlett Foundation
- Merle Maigre, Senior Expert on Cyber Security, e-Governance Academy (eGA)
- Alexander Niejelow, Senior Vice President, Cybersecurity Coordination and Advocacy, Mastercard
- Kate O'Sullivan, General Manager, Digital Diplomacy, Microsoft
- Martin Vetterli, President, Ecole Polytechnique Fédérale de Lausanne (EPFL)

Members who served during earlier periods covered in this report:

- Khoo Boon Hui, President, INTERPOL (2008-2012)
- Anne Marie Slaughter, Chief Executive Officer, New America
- Brad Smith, President and Vice Chair, Microsoft
- Eli Sugarman, Director of Content (Moderation), Oversight Board

Leadership and Staff

The Institute has a team of high-level professionals from diverse professional backgrounds with a broad range of expertise both inside and outside technology and cybersecurity-related sectors. The Leadership Team comprises :

- Marietje Schaake, President (2019-2021)
- Stéphane Duguin, Chief Executive Officer
- Francesca Bosco, Chief Strategy Officer
- Bruno Halopeau, Chief Technology Officer
- Klara Jordan, Chief Public Policy Officer
- Charlotte Lindsey (Curtet), Chief Communication Officer
- Adrien Ogée, Chief Operating Officer

Numbers and Growth

As of 31 December 2021, the Institute has 33 employees, of whom 20 are women (60.6%) and 13 are men (39.4%). 13 nationalities are represented.

WHO WE WORK WITH: PARTNERS AND NETWORK

A Multistakeholder Approach

At the Institute, we believe that meaningful change can occur when a diversity of perspectives, sectors and industries work together. To address the complex challenges related to ensuring cyberpeace, we work with a wide range of actors at the global level from the private sector, civil society, academia, philanthropies, policy-making institutions and other organizations. The Institute can contribute by providing evidence-led knowledge, emphasizing the need to integrate a genuine human-centric approach in both technical and policy-related projects and processes, and by highlighting the civil society perspective to support and amplify existing initiatives.

The Institute actively supported the work of several initiatives in line with its mission and values, providing expertise, elevating the work of others and representing the voice of civil society in relevant multistakeholder initiatives. As an example, the Institute is an active member of the [Global Forum on Cyber Expertise](#) (GFCE), a key multistakeholder network with the mission to advance cyber capacity building at a global scale.

In the face of the hybrid threat of criminal groups and state actors, coalitions of private and public sector actors are key to success and bring benefit to the wider general public. As an example, the Institute joined the [Coalition Against Stalkerware](#), which convinced many organisations to partner against domestic surveillance by putting victims' interests at the heart of its actions.

The Key Role of Switzerland and International Geneva¹

The Institute was established in Geneva because the city has long been an esteemed global hub for international cooperation, notably for humanitarian and human rights organizations. As part of the integration and engagement with the stakeholder's ecosystem in Geneva, the Institute is a member of the Geneva Chamber of Commerce, Industry and Services (CCIG).

Various academic collaborations were ongoing during the period under review through participation in conferences, workshops and lectures, namely with the EPFL (C4DT), the University of Geneva and the Graduate Institute.

In September 2020, the Institute joined Trust Valley, a public-private partnership and centre of expertise which aims to promote digital trust and cybersecurity. Promising collaborations have been established with Swissnex and with the Federal Department of Foreign Affairs (FDFA) Division for Digitalization.

¹ The institutions mentioned in this section do not constitute an exhaustive list and they are intended to give diverse examples of the collaboration. The Institute is currently investing in widening its network via different engagement opportunities in Geneva and within Switzerland.

Awards

The Institute and its staff has received several awards for innovative and continuous efforts promoting cyberpeace:

2020 Geneva Centre for Security Policy, [Second Prize](#) for Innovation in Global Security



2021 Geneva Centre for Security Policy, [First Prize](#) for Innovation in Global Security



2021 Geneva Chamber of Commerce, Industry and Services (CCIG), [Prix de l'Economie](#)



HOW WE COMMUNICATE

From the outset, strategic communication has aimed to position the Institute as a key reference on cyberpeace and to reach a broad spectrum of essential audiences in order to:

- Build greater visibility and awareness of the Institute's work and of threats to cyberpeace
- Disseminate key messages and drive engagement on topics and issues of importance
- Enhance the understanding of and influence policymakers, governments and professionals in the cyberpeace domains
- Participate in advocacy efforts with other organizations in civil society to change attitudes, practices and behaviors
- Contribute to fundraising ambitions of the Institute.

