IGF 2024
Best Practice Forum Cybersecurity
(BPF Cybersecurity)

IGF 2024

Best Practice Forum Cybersecurity

Mainstreaming capacity building for cybersecurity, trust , and safety online

Output report

January 2025

The *Best Practice Forum on Cybersecurity capacity building* is an open multistakeholder effort conducted as an intersessional activity of the *Internet Governance Forum (IGF)*.

This BPF output is the product of the collaborative efforts and valuable insights of the numerous contributors who participated in BPF meetings throughout the year and the BPF main session organised at the IGF 2024 in Riyadh, Saudi Arabia, or provided feedback on the mailing list or requests for input.

Acknowledgements.

We extend our gratitude to all participants of the BPF activities and main session for their valuable contributions.

The BPF activities were prepared and coordinated by a *BPF Coordinating team: Ms Josephine Miliza (IGF MAG member)*, *Ms Carina Birarda (IGF MAG member)*, *Mx Oktavía Hrund G Jóns (IGF MAG member), Ms Hariniombonana Andriamampionona (BPF co-facilitator, former MAG member), Mr Dino Cataldo Dell'Accio (BPF co-facilitator, UNJSPF rep. to the MAG), Mr Wim Degezelle (*BPF Cybersecurity consultant, IGF Secretariat).

Disclaimer:
The views and opinions expressed herein do not necessarily reflect those of the United Nations Secretariat. The designations and terminology employed may not conform to United Nations practice and do not imply the expression of any opinion whatsoever on the part of the Organization.

Table of content

IGF Best Practice Forum Cybersecurity
Mainstreaming capacity building for cybersecurity, trust, and safety online

Executive Summary

Cybersecurity and trust emerged as paramount concerns in the community consultation that was held to inform the planning and thematic focus of the IGF 2024 process and the 19th annual meeting in Riyadh. The topic breaks down into a complex array of issues, the Best Practice Forum (BPF) focussed on capacity building and fostering a culture of learning and continuous improvement to enhance cybersecurity and trust.

The BPF initially proposed to compile an overview of existing cyber-capacity building initiatives and present them in an informative database for those seeking such resources. However, when this work plan was presented to the stakeholder community, the feedback highlighted that such an effort would duplicate the work of several valuable initiatives that already map cybersecurity capacity building and provide tools to make these resources accessible. Instead, it was recommended that the BPF focus on facilitating access to the wealth of information available in mappings and inventories, ensuring it effectively reaches its target audiences.

This resulted in the formulation of a new problem statement as foundation for the BPF's work: *'While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity building offerings, overlaps and gaps in information exist and the information may not reach its target audience effectively.'* Experts and stakeholders that took part in BPF discussions largely agreed that the statement is both valid and necessary but emphasized the importance of context and experience.

Consistency is essential to creating meaningful impact in capacity-building efforts. Initiatives must be rooted in local contexts while being shared globally to ensure relevance and scalability. Localisation is pivotal to making resources accessible and fostering wider adoption. A commitment to building trust is key, achieved through actions like sharing knowledge, listening to feedback, implementing strategies, and embracing change.

Capacity-building efforts should **make full use of existing mechanisms, processes, and practices.** Existing mechanisms, including platforms such as the IGF should be utilised more effectively for capacity building activities. Cyber capacity building should be understood as an ecosystem of interconnected initiatives and practices that work together, and engagement on multiple levels, leveraging knowledge and know-how.

A participatory, multi-stakeholder approach is crucial for sustainable and inclusive cyber capacity building. Efforts should be optimized through mapping, coordinating, collaborating, and fostering dialogue, especially in low-resource environments. Cybersecurity should be demystified through accessible resources, framed as an investment in the resilience of future generations. Effective capacity-building should be consistent, localised, contextual, relevant, and well-resourced to ensure accessibility.

The BPF Cybersecurity 2024 report is published on the IGF website.

Over the years, the BPF Cybersecurity has explored various aspects of culture, norms, and values in cybersecurity. These reports, based on insights from the IGF stakeholder community, offer valuable perspectives and are accessible on the BPF's webpage.

IGF Best Practice Forum Cybersecurity

Mainstreaming capacity building for cybersecurity, trust, and safety online

1. The IGF Best Practice Forum on Cybersecurity

1.1. Internet Governance Forum

The Internet Governance Forum (IGF), convened by the United Nations Secretary General[1], brings stakeholder groups together as equals in discussions on public policy issues relating to the Internet. The IGF's mandate is set out in paragraph 72 of the Tunis Agenda for the Information Society[2] and its first meeting convened in Athens, in 2006. The mandate of the of the IGF was extended with 10 years in 2015 by the UN General Assembly's resolution (70/124) 'Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society'[3]. Nineteen annual meetings of the IGF have been hosted by various governments.

In 2024, the IGF held its 19th annual meeting in Riyadh, hosted by the Government of the Kingdom of Saudi Arabia, under the overarching theme 'Building our multistakeholder digital future'.

[1] Resolution adopted by the UN General Assembly on 16 December 2015, (70/125), extending the IGF's mandate set out in par. 72 to 78 of the Tunis Agenda. https://unctad.org/system/files/official-document/ares70d125_en.pdf

[2] Tunis Agenda for the Information Society. https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[3] Resolution A/RES/70/125. https://documents.un.org/doc/undoc/gen/n15/438/42/pdf/n1543842.pdf

1.2. The IGF Best Practice Forum on Cybersecurity

Best Practice Forums (BPFs) were introduced in 2014 as part of the intersessional programme to complement the IGF communities activities and develop tangible outputs to 'enhance the impact of the IGF on global Internet governance and policy'[4]. BPFs aim to facilitate dialogue and collect emerging and existing practices to address specific issues or themes. BPFs foster a common understanding of concrete policy challenges. The objective is not to develop new policies or practices, but rather to collect existing good practices, share positive and negative experiences, and flag challenges that require additional multistakeholder dialogue and/or require the attention of policymakers, including in specified decision-making bodies.[5] BPFs follow an open, bottom-up, and collective approach to ensure community-driven outcomes, with flexibility to define their scope, methods, and work plans based on their theme's specific needs.

