Closing the Cyber Capacity Gap in Digital Financial Inclusion: A Critical Analysis of Prevailing Narratives and Approaches

Nanjira Sambuli and Aditi Bawa

This is a non-final preprint version of a forthcoming chapter from "Responsible behaviour in cyberspace: Global narratives and practice (forthcoming/2023) edited by François Delerue, Arun Sukumar and Dennis Broeders. EU Cyber Direct / EU Publications Office."

Introduction

In discussions about governing cyberspace, cyber diplomacy, and digitalization more broadly, it is common to find capacity building and/or development highlighted as either a challenge, opportunity, or recommendation. This is especially so regarding developing countries. Capacity building as a definitional concept in international development traces its origins in the mid 1990s, when shortcomings were identified in the prevailing approaches to development aid and technical assistance, in place since the 1950s. The lack of domestic ownership, shortcomings in tailoring aid delivery to local demand signals, poor coordination, and the inability to effect sustainable change are among some of the issues identified as perceived failings of the 'traditional' approach.[1]

Capacity building is sometimes conflated with, and other times distinguished from capacity development.[2] The Organization for the Economic Cooperation and Development (OECD) defines capacity development as "the process whereby people, organizations and society as a whole unleash, strengthen, create, adapt and maintain capacity over time." The United Nations Development Program's (UNDP)[3] definition is similar to OECD's and distinguishes capacity development from capacity building by noting that the latter is a "process that supports only the initial stages of building or creating capacities and assumes there are no existing capacities to start from." While this is an important distinction to note, the terminology is less vital than the concept itself. For the purposes of this paper, we will be using cyber capacity building and development interchangeably.

---

[1] *Understanding Capacity-Building/Capacity Development: A Core Concept of Development Policy* (France: European Parliament, 2017) https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/599411/EPRS_BRI(2017)599411_EN.pdf

[2] *Perspectives Note: The Enabling Environment for Capacity Development (*The Organization for Economic Cooperation and Development, France: 2008), https://www.oecd.org/development/accountable-effective-institutions/48315248.pdf

[3] *Capacity Development: A UNDP Primer (New York:* United Nations Development Program, 2015),https://www.undp.org/publications/capacity-development-undp-primer

As the internet and ICT for development space emerged in the early 2000s, international conversations naturally turned to capacity building. Cyber capacity building is often approached through a development angle, so in the mid-2000s actors from technologically advanced countries initiated cross-border mechanisms to assist countries and organizations in maintaining a safe, secure, and open use of the digital environment.[4] For international organizations and partnerships to prioritize cyber capacity development concurrent to the digital space's creation itself shows a clear initiative to expand the benefits of cybersecurity. According to the Open-ended Working Group[5] (OEWG) report, cyber capacity building/development is useful to help develop the necessary social capacities — skills, human resources, policies, and institutions—that enable a more secure, stable, and resilient ICT environment. The report further recognizes that the capacity of each state to prepare for and respond to emerging cyber threats informs the international community's collective ability to do the same.

Capacity-building/development recommendations are typically centered around training efforts for financial regulators, technical individuals, not for profit institutions and end users. But other needs may be equal to or greater than training, for example, sustained institutional funding. And, within training programs, there might be underappreciated need to include underrepresented groups. A critical reading of these calls for capacity building highlights that it is not entirely clear for whom capacity is being developed, if it is demand-driven, or based on contextual needs analysis, or even what exactly counts as successful capacity building. Furthermore, literature is yet to show how cyber capacity building works in practice; it also does not explore unintended consequences of prevailing approaches or areas where changes in approach could be beneficial. For instance, it is difficult to ascertain which training approaches work well in environments where technological leapfrogging presents novel cybersecurity challenges.

