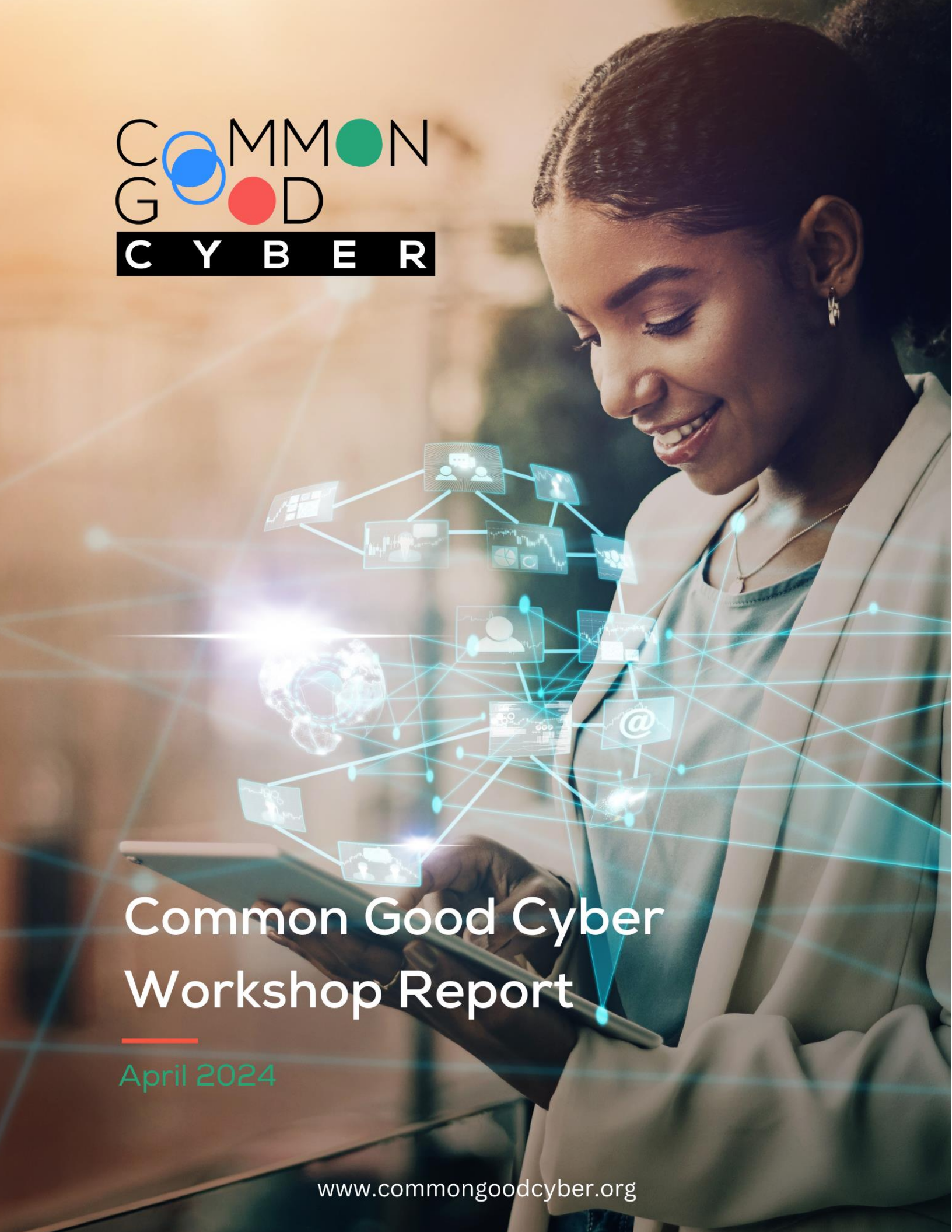


COMMON GOOD CYBER

Common Good Cyber Workshop Report

April 2024

www.commongoodcyber.org

Background and Executive Summary

The Common Good Cyber initiative is focused on taking concrete steps to collectively address the challenge of sustaining the nonprofit and public interest organizations involved in critical cybersecurity functions for the broader Internet community. In February 2024, the Cyber Threat Alliance, the CyberPeace Institute, the Forum of Incident Response and Security Teams (FIRST), the Global Cyber Alliance, the Institute for Security and Technology (IST), and the Shadowserver Foundation hosted a workshop at the National Press Club in Washington, D.C., United States, launching the Common Good Cyber initiative.

