GLOBAL FORUM ON CYBER EXPERTISE

OAS

GFCE ANNUAL MEETING 2024

Report

Theme: Unifying efforts to bridge cyber capacity gaps

Table of Contents

Program Overview	3
Executive Summary, Statistics & Event Photography	7
Community Showcase	10
Working Group A session	12
Working Group B session	15
Working Group C session	18
Working Group D session	22
Working Group E session	24
Western Balkans Cybersecurity	26
Opening Ceremony	30
The Future of the GFCE: Open Discussions with the SSC	33
GC3B: Catalyzing Action for Cyber Resilient Development	36

Table of Contents

Africa Cyber Capacity Building Initiatives	40
Women in Cyber Capacity Building (CCB) Breakfast	43
Navigating the Web of International Cyber Processes	48
Bridging Gaps in Cyber Capacity Building: Approaches and Tools for Better Results	50
Building Cyber Resilience: Leveraging Public Tools for Global Cyber Resilience	52
Why do Civil Society Organizations (CSOs) play a key role within CCB?	55
Regional Approach to Cyber Capacity Building: A Reality Check	57
Exploring GFCE role(s) in disrupting internet-enabled child sexual exploitation	60
Projects & Programmes Showcase	63
At the Cutting Edge: What Emerging Technologies Mean for Cyber Capacity Building	65
Global Cyber Expertise Magazine	67
Contact Us	68

September 10, 2024

GFCE ANNUAL MEETING

– DAY 1 –

8:00 Registration

	Hall of Americas	Salón Guerrero	Salón San Martín	General Secretariat Building
9:00 - 10:30	Community Showcase	Building Synergies to fill the coordination gaps: what are incident response and CIP communities missing from CCB? **(Working Group B)**	How is Cyberdiplomacy Evolving? The Future of Cyberdiplomacy and Its Relevance to Cybersecurity Capacity Building **(Working Group A)**	
10:30 - 10:45	**COFFEE BREAK**			
10:45 - 12:15	Community Showcase continued	Cyber Capacity Building to Meet the Challenges of a Post-Quantum World **(Working Group E)**	The impact of legislation on Public-Private Partnerships in countering cybercrime **(Working Group C)**	Western Balkans Cybersecurity: Progress in National Cyber Authorities Establishment and Skills Development (10:30 - 12:00)
12:15 - 13:15	**LUNCH**			
13:15 - 14:00	**OFFICIAL OPENING CEREMONY**			
14:00 - 15:15	**THE FUTURE OF THE GFCE: OPEN DISCUSSIONS WITH THE GFCE STRATEGIC STEERING COMMITTEE**			

September 10, 2024

GFCE ANNUAL MEETING
– DAY 1 –

	Hall of Americas	Salón Guerrero	Salón San Martín
15:15 - 15:30	COFFEE BREAK		
15:30 - 16:30	GC3B: Catalyzing Action for Cyber Resilient Development	Africa Cyber Capacity Building Initiatives (15:30 - 16:50)	Advancing Cybersecurity Workforce Development for Critical Infrastructure **(Working Group D)** (15:30-16:50)
18:00 - 20:00	COCKTAIL RECEPTION (DIRTY HABIT)		

*subject to change

September 11, 2024

GFCE ANNUAL MEETING

– DAY 2 –

8:00 Registration

	Simon Bolivar	Salón Guerrero	Salón San Martín	Hall of Americas
8:30 - 10:00	Navigating the web of international cyber processes (9:00-10:00)	Bridging Gaps in Cyber Capacity Building: Approaches and Tools for Better Results (9:00 - 10:00)		WiCCB Breakfast: Actionable Pathways for Gender Mainstreaming in Cybersecurity (8:30 - 11:00)
10:00 - 11:00	Building Cyber Resilience: Leveraging Public Tools for Global Cybersecurity	Why do Civil Society Organizations (CSOs) play a key role within CCB? Hearing from experiences of the GFCE community and looking ahead		
11:00 - 11:15	COFFEE BREAK			
11:15 - 12:15		Community Showcase	Protecting the Future: Exploring GFCE Roles in Disrupting Internet-Enabled Child Sexual Exploitation	Regional Approach to Cyber Capacity Building: A Reality Check (11:15 - 12:15)
12:15 - 13:15		Projects & Programmes Showcase		At the Cutting Edge: What Emerging Technologies Mean for Cyber Capacity Building (12:15 - 13:15)
13:15 - 14:30	CLOSING REMARKS & LUNCH IN HALL OF THE AMERICAS			

