Solidarity Action Network

Navigating cybersecurity: Guidance for (I)CSO professionals

International Civil Society Centre

CyberPeace Institute

solidarityaction.network

Why are we talking about cybersecurity?

Over the past decade, civil society organisations have increasingly relied on the use of digital technologies to provide essential services to communities. Despite the many advantages of technology, there are also many challenges that international civil society organisations (ICSOs) and local civil society organisations (CSOs) have struggled to proactively tackle.

In recent years, (I)CSOs have faced an increase in digital threats and cyberattacks carried out by malicious actors interested in financial gains and access to sensitive data or identifiable personal information. The number of ransomware attacks, distributed denial-of-service (DDoS) attacks and data leaks targeting ICSOs and CSOs is growing. These actors are an easy target for cybercriminals because they often do not have sufficient cybersecurity plans in place due to budget restrictions or a lack of expertise or time. Therefore, there is a pressing need for (I)CSOs to prioritise cybersecurity to protect the communities they serve and their own work.

Within the framework of the **Solidarity Action Network (SANE)**, the **International Civil Society Centre** and the **CyberPeace Institute** convened a series of SANE curated conversations to exchange know-how and strengthen the cybersecurity capacity of (I)CSOs. Based on key insights from these conversations, the CyberPeace Institute has developed this cybersecurity guidance to help you navigate through the overwhelming amount of information available online regarding digital security, digital threats and cyberspace. The guidance will provide you with steps to better protect your organisation online, as well as relevant resources and initiatives.

Who is this for and what is it?

This cybersecurity guidance is designed for ICSOs and CSOs to learn about cybersecurity and strengthen the security of their online activities. It addresses (I)CSO professionals across different departments as cybersecurity needs to be everyone's responsibility. The guidance aims to share know-how and best practices to help civil society actors better respond to cybersecurity challenges and digital threats. It further strives to encourage (I)CSOs to shift from reactive to proactive measures and narratives so that they can actively contribute to promoting cyberpeace.

The guidance presents the main takeaways from three SANE curated conversations on cybersecurity and showcases relevant resources and expert contacts. It focuses on three interrelated topics:

1) Data protection and security – to equip (I)CSOs with knowledge and tools to protect the sensitive data of marginalised communities and vulnerable populations while providing essential services

2) Prevention and mitigation of cyberattacks – to raise awareness of digital threats that can affect (I)CSOs and how they can prepare for and respond to cyberattacks

3) Sustainable cybersecurity support for local civil society – to ensure that ICSOs also prioritise the cybersecurity of local civil society partners with whom they work, who are indispensable for understanding the local context and accessing local communities and vulnerable populations

Part 1
Data protection and security

Why is this important?

Every activity you carry out online creates data, which often contains sensitive personal information about you, the organisation you work for and the partners and communities you work with. Personal data protection is a fundamental right of individuals; like other fundamental rights, it is integral to the protection of life, integrity and dignity.[1] For this reason, it is the responsibility of (I)CSOs to use layered security measures to protect the data they create and obtain.

Data protection is the process of safeguarding important information from corruption, compromise or loss. This process involves the collection and dissemination of data and technology, public perceptions and expectations of privacy and the legal underpinnings surrounding the collection and dissemination of data. Data protection must strike a balance between individual privacy rights and the use of data for organisational purposes.

A data protection framework should be built on the following general principles:

- Fair and lawful processing
- Purpose specification
- Data minimisation
- Data quality
- Data retention
- Transfer and processing of data

As discussed in the Handbook on data protection in humanitarian action developed by the International Committee of the Red Cross (ICRC), the process of managing data is closely related to the implementation of a data protection framework in that the integrity and security of data must be ensured. Therefore, in the case of a data breach, (I)CSOs are obligated to notify the data protection authority and the data subject.[2]

1 ICRC: Handbook on data protection in humanitarian action, p. 28.
2 Ibid., p. 32–33.

What are the challenges?

Data protection requires a distinct but coordinated approach with information security experts, including the concepts of data protection by design and by default, as the first step in the risk assessment process of a new product, project or programme. Coordination of the data protection framework must include the phases of prevention, analysis, response and remediation to threats targeting data.

Data protection presents many challenges, the first of which is clearly defining what data protection means for your organisation and activities in your specific context and geographical area. It cannot be replaced by the implementation of privacy measures. Another challenge is identifying how to process specific data that are sensitive in nature (e.g., related to health, religious affiliation, sexual orientation, political orientation) within the context of legal frameworks. Ultimately, the processing of data should continue only until it meets the purpose of the product, project or programme. It is important that (I)CSOs are held accountable for the personal data they manage during data collection and processing as well as data deletion.

