Cybersecurity and Civil Society: The Global Imperative of an Underestimated Public Good

Francesca BOSCO
Chief Strategy Officer
CyberPeace Institute

In our rapidly evolving digital age, cybersecurity has emerged as a critical issue, demanding immediate and widespread attention. Yet, the narrative is often dominated by high-profile attacks on governments and multinational corporations, overshadowing an important reality: cyberattacks affect all of us. In addition, cybersecurity is often seen as a purely private good, in which an organisation's security solely depends on its own investments.

However, this misses a crucial point. Cybersecurity, just like global peace, environmental protection and elements of global health, must be treated as a public good. We recently saw how concerted efforts across the globe were required to combat COVID-19; a similar collaborative approach is needed to protect cyberspace. The interconnectedness of digital infrastructures means that a breach in one country can have ripple effects across borders, similar to how a virus can spread from one region to the entire world. Therefore, investment in cybersecurity, like investments in global health, benefits everyone through upholding collective security and thereby ensuring stability within cyberspace.

This article explores the concept of cybersecurity as a public good, highlighting the heightened implications for vulnerable communities - in particular civil society organisations (NGOs). In illustrating the necessity for global collaboration, we advocate for a collective defence strategy as a way to protect those most vulnerable to cyberattacks.

Cybersecurity as a Public Good: Perspectives and Challenges

When assessing the importance of cybersecurity, one can imagine a world in which cybersecurity is not present. Personal and sensitive data could be seized without a trace, serious harm could easily be inflicted by malicious actors taking down services which help the most vulnerable. Anybody linked to an organisation which has been attacked would be immediately threatened. The importance of cybersecurity cannot be overemphasised. Furthermore, the interconnected nature of cyberspace, in which having additional security can ensure the security of a vast range of stakeholders, means that cybersecurity can be viewed as a public good. Consider a local NGO supporting efforts in healthcare; if they have strong cybersecurity, they not only can protect their mission, but also ensure that their beneficiaries, partners, donors, team members, volunteers or those that are in any way

connected to the organisation are secure. In reality, everyone is somehow connected to cyberspace, and so cybersecurity benefits every individual, thereby requiring everyone to ensure that the cyberspace is secure.

However, the necessity of having a secure cyberspace for all individuals is frequently overlooked by many organisations and stakeholders. An important factor preventing this is that discussions about cybersecurity are still frequently confined to businesses and governments, whilst non-profit organisations and smaller entities are very frequently ignored. These stakeholders are an integral part of our digital world thanks to the expertise they have acquired, and can suffer disproportionately from cybersecurity threats. Including these communities in cybersecurity discourse is not just a matter of fairness; rather it is a necessity for a safe and secure cyberspace.

Public recognition of cybersecurity as a public good would give us much greater leverage for protection of vulnerable communities and also helps us ensure more equitable access to the digital world with all its benefits. It would also underscore ideas of collective responsibility in the protection and promotion of cybersecurity.

Cybersecurity: A Crucial Issue for Vulnerable Communities

Within this vast and interconnected digital ecosystem, vulnerable communities occupy a particularly precarious position. NGOs are particularly vulnerable to cyberattacks, with them both having limited access to resources, either financial or technical, whilst being laden with high-stake, sensitive data on their donors and beneficiaries. Obtaining this data can be a treasure trove for cybercriminals, making these communities ideal targets. NGOs are also highly targeted because of the critical services they offer to the population. Despite the severity of these threats, vulnerable communities are frequently underequipped in terms of cybersecurity defences. This is due both to financial constraints, and a lack of specialised knowledge and personnel in cybersecurity. Research has shown [1] that less than 15% of NGOs have cybersecurity experts on their staff and 33% of NGOs do not have dedicated IT
or security resources available. As a result, these organisations often resort to basic security measures, far from the sophisticated defences deployed by larger corporations or governments. This mismatch between the scale of the threat and the level of protection creates a high-risk environment that malicious actors are able to exploit.

Several alarming incidents in the civil society sector have underscored the scale of this problem. Roots of Peace [2], a humanitarian non-profit organisation replacing the scourge of landmines with sustainable agricultural farmland, faced a series of attacks in 2020 leading to the loss of hundreds of thousands of dollars. In April 2022, Insecurity Insight [3], a humanitarian NGO that examines the threat landscape of dangerous environments, received a string of malicious links and pornographic material through their personal devices and organisational systems. Malicious actors gained control over the system and the NGO lost control over their information and means of communication. Earlier this year, an NGO that provides health care to children [4] around the world was threatened by a ransomware attack. As a twisted form of courtesy,

[1] https://cyberpeaceinstitute.org/humanitarian-cybersecurity-center/
[2] https://cyberpeaceinstitute.org/news/2020-07-14-hackers-trick-humanitarian-non-profit-into-big-wire-transfers/
[3] https://cyberpeaceinstitute.org/news/cyberpeace-builders-program-safeguarding-ngos-from-cyberattacks/
[4] https://www.mastercard.com/news/perspectives/2023/who-protects-the-humanitarians-as-warfare-becomes-digital-ngos-are-in-the-cyber-crossfire/

the cybercriminals brazenly offered 'discounted' ransoms to NGOs, highlighting the exploitation of their vulnerability. In June of 2022, the International Committee of the Red Cross (ICRC)[5] reported a cyberattack that compromised data of over 500,000 people worldwide. These attacks have led to breaches of sensitive humanitarian data, jeopardising the safety of the individuals these organisations serve, and undermining the trust placed in them.