Since 2014, IGF BPFs have focused on cybersecurity related topics. Between 2018 and 2023, the BPF Cybersecurity focussed on the development, value and application of cybersecurity norms agreements.

IGF BPF Cybersecurity work on cyber norms agreements - outputs

- Lessons from cybersecurity events to inform cybersecurity policy and norms deliberations.
  IGF 2023 - report
- Consolidated output of the BPF workstreams.
  IGF 2022 - report
- Ad hoc paper. Mythbusting: cybercrime versus cybersecurity.
  IGF 2022 - paper
- The use of Norms to foster Trust and Security.
  IGF 2021 - report
- Exploring best practices in relation to international cybersecurity agreements.
  IGF 2020 - report
- BPF cybersecurity on international cybersecurity agreements.
  IGF 2019 - report
- Cybersecurity Culture, Norms and Values.
  IGF 2018 - report

[4] The intersessional programme was designed in accordance with the recommendations of a 2012 report by the UN Commission on Science and Technology for Development (CSTD)'s Working Group on IGF Improvements. https://unctad.org/system/files/official-document/a67d65_en.pdf

[5] IGF Best Practice Forums. Definitions, Procedures, and Modalities. https://www.intgovforum.org/en/filedepot_download/3405/2270

2. A BPF Cybersecurity capacity building

2.1. Introduction

Cybersecurity and trust emerged as paramount concerns in the community consultation[6] that was held to inform the planning and thematic focus of the IGF 2024 process and the 19th annual meeting in Riyadh. The topic of cybersecurity breaks down into a complex array of issues. Recognising this complexity, a proposal[7] was developed to have a BPF focussed on capacity building and fostering a culture of learning and continuous improvement to enhance cybersecurity, trust, and safety online. The IGF Multistakeholder Advisory Group (MAG) confirmed the BPF on cybersecurity capacity building at the Open Consultations and MAG Meeting in February.[8]

2.2. Community feedback on the BPF work plan

The BPF initially proposed to compile an overview of existing cyber-capacity building initiatives and present them in an informative database for those seeking such resources. It was argued that such a mapping, database, or inventory would be a useful tool to foster a culture of learning and continuous improvement within the cybersecurity capacity building field. It was also expected that mapping our initiatives would be a way to discover where there exist overlap, duplication and potential gaps in the offer of cyber capacity building as such leads to inefficient use of the limited resources.

However, when this work plan was presented to the stakeholder community, amongst other at a dedicated BPF call[9], the feedback highlighted that such an effort would duplicate the work of several valuable initiatives that already map cybersecurity capacity building and provide tools to make these resources accessible. Moreover, some warned that creating another BPF or IGF mapping of cybersecurity capacity building initiatives would risk adding an extra layer of complexity to an already crowded landscape and could easily duplicate or compete with existing efforts.

Instead, it was recommended that the BPF focus on facilitating access to the wealth of information available in already existing mappings and inventories, ensuring it effectively reaches its target audiences.

[6] IGF 2024 Call for thematic inputs (results) : https://intgovforum.org/en/filedepot_download/309/27171
[7] Proposal BPF Cybersecurity capacity building: https://intgovforum.org/en/filedepot_download/314/27194
[8] https://intgovforum.org/en/content/igf-2024-first-open-consultations-and-mag-meeting
[9] BPF cybersecurity, call 20 June 2024, summary: https://intgovforum.org/en/filedepot_download/56/28070

2.3. An updated draft methodology

Overlap, duplication, and gaps in cybersecurity capacity building leads to inefficient use of limited resources. However, there is no need for the BPF to create another mapping of initiatives, as many valuable efforts already exist, such as the Cybil portal by GFCE, the UNIDIR cyberportal, or the Global Cybersecurity Capacity Centre. However, enhanced cooperation and information exchange between existing initiatives that map cybersecurity capacity building could yield significant benefits and help to build a comprehensive understanding of who is doing what and with what focus and pue. Such an overview is important to avoid redundancy among these efforts.

Building on these insight, based on community feedback, the BPF designed[10] a draft methodology which included the following steps:

1. Defining the Issue: Clearly articulate the problem of overlap in cybersecurity capacity building efforts and its negative consequences.
2. Compiling an Overview of Existing Mappings: Gather and categorise current mappings and inventories of cybersecurity capacity building initiatives by focus areas, topics, target users, and other relevant criteria.
3. Collect Case Studies: Assemble case studies showcasing cooperation and coordination between different mapping and inventories to extract lessons on perceived benefits and obstacles.
4. Preparing Draft Conclusions and Recommendations: Develop preliminary conclusions and actionable recommendations to discuss at the BPF session during IGF 2024 in Riyad.

Subsequently, the BPF began executing this methodology. A problem statement was developed and discussed with the community. Furthermore, a crowdsourcing initiative was launched to collect examples of mappings, and the BPF held its first discussion on how to address the identified challenges. These efforts are detailed in the following sections of the report.

[10] BPF Cybersecurity call, 26 September 2024, summary https://intgovforum.org/en/filedepot_download/56/28159

2.4. Defining the Issue - problem statement

The BPF worked to develop a thorough and detailed problem statement, addressing the key challenges and underlying issues within the scope of the initiative. The problem statement highlights that ‘While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity building offerings, overlaps, and gaps in information exist and the information may not reach its target audience effectively.’ This statement forms a guiding framework for further discussions.

Problem statement

> “While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity building offerings, overlaps, and gaps in information exist and the information may not reach its target audience effectively.”

2.5. Feedback on the problem statement

The BPF presented the problem statement to the community and invited feedback, including during at a BPF call organised on 27 November 2024 and during the BPF main session at the IGF meeting in Riyadh.

In general, the problem statement was well received and it was highlighted that there exists indeed a proliferation of cybersecurity capacity building information, much of which is not tailored or targeted to the recipients. As a consequence, capacity building efforts often fail to address specific needs, as they are not designed in consultation with the intended recipient country, organization, or partner, and adapted to their unique context and circumstances.

