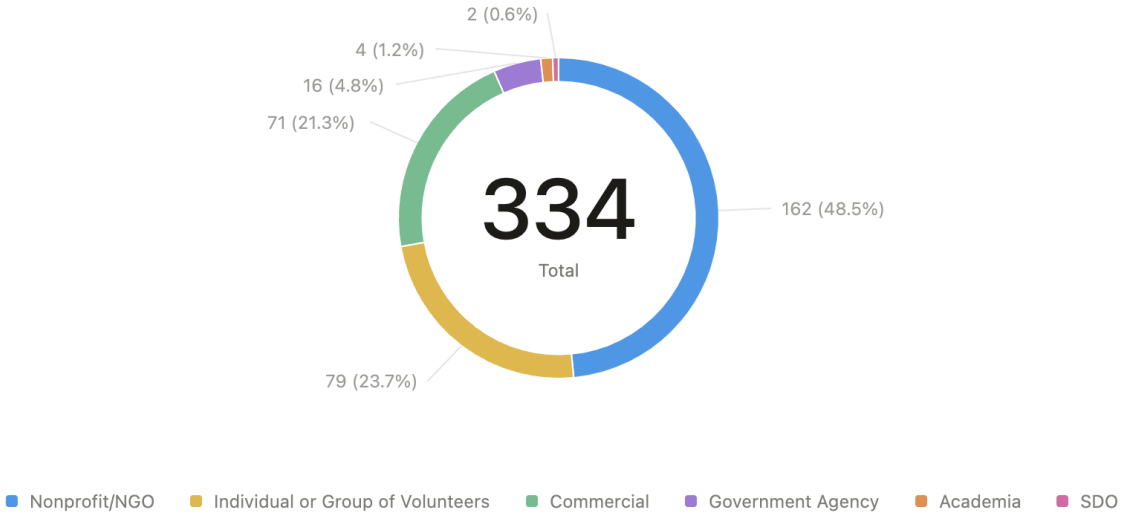
Nonprofit Contributions to Cybersecurity: Stories, Gaps, and Opportunities for Policy and Collaboration

The increasing complexity of cyber threats poses a serious challenge to our global digital ecosystem. Securing critical infrastructure and defending individuals from phishing, ransomware, and other malicious activities requires collaborative solutions beyond national borders. We draw your attention to the vital contributions of nonprofit organizations to global cybersecurity. They provide essential tools and services, most often at no cost to the user, benefiting diverse actors, including critical infrastructure operators and underserved populations.

Nonprofit Contributions

Over the past year, and with the support of the UK Foreign, Commonwealth & Development Office and the European Union Institute for Security Studies, Common Good Cyber conducted a review of the cybersecurity tools, services, and platforms deployed in the public interest to secure networks, empower Internet users, and increase resilience across sectors, like the examples we just mentioned. This mapping is available in the Knowledge Hub on commongoodcyber.org. Out of the 334 solutions identified, 162 are maintained by nonprofit organisations.



Nonprofits have demonstrated remarkable achievements in both endpoint security and the protection of digital commons. On the one hand, they provide direct assistance to vulnerable groups by promoting training resources and free-to-use tools, and providing rapid response assistance. They expand and adapt direct assistance to new groups and regions that need it most, particularly in the Global South, where resources are limited but threats are escalating.

A few examples include:

- The CyberPeace Institute's CyberPeace Builders program, which connects NGOs with cybersecurity professionals, supported 437 NGOs in 121 countries, enhancing their security posture and mitigating breaches.
- Access Now's Digital Security Helpline, which offers 24/7 emergency assistance in 10 languages, handled 4,419 digital security requests originating in 146 countries in 2024, helping activists, journalists, and marginalized communities combat surveillance and cyber incidents.
- GCA Cybersecurity Toolkits, which have more than 2 million visitors, have been seamlessly integrated into Ghana's Vigilance First awareness campaign since 2021. For a small organization like Ghana's Cyber Intelligence and Security Aid Bureau (CISAB), the GCA toolkits offer critical in-kind support and resources that would otherwise be unaffordable.

On the other hand, nonprofit organisations work at the infrastructure level to secure the digital commons like routing, the Domain Name System, and threat intelligence systems, and deploy workforce skills initiatives to expand cybersecurity expertise globally and make the whole ecosystem more resilient.

A few examples include:

- The Global Forum on Cyber Expertise (GFCE) fosters sustainable regional ecosystems, exemplified by the African Cyber Experts (ACE) Community. The ACE community has strengthened collaboration among cybersecurity professionals from over 30 African Union Member States.
- CREST pursues the mission to standardize cybersecurity practices globally. Through the CREST Accelerated Maturity Programme (CAMP) programmes, CREST accelerates the growth and maturity of local cybersecurity service providers in 12 countries in Europe, Africa, Asia and the Middle East.
- By becoming the secretariat of MANRS (Mutually Agreed Norms for Routing Security), the Global Cyber Alliance has ensured a stronger, more secure routing system worldwide. It achieved a 12.5% growth in participation in 2024, expanding from 1,071 to 1,190 participants.
- The Shadowserver Foundation provides daily alerts about vulnerable devices to over 9,000 organizations, such as hospitals, NGOs, schools, and critical infrastructures, enabling timely security interventions.

These efforts secure networks, empower communities, and increase resilience across sectors. Despite their impact, NGOs often operate in silos and face barriers to engagement in multilateral policy forums like the United Nations Open-ended Working Group on security of and in the use of information and communications technologies 2021–2025 (OEWG).

Challenges and Recommendations

Nonprofits encounter limited recognition, funding shortages, and bureaucratic hurdles in participating in global cybersecurity policy making processes. To harness their full potential, we recommend:

1. **Simplifying engagement processes:** Streamlining requirements for nonprofits' participation in the OEWG, like accreditation procedures.
2. **Providing financial and logistical support:** Offering hybrid options, or travel and logistical funding to encourage participation.
3. **Facilitating knowledge sharing:** Promoting solutions repositories, such as the Common Good Cyber mapping, to prevent redundancy and promote cooperation.
4. **Fostering meaningful contributions:** Holding solutions-oriented workshops and 1:1 meetings where nonprofits can present insights and share expertise on specific themes alongside national representatives.