How to deal with these challenges?

Data plays a valuable role for (I)CSOs, and the collection of granular data may strengthen the positive effects of programmes and policies on communities. However, more collection of granular data leads to more processing of identifiable information. Organisations that work with disaggregated data, like ICRC and Development Initiatives, are aware of the inherent risks of doing so. Therefore, they recommend applying data protection throughout the data life cycle.

In the scope of the Leave No One Behind Partnership, Development Initiatives introduced basic guidelines that organisations should consider at every stage of the data life cycle to minimise risks. Within a six-step process (preparation, collection, storage, processing, publication and retention and destruction), the guidelines describe concrete actions to ensure the proper application of a data protection framework.

Beyond this six-step process, there are other tools (I)CSOs can implement to be responsible and accountable for the data they manage. One such tool is the Data Protection Impact Assessment (DPIA), which can be used to identify, evaluate and address the risks to personal data – and ultimately to the data subject – that arise from a project, policy, programme or other initiative.[3] A DPIA can help your organisation to avoid, minimise and protect your work from the risks arising out of the processing of data. The assessment must be applied to all steps of the data life cycle and should be revisited as the project or programme undergoes changes or as new risks arise.

However, the DPIA is not a one-size-fits-all tool. To be effective, it must be conducted by the team managing the project or programme, and requires expertise regarding the environment that a specific project or programme is developed for and implemented within.

Appendix I of the ICRC Handbook provides a DPIA template that can be used for a specific project. Alternatively, you can use a DPIA template created by the UK's Information Commissioner's Office. More information about how to conduct a DPIA and related requirements under the GDPR can be found here.

ADDITIONAL RESOURCES ON DATA PROTECTION AND SECURITY

- **DigitHarium**, a global forum to discuss and debate digital transformation within the humanitarian sector, with a focus on humanitarian protection, policy, ethics and action
- **Data minimization**: Key to protecting privacy and reducing harm, a resource developed by Access Now regarding how to reduce harm by limiting the amount of information collected online
- **Data Protection Officer (DPO) Humanitarian Action Certification**, a course created and offered by Maastricht University based on the ICRC Handbook

3 ICRC: Handbook on data protection in humanitarian action, p. 84.

Part 2
Preventing and mitigating cyberattacks

Why is this important?

The increasing number of digital threats and cyberattacks targeting (I)CSOs is driven by the state of (I)CSOs' cybersecurity and the information criminal actors can gather on (I)CSOs. (I)CSOs often lack the financial resources, expertise and time needed to develop a solid cybersecurity strategy that could shield them from increasing digital threats. The CyberPeace Institute has found that civil society actors are not well protected; only 1 in 10 NGOs train their staff in cybersecurity, only 1 in 4 NGOs monitor their ICT networks for vulnerabilities and only 1 in 5 NGOs have cybersecurity plans in place. Additionally, (I)CSOs manage a significant amount of donations and sensitive data, which makes them attractive to cybercriminals. As seen in recent cases, cybercriminals consider cyberattacks on (I)CSOs to be low-risk operations that can lead to a high pay-out. In such scenarios, the targets of cyberattacks are not only (I)CSOs but also the vulnerable communities they serve. Therefore, (I)CSOs must prioritise cybersecurity to protect the communities they serve and their own work.

Even though cybersecurity may sound complicated and out of your organisation's normal scope of activities, it is time for you to take control of your cybersecurity and develop digital resilience to be better protected online. To do so, (I)CSOs must be equipped with knowledge, skills and tools to prevent and mitigate cyberattacks, both by empowering their employees and by working with external actors who specialise in providing cybersecurity support to the civil society sector.

In this section, we spotlight three digital threats that are increasingly affecting (I)CSOs and their work.[4] Bearing in mind that effective cybersecurity relies on three main aspects – **people, technology and processes** – we present measures and tools your organisation can apply to prevent and mitigate these digital threats.

4 Please note that this list of digital threats and cyberattacks is not exhaustive.

What are the main digital threats (I)CSOs are facing?