It was acknowledged that the IGF is a natural platform for discussions on capacity building, although its full potential in this field has yet to be realised. The establishment of a Best Practice Forum (BPF) on capacity building is therefore seen as a positive step to address related challenges. Initiatives that map, inventory, and share information on capacity building can benefit from learning about each other’s approaches, collaborate, and build upon one another’s work. The IGF can serve as a good place to start these conversations.

It was also highlighted that while there is a proliferation of cybersecurity capacity-building information, there may still be unmet needs. For instance, the rapid growth of e-health practices has created a need for specific capacity-building focused on the security of e-health data, particularly for healthcare practitioners. Additionally, access to information on cybersecurity capacity building remains a challenge for certain groups. Accessibility is especially crucial for underserved communities, with a focus on ensuring that materials are available in local languages and optimised for mobile devices, which are often the primary means of access in many regions.

2.6. Compiling an overview of existing mappings

To compile an overview of existing mappings of cybersecurity capacity offerings and initiatives, the BPF decided to crowdsource input from the community. This was done through an online form shared on the BPF webpage, mailing list, and IGF social media channels. By the IGF meeting in Riyadh, 29 responses were received.

The questionnaire sought information on existing mappings and inventories of cybersecurity capacity building initiatives, excluding individual capacity building efforts. It included questions designed to capture key details about each inventory or mapping, such as:

- The topic and scope of the inventory/mapping
- The geographic focus of the inventory/mapping
- The target users of the inventory/mapping
- The date the information was collected or if it is regularly updated
- Known cooperation with other similar initiatives
- The definition of cybersecurity used

This collaborative effort helped to gather valuable information. Below is a list of the initiatives for which information was submitted to the BPF. Details can be found in the annex. An important disclaimer: the information was crowdsourced, meaning the person who submitted the information is not necessarily linked to the initiative they provided details on. Furthermore, the organisation behind the initiative and the people involved have not reviewed the information.

- UNIDIR's Cyber Policy Portal
  https://cyberpolicyportal.org
- The Cybil Portal
  https://cybilportal.org
- CyberSeek
  https://www.cyberseek.org
- The Global Cybersecurity Capacity Program
  https://cybilportal.org/projects/global-cybersecurity-capacity-program-i/
- EU Cybernet's CCB Projects Mapping
  https://www.eucybernet.eu/ccb-table/
- The Global Forum on Cyber Expertise (GFCE) Clearing House
  hhttps://thegfce.org/clearing-house/
- ENISA's European Cybersecurity Skills Framework (ECSF)
  https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework
- Prioritising security-related Internet standards and ICT best practices
  https://is3coalition.org/docs/is3c-working-group-5-report-and-list/
- Bricade
  https://bricade.com
- IS3 Coalition Working Group on DNSSEC and RPKI
  https://is3coalition.org/working-groups/
- Digital Watch Observatory
  https://dig.watch/topics/cybersecurity
- Forum of Incident Response and Security Teams, FIRST
  https://www.first.org/
- Cyber Security Agency of Singapore, CSA
  https://www.csa.gov.sg/
- Development Asia
  https://development.asia/
- Global Partners Digital
  https://www.gp-digital.org/
- Global Encryption Coalition, GEC
  https://www.globalencryption.org/
- ASEAN-Japan Cybersecurity Capacity Building Centre, AJCCBC
  https://ajccbc.ncsa.or.th/
- CyberASEAN
  https://cyberasean.pacforum.org/
- UQ Cyber Research Centre, The University of Queensland, Australia

https://cyber.uq.edu.au

- World Bank Cybersecurity Multi-Donor Trust Fund
  https://www.worldbank.org/en/topic/digital/brief/cybersecurity
- MRU Cybersecurity Readiness and Capacity Assessment Program
  mruigf.org
- Closing the gap between the needs of the cybersecurity industry and the skills of tertiary graduates.
  https://www.is3coalition.org
- CISA's Cybersecurity Resources for High Risk Communities
  https://www.cisa.gov/audiences/high-risk-communities/cybersecurity-resources-high-risk-communities
- Common Good Cyber
  https://commongoodcyber.org/
- Non-Profit Cyber
  https://nonprofitcyber.org/
- Tech Policy Atlas
  https://techpolicydesign.au/tech-policy-atlas
- FIRST (Forum of Incident Response and Security Teams)
  https://www.first.org
- Postal Sector Information Sharing & Analysis Centre (POST-ISAC) including SECURE.POST
  https://secure.post
- South School on Internet Governance
  https://www.gobernanzainternet.org/ssig2025/en/

2.7. Discussion: How to avoid duplication, gaps, and identify needs in cyber capacity building ?

After developing the problem statement, the BPF shifted its focus to addressing the identified issues. Specifically, the discussion centred on how to prevent duplication while simultaneously identifying any gaps that may exist in the available resources.

It is crucial to have this conversation, as there are many portals and resources available—some of which may be similar but not identical. The biggest risk is falling into a tunnel vision, where each entity continues its work in isolation without collaboration.

However, there are examples of successful cooperation, such as the collaboration between the Cybil portal and the UNIDIR Cyber Policy Portal. While the Cybil portal maps resources, tools, and projects related to cybersecurity, UNIDIR offers a one-stop shop focused on the cybersecurity situation at the country level. Integrating these resources seems like an obvious step, but to make it happen, technical challenges related to interoperability had to be addressed.

Countries or organisations preparing a capacity-building project would do well to consult existing portals and mappings. This can help avoid that they later have to discover that similar initiatives are already in place, and their new initiative is duplicative .

It is essential for all parties involved in cybersecurity capacity building—such as organisers of cybersecurity capacity building, donors, and recipients—to come together. For instance, the Australian government hosts an annual cyber coordination conference[11] to facilitate this exchange, networking and collaboration. However, it does not necessarily require additional mechanisms or processes, but rather a commitment to making the most of the existing ones. When areas of misalignment or duplication are identified, one should be ready and willing to adjust programming accordingly. At times, donors—whether countries or organisations—may place too much emphasis on their internal budgeting and programming processes, which can reduce flexibility. However, it is crucial to remain adaptable and open to feedback, ensuring we are responsive to emerging needs.