KEY COMMUNICATION ASSETS

The Institute focuses on digital communication through its website and social media presence as the primary audiences of the Institute are adept at accessing materials and information online. In 2021, the Institute publicly launched the Call to Governments, the Strategic Analysis Report Playing with Lives; Cyberattacks on Healthcare are Attacks on People, and an Addendum to the report, as well as the Cyber Incident Tracer #HEALTH, the CyberPeace Builders program, and the Multistakeholder Manifesto. Communication activities amplified the profile of Institute participation in a range of public events from RightsCon, to the Paris Peace Forum.

Key highlights of the period:

- **Website**
 - ◊ In 2021, some 55 articles and blogs and 10 news releases were published on the Institute's website highlighting key topics and challenges, such as the submissions to the UN fora, cyberattacks against humanitarian NGOs and attacks against healthcare. Increasingly communications were also available in French.
- **Social media accounts**
 - ◊ The Institute has a presence on Twitter, LinkedIn, YouTube, Instagram and Facebook. The percentage increase in audience growth for platforms such as Twitter and LinkedIn in 2021 were 47.5% and 86.3%, respectively.

- **Videos**
 - ◊ 15 videos were produced on key topics such as cyberattacks on healthcare and on humanitarian NGOs.
- **Newsletter**
 - ◊ The Institute launched its first Newsletter in the last quarter of 2021. The monthly Newsletter provides a short digest of compelling stories relevant to cyberpeace.
- **Media outreach and engagement**
 - ◊ Media outreach to general and specialist media in English and French was a key focus of 2021. Some highlights included coverage of the Cyber Incident Tracer #HEALTH on the front page of the Financial Times, an article in [Foreign Policy](#), and a film for the Defenders of Digital series exclusively focused on the Institute's work as well as coverage in media such as Le Temps, Al Jazeera and the World Economic Forum.
- **Events**
 - ◊ Experts from across the Institute participated as key speakers at events almost weekly, and their presence was leveraged across social media in order to highlight the challenges of, and recommendations for strengthening cyberpeace.

FINANCE AND FUNDING

In accordance with its core principle of independence, the Institute operates free from the direction, control or interference of any actor, including states, industry or any other organizations.

The Institute relies on voluntary donations and independently fundraises to support its operations while ensuring that donations are in keeping with its mission, principles and standards of due diligence. The financial report of the organization analyses the first 14 months of activity of the Institute, from 15 November 2019 to 31 December 2020. The financial report has been audited by Deloitte in compliance with legal requirements.

[Financial report](#)

CONTRIBUTE TO CYBERPEACE





At the heart of the CyberPeace Institute’s efforts is the recognition that cyberspace is about people. We support providers of essential services to the most vulnerable members of our society, ultimately benefiting us all, like NGOs and the healthcare sector personnel. Attacking them can have a devastating impact on their beneficiaries and patients, putting their rights and even lives at risk.

To deliver on this mission, the Institute relies on donations and the generosity of individuals, foundations, companies and other supporters. Support received serves to assist NGOs in securing their resources and enhancing their resilience to cyberattacks. It also serves to provide evidence-based knowledge and foster awareness of the impact of cyberattacks on people, empower victims to claim their legitimate rights and to give a voice to victims and committed actors who want to see the change needed to secure the digital future for us all.

Mission Statement

The **CyberPeace Institute** is an independent and neutral non governmental organization whose mission is to ensure the rights of people to security, dignity and equity in cyberspace. The Institute works in close collaboration with relevant partners to reduce the harms from cyberattacks on people’s lives worldwide, and provide assistance. By analyzing cyberattacks, the Institute exposes their societal impact, how international laws and norms are being violated, and advances responsible behaviour to enforce cyberpeace.

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

-  cyberpeaceinstitute.org
-  [@CyberPeace Institute](https://www.linkedin.com/company/cyberpeaceinstitute)
-  [@CyberpeaceInst](https://twitter.com/CyberpeaceInst)
-  [@CyberpeaceInst](https://www.instagram.com/CyberpeaceInst)