*subject to change

EXECUTIVE SUMMARY

The Global Forum on Cyber Expertise (GFCE) Annual Meeting 2024 was held on September 10-11 in Washington, D.C., under the theme **unifying efforts to bridge cyber capacity gaps**. This year's gathering marked a significant milestone in the ongoing journey to enhance global cyber capacity building efforts. With the cyber landscape becoming increasingly complex and interconnected, the imperative to unify efforts and avoid fragmentation was central to the discussions.

Over the past nine years, the GFCE has played a crucial role in fostering collaboration among many stakeholders in the cyber capacity-building ecosystem. The 2024 Annual Meeting served as a platform to reflect on the progress made, review the GFCE's activities, and reinforce its role in coordinating efforts across key areas, including emerging technologies, alignment with international processes, gender inclusivity and strengthening regional initiatives.

The 9th edition of the Annual Meeting, held at the Organization of American States (OAS) headquarters, provided a unique opportunity for the GFCE community to engage in meaningful dialogue, share updates on emerging issues, and explore strategies to address contemporary challenges in cyberspace. Networking opportunities throughout the two-day event facilitated collaboration and knowledge exchange among participants, reinforcing the importance of unified action.

The Annual Meeting was preceded by the **GFCE Regional Meeting for the Americas and the Caribbean** on September 9, which further emphasized the need for regional cooperation in building cyber capacity. Both meetings underscored the GFCE's commitment to enhancing global coordination and strengthening cyber resilience worldwide.

This report summarizes the key **discussions, outcomes, and strategic insights** from the GFCE Annual Meeting 2024, reflecting the collective effort to bridge cyber capacity gaps and build a safer and more inclusive digital future for all.

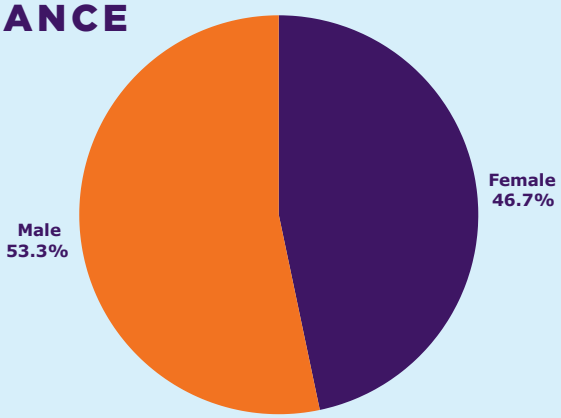
ANNUAL MEETING IN NUMBERS

The 9th edition of the Annual Meeting brought together both old and new members and partners of the GFCE global community. We are grateful for the attendance of leaders, policy-makers and experts from all sectors and regions, fostering a true multi-stakeholder inclusive approach in cyber capacity building. We are pleased to share some key numbers on participant representation at the Annual Meeting below.