Increasingly, there are also geopolitical connotations to consider when thinking about cyber capacity building. For example, the U.S. and EU recently created a plan to support critical infrastructure technology in developing countries. This initiative is being framed as assistance to 'counter China'[6] and dissuade countries from accepting China's support, as well as to defend digital democracy.[7] Elsewhere, cyber capacity building initiatives supported by the U.S. government speak of "helping establish the U.S. as the cyber development partner-of-choice in

---

[4] Robert Collett, "Understanding Cybersecurity Capacity Building and its Relationship to Norms and Confidence Building Measures," *Journal of Cyber Policy* 6, no. 3 (Summer 2021): 298-317, https://www.tandfonline.com/doi/full/10.1080/23738871.2021.1948582

[5] Open Ended Working Group, *Open Ended Working Group on Development in the Field of Information and Telecommunications in the Context of International Security* (Geneva: UN General Assembly, 2021), https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[6] Catherine Stupp, "U.S., EU Plan Joint Foreign Aid for Cybersecurity to Counter China," *The Wall Street Journal,* https://www.wsj.com/articles/u-s-eu-plan-joint-foreign-aid-for-cybersecurity-to-counter-china-11655285401

[7] Matthew Gooding, "US and EU Could Fund Cybersecurity Improvements in Developing Countries," *TechMonitor* https://techmonitor.ai/policy/geopolitics/us-eu-cybersecurity-china-russia

areas contested by China and Russia".[8] This framing further complicates how cyber capacity building supply matches local demand, as technological great power competition may not be a priority for developing countries.[9]

This paper aims to help proponents and providers of capacity building to better understand what capacities and resources various constituencies in developing countries most need. This may not be what supply-driven capacity-building programs often provide. The paper is informed by the authors' ongoing work to coordinate global efforts to advance cybersecurity as a priority consideration in digital financial systems, with a special focus on cybersecurity considerations for digital financial ecosystems across Africa. Digital financial inclusion is a key driver of digital technology adoption across the continent. Through experience gained by leapfrogging legacy infrastructure and systems and contextually adapting varied technologies to connect the unconnected, Africa has a lot to contribute to prevailing discourses on capacity-building based on the fast-growing fintech sectors in several countries. Furthermore, fintech and digital financial inclusion developments intersect uniquely with other digital development goals such as access to education, health, reliable energy and more, therefore gains made in clarifying what capacity building entails in these dynamic digital finance environments could have far-reaching benefits across other domains. Enhanced and nuanced understanding of capacity-building challenges in developing and emerging markets can help elevate everyone's contributions to the global governance of cyberspace and digital technologies.

Cyber, capacity and the financial system: insights from the FinCyber Strategy

The financial sector has been particularly attuned to cyberspace's opportunities and threats. Following a series of cyber-attacks that laid bare systemic risks that cyberspace poses to financial stability, stakeholders worked together towards a strategy for the international community to better protect itself against cyber threats.[10] Capacity building was identified —alongside cyber resilience, cyber workforce challenges, as well as international norms and collective response mechanisms— as a priority in the resulting "FinCyber" strategy.[11] As noted in the strategy report, 'Cybersecurity capacity-building has therefore become a growing priority, especially considering the rising

---

[8] Bill Eidson, "MITRE Strengthens Cyber Capacity of Developing Nations," *MITRE,* December 2019, https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations

[9] David Ehl, "Africa embraces Huawei technology despite security concerns," DW February 8, 2022. https://www.dw.com/en/africa-embraces-huawei-technology-despite-security-concerns/a-60665700.

[10] Tim Maurer and Arthur Nelson, *International Strategy to Better Protect the Financial System Against Cyber Threats* (Washington, DC: Carnegie Endowment for International Peace, 2020). https://carnegieendowment.org/2020/11/18/priority-5-capacity-building-pub-83113

[11] The project was led by Carnegie and comprised an international advisory group as well as inputs by over 200 stakeholders. Carnegie Endowment for International Peace, "FinCyber Strategy Project: Cybersecurity and Financial Inclusionhttps://carnegieendowment.org/specialprojects/fincyber/financialinclusion/

numbers of state-sponsored attacks and the increase in fraud during the coronavirus pandemic. At the same time, "capacity-building" is an amorphous term and requires clarification before anyone can progress from concept to action'.[12]