When discussing mapping and identifying gaps in cybersecurity capacity building, one specific gap that frequently arises is the lack of follow-up initiatives. This gap is often a result of budget constraints and limited funding availability. Therefore, mapping cybersecurity capacity building efforts should also focus on what happens afterward, ensuring that next steps and follow-up actions are considered.

Young people, including young girls, are a critical group with specific needs when it comes to cybersecurity capacity building. For example, they need to understand how to secure their data or learn how to recognise and handle mis- and disinformation. Online capacity training and awareness-raising on cybersecurity threats for young people, such as the valuable work being done by IGF ISOC Benin, are essential.

Sharing information and being open about one’s own initiatives is crucial in order to avoid duplication and overlap. Unfortunately, many organisations fail to recognise the benefits of sharing details about their activities and upcoming plans, or may hesitate to do so for various reasons. For example, some may fear losing control over their projects or funding, or

[11] https://melbourne2024.cyberconference.com.au/

worry that others might copy their initiatives if too much information is shared. It is essential to change this mindset, as collaboration and transparency can lead to stronger, more impactful efforts, benefiting everyone involved.

When efforts are uncoordinated, it can lead to missed opportunities. For instance, if an implementer arrives and is unaware that a similar project was carried out by someone else, for example the year before, this creates a lost chance to build on the previous work. Instead of reinventing the wheel, they could have leveraged the earlier project to enhance their own initiative, ultimately creating a larger and more lasting impact.

Furthermore, if every organisation or country pursues their own independent project without coordinating, the target audience or receiving country may become overwhelmed. Multiple, uncoordinated efforts can lead to confusion, redundancy, and resource strain, making it harder for the targeted community to engage meaningfully and benefit from the work being done. It is essential to approach projects with collaboration in mind, ensuring that all efforts contribute to a unified, impactful outcome.

Cyber capacity building must adopt a whole-of-nation approach, involving all stakeholders. Building cyber resilience and capacity should not be seen as solely the responsibility of the government, but as an initiative that engages industry and the community. It is essential that this effort is embraced collectively, rather than being viewed merely as a government programme. Since most infrastructure is interconnected, involving all sectors in the response is crucial to creating a robust and sustainable cybersecurity environment.

he approach to cybersecurity capacity building must encompass a broad range of stakeholders, including government entities, private sector operators responsible for civilian infrastructure, educational institutions, schools, and universities. It is essential to engage across the full spectrum of society, as cybersecurity is not just a technical issue, nor is it solely a government concern. Rather, it is a whole-of-nation issue that requires the collaboration of all sectors to ensure a secure and resilient digital environment for everyone.

To increase the impact of cybersecurity capacity building, greater cooperation is essential. Efforts must be combined, bringing together different experiences and initiatives. A challenge faced in one community could offer valuable lessons for an organisation in another part of the world. Finding ways to collaborate is crucial, as it enables a larger impact and facilitates progress on challenges that have previously been difficult to overcome.

Measuring the impact of cybersecurity efforts remains a challenge for many. The question often arises: how can it be determined if programmes are truly effective? While it’s clear that cyber incidents continue to worsen, and despite our best efforts, more incidents are likely to occur, the success of cybersecurity initiatives cannot be measured solely by the reduction of incidents. In cybersecurity, qualitative information plays a crucial role. One of the most effective ways to assess improvements in arrangements, capacity, and preparedness is through testing, such as conducting exercises that provide valuable qualitative insights into progress.

2.8. Recommendations & way forward

Drawing from the exchanges summarised above, three key recommendations can be derived.

Consistency is essential to creating meaningful impact in capacity-building efforts. Initiatives must be rooted in local contexts while being shared globally to ensure relevance and scalability. Localisation is pivotal to making resources accessible and fostering wider adoption. A commitment to building trust is key, achieved through actions like sharing knowledge, listening to feedback, implementing strategies, and embracing change.

Capacity-building efforts should **make full use of existing mechanisms, processes, and practices.** Existing mechanisms, including platforms such as the IGF should be utilised more effectively for capacity building activities. Cyber capacity building should be understood as an ecosystem of interconnected initiatives and practices that work together, and engagement on multiple levels, leveraging knowledge and know-how.

A participatory, multi-stakeholder approach is crucial for sustainable and inclusive cyber capacity building. Efforts should be optimized through mapping, coordinating, collaborating, and fostering dialogue, especially in low-resource environments. Cybersecurity should be demystified through accessible resources, framed as an investment in the resilience of future generations. Effective capacity-building should be consistent, localised, contextual, relevant, and well-resourced to ensure accessibility.

3. Conclusion and follow up

For the first time, a Best Practice Forum (BPF) on cybersecurity focused specifically on the topic of cybersecurity capacity building. It is widely believed that mainstreaming cybersecurity capacity building is a vital contribution to enhancing cybersecurity, trust, and safety online.

The BPF followed an interesting trajectory, as its initial plan was modified based on valuable input from the community. This shift represents an important lesson and a key outcome of the BPF’s work this year.

The BPF developed a sound methodology aligned with its renewed focus and began working on several tasks and steps. However, it was not able to fully achieve all of its goals, and the plan remains open for further completion.

As the BPF is a MAG-led intersessional activity, it is up to the incoming 2025 MAG to decide whether it should continue into the 2025 IGF cycle and further explore cybersecurity capacity building.

Crowdsourced examples of cybersecurity capacity building mapping and inventories

IGF 2024

Best Practice Forum Cybersecurity Capacity Building

The ***IGF Best Practice Forum (BPF) on Cybersecurity Capacity Building*** seeks to promote collaboration to maximise the efficient use of limited resources in the field of cybersecurity capacity building. As part of its activities in 2024, the BPF is collecting information on existing **mappings and inventories of cybersecurity capacity building** initiatives. The BPF is an IGF intersessional activity. More on the BPF's webpage.