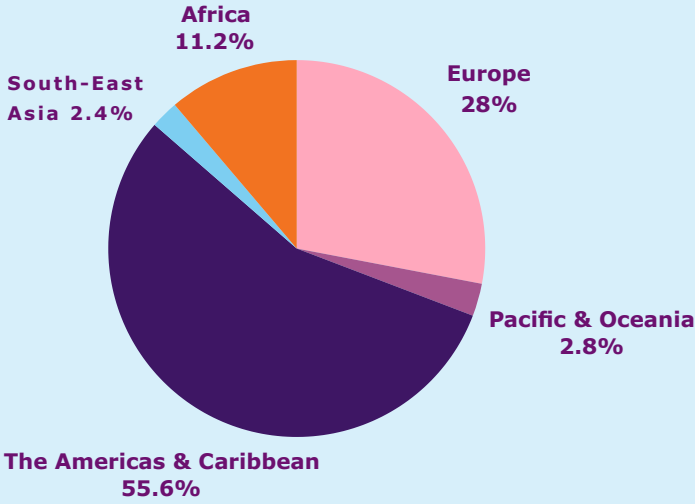
+200 PARTICIPANTS

from all over the world

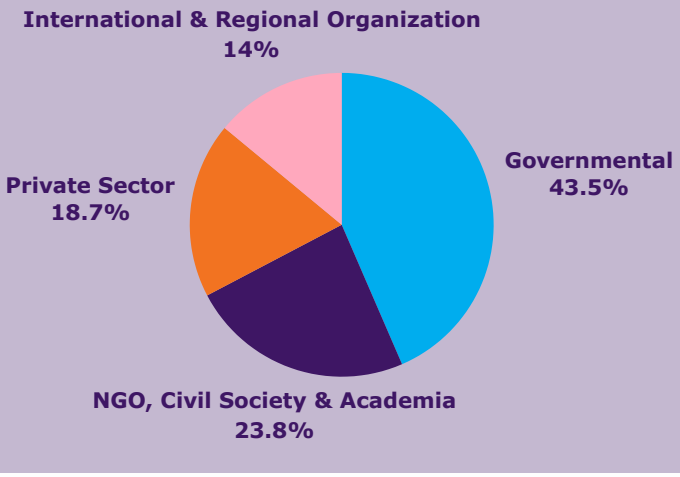
GENDER BALANCE



REGIONAL REPRESENTATION



STAKEHOLDER REPRESENTATION

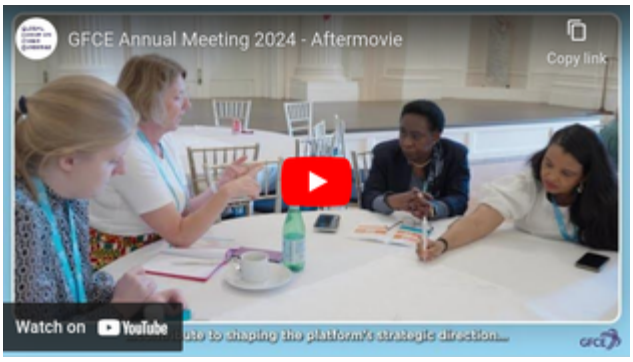


EVENT PHOTOGRAPHY

You can use the link below to access the GFCE Flickr Account, where you can see and download the photos from the Annual Meeting 2024.

If you share them on social media, don't forget to tag us and use the meeting's hashtag **#GFCEAM24**

ACCESS THE PHOTOS HERE



Plenary Session

GFCE Community Showcase 2024

BACKGROUND OF THE SESSION

The Community Showcase served as a valuable platform to highlight the work of GFCE Members and Partners, promoting enhanced collaboration, knowledge sharing, and information exchange within the GFCE Community. Featuring eleven showcases, the session offered an opportunity to present recent achievements, best practices, and new initiatives.

SPEAKERS

- **Ms. Nicole Isaac (CISCO) & Ms. Kendra Gaither (US Chamber of Commerce)** - *Building Africa's Digital Future.*
- **Mr. David Satola (World Bank) & Mr. Keongmin Yoon (World Bank)** - *World Bank Update on Combatting Cybercrime: Tools and Capacity Building for Emerging Economies.*
- **Ms. Bridget Chan (New America) & Ms. Pavlina Pavlova (UNODC) -** *Diversity as Strength: Investing in Next-Generation Ideas in Cybersecurity.*
- **Ms. Catherine Newcombe (US Department of Justice) –** *The ICHIP Program : International Computer Hacking & Intellectual Property Attorney Advisors.*
- **Mr. Robert Collett (Chatham House) -** *A Principles-Based Approach to Cyber Capacity-Building (CCB): Understanding and Operationalizing the OEWG CCB Principles.*
- **Mr. Bertie Kerr (Bae Systems) -** *Delivering Cybersecurity Capacity Building across the Indo-Pacific: How to Achieve Strategically Significant Change.*
- **Mr. Rob Davidson (Information and Communication Technology's Council) -** *Canada's Information & Communication Technology Council: Entering a Fourth Decade of Cyber Capacity Building.*
- **Mr. Alexander Beatty (Atlantic Council) -** *The Cyber 9/12 Strategy Challenge in San José - Takeaways for Capacity Building and Cyber Workforce Development in Latin America & the Caribbean.*
- **Ms. Carolin Weisser Harris (GCSCC) & Mr. Phil Sheriff (GCSCC) -** *Evaluating the Impact of Cyber Capacity Building – Typologies and Outcomes***.**
- **Mr. Olly Jones (PGI) -** *Tackling Hybrid Threats - Taking a Holistic View to Digital Resilience.*
- **Ms. Estefania Belen Vergara Cobos (World Bank) -** *Cybersecurity Economics for Emerging Markets.*