Existing international cyber capacity building recommendations and initiatives for the financial system vary. They encompass efforts to increase financial institutions' cyber resilience and strengthen law-enforcement, supervisory and regulatory capacity.[13] Others include providing resources and coordination centers to support information sharing and cybersecurity coordination to bolster cybersecurity norms,[14] as well as private sector driven capacity building through training and education for clients.[15] These efforts are increasingly targeted at low-income and developing countries, recognizing that regions like Africa have also seen a surge in cybercrime activities.[16] Furthermore, given the variance of financial systems in Africa, where mobile technology has been a key driver of financial inclusion, the cybersecurity and cyber resilience framing expands beyond traditional financial systems such as banks.[17] The nexus of financial inclusion and cybersecurity requires capacity builders with expertise on financial inclusion as well as cyber security to ideally coordinate their efforts in ways that will bolster cyber capabilities for digital financial inclusion.

Cyber capacity building efforts for digital financial inclusion —that the authors are observing through an ongoing project dubbed 'CyberFI'[18] — typically comprise 'top-down' development sector approaches to supporting developing countries. That is, capacity is considered to come from the developed markets, to be passed along to developing countries. This is noted in the concentration of trainings as a focus for capacity building, as well as the overwhelming reference to capacity building, rather than capacity development. The latter would proceed more from the ground up and incorporate the insights and practical expertise of intended beneficiaries. Furthermore, cyber capacity building for developing countries would factor in the reality that many

---

[12] Tim Maurer and Arthur Nelson, *International Strategy to Better Protect the Financial System Against Cyber Threats* (Washington, DC: Carnegie Endowment for International Peace, 2020). https://carnegieendowment.org/2020/11/18/priority-5-capacity-building-pub-83113

[13] Cyber Resilience and Financial Organizations: A Capacity Building Toolbox," Carnegie Endowment for International Peace, 2021, https://carnegieendowment.org/specialprojects/fincyber/guides

[14] Silvia Baur-Yazbeck and Jean-Louis Perrier, , "Regional Center Can Help Low-Income Countries Build Cyber Resilience," *CGAP,* July 8, 2020. https://www.cgap.org/blog/regional-centers-can-help-low-income-countries-build-cyber-resilience

[15] "Helping Customers Strengthen Their Cyber Defences," SWIFT https://www.swift.com/myswift/customer-security-programme-csp

[16] Staff Reporter, "There Are More Cyberattacks in Africa Than Anywhere Else," *WeeTracker,* January 12, 2022, https://weetracker.com/2022/01/12/there-are-more-cyberattacks-in-africa-than-anywhere-else/

[17] Nanjira Sambuli and Taylor Grossman,, ,"Introducing CyberFi: Perspectives on Cybersecurity, Capacity Development, and Financial Inclusion in Africa", Carnegie Endowment for International Peace, May 2, 2022, https://carnegieendowment.org/2022/05/02/introducing-cyberfi-perspectives-on-cybersecurity-capacity-development-and-financial-inclusion-in-africa-pub-87001

[18] Carnegie Endowment for International Peace, "Securing Digital Financial Inclusion," https://carnegieendowment.org/programs/technology/securingDigitalFinancialInclusion

are primarily focused on advancing a domestic agenda of digital inclusion before prioritizing cybersecurity, even as technological leapfrogging introduces vulnerabilities.[19]

There are ongoing efforts on knowledge dissemination and resource mapping with the aim of improving coordination and collaboration between disparate cybersecurity and digital financial inclusion stakeholder groups. Typical stakeholder groups targeted by cyber capacity building endeavors include developing country governments and their cybersecurity capacity at the national level; financial institutions and their organizational and clients' cyber security; as well as small businesses, which are increasingly vulnerable to cyber threats.[20] Products range from toolkits to technical assistance, consultancy and advisory services,[21] research methodologies and maturity assessments,[22] as well as opt-in operational assessments of existing cybersecurity processes for small and medium size enterprises.[23] A portal managed by a core coordinating body, the Global Forum for Cyber Expertise (GFCE) serves as one repository of projects, tools, publications, and other resources pertaining to cyber capacity building for financial inclusion,[24] signaling an appreciation for mapping existing and upcoming initiatives in a sector gaining interest and focus by the international community and its support for low income and developing countries' financial systems.