* Disclaimer : The information presented in this table has been crowdsourced by the BPF. It is provided as received, without having been reviewed or categorised. It will serve as a preliminary input for the development of the BPF's output and may be subject to further verification and classification. This collaborative effort helped gather valuable insights into the state of cybersecurity capacity building initiatives and their coverage.

Name	**Description**	**Target area / Target users / Key topics**	**Additional information**
UNIDIR's Cyber Policy Portal https://cyberpolicyportal.org	Map of national cybersecurity policies and initiatives globally		
The Cybil Portal https://cybilportal.org	The Cybil Portal: Comprehensive knowledge portal that maintains an overview of existing and past cyber capacity building projects and programs worldwide. It categorizes projects along five key capacity-building themes and allows filtering by various criteria like region, actor type, and status.		

Name	Description	Target area / Target users / Key topics	Additional information
CyberSeek https://www.cyberseek.org	Focused on the U.S. job market, CyberSeek provides detailed data on cybersecurity supply and demand, including interactive tools to explore career pathways and identify skill gaps		
The Global Cybersecurity Capacity Program https://cybilportal.org/projects/global-cybersecurity-capacity-program-i/	World Bank initiative has helped strengthen cybersecurity capacities in multiple countries through tailored national and regional technical assistance schemes		
EU Cybernet's CCB Projects Mapping https://www.eucybernet.eu/ccb-table/	This effort maps cybersecurity capacity building projects across the European Union		
The Global Forum on Cyber Expertise (GFCE) Clearing House https://thegfce.org/clearing-house/ https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communi	This tool aims to facilitate matchmaking between GFCE members with cyber capacity needs and partners who can offer support		

Name	Description	Target area / Target users / Key topics	Additional information
cation_Technologies_-_(2021)/Global_Forum_on_Cyber_Expertise_(GFCE)_UN_OEWG_Submission_-_Mapping_ICT_Capacity_Building.pdf			
ENISA's European Cybersecurity Skills Framework (ECSF) https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework	Comprehensive overview of cybersecurity roles, skills, and competencies within the European Union		
Prioritising security-related Internet standards and ICT best practices https://is3coalition.org/docs/is3c-working-group-5-report-and-list/	It contains a checklist of Internet standards for secure communications', of the most important and critical security-related Internet standards which the coalition's members believe that all public administrations and private organisations should require to be integrated in the design of the ICT products, services or devices which they procure. The list of agreed upon by consensus and after a public consultation.	Global Governments, (internet) industry, consumers Deployment of security-related internet standards and ICT best practices. The scope is global, public and private.	Updated - 2023 Cooperation with www.internet.nl IS3C is a UN Internet Governance Forum Dynamic Coalition with the goal of making online activity and interaction more secure and safer by achieving more widespread and rapid deployment of existing, security-related Internet standards and best practices.

Name	Description	Target area / Target users / Key topics	Additional information
			IS3C has recently published reports on security by design in the Internet of Things, on cybersecurity education and skills, and on procurement and supply chain management. You can find more information on IS3C here: https://is3coalition.org/.
Bricade https://bricade.com	Bricade provide Fore-Warning Alerts on potential risks long before they affect your organization, empowering senior leadership to act with confidence and precision.	Global Boards, C-Level Executives, and Directors Unlike conventional cybersecurity firms that focus on reacting to incidents as they happen (Now-Warning), Bricade specializes in Fore-Warning. This means we alert you to emerging business risks before they materialize, helping you prevent crises rather than just respond to them. We simplify complex information into actionable insights, providing you with the foresight to manage risks effectively—before they impact your	Private initiative Dating back to 2006 and updated daily with 100-400 new entries, our database provides a living, breathing source of intelligence that is always comprehensive, current, and reliable. At the heart of Bricade's offering is the world's largest risk database, encompassing more than 20,000 topics that span cyber threats, organizational vulnerabilities, and beyond. Unlike other risk intelligence firms, Bricade's

Name	Description	Target area / Target users / Key topics	Additional information
		business operations.	database is curated by human analysts—a powerful differentiator in ensuring relevance and accuracy.
IS3 Coalition Working Group on DNSSEC and RPKI https://is3coalition.org/working-groups/	This working group focuses on outreach and engagement efforts to increase trust in, and contribute to the wider deployment of, DNSSEC and RPKI. This working group provides a work plan, containing among others a new and different narrative and recommendations for the next phase, including an outreach plan at the global level.	Global Network operators DNSSEC deployment, RPKI deployment	information is regularly updated
Digital Watch Observatory https://dig.watch/topics/cybersecurity	An internet governance issue observatory website. There is not only cybersecurity issues but also more internet and diplomacy news on the website. The cybersecurity column also includes cybercrime, online children safety, network security, cyberconflict and warfare, etc.	Global The topics are cybercrime, encryption, child safety online, critical infrastructure, cyber norms, cyberconflict and warfare, etc.	update the news everyday.
Forum of Incident Response and Security Teams, FIRST https://www.first.org/	A global cybersecurity forum for CIRTs ,PSIRTs, and security researchers	Global cybersecurity teams and cybersecurity technical experts CIRTs basic courses, Threat intelligence fundamentals Course,	

Name	Description	Target area / Target users / Key topics	Additional information
		Malware Analysis, DDoS Mitigation Fundamentals, technical trainings.	
Cyber Security Agency of Singapore, CSA https://www.csa.gov.sg/	It's a Singapore government website. CSA was formed in 2015. The CSA is part of the Prime Minister's Office and is managed by the Ministry of Digital Development and Information (MDDI).	Singapore Citizens in Singapore. Besides the news, events and legislation, the CSA website also publish the cybersecurity alerts and online safety for people in Singapore. They also do Internet Hygiene evaluation for Singapore websites and publish the result online for their people. The evaluation may help to build the trust between the websites and users.	Last update Oct 22, 2024 Cooperation with SingCERT, FIRST, APCERT Singapore is a benchmark country of Smart Nation in the Asia Pacific region. The website also provides tools to check the safety of websites, and it is very useful to build the concept for people to check the website's health.
Development Asia https://development.asia/	Development Asia is the Asian Development Bank's knowledge collaboration platform for sharing development experience and expertise, best practices, and technology relevant to the Sustainable Development Goals. The ADB Knowledge Events website records many events of the Asian Development Bank(ADB), which also includes cybersecurity and other ICT related events.	Asian Countries. Member nations of ADB The topics on the websites are not only for cybersecurity but also about economic, development in Asia.	Last update Oct 22, 2024 The cybersecurity is an issue under the information and communication technology topics. And ADB seems focus on economic development issues more than cybersecurity issues.