At the workshop, over 100 stakeholders representing government (United States, Canada, Switzerland, Singapore), multilateral organizations (World Bank, OAS, and OECD), civil society (CREST, OWASP, Global Forum on Cyber Expertise), foundations (Craig Newmark Philanthropies, Gula Tech Adventures, Schmidt Futures), business (Cisco, Google, Mastercard, and Microsoft), academia (Columbia University and Carnegie Mellon University) and more than 200 people online convened to discuss the systemic underfunding of cybersecurity nonprofits and the best approaches to sustainably funding those organizations.

Key Workshop Metrics

- Number of Total Attendees: 114
- Number of Attendees representing government: 15
- Number of Attendees representing the private sector and the industry: 25
- Number of Attendees representing foundations or other funders: 6
- Number of attendees representing nonprofits: 66
- Number of attendees representing academia: 2

The workshop was divided into two key parts. The first part of the workshop was designed to ensure a holistic understanding of the need to find sustained funding and resources for those organizations working to maintain core cybersecurity capabilities. The second part of the workshop was to identify tangible solutions to address this need, and to outline the underlying challenges, parameters, and stakeholders necessary to keep in mind to achieve their mission.

Organized to hear as many perspectives as possible, the workshop confirmed the original hypothesis[1]: there are organizations operating on razor-thin budgets or through the support of volunteer networks that are significant contributors to maintaining the availability and security of the Internet.

[1] For more details, please refer to our first workshop pre-brief: "Cybersecurity for the Common Good: The Imperative for Sustainable Mechanisms", available online: https://commongoodcyber.org/wp-content/uploads/2024/02/Pre-Brief-1_The-Imperative-for-Sustainable-Mechanisms.pdf.

The discussions also covered the potential mechanisms[2] through which these organizations could be better supported. There is support for building the business case for those cybersecurity organizations supporting the common good in cybersecurity; the need to develop an accelerator model - or resource hub - to support capacity needs; and establishing a joint funding effort - including one or both building a joint fund and creating joint fundraising capabilities, sustained by multiple different donors - that would have an established governance and criteria for fund distribution.

The workshop concluded with a call for a long-term, collaborative joint funding effort in cybersecurity. This would involve bringing together a diverse range of stakeholders, including government, private sector, and civil society, in the decision-making process.

Key Workshop Outcomes

As a result of the workshop, three solutions were identified:

1 - Raising our understanding and building a business case by mapping the cybersecurity nonprofit and public interest organization ecosystem to document what service they provide, who depends on that service to demonstrate their contribution to maintaining global and regional cybersecurity, and what the economic impact would there be if one or more of these services failed or ceased to exist;

2 - Delivering capacity support and acceleration for cybersecurity nonprofits and public interest organizations, by offering services like or training regarding marketing, joint fundraising, and grant writing that often fall outside of their core mission;

3 - Establishing a joint funding mechanism - including one or both joint fund and joint fundraising capabilities and sustained by multiple different donors – that would have an established governance and criteria for fund distribution to maintain critical cybersecurity functions for the broader Internet community.

Key Initiative Next Steps

Get involved!

1 - Support the creation of a roadmap – a work plan with detailed milestones – that will drive forward the efforts.

2 - Mobilize volunteers and funders to advance the goals of Common Good Cyber.

3 - Raise awareness about challenges in maintaining core cybersecurity capabilities and share progress as the initiative evolves.

This report offers an overview of the key discussion points during the workshop, including outstanding questions and next steps. Note that panels were on the record[3] and all breakout discussions were under Chatham House rule. The report reflects this.

For a full agenda highlighting the talented speakers and sessions at the workshop, please click here[4].

[2] For more details, please refer to "Cybersecurity for the Common Good: A Survey of Potential Solutions", available online: https://commongoodcyber.org/wp-content/uploads/2024/02/Pre-Brief-2_Potential-Approaches.pdf

[3] For watching the panel recordings, wrap-up video, and various interviews of experts, please visit our YouTube Channel: https://www.youtube.com/channel/UCCCX1n7Ni8gPGGi6WBSxhog

[4] Common Good Cyber February 2024 Workshop Agenda, available online: https://commongoodcyber.org/wp-content/uploads/2024/02/Common-Good-Cyber-February-Workshop-Agenda-1.pdf

Acknowledgements

This effort would not have been possible without the generous support of the Embassy of Canada to the United States, who hosted the initial brainstorm for this workshop, to Craig Newmark for his dedication to the Cyber Civil Defense coalition through which this idea first happened, and to the Cyber Threat Alliance and the Chertoff Group who helped sponsor the Common Good Cyber Workshop at the National Press Club in Washington D.C.