CyberFI has also noted the importance of focusing on gender and cybersecurity if the overall goals of secure development are to be achieved. Identified efforts entail a focus on gender disparities in the cyber workforce[25] as well as the gendered impacts of cybersecurity threats, where women in developing countries are more susceptible to cyber fraud because of existing gender inequalities.[26] Gender mainstreaming in cyber capacity building for digital financial inclusion is a welcome progress, and one that signals the influence the development community can wield in shaping capacity resources at this intersection.

---

[19] Melissa Hathaway and Francesca Spidalieri, *Integrating Cyber Capacity in the Digital Development Agenda* (Global Forum on Cyber Expertise, 2021), https://thegfce.org/wp-content/uploads/2021/11/Integrating-Cybersecurity-into-Digital-Development_compressed.pdf

[20] Cybil Portal, "Design of a Cyber Security Capacity Building Tool Kit for Governments," Global Forum for Cyber Expertise, April 2018, https://cybilportal.org/projects/design-of-a-cyber-security-capacity-building-tool-kit-for-governments/

[21] Bill Eidson, "MITRE Strengthens Cyber Capacity of Developing Nations," *MITRE,* December 2019, https://www.mitre.org/publications/project-stories/mitre-strengthens-cyber-capacity-of-developing-nations

[22] Cybersecurity Multi-Donor Trust Fund, "The World Bank Announces the Launch of a New Trust Fund on Cybersecurity," The World Bank, https://www.worldbank.org/en/programs/cybersecurity-trust-fund/overview

[23] "Cylab - Africa Operational Assessment Research," Carnegie Mellon University Africa, https://cylab.africa.cmu.edu/

[24] Cybil Portal, "Financial Inclusion," https://cybilportal.org/projects-by?page=tag&_sft_post_tag=financial-inclusion

[25] Muhammad Khurram Khan, "Overcoming Gender Disparity in Cybersecurity Profession," *G20 Insights, Global Foundation for Cyber Studies and Research,* December 2020, https://www.g20-insights.org/policy_briefs/overcoming-gender-disparity-in-cybersecurity-profession/

[26] Michael Wechsler and Samikshya Siwakoti, "Gender, Cybersecurity & Fraud (Spring 2022) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4103747

Towards effective and sustainable cyber capacity building and digital financial inclusion: tensions and emerging questions.

Cybersecurity will continue to gain momentum as a digital development priority. As stakeholders work to boost cyber capacity within the digital financial ecosystem, we note the following tensions at this intersection that warrant more debate, reflection, and deliberation among development practitioners.

Firstly, there is an insufficient or unclear delineation of intended beneficiaries of cyber capacity building within the digital financial ecosystem. For instance, initiatives targeting government officials would do well to specify further which arms of government are targeted, as well as the specific objectives informing the endeavor. For instance, ministry officials, sector regulators, legislators, judicial officers, and law enforcement are all government stakeholders. Yet, their cyber capacity needs will vary. Generalizations such as 'cyber capacity building for government officials' could inadvertently lead to a skewed focus on some stakeholder groups more than others. This could be further complicated by 'scaling', where what is seen to work in one context is then supported for replication in another context. This assumes that a subset of approaches, such as support in developing legislative frameworks, and stakeholder groups such as regulators, are the main functions and constituencies in need of capacity support. A specificity of objectives, and of which actors are targeted or reached by cyber capacity building will improve collective understanding on whether efforts undertaken are one-off or continuous engagements.

