ARTICLE

Toward Inclusive and Equitable Cybersecurity Governance

KAYLE GIROUD
DIRECTOR, COMMON GOOD INITIATIVES AT GLOBAL CYBER ALLIANCE

ABSTRACT:
The digital age offers unparalleled connectivity but also exposes societies, economies, individuals, and governments to sophisticated cybersecurity risks. As Ingolf Pernice noted, cyberspace presents a Hobbesian "state of nature" where all are both potential victims and attackers. Current cybersecurity approaches, often accessible only to those with sufficient resources, exacerbate inequalities and foster inefficiencies. This article advocates for democratizing cybersecurity as a common good to enhance collective security and reduce sector-wide threats. It explores a multi-level governance framework—the "digital constellation"—which emphasizes cooperation at local, national, regional, and global levels, engaging and recognising the role of all key actors and resourcing them to foster resilient, inclusive, and secure digital environments that benefit all, particularly the most vulnerable.

Keywords: cybersecurity, internet governance, multi-stakeholder approach, digital commons

The digital age has brought unprecedented connectivity, but it has also exposed societies, economies, and governments to complex cybersecurity risks. What Ingolf Pernice noticed in 2018 is still true today: *"As everybody is a potential victim and a potential attacker in cyberspace, we find ourselves back in a Hobbesian 'state of nature' – potentially a war of everybody against everybody"*[1].

Security is an ambiguous yet recurrent theme in Internet governance debates, and prompts the question: what constitutes security in a digital world?

The motivations and security notions of cybersecurity actors vary significantly. Governments prioritize national security and economic stability; private companies focus on market demands, reputation management, and compliance; civil society advocates for privacy and transparency; international organizations seek harmonization and capacity building; and individual users strive for personal data protection and safe digital experiences.

Notably, in this Hobbesian 'state of nature', only those who can afford to be secure will feel secure. Governments, private companies, and individuals who can afford it will spend on self-defensive measures but this approach is not cost-effective.

As digital threats grow more complex and pervasive, cybersecurity can no longer be treated as a luxury accessible to a privileged few—it must be democratized for the common good. Democratizing cybersecurity offers significant benefits across industries. Investing in cybersecurity at scale not only strengthens individual organizations but also reduces risks across entire sectors, creating a form of "herd immunity" against cyber threats. For instance, the Let's Encrypt initiative provides free SSL certificates, enabling countless organizations to adopt HTTPS without barriers. This global improvement in web security has lowered operational costs while enhancing compliance and reducing reputational damage. In this era, democratizing cybersecurity is not just a social responsibility but a strategic investment with substantial financial and operational benefits.

Rather than focusing solely on digital sovereignty or international cooperation, what is needed is a global constitutional approach to governance and regulation, rooted in digital competence, resilience, and diligence.

Ingolf Pernice referred to this as the 'digital constellation'[2] — a multi-level approach relevant to the entire globalized society:

- Local Level: Cybersecurity tools, services, and platforms for the public interest empower individual users and businesses for self-protection, digital literacy, and resilience.
- National Level: States create legislation, establish cybersecurity agencies, and foster public-private partnerships.
- Regional Level: Bodies such as the European Union harmonize cybersecurity policies and set collective standards, including cybersecurity-by-design principles enforced through regulations like the Cyber Resilience Act (CRA).
- Global Level: Multi-stakeholder mechanisms, international organizations, and global treaties facilitate cooperation.

Effective multi-level cybersecurity governance depends on the interaction and synergies between diverse actors. As core principles, this cybersecurity

1 PERNICE, I. (2018) 'Global cybersecurity governance: A constitutionalist analysis', Global Constitutionalism, 7(1), pp. 112–141. doi:10.1017/S2045381718000023.

2 PERNICE, I. (2018) 'Global cybersecurity governance: A constitutionalist analysis', Global Constitutionalism, 7(1), pp. 112–141. doi:10.1017/S2045381718000023.

governance is based on shared responsibility, recognizing the roles of every key actor. Understanding the roles and dynamics of key actors is therefore critical for policy development and resilience-building as cybersecurity threats become more sophisticated and global in scope.