1. Phishing attack and domain spoofing

A phishing attack is a common cyber threat that consists of a fraudulent communication posing as a reputable source. It aims to trick the recipient into providing sensitive data or installing malware.[5] Phishing attacks are not only increasing in number[6] but posing more sophisticated threats, such as spear phishing (targeted phishing that exploits real information about the victim to make the source of the attack seem credible[7]), and malspam (malware delivered as malicious attachments in spam email[8]). Emails remain the most used vector to launch phishing attacks and campaigns, often containing malicious links and attachments that hide malware. Phishing attacks often rely on domain spoofing, which is a fake website name or email domain created to trick the user into sharing personal information (such as login credentials or credit card details) or downloading malware.[9]

(I)CSOs are not excluded from being targets of phishing attacks launched by malicious actors, including states and state-sponsored groups. We have seen (I)CSOs hit as part of a larger attack on the humanitarian sector. An attack may be multifaceted as cybercriminals pursue different approaches to breach the organisation's defences.

How to prevent and mitigate phishing attacks?

PEOPLE

- Check if the domain name or email address is spelled correctly (https://www.facebook.com instead of https://www.facebok.com).
- Think about the context: Does it make sense that you are receiving this type of email from a manager/colleague/partner you have never talked to before?
- Encourage your staff/colleagues to report phishing emails or other threats. To inform your staff/colleagues about a phishing email, take a screenshot of it instead of forwarding the email itself.

TECHNOLOGY

- Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) to avoid your domain being spoofed in phishing campaigns.
- Enforce multi-factor authentication or two-factor authentication on email systems and social media platforms.
- Use password managers (e.g., LastPass or Remembear) for all staff, creating shared folders for collaboration. This strategy will avoid the sharing of credentials between colleagues via email or other communication channels.

5 Definition by the CyberPeace Institute.
6 ESET: Threat Report T2 2021.
7 Definition by the CyberPeace Institute.
8 Definition by the CyberPeace Institute.
9 Cloudflare: What is domain spoofing? Website and email spoofing.

PROCESSES

- Dedicate time to create and implement a cybersecurity plan that enables you to know the location of your organisation's resources.
- Continue to train your staff and colleagues on common digital threats, like phishing.
- Understand the threat model of your organisation to be better prepared for possible scenarios.

2. Ransomware attack

Another common cyberattack that targets (I)CSOs is ransomware – a type of malware designed to extort money from victims by encrypting or blocking access to their data, files or computer systems until they pay a ransom.[10] This type of cyberattack can severely disrupt organisation's activities, causing short- and long-term damage.

In addition to causing the inability to access data and digital assets/devices, such a threat can paralyse an organisation's functioning and incident response mechanisms. (I)CSOs hit by a ransomware attack not only face the challenge of dealing with cybercriminals and restoring their IT infrastructure but also struggle to figure out the most appropriate way to communicate about the incident – if they decide to do so – with donors, partners, ICSO and CSO peers and the communities they serve.

How to prevent and mitigate ransomware attacks?

PEOPLE

- Actively involve employees in testing incident response plans, with a focus on specific disruptive threats such as ransomware attacks.
- Train your staff on cybersecurity awareness and best practices in case of a cyberattack.
- Build and spread a no-blame culture in which employees are not afraid to report if they click on the wrong link or open the wrong attachment.

TECHNOLOGY

- Set up automatic backup software and tools and ensure offline backups of your data.
- Do not use cracked software programs, as they are not up to date and can be leveraged to open security breaches.
- Rely on a next-generation antivirus solution that analyses processes and behaviours (e.g., Bitdefender).

10 Definition by the CyberPeace Institute. See here for further cybersecurity definitions.

PROCESSES

- Implement a vulnerability management process to identify, evaluate, treat and report on security vulnerabilities in the organisation's systems and software. This process helps to prioritise possible threats and minimise attack surfaces.
- Apply network segmentation to divide the organisation's network into small and distinct sub-networks, and implement unique security controls and services in each sub-network.
- Implement the practice of application whitelisting by specifying a list of approved software applications or executable files (.doc, .pdf, etc.) that are permitted to be present and active on a computer system within the organisation. The goal of whitelisting is to protect computers and networks from potentially harmful applications.

3. Distributed denial-of-service (DDoS) attack

Several disruptions can affect the functioning and availability of an organisation's website, from the website being blocked by filters to coding malfunctions. Another cause of disruption is a distributed denial-of-service (DDoS) attack – a technique that involves flooding a network, service or server with excessive traffic to make it cease normal function.[11] The two key indicators of a potential DDoS attack are if a website is repeatedly and unexpectedly unavailable and/or takes a long time to access. DDoS attacks are mostly run on malware, often on rented servers known as "stressor services". This type of attack has been widely used as an online tool of censorship and repression, as well as to disrupt services to an (I)CSO's target communities via their website.