We extend our sincerest gratitude to the Secretariat of Common Good Cyber for their unwavering dedication and commitment to advancing the cause of cybersecurity for the common good. This initiative, coordinated by the Global Cyber Alliance, has been made possible through the collaborative efforts through a Secretariat of numerous organizations who have contributed their expertise, resources, and passion towards this noble endeavor: the Cyber Threat Alliance, the CyberPeace Institute, the Forum of Incident Response and Security Teams (FIRST), the Global Forum on Cyber Expertise (GFCE), the Institute for Security and Technology (IST), the Shadowserver Foundation, and the Canadian Centre for Cyber Security.

Setting the Stage

The Common Good Cyber Workshop kicked off with a keynote address by Kemba Walden, president of Paladin Global Institute.

Ms. Walden's speech highlighted that the Internet has become a public good. It enables societies to communicate, fight pandemics and provides avenues to advance human rights and fight climate change. As a result, securing the Internet is key to the prosperity of societies. She concluded that the reliance on civil society – the groups, organizations, and individuals– operating on razor-thin budgets to help protect the security of the Internet is unsustainable and the cost of doing nothing to address this problem is too high. Her remarks set the stage for the rest of the workshop.

> *"Nonprofits are key elements of civil society in pursuit of a safe, secure Internet. But they are doing that work with a razor-thin budget and uncertain funding. [...] The objective of Common Good Cyber is to find new ways to build adequate funding sufficient to move the common need for cybersecurity. Today we aim to find and identify tangible action, and while we do, please consider the cost of not doing something!"*
> — Kemba Walden, Paladin Capital Group[5]

Illustration of the Problem

Part One of the workshop focused on dissecting the problem from the perspective of nonprofits, government, and academia. During the initial break-out session and panel discussions, several key points were raised related to external and internal challenges:

External Challenges

(1) Funding awarded often has a short term horizon or is focused on new solutions, rather than sustaining existing ones that work.
(2) While funding shortfalls are a familiar hurdle across the nonprofit landscape, cyberthreats do not respect traditional borders and cooperation mechanisms. This means that responding to cyberthreat challenges requires global cooperation and new approaches to resource sharing to ensure the security of the Internet is maintained for the common good.
(3) Challenges to promoting global collaboration are exacerbated by a disconnect between those nonprofits providing cybersecurity for the common good and potential funders of those solutions. Foundations and governments often build milestones that are not in line with actual

[5] For more information from Kemba Walden, please watch her interview available online at: https://www.youtube.com/watch?v=5TR8CoGtebo

needs served by the cybersecurity nonprofit and public interest organizations. It was highlighted that grant managers often do not have the technical expertise to evaluate the cybersecurity initiatives they are meant to fund, creating confusion between the funder and the funded.

(4) Many nonprofits and civil society organizations offer similar cybersecurity services and from the funders perspective there is lack of clarity as to what differentiates them.

Internal Challenges

(1) Nonprofits and civil society organizations often lack the in-house talent needed to pursue funding opportunities and often require such a high level of effort that diverts resources away from their core mission. Nor do they have the resources to tailor their marketing to each prospective funder or hire human capital to manage reporting requirements associated with each awarded grant or contract. Some estimated that responding to grant applications and meeting the varied reporting requirements of different funders can consume up to 30 percent of their resources.

(2) The short-term horizon of awarded grants forces nonprofits and civil society to constantly be chasing the next grant or funding opportunity, diverting resources away from their core mission.

(3) Available funding is often focused on specific key performance indicators that do not necessarily align with nonprofit missions, potentially leading to mission drifts.

(4) Nonprofits and civil society organizations need to strengthen their collaboration to create more effective initiatives and/or projects to advance cybersecurity for the common good.

"We also need to clean our front doors. A lot of civil society organizations are in competition to reach funders and should be better at cooperating to build a stronger business case to go to funders and make it happen."

- Stéphane Duguin, CyberPeace Institute[6]

"MITRE is a research-focused organization. The funding for ATT&CK comes directly at the expense of another research. We're supposed to be always moving on, looking at the next thing and tackling the next problem. By focusing so many resources on ATT&CK - because it has become an essential infrastructure to so many entities - it undermines MITRE's ability to deliver on its greater mission, so it creates a tension which puts the sustainment of ATT&CK at risk."