As noted by Philip Reitinger and Stephane Duguin, the collective imagination thinks for-profit companies like Apple, Google and Microsoft are responsible for keeping digital ecosystems together[3]. However, Big Tech represents just one piece of the puzzle. A significant portion of securing the Internet is shaped and sustained by a wide network of nonprofit organizations. These groups hold substantial digital space and play a crucial role in maintaining the Internet's backbone by establishing technical standards, developing open-source software, and creating tools that boost efficiency, streamline processes, and ensure dependable performance. Together, they form a dedicated ecosystem safeguarding the Internet's foundation and individual users. They safeguard digital spaces and ensure secure operations:

- Securing the Digital Commons – Domain Name System, Routing: global initiatives like MANRS (Mutually Agreed Norms for Routing Security) and Domain Trust ensure that the common digital infrastructure we all rely on is maintained and secured.

- Threat Analysis: The Shadowserver Foundation, ATT&CK, and Cyber Threat Alliance help identify and mitigate threats at scale, reducing risk for all.

- Emergency Response: The Access Now Digital Security Helpline and FIRST (Forum of Incident Response and Security Teams) provide vital support during cyber incidents.

3 REITINGER, P., DUGUIN, S. (2024), 'The Internet's Defenders Are Running Out of Money—And We're All at Risk', International Business Times. https://www.ibtimes.com/internets-defenders-are-running-out-money-were-all-risk-3749592

- Capacity Building: Initiatives like GCA Cybersecurity Toolkits offer accessible resources, while CyberPeace Builders match technical expertise with mission-driven organizations.

- Workforce Development: Initiatives like CREST Accelerated Maturity Programme (CAMP) speed up the growth and sophistication of local cybersecurity service providers, ensuring a global availability of skills.

The 'digital constellation' governance offers flexibility, resilience, and inclusivity. Understanding and recognising the role of all key actors is critical to its success. However, other challenges persist, notably resource disparities and coordination difficulties.

Large technology firms possess vast resources, while smaller states, nonprofits, and individuals often lack adequate cybersecurity protections, creating systemic vulnerabilities.

Addressing this gap requires a shift toward an equitable cybersecurity market and providing sustainable resources to key actors. As highlighted by Philip Reitinger and Stephane Duguin, and demonstrated by the Common Good Cyber knowledge hub, nonprofit organizations and volunteers play a crucial but often overlooked role in maintaining critical cybersecurity services and tools, and in empowering individual users and businesses through the deployment of the majority of existing cybersecurity tools, services, and platforms for the public interest. Despite their essential contributions, nonprofits are frequently underfunded. To ensure equitable and democratized cybersecurity, sustainable funding models for cybersecurity nonprofits must be prioritized.

As cyber threats continue to evolve, fostering a cybersecurity governance model that harnesses the strengths of diverse actors is crucial. By embracing a multi-stakeholder approach that includes public actors, private companies, civil society, and empowered individuals, Europe and the global community can build a secure, resilient, and inclusive digital environment that benefits all, especially the most vulnerable. Marina Kaljurand, Member of the European Parliament aptly noted, *"just as we view clean air, water, and a peaceful society as essential to all, cybersecurity must be seen as a global common good, critical for the stability of peace and justice"*[4].

4 KALJURAND, M. (2024), '"Cybersecurity must be seen as a global common good," says MEP Marina Kaljurand', Common Good Cyber. https://commongoodcyber.org/news/marina-kaljurand-speech/

About the author:

Kayle Giroud is a project management professional based in Brussels, Belgium. With a rich international background and several years of experience in international cooperation working for the United Nations, the Swiss Federal Department of Foreign Affairs, and various organizations, Kayle has developed an expertise on cybersecurity and a passion about the impact of emerging technologies on society and fundamental rights. Currently, she serves as the Director for the Common Good Initiatives at the Global Cyber Alliance.

Kayle is pursuing a PhD in contemporary history at the University of Bordeaux. She holds an Advanced Master in Interdisciplinary Analysis of European Construction and a B.A. in Political Science from UCLouvain Saint-Louis-Brussels, an MSc in Defense, Development and Diplomacy from Durham University, a PMI PMP® Certification, and a ISC2 Cybersecurity Certification®.