Secondly, it is not evident whether cyber capacity building initiatives for digital financial inclusion are driven by the people and institutions who seek assistance or by those who seek to supply it. Do programs follow from locally driven needs-based assessments, or from external actors' assumptions about what should be needed? If the latter, to what extent are external actors' assumptions rooted in the local digital finance ecosystem—including sometimes-idiosyncratic fintech dynamics—versus presumptions of more traditional, formal financial systems? For instance, cyber capacity building efforts often aim to address a lack of appropriate regulation or 'indigenous expertise' in developing countries by drawing on experience and expertise gained in technologically advanced countries. However, this approach may fail to account for the disproportionate adoption rates of innovative financial technology – for example, the ubiquitous M-PESA system in Kenya – and therefore incorrectly account for the unique challenges and opportunities for capacity development in such a financial landscape.

The unique capacities among regulators, service providers, or consumers ought to be factored into framing how cyber capacity building for an ecosystem like Kenya's, for example, is both conceptualized as well as deployed and monitored for impact. In this case, the most pressing capacity needs for Kenya's regulators —who have otherwise been trailblazers in mobile money

regulation[27]—might not be training, but instead strengthening coordination between line ministries, for example. Other developing markets in Africa could also benefit from capacity building efforts that feature Kenyan regulatory actors' experience and expertise as a knowledge resource or as a peer exchange mechanism.

Third, as cybersecurity in digital financial inclusion gains further credence, a significant consideration is how to foster coherence and synergies in cyber capacity building efforts for all stakeholders in the ecosystem. There is the risk of duplication of initiatives as more actors become interested in building cyber capacity for digital financial inclusion. As mentioned previously, there tends to be a strong focus— on the supply side of cyber capacity building for digital financial inclusion—on training and accreditation, knowledge repositories and mapping of stakeholders. However, in some jurisdictions, the most impactful cyber capacity support could be sustained financial resources to implement good practices, such as national or financial sector-specific cyber emergency response teams (CERTs). Fitting demand and context-driven capacity needs to already-defined capacity support mechanisms risks undermining local ecosystems' incentives to critically assess where they fall short, to develop suitable approaches to good practices like information sharing, and even for recipient governments to bypass consulting local experts and stakeholders in favor of the 'international expertise' that shapes capacity building support. This creates a compounding risk over time, in which knowledge and financial investments may not lead to more, improved, or sustainable cyber capacity. Related to this is the perennial question of how to go beyond developed-developing, donor-beneficiary dichotomies that assign expertise and capacity needs. How can bottom-up insights be incorporated into cyber capacity building or development endeavors, especially in the case of developing countries whose digitalization trajectories have entailed aspects of leapfrogging and agility, both in infrastructure and of personnel?

Fourth, although there is a plethora of literature on cyber capacity building, there aren't readily available assessment frameworks for what does and does not count as a successful cyber capacity building measure, even in a sub-sector like digital financial inclusion. It is widely accepted in the development sector that "trainings" and education are the key to building capacity. We contend, however that the priority placed on training and education, often conducted in one-sided and non-collaborative formats, assumes that recipient countries lack vital knowledge. This model may diminish opportunities for co-learning and regional or community-specific solutions to cyber capacity needs. It also may overlook the contributions of self-taught practitioners.

[27] Njuguna Ndung'u, "A Digital Financial Services Revolution in Kenya: The M-PESA Case Study," *African Economic Research Consortium,* November 2021, https://aercafrica.org/african-governments-challenged-to-rethink-fiscal-policy-as-part-of-economic-recovery/

What Will Count as Successful Cyber Capacity Building?