Name	Description	Target area / Target users / Key topics	Additional information
Global Partners Digital https://www.gp-digital.org/	It's a UK-based organisation that supports global human rights initiatives. It engages in human rights in technology development, policy-making, and internet governance forums.	Global Policy makers and diplomats. But they try to awake the awareness of each every internet user to engage and focus on human rights and technology. Trust and Security, Emerging technology, and Platform and content governance	the websites updated monthly Cooperation with Global Encryption Coalition They also engaged in events in Latin America.
Global Encryption Coalition, GEC https://www.globalencryption.org/	The GEC is a global coalition attempting to initiate the protection of encryption and privacy. 400 members across 103 countries form it. The encryption is a basic to protect the security, privacy, and freedom online of expression.	Global Government, internet users Besides their initiatives, they also provides toolkits and some simple guidances for parent, children and family to understand the importance of encryption.	the website updates monthly Cooperation with Global Partners Digital and their members. The GEC thinks encryption is the first line to protect online security, safety, and privacy.
ASEAN-Japan Cybersecurity Capacity Building Centre, AJCCBC https://ajccbc.ncsa.or.th/	ASEAN-Japan Cybersecurity Capacity Building Centre is a centre for cybersecurity training for Government and CI cyber professionals from ASEAN Member States with the endorsement of ADGMIN and ADGSOM. The centre is managed by the National Cyber Security Agency (NCSA) of	Southeast Asia, ASEAN ASEAN People, whose job is about cybersecurity and security incidents management. Their training is not for general people.	Cooperation with FIRST

Name	Description	Target area / Target users / Key topics	Additional information
	Thailand and the Japan International Cooperation Agency (JICA).		
CyberASEAN https://cyberasean.pacforum.org/	Cyber ASEAN is a capacity-building and development initiative that aims to advance Southeast Asia's proactive role in strengthening its overall cybersecurity and resiliency posture. The Australian government and the Pacific Forum supported the project. It seems to be maintained by the Pacific Forum.	Indonesia, Malaysia, the Philippines, and Viet Nam ASEAN people They doesn't provide the topics on the websites. But they developed the Cyber threat tracker to trace the cyber incidents.	Cooperation with Pacific Forum
UQ Cyber Research Centre, The University of Queensland, Australia https://cyber.uq.edu.au	UQ Cyber Research Centre (UQ Cyber) is an interdisciplinary research centre based at the University of Queensland (a global Top-50 ranked university), which is also home to the Australian Cyber Emergency Response Team (AUSCERT), the world's second oldest CERT established in 1992 after Carnegie Mellon University's CC/CERT. UQ Cyber integrates its 100+ industry members, and AUSCERT's 600+ corporate members from around Oceania into its research and teaching. Its interdisciplinary Master of Cyber Security and postgraduate program is accredited by the Australian	Oceania, Australia, New Zealand, 17 Pacific Island Nations Interdisciplinary cyber security education. Cyber resilience education. Competitions for capacity building (e.g. Capture-the-Flag competitions)	Cooperation with Australian Department of Foreign Affairs and Trade (DFAT), Department of Home Affairs Cooperation with PaCSON (Pacific Cyber Security Operations Network), government incident response teams across 17 member nations in the Pacific. Cooperation with AUSCERT members; Through AUSCERT, cooperation with APCERT,

Name	Description	Target area / Target users / Key topics	Additional information
	Computer Society, and is aligned to NIST's National Initiative on Cybersecurity Education (NICE) Framework. It hosts the Pacific Telecommunications Security Experts Forum (PTSEF), and several engagements across the Pacific. The Master of Cyber Security has four specialisations: Cyber Defence, Leadership, Criminology, Cryptography. The model is now being duplicated across other universities and higher education institutions in Australia. Through AUSCERT, it runs executive cyber training and runs a Queensland statewide, vendor-free Cyber Leaders Network for senior cyber leaders across the public and private sectors to network and apply new concepts into their organisations. It also hosts the annual Oceania Cybersecurity Challenge, which qualifies Team Oceania for the International Cybersecurity Challenge - the global 'World Cup' of cybersecurity competitions for youths between 18 to 25 years old.		FIRST. Cooperation with governments of Singapore, Japan, Korea and UAE.

Name	Description	Target area / Target users / Key topics	Additional information
World Bank Cybersecurity Multi-Donor Trust Fund https://www.worldbank.org/en/topic/digital/brief/cybersecurity	Provides funding and technical assistance for capacity building initiatives in developing countries across all regions	Global CCB	
MRU Cybersecurity Readiness and Capacity Assessment Program mruigf.org	This program would aim to comprehensively map, assess, and monitor the cybersecurity capabilities across each country, with a specific focus on key metrics such as legal frameworks, technical capabilities, human resource capacity, and incident response readiness.	Mano River Union (MRU) region, specifically targeting Liberia, Guinea, and Sierra Leone. Mano River Union (MRU) region, specifically targeting Liberia, Guinea, and Sierra Leone. Key topics description (see below)*	
Closing the gap between the needs of the cybersecurity industry and the skills of tertiary graduates. https://www.is3coalition.org	In 2021, the IS3C (a dynamic coalition within the IGF focusing on Internet Standards, Security and Safety) launched a study to better understand the skill shortage in the cybersecurity sector. After a series of interviews conducted with industry, business and tertiary education leaders in 14 countries, a short list of transversal and professional skills was defined as the	66 countries worldwide cybersecurity industry, academic and research institutions, student bodies cybersecurity education, skill set of tertiary graduates, needs of cybersecurity industry	2022, not updated The research highlights the need for cybersecurity to become a school subject integrated from the moment children use digital technology.