- Jon Baker, MITRE

[6] For more information from Stéphane Duguin on this topic, please watch his interview available online at: https://www.youtube.com/watch?v=-HxXCO_Ge30

The Funders' Perspectives

In a Fireside chat, representatives from various funding organizations– Gula Tech Adventures, a former Hewlett Foundation representative, Craig Newmark Philanthropies, and Google.org– shared their perspectives on what incentivizes funders to contribute to cybersecurity and what funders look for in their grantees. Several themes emerged from their conversation:

A) Responsibility, Collaboration, and Partnership: Achieving cybersecurity at scale or for the common good requires a collective, whole-of-society effort, meaning there needs to be more collaboration between funders, organizations, governments, and individual citizens.

   Funders see value in working together to achieve common goals, recognizing both the role of industry initiatives - like those from Google.org with the Cybersecurity Clinics - and the potential benefits of government funding.

   Craig Newmark also stressed individual responsibility, urging people to take proactive measures like installing updates. Through the Cyber Civil Defense initiative, Newmark framed cybersecurity as a form of modern patriotism, where public awareness and advocacy become ways to defend a nation.

B) Sustainability and Scalability: Historically, the Hewlett Foundation played a critical role in funding cybersecurity nonprofits. Part of its grantmaking activities focused on strengthening organizations' ability to be self-sustaining. That legacy remains in current investments funded by others, including Google.org, with a further focus on the importance of scale. To encourage self-investment and fuel entrepreneurship, Ron Gula pointed out the need for a more accessible "public exit" for cybersecurity organizations to keep the landscape competitive, given that competition can also be a driver of innovation.

C) Money is one aspect among others: Most funders reported doing more than providing funds for their grantees, like increased visibility or guidance on how to attract more funders in the future.

D) Diversity and Inclusivity: Funders echoed the global acknowledgment that the cybersecurity profession needs more diversity amongst underrepresented groups, but also that the work of cybersecurity organizations must also focus on strengthening the cybersecurity resilience of these communities and groups.

"A lot of the cyber startups solve the same problems that the cyber nonprofits do. [...] They have to be very specific on what problem they solve, how they solve it, including proof of what they've done, what they're going to do with that money, and what their vision of

success looks like. Those are the five things we typically ask these cyber nonprofits, and they are the same questions we ask to startups."
- Ron Gula, Gula Tech Adventures

"One of the types of grants the [Hewlett Foundation] cyber initiative would offer grantees were 'Organizational Effectiveness grants' which complimented an existing grant for them to strengthen capacity in areas such as communications; fundraising; and diversity, equity, and inclusion. This was a way for grantees to build strengths across different operational areas and ultimately become more sustainable beyond the grant they received to conduct their cyber-related work."
- Monica M Ruiz Forscey, Microsoft and formerly at the Hewlett Foundation

Potential Solutions and Solutions Deep Dive

Part Two of the workshop delved into the potential models that can address the resource gap for cybersecurity nonprofits and public interest organizations. To inform the conversation, the examination began with a panel where leaders of existing multi-stakeholder efforts addressed other funding mechanisms used for other global and complex issues, like health, human rights, and affordable housing. This discussion informed subsequent conversations about potential solutions that could be applied to cybersecurity given the challenges discussed in part one, which resulted in participants coalescing around four (4) models that the group concluded might best support the sustainability of cybersecurity nonprofits and public interest organizations. Those four models are (not in order of support):

(1) **Building the Business Case**: Map the ecosystem of cybersecurity nonprofits and public interest organizations, including areas in which they work and documenting how they contribute to the security of the Internet, and develop the evidence base and storytelling for the value these organizations bring to global Internet users, quantify the financial need, and evaluate the effectiveness of the approach Common Good Cyber develops in collaboration with its partners.
(2) **Accelerator/Resource Hub**: Provide services and tools and build capacity to cybersecurity nonprofits and public interest organizations addressing capabilities that are not part of the nonprofits' core missions, for instance marketing, stakeholder engagement, or grant writing.
(3) **Establishing a Joint Fund**: Develop a global fund to assist in supporting common good cybersecurity activities that are essential to maintain, including building an understanding of the legal requirements to set up a fund that is supported by multiple different donors and includes public, private and civic voices. The goal of the fund would be to provide a venue for long-term sustainable funding, rather than short-term grants that, while helpful, do not provide organizational stability. As part of this effort, it will be key to develop a multistakeholder governance structure to manage the fund, ensuring transparency and accountability, while also creating a set of criteria for fund allocation.