DDoS attacks are not often sophisticated cyberattacks, but they can be used by cybercriminals to distract their target and leverage other vulnerabilities. Unfortunately, mitigation strategies are not possible while under this type of attack, so it is important to prevent DDoS attacks. In general, it is good practice to monitor the functioning of your (I)CSO's website/s from both a performance and security perspective.

How to prevent and mitigate DDoS attacks?

PEOPLE

- Ask for help from partners and organisations with technical expertise.
- Raise concerns about cybersecurity and the need for technical help with donors and foundations.
- Join trusted networks of civil society organisations in which best practices are shared.

TECHNOLOGY

- Explore solutions for non-profit organisations to add a DDoS protection and security layer, such as Deflect or Project Galileo.
- If you have a donation page on your website, ensure that you use PayPal or credit card payments through reliable providers and that your donors can easily find the provider details and policies.
- On your website login page, set up automatic blocking messages after too many login attempts.

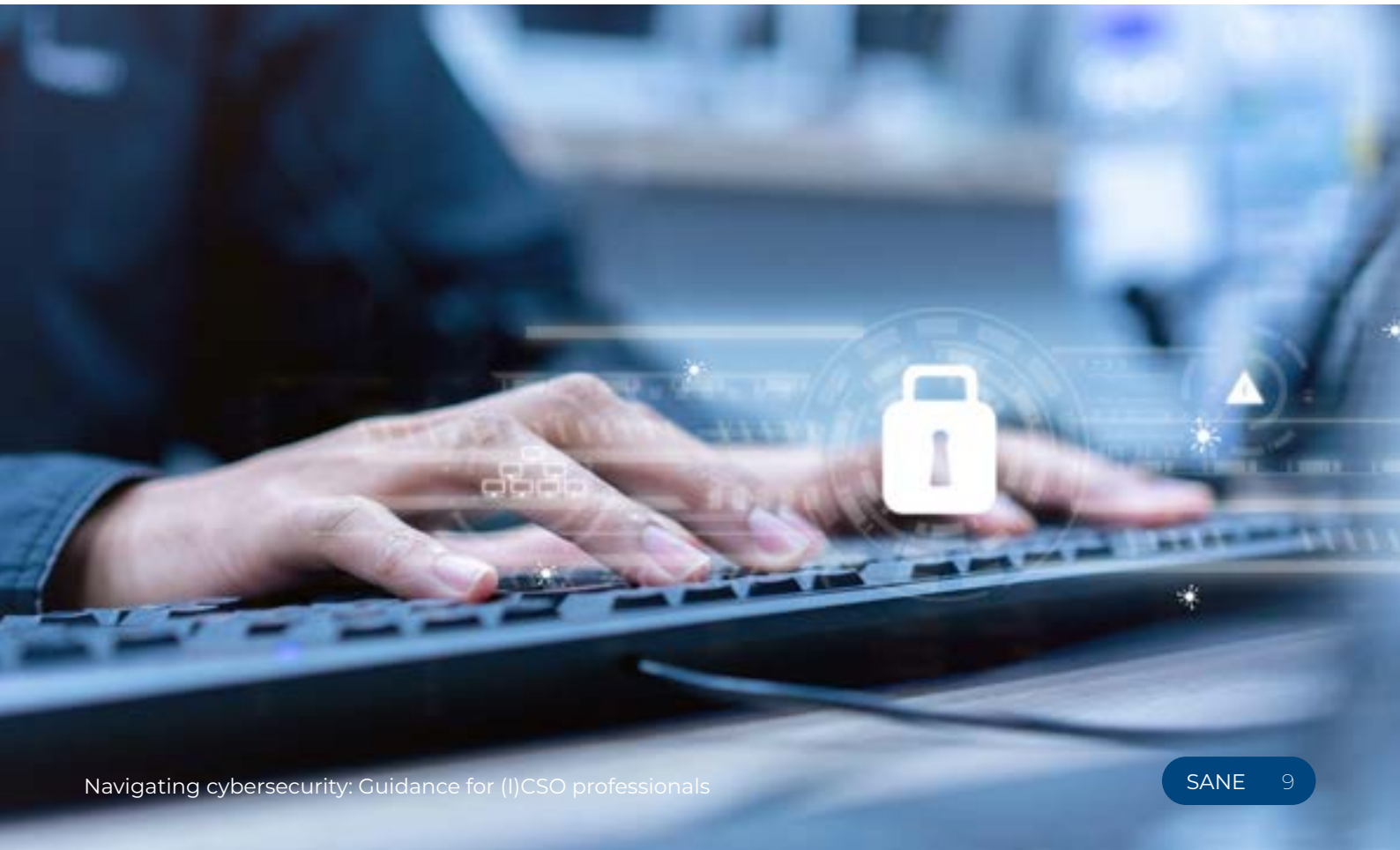
11 Definition by the CyberPeace Institute.