Name	Description	Target area / Target users / Key topics	Additional information
	base-line in a survey set up to seek the viewpoint of a broader population. 235 respondents from 65 countries worldwide completed the survey. Only one in four respondents were women and more than 80% were aged above 30 years. This reflects the lack of diversity across the cybersecurity sector which, according to many interviewees and survey respondents, largely contributes to the skill shortage the sector is facing.		
CISA's Cybersecurity Resources for High Risk Communities https://www.cisa.gov/audiences/high-risk-communities/cybersecurity-resources-high-risk-communities	Web page with index of resources	Civil society and high risk actors	Developed through the Joint Cyber Defense Collaborative process with civil society and industry
Common Good Cyber https://commongoodcyber.org/	Common Good Cyber is a global initiative with the goal of identifying and implementing innovative models for sustaining groups, organizations, and individuals involved in critical cybersecurity functions for the broader Internet community.	Global Non-profit organizations, public, cyber capacity builders cybersecurity	Non-Profit Cyber, Global Cyber Alliance, Cyber Threat Alliance, FIRST, Shadowserver, IST, GFCE, Cyber Peace Institute

Name	Description	Target area / Target users / Key topics	Additional information
Non-Profit Cyber https://nonprofitcyber.org/	Nonprofit Cyber is a coalition of implementation-focused cybersecurity nonprofits to collaborate, work together on projects, voluntarily align activities to minimize duplication and increase mutual support, and link the community to key stakeholders with a shared communication channel.	Global Non-Profit Organizations Cyber Public Good, Cyber Capacity Building	
Tech Policy Atlas https://techpolicydesign.au/tech-policy-atlas	The Global Tech Policy Atlas is a public repository of national tech policy, strategy, legislation and regulation. Its purpose is to assist policymakers and researchers conduct evidence-based independent research. We rely on contributions from users to expand and update the dataset.	Global Policy makers, researchers Tech Policy	
FIRST (Forum of Incident Response and Security Teams) https://www.first.org	FIRST, the Forum of Incident Response and Security Teams, is a global community for incident response teams and practitioners. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large. A community of practitioners, FIRST aspires to bring together incident response and security teams from every country across the world to ensure a	Global Incident Response practitioners, CERT/CSIRT/PSIRT, operational cybersecurity practitioners Incident response, operational cybersecurity, CERT/CSIRT/PSIRT, cyber capacity building	

Name	Description	Target area / Target users / Key topics	Additional information
	safer Internet for all. Together, FIRST and its community provide a trusted platform for information sharing, trust building, standards and good practice development, events, workshops, education, training, and capacity building.		
Postal Sector Information Sharing & Analysis Centre (POST-ISAC) including SECURE.POST https://secure.post	The postal sector is at increasing risk of cyberattacks, which can result in loss of data, disruption of services, and damage to reputation. There is therefore a need to provide a public information portal to provide Posts, and the wider postal sector (including private sector actors), with access to Cyber Capacity Building materials from globally reputable content partners to better understand and manage cybersecurity risks, enhance their resilience to cyberthreats, and maintain the trust of their customers and stakeholders. As part of its Abidjan cycle work proposal 1.1.15, the Universal Postal Union (UPU), through the .POST Business Management Unit within the Postal Technology Centre has commenced implementation of the Postal Sector Information Sharing & Analysis Centre (POST-ISAC) including	Global Wider Postal Sector - includes designated postal operators (i.e. post offices and similar national entities), Wider postal sector players include private companies and partner organizations, such as e-retailers, courier companies, logistics service providers, financial service providers, airlines, railways and other transport companies, customs organizations, manufacturers of postal and postal industry-related solutions, customer associations, unions and postal worker associations, among others. Cybersecurity, Cyber Resilience, Cyber sensitization & awareness	The design of the inventory ensure that the Information is updated as frequently as the information providers' assets are updated. The list of Information Providers is reviewed regularly. Cooperation agreements have been signed with Alliances such as the Global Cyber Alliance, the Global Anti Scam Alliance and the Global Forum on Cyber Expertise.

Name	Description	Target area / Target users / Key topics	Additional information
	the SECURE.POST Online Cybersecurity Capacity Building Portal. The POST-ISAC design contains a comprehensive inventory of global Cyber Capacity Building actors - these actors are those with whom the UPU has secured and will continue to secure Cooperation Agreements to feed the SECURE.POST portal. This SECURE.POST portal will comprise, inter alia, an inventory of Cyber Capacity Building materials and resources utilizing an intuitive Natural Language Processing (NLP) model to provide all UPU members and stakeholders with access to up-to-date information, tools and resources to help them prevent and mitigate cyberthreats.		
South School on Internet Governance https://www.gobernanzainternet.org/ssig2025/en/	The main objective of the South School on Internet Governance SSIG is to train new leaders of opinion in all aspects related with Internet Governance, from a global perspective and with focus on the Latin America and Caribbean Region.	Global Internet community in general Internet governance - Cybersecurity - Cybecrime - Turst in the Internet - Privacy - Artificial Intelligence	SSIG is a founding member of the Dynamic Coalition of Schools on Internet Governance of the IGF. Collaboration is done with several universities and governments of the Americas.

Name	Description	Target area / Target users / Key topics	Additional information
	An important part of the SSIG program is devoted to capacity building in cybersecurity and cybercrime. The program trains university and postgraduate students from the region and from the rest of the world in understanding the complexity related with Internet Governance and its importance in the future of the Internet. SSIG has partnered University of Mendoza for granting a "University Diploma on Internet Governance and Regulations" to those fellows who complete the training and works on a research paper with tutors from this university. This initiative has recieved the WSIS 2024 Prize and other international recognitions. The mission of the South School on Internet Governance is to: - Increase the number of representatives of the Latin American and Caribbean region in the international Internet Governance debate spaces.		

Name	Description	Target area / Target users / Key topics	Additional information
	- Motivate the new regional leaders of opinion to becoming active participants in Internet Governance meetings and activities, where the future of the Internet is shaped. - Make them the future leaders on Internet Governance in their countries and regions.		