DISCUSSION

The discussions brought forward projects and initiatives from key GFCE regions, spanning across Latin America & the Caribbean, Africa, Asia, the Pacific, North America, and Europe. Speakers delved into various topics, including Cyber Capacity Building, Emerging technologies, Cybersecurity Workforce Development, Digital Crime, Justice and Resilience, and Emerging Markets. These themes, closely linked to both current and future trends in cyber capacity building, underscored the global expertise of the GFCE Community.

KEY TAKEAWAYS

The Community Showcase was instrumental in fostering deeper collaboration, facilitating the exchange of information, and promoting knowledge sharing among GFCE Members and Partners. Providing a platform for open dialogue helped strengthen the network of relationships within the GFCE community. Experts shared valuable insights, allowing participants to identify gaps and to highlight key lessons learned from previous experiences. The discussions emphasized best practices and uncovered opportunities for new partnerships and cooperative efforts. As a result, the showcase set the stage for enhanced coordination and future collaboration between GFCE Members and Partners, paving the way for innovative projects and joint initiatives to address global cyber capacity building challenges.

Working Group A Breakout Session:

How is Cyberdiplomacy Evolving? The Future of Cyberdiplomacy and Its Relevance to Cybersecurity Capacity Building

SPEAKERS

- Moderator: Heli Tiirmaa-Klaar, Chair of IT Coalition Steering Group, Chair of Global Cyber Alliance Board of Directors
- Isaac Morales Tenorio, Senior Director for Cybersecurity and Data Privacy Communications, LATAM at FTI Consulting
- Pavlina Ittelson, Executive Director, Diplo Foundation US
- Pablo Castro, Cybersecurity Coordinator at the Ministry of Foreign Affairs - Government of Chile
- Moctar Yedaly, GFCE Africa Hub Director

BACKGROUND OF THE SESSION

This Working Group A panel explored emerging trends and strategic priorities of cyberdiplomacy. It focused on geopolitical dynamics, the role played by non-state and regional actors, and how emerging technologies such as AI, blockchain, IoT, and quantum computing influence cyberdiplomacy, presenting both opportunities and challenges.

Overall, the panel aimed to enhance understanding of cyberdiplomacy's future directions and strategic relevance to global cyber capacity building (CCB) efforts.

DISCUSSION

The session opened with the question on how cyberdiplomats can strengthen CCB and what has been achieved so far. From the perspective of the Latin American and Caribbean (LAC) region, cyberdiplomacy is a relatively new but significant topic. Confidence-Building Measures (CBMs) are central to fostering regional collaboration in these efforts. It is crucial for Ministries of Foreign Affairs (MFAs) and Ministries of Interior to stay informed about regional initiatives and effectively leverage available opportunities. Programs from the Organization of American States (OAS) have significantly enhanced the region's cyber capabilities, providing valuable resources. To fully benefit from these initiatives, countries must first assess their needs and prioritize actions at the national level. Adhering to national strategies is essential for ensuring continuity, and prioritizing national coordination is critical.