Many aspects could be classified as cyber capacity building/development for and in digital financial inclusion—from digital forensics skills for law enforcement and cybercrime incident response teams, to digital financial literacy tools and cybersecurity awareness training for end users. Arguably, even physical infrastructure that connects people to digital financial products and services can be considered capacity building. All are key components to advancing inclusive participation in cyberspace. However, for many important stakeholders, such as NGOs, international organizations, and funding institutions, there remain fragmented definitions and distribution of resources to increase capacity building/development. To improve the outcomes of cyber capacity building in digital development, and digital financial inclusion more specifically, we recommend more debate and reflection on the tensions discussed above. To this end, we propose an analytical framework to assess successful cyber capacity building measures. An important aim would be to create guidelines for capacity building measures that could mitigate unintended consequences and problematic "solutions." The points outlined below are framed within the context of digital financial inclusion but may be of relevance to broader digital transformation cyber capacity building endeavors.

1. *Context-rooted training as a cyber capacity building measure.*

   Training, evidently, is a favored approach for enhancing cyber capacity. To help stakeholders get a better sense of what works — be it to impart technical skills or to develop legislative frameworks— we propose that those conducting such trainings outline if they refer to or conduct one-off or continuous trainings. Additionally, post-training assessments should be conducted to evaluate which approaches work and under what conditions. Such assessments can enable iterative improvements and replication of the most effective models.

   Self-training modules can further complement time-bound cyber capacity training such as through workshops, to allow for in-person engagements to be more interactive and engaging for participants. Existing mechanisms such as the Global Forum on Cyber Expertise could facilitate vibrant exchanges and mapping of the cyber capacities most needed in given development contexts. This mapping could identify types of training that would be more demand-driven as well as those that are already being provided and by whom. This will augment international coordination efforts to better identify gaps and redirect resources from crowded domains.

   For instance, MITRE's National Cyber Strategy Development & Implementation (NCSDI) framework[28] — through consultation with intended beneficiaries—can serve as a starting point

[28] Cybil Portal, "National Cyber Strategy Development & Implementation Framework - Assessment Phase," Global Forum for Cyber Expertise, May 2020, https://cybilportal.org/wp-content/uploads/2020/05/Cyber-Capacity-Assessment-Phase-Overview1.pdf

for mapping different aspects of cyber capacity needs and demands in a government context. It outlines eight strategic areas across two analytical levels in identifying existing capacity and aspirational needs. Other frameworks — overarching or niche — can be developed by interested parties to help take stock of the overall cyber capacity building efforts underway, or that need undertaking, so that training supply better meets demand.

2. Demand-driven and contextual cyber capacity building efforts

We posit that cyber capacity building efforts ought to be implemented following a comprehensive assessment of the needs (demands) of the intended beneficiaries. This necessarily includes the establishment of success metrics. The onus is on the development community to test their assumptions before designing programs, financial resources, or assistance mechanisms. One-size-fits-all approaches that tend to be popular in development assistance can fail to accommodate the complexities of the different ecosystems, a particularly important consideration as pertains to digital financial inclusion.

It is important to factor in the different politico-economic dynamics that will inform the unique determinants of what ends up being considered successful and thus scalable.[29] An insistence on scaling of top-down approaches risks undermining the agency of recipient countries in assessing and articulating their capacity needs. This can disincentivize commitment to the prevailing capacity building approaches, which could undermine motivation that is a crucial success determinant. Development practitioners ought to instead frame scaling as an interoperability of diverse and sustainable approaches and modalities, rather than a cut-and-paste from one context to another.

3. Interdisciplinary approaches

Neither cybersecurity nor capacity building are a singular issue, and cyber capacity building isn't either. Interdisciplinary approaches are key to addressing cyber capacity building challenges. Interdisciplinarity in general is one of the most vital concepts that can be applied to sustainable global development. Social, political, and economic dynamics are critical in closing the very gaps that technologies may create. We contend that it is important to ensure that cyber capacity training is not only framed as an imparting of technical skills: psychology, behavioral analysis and other non-technological fields also have a lot to offer to the cyber workforce.[30] For instance, social engineering is a common cybercrime tactic[31] with regards to