The impacts of these cyberattacks can be significant and multifaceted. On a functional level, the attacks can disrupt services and lead to financial losses. From an ethical perspective, they can compromise sensitive personal data, putting individuals at risk and potentially violating privacy rights; this also increases risks of there being another attack against them due to data seizure. Yet what is vital is to note the real human impact, and the destruction these attacks cause to many lives across the world. Furthermore, the fallout from these attacks can undermine public confidence in these organisations, hampering their vital work. Given the essential services these communities provide, often to marginalised and at-risk populations, the damage caused by cyberattacks extends far beyond the immediate victims, affecting society's most vulnerable more broadly.

The Call to Action: The Need for Global Collaboration for Sustainable Cybersecurity

Recognising cybersecurity as a public good and addressing the cybersecurity vulnerabilities of these communities is an urgent task that calls for global, collective action and collaboration. This effort should involve a diverse set of stakeholders - governments, private companies, individuals, and the NGOs themselves. Each of these entities has a unique role to play, yet their combined efforts are necessary to create a comprehensive and robust cybersecurity infrastructure that can protect even the most vulnerable in our society.

As NGOs often operate under significant financial constraints - with the majority of their resources dedicated to their core mission - allocating funds for cybersecurity is a challenge, despite the clear need. This can be achieved by donors dedicating funds specifically to the cybersecurity operations of NGOs. However, innovative solutions that bring together stakeholders and foster collaboration are needed to ensure the public good of cybersecurity is provided. Besides, the cybersecurity of NGOs is not just a financial issue, but also a question of awareness of the threats and the operational and human resources needed to address them.

One such initiative is the CyberPeace Builders (CPB) program[6]. The CPB program is designed to foster collaboration between cybersecurity professionals and NGOs, facilitating the acquisition/development of crucial skills and knowledge. This free service offered by CPB allows NGOs to significantly enhance their cyber defences without having to shoulder prohibitive costs. The CPB program is further strengthened by the increasing adoption of Environmental, Social, and Governance (ESG) strategies in the private sector. Corporations are becoming more attuned to their roles in addressing societal challenges; cybersecurity is one area where they can make a significant impact. Their engagement with initiatives like the CPB program contributes to enhancing global cybersecurity, aligned with their societal commitments, and promoting cybersecurity as a global public good. In this sense, global collaboration between different sectors can only be beneficial for building a sustainable cybersecurity.

[5] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know#:~:text=Update%3A%2024%20June%202022.,in%20a%20sophisticated%20cyber%20attack

[6] https://cyberpeaceinstitute.org/cyberpeace-builders/

These partnerships not only help vulnerable communities but also contribute to the overall health of the digital ecosystem. By investing in cybersecurity as a global public good, corporations can help build a more secure digital landscape that benefits everyone - themselves included. This collaborative approach represents a significant step towards sustainable cybersecurity, ensuring that no community is left defenceless in the face of growing cyber threats. It illustrates how shared responsibility and collective action can result in a safer, and more inclusive digital world.

Conclusion

Overall, in the ever-expanding digital world, cybersecurity is not merely an issue of technological defence. It's a matter of public welfare. We have underscored the necessity of viewing cybersecurity as a public good, highlighting the interconnectedness of our digital ecosystem where a vulnerability in one corner can cascade into a threat against all because of the spillover effect. This perspective urges a collective responsibility to safeguard cybersecurity, with particular attention towards vulnerable communities, who are frequently neglected in this conversation in spite of suffering the consequences of the threats.

Civil society organisations are crucial threads in the social fabric. Yet, they often become targets of cyberattacks due to their inherent vulnerabilities, and their handling of sensitive and high-stakes data, but they often can't deal with the consequences of these attacks. When these entities are compromised, the ripple effects are far-reaching, impacting not just their operations and finances, but also the individuals and causes they aim to help.

Addressing this challenge requires a collaborative global effort, transcending sectors and borders. It demands resource pooling and knowledge sharing among governments, NGOs, corporations, and individuals. Initiatives like the CyberPeace Builders program exemplify the kind of innovative solutions that such cooperation can engender; cybersecurity professionals are connected with NGOs to strengthen defences, without imposing financial strain or constraints.

In conclusion, the task ahead is significant but not insurmountable. The urgency for a more secure digital future demands immediate action. By viewing cybersecurity as a public good, we can realise the importance of collective responsibility in the protection and promotion of cybersecurity. By adopting a collaborative approach and prioritising the needs of vulnerable communities, we can fortify our collective defences, ensure sustainable cybersecurity for all, and prevent the next cyberattack targeting NGOs that provide essential services to the most vulnerable.