In the Africa region, the term "cyberdiplomat" is unfamiliar to many diplomats, and the concept of cyberdiplomacy is often absent across the continent. This lack of awareness is evident in the region's limited participation in UN cyber processes. Key challenges include a shortage of expertise and resources, as securing funding for diplomats to attend crucial conferences is often difficult. The GFCE is supporting the alignment of donors in the region and collaborating with various institutions to strengthen CCB efforts, enhance knowledge of cyber laws and legislation, and promote awareness of cyberdiplomacy. The growing risks posed by AI and emerging technologies, particularly from the East, highlight the urgent need for the region to prepare collectively for these challenges.

Within the broader cyberdiplomacy ecosystem, DiploFoundation plays a key role in ensuring that cyber negotiations are inclusive, particularly for smaller developing states. It is equally important to clarify the roles of non-state stakeholders in these negotiations and to engage young people early on to equip them with the necessary expertise for the future. One notable initiative led by DiploFoundation is the Geneva Dialogue on Responsible Behaviour in Cyberspace, which produced the Geneva Manual on Responsible Behaviour in Cyberspace. This manual primarily targets non-state stakeholders, offering guidance on implementing norms related to vulnerabilities and reporting vulnerabilities, while also addressing the protection of critical infrastructure.

With rapid technological advancements on the rise, it is crucial for diplomats to stay informed about these developments. DiploFoundation actively encourages diplomats to address and anticipate the challenges associated with emerging technologies. Prevention through diplomacy and knowledge is crucial, especially for countries that feel they are falling behind. This approach involves engaging with tech experts to foresee upcoming challenges and, consequently, guide diplomats in determining where their governments should invest. However, creating policies that are robust enough to endure over time while remaining flexible enough to adapt to emerging technologies presents a significant challenge.

Cyberdiplomacy also encompasses the private sector. In the LAC region, for instance, both public and private sectors play a significant role in advancing cyberdiplomacy, and public-private partnerships (PPPs) are essential for preventing cyber-attacks. By examining private sector practices and industry standards, we can identify concrete measures that, while not directly linked to cyberdiplomacy, can still be viewed as forms of implementation. Collaboration between the private and public sectors is mutually beneficial, especially in efforts to mitigate large-scale cyber-attacks.

KEY TAKEAWAYS

Confidence-building measures (CBMs) are essential for fostering regional collaboration in cyberdiplomacy efforts.

Ministries of Foreign Affairs (MFAs) and Ministries of Interior must stay informed about regional initiatives and leverage available opportunities effectively. Countries must assess their needs and prioritize actions at the national level to benefit fully from regional initiatives.

Adhering to national strategies and ensuring national coordination is crucial for the continuity of cyberdiplomacy efforts.

The growing risks posed by AI and emerging technologies necessitate collective preparation. Diplomats must stay informed about rapid technological advancements and anticipate challenges associated with emerging technologies.

Collaboration between the public and private sectors is essential for advancing cyberdiplomacy and preventing cyber-attacks. Examining private sector practices and industry standards can help identify concrete measures to implement cyberdiplomacy effectively.

Creating policies that are robust yet flexible enough to adapt to technological advancements is a significant challenge in cyberdiplomacy.

Working Group B Breakout Session:

Building Synergies to fill the coordination gaps: What are incident response and CIP communities missing from CCB?

SPEAKERS

- **Moderator: Marc Henauer,** Senior Political and International Affairs Officer, Federal Office for Cyber Security NCSC / GFCE WG-B CIP Lead
- **Tracy Bills**, Chair of the Board of Directors of the Forum of Incident Response and Security Teams (FIRST.org) (SEI/CMU)
- **Carlos Leonardo,** CSIRT-RD
- **Dr. Vilius Benetis**, NRD CS / GFCE WG-B CIM Lead

BACKGROUND OF THE SESSION

This Working Group B session brought together cyber capacity building (CCB) practitioners working on incident response and critical infrastructure protection (CIP) to discuss what more could be done to build capacities and coordinate efforts globally.

A panel composed by experts from different regions and backgrounds working on CCB analysed what is the current status: what is working and could be exported to other regions, what could be improved in the short term and ambitions for the long term.