Annex to table

* Key topics description *MRU Cybersecurity Readiness and Capacity Assessment Program*

MRU Cybersecurity Readiness and Capacity Assessment Program: A Comprehensive Initiative for Liberia, Guinea, and Sierra Leone The MRU Cybersecurity Readiness and Capacity Assessment Program will conduct a thorough examination of the cybersecurity landscape in Liberia, Guinea, and Sierra Leone. The program covers a wide array of critical topics and scope areas to assess and strengthen regional cybersecurity capabilities effectively. Below is a detailed breakdown of the program's focus areas: 1. Policy and Regulatory Framework Scope: Reviewing current national cybersecurity policies, regulations, and strategies. Key Topics: Effectiveness of national cybersecurity laws. Cross-border cooperation policies within the MRU region. Gaps and strengths in data protection laws and policies. Alignment with international frameworks like the African Union Convention on Cybersecurity and Personal Data Protection. 2. Cybersecurity Workforce Development and Education Scope: Mapping available education, training, and certification programs in each country. Key Topics: Availability and quality of cybersecurity degree programs, certifications, and vocational training. Identifying skill gaps in critical areas (e.g., incident response, ethical hacking, network security). Initiatives to increase youth and women’s participation in cybersecurity. Collaboration with educational institutions to integrate cybersecurity into curriculums. 3. Technical Capacity and Infrastructure Scope: Assessing current cybersecurity infrastructure and technical tools protecting critical assets. Key Topics: Presence and capabilities of Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs). Security protocols and tools used within public and private sectors. Protection measures for critical sectors (e.g., energy, finance, healthcare, telecom). Adoption of advanced technologies (e.g., AI, threat intelligence platforms) in security frameworks. 4. Cyber Threat Landscape and Incident Response Scope: Analyzing the current threat landscape, frequent cyber threats, and incident response capabilities. Key Topics: Types and frequency of cyber threats experienced by each country. Incident response mechanisms in government and critical industries. Processes for reporting, tracking, and responding to incidents. Cross-border information-sharing protocols and MRU-based CSIRT collaboration. 5. Public Awareness and Cyber Hygiene Scope: Gauging public awareness on cybersecurity best practices and online safety. Key Topics: Campaigns addressing phishing, ransomware, and social engineering. Programs promoting cyber hygiene among citizens and businesses. Cybersecurity awareness integration in schools and community initiatives. Private sector's role in promoting cybersecurity education. 6. Private Sector Engagement and Public-Private Partnerships Scope: Evaluating the collaboration between government and private sector to strengthen cybersecurity. Key Topics: Engagement of ISPs, financial institutions, and tech firms in cybersecurity initiatives. Public-private partnerships for information-sharing, capacity-building, and incident response. Policies to support SMEs in strengthening cybersecurity. Accessibility of cybersecurity resources and tools for small businesses. 7. Digital and Financial Inclusion Scope: Balancing digital access with managing cybersecurity risks, particularly in financial services. Key Topics: Cybersecurity readiness for mobile money platforms and digital financial services. Security of e-government services, especially in handling personal data. Protective measures for rural citizens new to digital services. Education on secure digital transactions for safe usage. 8. Cross-Border Cybersecurity Collaboration Scope: Exploring potential and existing cross-border frameworks within the MRU region. Key Topics: Opportunities to harmonize cybersecurity policies across MRU countries. Joint cybersecurity training exercises and workshops. Shared incident response protocols for cross-border cyber threats. Strategies for information-sharing and resource-pooling among MRU countries. 9. Funding and Sustainability of Cybersecurity Initiatives Scope: Evaluating current funding sources and sustainable ways to support cybersecurity efforts. Key Topics: Government and international funding opportunities for cybersecurity projects. Sustainable models for ongoing capacity-building in cybersecurity. Role of regional and international donors in MRU cybersecurity initiatives. Models for creating self-sustaining training and awareness programs. 10. Research and Development in Cybersecurity Scope: Promoting research and innovation in cybersecurity to address regional-specific challenges. Key Topics: Current research on local cyber threats and security technologies. Collaborations with universities and tech hubs to foster innovation. Support for local solutions to combat cyber threats. Opportunities for regional collaboration in cybersecurity R&D.

Main session BPF Cybersecurity Capacity Building at IGF 2024

17 December, 16:45-18:00, Riyadh (online 13:45-15:00 UTC)

Recording

https://www.youtube.com/watch?v=od-6fsiEUYA

Transcript

https://intgovforum.org/en/content/igf-2024-day-2-plenary-main-session-best-practice-forum-on-cybersecurity

Session outline

Problem Statement

While various mappings, inventories, and initiatives provide a wealth of information on cybersecurity capacity-building offerings, overlaps and gaps in information exist and the information may not reach its target audience effectively.

Session Objectives

The BPF will explain how it discussions led to the above problem statement and invite panellists and participants to comment on the problem statement, share their own experiences, and make suggestions to refine or rephrase if needed. The second part of the session will zoom in on actionable solutions, best practices and recommendations to address or avoid the problem

Agenda

1. Welcome & opening of the meeting (5 min)
2. Introduction: the BPF on Cybersecurity Capacity Building (10 min)
3. Panel discussion & participant feedback
   Round 1 Feedback on the problem statement (25 min)
   Round 2 How to address and do better (25 min)
4. Summary and closing remarks (10 min)

Panel and moderation

Panelists

- Ms Tereza Horejsova (GFCE)
- Ms. Mevish P Vaishnav, Academy of Digital Health Sciences
- Ambassador Brendan Dowling (Australia)
- Mr João Moreno Falcão (ZKM)
- Mr Yao Amevi A. Sossou (Youth IGF Benin)

Moderation

- Ms Carina Birarda (BPF co-facilitator), Mx Oktavía Hrund G Jóns (BPF co-facilitator), Ms Josephine Miliza (BPF co-facilitator), Mr Dino Cataldo Dell' Accio (BPF co-facilitator), Ms Hariniombonana Andriamampionoma (BPF co-facilitator), Mr
- Wim Degezelle (BPF Consultant, IGF Secretariat)