PROCESSES

- Before purchasing a tool, conduct due diligence of the company that makes it.
- Implement a recurrent process of network monitoring.
- Track your organisation's hardware, software, and sensitive information with this template.

FURTHER RESOURCES ON PREVENTING AND MITIGATING CYBERATTACKS

- **No More Ransom**, an initiative that helps victims of ransomware retrieve their encrypted data without having to pay the criminals. This initiative also educates users about ransomware and the countermeasures that can be taken to effectively prevent attacks.
- **Toolkits and Best Practices: Protecting Yourself is Protecting Others**, a selection of toolkits and sets of best practices curated by the CyberPeace Institute, which anyone can use in their everyday life to defend themselves and avoid spreading cyberthreats.



Part 3
Promoting sustainable cybersecurity support for local civil society

Why is this important?

In many countries, ICSOs implement their projects in collaboration with local CSOs and civil society partners that work directly with local communities and vulnerable populations. Local CSOs and partners collect data, share the (personal) information of people involved in projects and manage funds. These partners have varying levels of preparation for digital risks and thus could potentially be easy targets for cybercriminals. Therefore, strengthening cybersecurity knowledge and expanding technical skills should be a priority not only of local civil society actors alone but also of ICSOs to better support their local partners.

What are the main challenges and how can they be addressed?

- **Local CSOs and partners may consider cybersecurity a complicated topic.**
  - ICSOs can support local CSOs and partners by providing trainings on cybersecurity and encouraging local staff to prioritise cybersecurity.
  - ICSOs can encourage local CSOs to incorporate cybersecurity trainings into their onboarding process for new staff.
  - ICSOs can advise local CSOs on how to encourage interest in cybersecurity among all staff, not just IT experts.

- **Local CSOs and partners may lack the knowledge and skills to understand the digital context in which they operate, the digital threats they could face and their cybersecurity needs.**
  - ICSOs can foster the creation of a “train the trainers” programme for local actors, with the aim of embedding cyber hygiene best practices and basic policies in local structures.
  - ICSOs can encourage digital champions within an organisation. A digital champion is a mentor or go-to person in a local CSO who promotes localised knowledge sharing regarding cybersecurity.
  - ICSOs can map existing international and local digital resources to which local CSOs and partners can refer in case of a question or emergency.
- **Local CSOs and partners may operate in challenging environments with limited access to digital technologies and a lack of sustainable support tailored to their operating conditions.**
  - ICSOs need to consider geographical, political and societal aspects when providing support to local actors.
  - ICSOs can assist CSOs and partners by pointing them to local resources and encouraging them to ask for support from local networks.
- **Local CSOs and partners may be unwilling or unable to use their budget for cybersecurity.**
  - ICSOs can collaborate with donors and grant-making bodies to change existing funding mechanisms to incorporate cybersecurity support.
  - ICSOs can facilitate the creation of funds specifically for cybersecurity and IT, as well as monitoring mechanisms.

You are not alone, ask for help!

There are many organisations whose mission is to provide digital and cybersecurity support to ICSOs, local CSOs, vulnerable communities and individuals. You can find tailored support depending on your needs, your local partners' needs and the needs of the communities you work with.

In fact, relying on a one-size-fits-all approach can be detrimental to your work. Reach out to some of the organisations below and their respective initiatives to seek support for your organisation or advice for your local partners. The following list is not exhaustive but showcases organisations and initiatives that were presented during the SANE curated conversations.

CYBERSTAR (CYBER SAFETY ASSESSMENT AND RESPONSE)

The **CyberSTAR** project supports civil society and independent media organisations in the Eurasian region in protecting their operations, information, communications and beneficiaries from cybersecurity breaches and routine data loss. It helps small organisations and individuals to understand, learn about and manage digital safety by focusing on six thematic areas: digital risks, digital identity, passwords, devices, data and conversations.

