As digital threats continue to grow in speed and sophistication, civil society cannot afford fragmented, ad hoc defenses. We require collective action—donors, volunteers, industry, and policymakers all playing a role. Together, we can sustain the nonprofits that protect the digital foundation of modern life.

—Philip Reitinger, Chair, Common Good Cyber Fund Strategic Advisory Committee; Senior Advisor and President Emeritus, Global Cyber Alliance

The Global Cyber Alliance works in favor of an Internet fostering human connection, progress, and trust. It puts in place a hands-on approach to making this vision a reality. It offers practical tools that can be used by anyone who is a target in cyberspace in order to ensure their safety.

PERSPECTIVE: Cyber Civil Society—The Internet Society

For the Common Good: Why Civil Society Needs a Digital Shield

Civil society clings to a dangerous myth: that good "cyber hygiene" will protect individuals from even the world's most powerful attackers. Human rights defenders, journalists, and NGOs are urged to use longer passwords, enable two-factor authentication, and keep their software up to date. Make no mistake, these steps are crucial. But against million-dollar spyware attacks, "hygiene" is an unlikely savior.

Too often, civil society is the first target of sophisticated state-sponsored and criminal attacks. Tactics tested on NGOs and journalists today, whether by nation-states or

(*continued*)

(*continued*)
organized cybercrime, are often unleashed on governments and infrastructure tomorrow. The imbalance is stark: unlimited adversarial budgets versus finite nonprofit resources.

This is a market failure, plain and simple. The companies entrusted with "securing the Internet" mostly secure it for those who can afford it—not out of malice, but because market incentives reward enterprise customers. To make the Internet safe for everyone, we can't keep placing the burden of defense on vulnerable or lower-resourced communities. We need a cyber civil defense: a layered ecosystem that protects the common good by default.

The first layer is the terrain itself. Security cannot be a luxury add-on that users must spend time and money to configure. We must fund and maintain critical cybersecurity infrastructure so that safety is woven into the Internet's very fabric. That means supporting open-source protocols and nonprofit infrastructure providers—the unsung heroes who help keep the Internet safe. This goes beyond encryption; it means, for example, funding the rewrite of the Internet's core code into memory-safe languages to eliminate entire classes of vulnerabilities, and supporting the large-scale sinkholing of botnets before they ever reach a user's device.

When encryption keeps our data private, and when the software we download is hardened to ensure it has never been tampered with, the burden of defense shifts from the vulnerable journalist in a conflict zone onto the infrastructure. It shifts because security is baked into the tools they rely on, effectively removing the "user error" variable entirely.

Even with the safest, most robust terrain, something always gets through. When that happens, there needs to be a safety net. Currently, support is fragmented and ad hoc: if an NGO is targeted, they may know a friendly researcher or a tech company employee who might be able to help—but personal connections aren't a sustainable strategy.

We need a scalable layer of digital first responders. It's time to weave the isolated strands of our current ecosystem—helplines, threat intelligence providers, incident response teams—into a cohesive network. This requires funding the "connective tissue" of the ecosystem—the shared standards and trusted channels that allow defenders to share data instantly rather than comparing notes months later.

When a humanitarian group is targeted, that intelligence shouldn't die in a silo; it should be analyzed and shared to protect everyone. However, sharing requires breaking the silence. The NGO community is often still too inclined to treat cyber incidents as taboo, fearing reputational damage. We must create space for nonprofits to safely discuss threats, transforming individual incidents into public lessons that harden the entire landscape.

When attackers know that targeting one organization will immediately harden defenses across many, the economics of attack begin to shift.

Let's not forget: no defense force survives without supply lines. The biggest weakness in civil society's cyber defense isn't technical—it's economic. The open-source maintainers, the helpline operators, and the policy advocates who defend the Internet are burning out because

(*continued*)

(*continued*)
funding is precarious. Round-the-clock, relentless threats cannot be fought with overly restrictive project grants that force defenders to scramble for survival rather than focus on the adversary at the gates.

To achieve resilience, we must shift from a short-term mindset to a sustainability mindset—offering long-term, unrestricted support that keeps top talent on the frontlines. The "market failure" in cyber defense won't fix itself. That's why we created the Common Good Cyber Fund: to pool resources and build the architecture that brings these layers together—infrastructure, scalable support, and advocacy to protect the vulnerable.

The result is an integrated, resilient shield for civil society. When we treat cyber defense as a public good—not a luxury item—we can build an Internet where journalists, activists, humanitarians, and civil society aren't left to fend for themselves, but are instead protected by the ecosystem we've built together.

—Joseph Lorenzo Hall, PhD; Distinguished Technologist, the Internet Society

The Internet Society is a nonprofit working toward a safe Internet for all. It helps preserve the foundations on which it was originally built and fights for global and safe access, so that it can reach its full potential as a democratic and inclusive space.