DISCUSSION

The session focused on addressing key CCB coordination challenges in the context of incident response (IR) and the protection of Critical Infrastructure (CI). One of the primary activities discussed was the role of the Forum of Incident Response and Security Teams (FIRST) in providing global assistance to improve the capabilities of Computer Security Incident Response Teams (CSIRTs), with a special focus on national-level teams. A recurring theme was the lack of clarity in the roles and mandates of national CSIRTs, especially concerning their involvement in CI protection. This creates gaps in IR efforts, as not all national CSIRTs include CI within their scope. To address this, participants emphasized the importance of clearly defining roles and responsibilities, as well as expanding IR plans to bridge these gaps.

A significant challenge identified was the diverse approaches different countries take in identifying their CI sectors and managing cybersecurity risks. In some countries, like the Dominican Republic, critical sectors such as water, which is vital for agriculture, are not sufficiently prioritized, despite their importance to public well-being. There was a call to reevaluate the definition of CI based on usage patterns, dependencies, and the potential impact on public health and safety. Moreover, the need for countries to develop legal frameworks that properly reflect their national context and sector-specific criticalities was underscored, as was the need for accountability through audits and compliance measures.

Trust and communication between CI operators and government authorities were highlighted as essential for effective incident response. Successful case studies, such as the collaboration in Denmark's energy sector, demonstrated how building strong relationships among stakeholders can lead to a more resilient IR ecosystem without excessive regulation. Additionally, the role of knowledge-sharing platforms, like the Global Forum on Cyber Expertise (GFCE), was noted as critical for transferring good practices and avoiding the pitfalls of a one-size-fits-all approach to CCB.

Training also emerged as a key activity, with cross-sector initiatives designed not only to build technical skills but also to foster trust and interoperability among CI operators. The need to scale these efforts, especially in larger countries with extensive CI, was discussed, with the "train-the-trainer" model presented as a scalable solution to broaden the impact of CCB programs. Political buy-in was also seen as a crucial factor in promoting CCB initiatives, with participants stressing the importance of aligning cybersecurity risks with national security concerns to gain the attention of political leaders.

In smaller countries, the process of building a cybersecurity ecosystem was viewed as potentially more agile, as decision-makers and key stakeholders can more easily come together to align priorities and create a cohesive strategy. The example of the Dominican Republic's collaboration with external partners such as Estonia and the U.S. Department of State in conducting annual cybersecurity exercises (TTXs) was cited as a successful model of building continuous capacity and ensuring that both government executives and CIP providers understand their roles in an incident response scenario.

Ultimately, the session concluded that while frameworks and legal measures are essential, they are not enough on their own. There is a critical need for a cultural shift, where CIP operators take ownership of their cybersecurity responsibilities. The establishment of trust, open communication, and regular cooperation between governments, private sector operators, and international partners is crucial to building an effective cybersecurity ecosystem. The GFCE was highlighted as an important platform for fostering dialogue and collaboration, with participants calling for continued efforts to share good practices, refine incident response strategies, and adapt cybersecurity frameworks to the unique needs of each country.

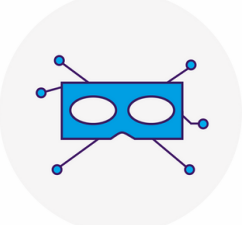
KEY TAKEAWAYS

It is necessary to define roles and mandates, there needs to be clarity on who is supposed to be doing what and how, within an oversight and accountability framework. It can be useful to look at what other countries are doing, but every country has their own interests and their own systems, so there is no one-fits-all approach to developing regulatory frameworks. CIP development approaches need to be tailor-made, and need to be framed in a way that appeals to political leadership.

The responsibility of effective CIP is to be shared among governments and service providers. Governments are responsible for creating an environment in which the cybersecurity ecosystem can grow independently.

It is important to exploit the momentum provided by cyber incidents and leverage it for resources and developing regulatory frameworks.

Training often happens in silos, but that should change. Creating training opportunities for CI operators from different sectors (eg. healthcare, civil aviation, etc.) can constitute a useful moment not only for learning and interoperability through the transfer of knowledge but also for building the ecosystem and trust across sectors, which is instrumental during CI incidents.