CyberSTAR provides support to CSOs to improve their online safety through:

- Organisational digital safety diagnostics
- Direct technical assistance
- Extended training and policy support

CyberSTAR's resources are available in English, Russian, Georgian, Uzbek and Romanian. Coming soon, the CyberSTAR Methodology and Training Kit will support at-risk CSOs to develop a sustainable culture of digital safety.

CyberSTAR is created and run by the SecDev Foundation, a not-for-profit organisation based in Canada that helps communities pursue digital opportunity, safety and citizenship. The SecDev Foundation has also created the following digital safety resources in Arabic, thanks to collaboration with local organisations:

- SalamaTech Resources
  - SalamaTech Facebook page, a resource for digital alerts and general guidance
  - SalamaTech Wiki, an online encyclopaedia of digital safety guidance and how-tos for beginners and experts
  - SalamaTech Web Portal, a collection of how-to guides for a non-tech audience
  - Salam@ Web Resource Portal, a specialised resource for women's digital safety
  - List of Salam@ channels in Algeria, Tunisia, Jordan, Morocco, Bahrain and Kuwait.

For further information, you can reach out to CyberSTAR at: **info@cyber-star.org**.

REDES AYUDA

Redes Ayuda is a non-governmental organisation with the mission of defending human rights in Venezuela and other Latin American countries through collaboration with local and international organisations. Redes Ayuda uses both digital and analogue social networks as its main communication tool to empower individuals.

Some of the activities that Redes Ayuda provides include:

- Training on digital safety for local organisations and their staff, with a particular focus on Latin America
- Development and implementation of tools to protect against harassment, threats and similar challenges
- Creation of interactive cybersecurity awareness and digital resilience content for organisations and individuals:
  - Check out the Empower Ranger videos on Twitter and Instagram, which provide humorous content in Spanish about the most common digital threats and how to respond to them.

For further information, you can reach out to Redes Ayuda at: **RedesAyuda@gmail.com**.

CYBERPEACE BUILDERS

CyberPeace Builders is a network of corporate volunteers that provide free pre- and post-incident assistance to humanitarian NGOs protecting vulnerable populations anywhere in the world. Expert volunteers are recruited from local and international companies and coordinated by the CyberPeace Institute. The Institute acts as a liaison between corporate volunteers and supported NGOs, thus providing a localised and contextualised approach that ensures the support provided is adapted to the needs of each NGO.

CyberPeace Builders supports organisations with the following services:

- Pre-incident services, including general security assessments, cybersecurity awareness training, vulnerability assessment of websites and advice on cyber insurance
- Post-incident services, including backup strategies, data recovery and digital threat notifications
- Support services, including marketing and internal/external communication support regarding cybersecurity topics and data protection advice

CyberPeace Builders offers support in several languages (e.g., English, French, Spanish, Italian, Romanian, Russian), but they do not provide incident response services. The humanitarian NGOs that are part of this programme can join the CyberPeace Café, a closed and trusted cybersecurity community for NGOs to explore avenues of collaboration, share best practices and stay informed about digital threats identified by the CyberPeace Institute staff. In addition, the CyberPeace Café has a public interface where you can find cybersecurity awareness-raising and support materials for all types of needs and from different parts of the world.

CyberPeace Builders was established by the CyberPeace Institute, a non-governmental organisation whose mission is 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 of cyberattacks on people's lives worldwide. By analysing cyberattacks, it exposes their societal impact, identifies violations of international laws and norms and advances responsible behaviour to enforce cyberpeace.

For further information, you can reach out to the CyberPeace Institute assistance team at: **assistance@cyberpeaceinstitute.org**.

FURTHER ORGANISATIONS, RESOURCES AND INITIATIVES

- **TechSoup** and their **offers for non-profit organisations**
- **HiveMind community** and its **space on digital security** (available in English, French, Spanish and other languages)
- **Digital First Aid Kit**, a collaborative effort of **RaReNet** and **CiviCERT**
- **SOAP**, a free online security policy generator for CSOs
- **Digital Security Helpline** by **AccessNow**
- **Security Planner** by **Consumer Reports** in collaboration with **The Citizen Lab** (available in English and Spanish).

Solidarity Action Network

Navigating cybersecurity: Guidance for (I)CSO professionals

April 2022

International Civil Society Centre

CyberPeace Institute

With support of

Sweden Sverige

FORD FOUNDATION