(4) **Joint Fundraising**: Establish a means through which cybersecurity nonprofits and public interest organizations can combine resources to pursue funding or grant opportunities together, amplifying their ability to support cybersecurity development in the public interest and capacity building, globally.

The following considerations and observations were raised throughout the workshop, as critical pieces that need to be evaluated or addressed to advance any output Common Good Cyber undertakes:

1. Strengthen the Community's Story:

Securing funding for cybersecurity initiatives requires a strong and articulate story. At present, the cybersecurity nonprofit and public interest community do not have a compelling narrative that clearly articulates the value proposition and societal impact. This is particularly true for garnering support from the non-technical communities. Mapping of existing services, and how they advance global Internet resilience would support this effort.

Critical to building the narrative will be developing specific goals, measurable metrics, and sharing real-world experiences about how these organizations are concretely helping to maintain the security of the Internet. Together, these efforts will help persuade a range of different stakeholders to invest in cybersecurity efforts, by demonstrating value via messages that resonate with specific audiences.

> *"Data is key. By understanding the threat landscape, we can identify where governments should invest and where nonprofits can provide support. This data can then be used to develop a self-sustaining business model for cybersecurity solutions. Finally, clear communication with policymakers is essential. Nonprofits need to effectively articulate the benefits they provide and the potential consequences of inaction."*
> - Florian Schuetz, Swiss Federal Office for Cyber Security and OECD Working Party on Digital Security

---

> *"First thing is framing. To call 'human trafficking', 'modern slavery' mobilized political will fight it. [...] Finally, leveraging data to show the extent of the problem and prove the intervention is working is essential to sustain political will for the Global Fund to Fight AIDS, Tuberculosis and Malaria".*
> - Mark Lagon, Friends of the Global Fight Against AIDS, Tuberculosis and Malaria

---

> *"Cyber is horizontal. It cuts across all sectors. Some funders will get that. Many won't, and will say how does this touch my vertical, such as health or climate change? So, we need both an overarching business case and vertical sector-based ones".*
> - Eli Sugarman, Schmidt Futures

2. Trust, Transparency, and Accountability

The workshop underscored the importance of trust, transparency, and accountability in cybersecurity efforts. Building trust between stakeholders, ensuring transparency in joint funding, and maintaining accountability in resource allocation were all highlighted as crucial for advancing any of the models discussed as part of Common Good Cyber.

> *"The number one thing is that there must be trust and transparency. To have that, you must have clear mission statements, clear governance models, clear charters, clear ethics statements— those are all critically important."*
> - Chris Painter, GFCE

3. Capacity Building and Acceleration

Capacity building and acceleration for nonprofits in the cybersecurity space were both mentioned as needs of the community. Both activities would offer access to resources to help organizations sustain their cybersecurity initiatives, while also supporting their growth. The community highlighted the need for strategic and infrastructural support, and the discussions explored ways to categorize different organizations based on specific needs of each organization to ensure the acceleration model brings the right resources to meet the needs of nonprofits and public interest organizations supporting core cybersecurity capabilities.

4. Foster Collaboration and Partnerships

The workshop highlighted the success of models like the Global Fund and the Global Equality Fund, where governments, the private sector, NGOs, and civil society work together to build funding to address complex global challenges. These cross-sector initiatives showed how a holistic approach, taking into consideration all the sectors impacted by cybersecurity will help grow the momentum in other fields. Aligning cybersecurity initiatives with broader global goals – like addressing climate change or other transboundary challenges – will build synergies across sectors and offer the opportunity to tap into resources that are earmarked for other global challenges (global health, climate change, etc.), yet are dependent on the availability and security of the Internet.

Additionally, cybersecurity nonprofit and public interest organizations need to partner more strategically to advance each other's contributions. Collaborative funding models, such as joint funds and federated giving, can incentivize those partnerships and disincentive duplicative efforts.

5. Advocate for Policy Support

Achieving cybersecurity success hinges on strong support in policy and from policymakers. The workshop emphasized the need for advocacy efforts to raise awareness and garner support from policymakers and funders, while acknowledging that many of the cybersecurity nonprofits and public interest organizations are registered in the U.S. as 501(c)(3) and therefore are legally limited in their ability to advocate for policies. An appropriate approach for policy advocacy must be considered as part of the next steps.

Educating policymakers about cybersecurity threats, opportunities, and solutions is crucial for securing the resources needed to build a robust defense system. Effective advocacy campaigns, educational initiatives, and strategic communication efforts can significantly increase awareness about cybersecurity issues and solutions, paving the way for supportive policies and frameworks that incentivize investments and foster public-private partnerships in this critical domain.