Working Group C Breakout Session:

The impact of legislation on Public-Private Partnerships (PPP) in countering cybercrime

SPEAKERS

- **Moderator: Nnenna Ifeanyi-Ajufo,** GFCE WG-C Chair
- **Taylor Grossman**, Deputy Director for Digital Security, Institute for Security and Technology
- **William Garrity**, Manager, Global Cybersecurity Policy, Mastercard
- **Pavlina Pavlova**, UN external expert on cybercrime & #ShareTheMicInCyber Fellow, New America

BACKGROUND OF THE SESSION

The Digital Services Act (DSA) represents a landmark in EU legislation, designed to create a safer and more trusted online environment by addressing the spread of illegal content while upholding users' fundamental rights. As this new regulatory framework comes into effect, its implications for public-private partnerships in the context of countering cybercrime are profound and multifaceted.

This Working Group C session explored the necessity of a legislative framework which envisions more integrated collaboration between the private sector and the public sector, particularly law enforcement agencies. Given the increasing complexity and volume of cyber threats, such partnerships are crucial to enhancing the capabilities of law enforcement and mitigating the burden they face. The session will analyze case studies and best practices on how to successfully carry out PPP in the countering of cybercrime.

DISCUSSION

The session commenced with Nnenna addressing the importance of public-private partnerships (PPPs) in the realm of cybercrime. She emphasized that leading up to the Cybercrime Convention, numerous discussions had centred around the topic of PPPs. Further dialogue is needed to address the implementation strategies and collaborative efforts required for effective cooperation between governments and private sector entities. Strengthening this integrated collaboration is crucial to building more robust and efficient PPPs.

This is also reflected at the regional level, particularly in Article 26 of the Malabo Convention, which emphasizes the significance of public-private cooperation in combating cybercrime. The rationale behind this emphasis is clear: effective cybersecurity requires joint efforts in infrastructure development and implementation between governments and private entities.

Pavlina highlighted the significant contributions of civil society in combating cybercrime, as noted in the report titled "Strengthening Public-Private Partnerships on Cybercrime: Regional Perspectives from the Americas, Africa, and Asia." The United Nations Office on Drugs and Crime (UNODC) has a robust global cybercrime program, which serves as a critical resource in this effort. Recognizing the growing importance of civil society's engagement, UNODC's Civil Society Unit has begun developing targeted initiatives on cybercrime to facilitate collaboration across stakeholders. These efforts are particularly focused on regions in the Global South, such as the Americas, Africa, and Asia.

The report acts as a practical and accessible tool, highlighting regional best practices, as well as the challenges and opportunities within existing partnerships. It stresses the need for enhanced partnerships by focusing on triangular cooperation among governments, private sectors, and civil society. This approach not only improves expertise and transparency but fosters trust—essential for effective partnerships.

One key finding emphasizes the importance of trust in forming effective partnerships. Pavlina noted that building this trust is necessary because the current landscape lacks it, hindering collaboration. Without trust, partnerships cannot flourish. Additionally, Pavlina stressed the need to understand the requirements on the ground, to better align resources and ensure stakeholder engagement from the outset. This includes recognizing the importance of bringing partners together and creating a sense of shared ownership in the partnership.

Challenges outlined in her speech include conflicting legislative frameworks, limited resources, and lack of coordination. The report also outlines specific opportunities, such as improving cooperation on data requests, supporting systematic information sharing, and addressing cybercrime inequalities. A multistakeholder approach remains critical, as partnerships can offer a path to better understand local needs and foster stronger cooperation.

Finally, Pavlina underscored the need to include all stakeholders from the beginning and emphasized the importance of adapting partnerships to evolving environments and changing stakeholder needs. She concluded by reiterating the necessity for countries to build the capacity to follow up on these reports and partnerships effectively.

Taylor focused on the topic of public-private partnerships (PPPs) to counter ransomware, referencing the report titled "Public-Private Partnerships to Combat Ransomware: An Inquiry into Three Case Studies and Best Practices." Published earlier in the year by the Institute for Security and Technology (IST), the report examines three key PPP models: Europol's European Cybercrime Centre (EC3), the United States Joint Cyber Defense Collaborative (JCDC), and the Institute for Security and Technology's Ransomware Task Force (RTF).