[29] Sebastian Pfotenhauer, Brice Laurent, Kyriaki Papageorgiou, and Jack Stilgoe, "The Politics of Scaling," October 8, 2021, https://journals.sagepub.com/doi/full/10.1177/03063127211048945

[30] Joanne Hall & Asha Rao, "Non-Technical Skills Needed by Cyber Security Graduates," IEEE, https://ieeexplore.ieee.org/document/9125105

[31] Silvia Baur-Yazbeck, Judith Frickenstein, and David Medine, "Cyber Security in Financial Sector Development," *CGAP,* November 2019, https://www.findevgateway.org/sites/default/files/publications/files/cyber_security_paper_november2019.pdf

digital financial ecosystems. Effective countermeasures demand more than technical capability to not only redress but also mitigate future digital finance-related cybercrimes. Configuring training to accommodate the interests and insights of these disciplines will likely vary depending on the local context. Attending to these local variations will help ensure that cyber capacity efforts are impactful beyond the training event.

There are a plethora of institutions and specializations involved in cyber capacity building. Resource management, cyber resilience, and organizational change in implementing bodies are among the functions that capacity building will need to address. Recently, the U.S. and the EU have introduced a wave of initiatives to "fund improvements to the cybersecurity of critical infrastructure in developing countries aiming to help these nations better withstand attacks and improve the international community's overall online resilience".[32] This seems promising; however, it is important for these efforts to be synergized and implemented in a manner that is not duplicative or siloed. These cybersecurity and cyber capacity building efforts must also be contextually appropriate to where, when, and how they are deployed.

4. Gender and Cyber Capacity Building

It is laudable that gender, as discussed earlier, is an early emphasis in discussions and resourcing for cyber capacity building. Creating inclusive cyber workforces is one important goal. The aim, however, should be not only to train, mentor, and support more women, but also to investigate and address the systemic issues that perpetuate a gendered divide in cybersecurity and technology workforces more broadly.[33] Another important priority is mainstreaming approaches to cybersecurity in which an appreciation can be cultivated of how gender shapes identities, roles, and expectations within society and even cybersecurity. Gender informs social structures and attendant hierarchies, often attributing technical expertise to masculinity, and skills such as communication, or initiatives promoting diversity, equity and inclusion as concerning women or femininity.[34] Gendered perspectives can sharpen cybersecurity design, defense, and response mechanisms to mirror the reality that neither technology broadly, nor cybersecurity more specifically, is gender neutral.

5. Complementarity of efforts by countries and institutions providing cyber capacity assistance

---

[32] Matthew Gooding, "US and EU Could Fund Cybersecurity Improvements in Developing Countries," *TechMonitor* https://techmonitor.ai/policy/geopolitics/us-eu-cybersecurity-china-russia

[33] Nanjira Sambuli, "Reflection on "Women in Tech" Narratives," *Observer Research Foundation,* October 2021, https://www.orfonline.org/expert-speak/reflection-on-women-in-tech-narratives/

[34] UNIDIR, "Gender Approached to Cybersecurity: Design, Defence and Response," *Association for Progressive Communications,* February 2021*,* https://www.apc.org/en/pubs/gender-approaches-cybersecurity-design-defence-and-response

One of the main goals of forums such as the CyberFI process is to identify and avoid gaps and duplications in cyber capacity building efforts. This can be done in many ways. The Cybil portal is one example of how initiatives can be mapped in a broad domain like cyber capacity building, with specific focus on niche areas like digital financial inclusion. If implementers continue to use and support such a tool both as a reference and as active contributors, duplication can perhaps be minimized, and resources better coordinated through strategic complementarities. Honest and authentic communication between funders, implementers and beneficiaries may also help mitigate some of the barriers that can arise from inadvertent duplications of cyber capacity efforts.