6. Long-term, Collaborative Joint Funding Effort

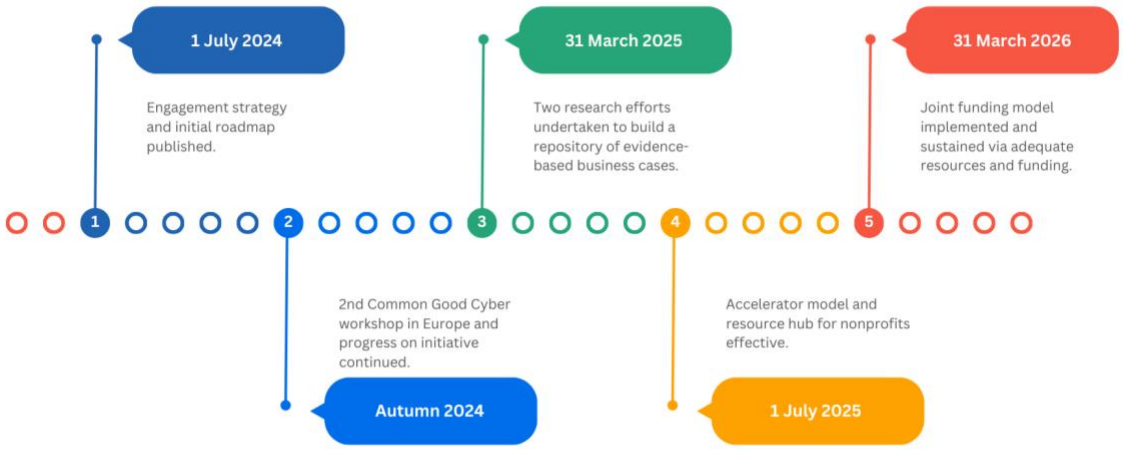
Recognizing the inefficiencies and fragmentation within the cybersecurity funding landscape, the workshop stressed the need for a more coordinated approach. Aligning funding efforts would ensure resources are used strategically, minimizing duplication, and maximizing impact.

Conclusion and Next Steps

1. Execution Plan

The immediate next step requires elaborating on the initial governance for the Common Good Cyber Initiative, with roles and responsibilities outlined. This will be discussed and moved forward by the Common Good Cyber Secretariat. Establishing clear roles and responsibilities will enable the creation of a roadmap – a work plan with detailed milestones – that will drive forward efforts to achieve the goals of Common Good Cyber.

High-level milestones that will need to be detailed are as follows, with notional and aggressive dates suggested:



2. Outreach and Engagement

Collaboration is key. The next steps involve mobilizing volunteers or funders to advance the goals of Common Good Cyber. Simultaneously, Common Good Cyber will continue to engage stakeholders from various backgrounds to ensure buy-in and contributions from a “big tent” of global actors. Engaging with policymakers and government agencies will be crucial to garner broader support and secure resources for long-term impact.

3. Advocacy and Awareness

The workshop highlighted the need for ongoing awareness efforts within the cybersecurity community and beyond. Building a shared understanding of the ecosystem and fostering a culture of continuous adaptation will equip this community to address the ever-evolving cybersecurity landscape. This will also feed into creating a persuasive narrative that resonates with different audiences, whether they come from various sectors or regions of the world where priorities and incentives differ.

To achieve this, we will keep the momentum on raising awareness about the challenges met by nonprofits and public interest organizations in maintaining core cybersecurity capabilities, and sharing progress as the models evolve at various cybersecurity events.

The next confirmed speaking engagement includes a spotlight talk at the European Cyber Agora in Brussels on April 23, 2024, and a panel at RSA 2024 in San Francisco on May 6, 2024. There will be a dedicated event to be confirmed in Europe before the end of the year.

Get involved!

Key Initiative Next Steps

- ⇒ Support the creation of a roadmap – a work plan with detailed milestones – that will drive forward the efforts.
- ⇒ Mobilize volunteers and funders to advance the goals of Common Good Cyber.
- ⇒ Raise awareness about challenges in maintaining core cybersecurity capabilities and share progress as the initiative evolves.

Reach out to the Secretariat at commongoodcyber@globalcyberalliance.org to express your interest in getting involved in the execution of this initiative and where you and your organization can best contribute. We also encourage you to sign up to receive the latest news here.