6. *Critical evaluations by funders and implementers on successes and gaps*

Sustainable cyber capacity building goes well beyond initial investments in the workforce and distribution of training and other resources. Continuous and retrospective evaluations of what has and has not been successful is key to future beneficial cyber capacity efforts. Sharing among implementers what works, and perhaps more importantly, what doesn't work — and drawing honest assessments from intended beneficiaries— is a crucial part of such evaluations. It can contribute to a vibrant information sharing culture within the cyber capacity building domain. Such evaluation exercises, however, ought to be mindful of placing an inadvertent burden on support recipients to continually explain the challenges and opportunities faced without deliberate and continual improvement in how support is tailored to address the identified pain points. Intermediary institutions, such as think tanks and other specialized nonprofits, can help facilitate dialogue between stakeholders and lend an outside analytical perspective.

7. *Sustained resources for institutions and programs*

One-off or time-bound cyber capacity building projects may serve as useful catalysts. However, and especially in development contexts, a bigger determinant of success and entrenchment of good practices is often tied to the continued availability of resources for programs that deliver, as well as the institutions in which the capacity efforts are supposed to benefit. It is one thing to train a CERT workforce; it is another for a national or sector-specific CERT to be adequately resourced to achieve the stated objectives. Thus, coupling resourcing needs with training and other capacity building modalities such as cyber strategies is imperative to secure short and long-term success in identifying, meeting, and sustaining cyber capacity.

Conclusion

As digital transformation continues to pervade nearly every sector, building and maintaining capacity to enable resilience against the inevitable cyber threats while simultaneously creating equitable and inclusive digital systems is no small feat. There are large differences in

cultures of information sharing and overall receptivity to technological shifts across regions. The digital finance system is a perfect example of this – informal cash-based banking ruled much of the infrastructure in African countries and the Indian subcontinent. Now, as there is a conspicuous shift towards and rapid uptake of mobile money banking, digital payment systems, and even cryptocurrency, cyber vulnerabilities are on the rise and will continue to persist. It is one thing to address these threats, it is another to do so in a manner that does not inadvertently undercut the people that the systems are working to serve.

Increasing cyber capacity is one way to work to enable resiliency of systems while investing in resources. However, without clear metrics or measures of success in the cyber capacity building community outlining what is and is not successful, even in a niche subset as the digital financial inclusion sector, efforts to bolster capacity may be shots in the dark. Within the digital financial space, it is still unclear not only what exactly the cyber capacity building measures are, but also who the intended beneficiaries are and what drives certain capacity building efforts over others. This is not to say that capacity building does not exist – rather that digital financial inclusion spaces do not have a clear picture of how cyber capacity building is measured and how successful capacity efforts are sustained to promote long-term cyber resilience.

We propose in this paper a few measures of cyber capacity building that stakeholders can look towards to assess whether capacity building measures are successful, inclusive, and sustainable. We posit that cyber capacity building initiatives— for digital financial inclusion and digital development writ large —will likely be more successful when i) training-based measures are coupled with other efforts to lessen solely "educate-first" narratives; ii) an interdisciplinary approach to cyber capacity is applied, encompassing intersectionality and unique efforts; iii) efforts are demand-driven and not based on an assumed or presumptive assessment of the cyber capacity needs of a given region; iv) capacity building efforts operate in alignment with the reality that technology is not gender neutral and therefore apply gender-responsive capacity approaches; v) cyber capacity efforts are not merely duplicates of prior or parallel and ongoing efforts; vi) communication between funders, implementers and beneficiaries is honest and authentic; and vii) there is regular feedback from implementers following cyber capacity efforts about what has and has not been successful in practice.

Cyber capacity building is, by nature, a broad term. As digital expansion and transformation accelerates at a historic pace, its effects are not distributed equally. This is clear in the digital financial sector. It is up to the organizations, funders, implementers, and institutions working on these issues to enable demand-driven efforts, as well as to establish clear measurements of success in capacity building so that digital financial inclusion advances as a cyber secure and cyber resilient undertaking. The framework proposed above can hopefully serve as a starting point to create fluency with regards to cyber capacity building or development, as we advance further into the digital age.