She emphasized that these partnerships have distinct structures and operate at different stages of the ransomware combat process. The report highlights how each partnership has evolved over time and the role they play in addressing ransomware threats. A central theme is the importance of information sharing. This is a key factor in successfully combating ransomware, as sharing data and intelligence across sectors helps to improve the overall response. IST facilitates these efforts by deconflicting activities and offering neutral platforms, such as the Ransomware Task Force, where different stakeholders can collaborate more effectively.

Taylor also underscored the significance of understanding the various incentive structures involved in PPPs. These structures differ between public and private actors, and aligning these interests is essential to forming sustainable and effective partnerships. One of the major recommendations from the report is the need to build trust between stakeholders. Trust is critical for any partnership, and Taylor pointed out that current PPPs often rely on ad hoc relationships rather than a systematic approach to fostering trust. Another important point was the need for stakeholders to become familiar with these systems before they are required to implement them. Being prepared in advance enables smoother operations when it becomes necessary to act in the face of ransomware threats.

Will emphasized the crucial role of trust in PPPs, noting that Mastercard's involvement in different partnerships stems from its business foundation of trust. In-person connections are key to building trust, enabling deeper collaboration than remote efforts allow. He highlighted that successful PPPs must be structured to meet community needs and should be stress-tested for resilience.

Will identified two focus areas for Mastercard's PPP efforts: capacity building for under-resourced communities by providing cybersecurity guidance and promoting secure digital inclusion, and driving information sharing well in advance of crises to build stronger, more effective partnerships. Looking forward, he stressed that PPPs must be tailored to fit the specific needs of different communities and regions. A flexible, localized approach ensures that partnerships can connect with and effectively support the communities they serve.

In the Q&A, the importance of designing partnerships with a clear understanding of partner motivations and shared ownership from the beginning was emphasised. Engagement should be built on trust and long-term commitment, as partners and motivations may change over time. Europol, for instance, regularly reassesses its partnership members. The discussion also highlighted the importance of including communities with firsthand experience, especially victims of cybercrime, and adopting an inclusive, multistakeholder approach. Effective engagement requires understanding overlapping goals, patient relationship-building, and stress-testing. To encourage information sharing, systems that protect anonymity while providing incentives for sharing are crucial.

In the breakout discussion, participants highlighted the importance of coordination and mutual trust between the private sector and government bodies, with the private sector needing to actively build trust with the public sector. There was agreement on the need for consistency in defining terms that signal the escalation of an event, though this is often lacking across sectors. Finally, discussions emphasized that partnerships must be tailored to fit the specific needs of different communities and regions, as what works in one jurisdiction may not be effective in another.

KEY TAKEAWAYS

- Flexibility in definitions and actions is crucial for effective partnerships.
- PPPs must be practical and driven by stakeholder input, allowing project managers to address challenges raised.
- Triangular cooperation enhances transparency while respecting privacy regulations like GDPR.
- Active in-person exchanges and pilot projects are important for building effective collaborations.
- Trust among stakeholders is essential, with continuous efforts needed to improve and maintain it.
- Partnerships must be dynamic and adaptable as actors change, requiring constant awareness of who the key players are.

Working Group D Breakout Session:

Advancing Cybersecurity Workforce Development for Critical Infrastructure

SPEAKERS

- **Moderator: Luanda Domi**, Facilitator of the Working Group D & Gender Mainstreaming and Cyber Skills Development Manager, GFCE
- **Todd Spires**, Director, Cyber and Digital Resilience Programs, CRDF Global & newly appointed Chair of the GFCE's Working Group D on Cybersecurity Culture and Skills
- **Roselle Safran**, CEO & Founder, KeyCaliber
- **Randy Pestana**, Director of Cybersecurity Policy, Florida International University (FIU)

BACKGROUND OF THE SESSION

This Working Group D session focused on the urgent need to advance workforce development in cybersecurity for critical infrastructure. With the escalation of cyber threats from state and non-state actors, it is essential to develop robust cybersecurity talent pipelines, supported by regulatory standards, industry best practices, and collaborative public-private partnerships.

GFCE also welcomed Todd Spires as the new Chair of Working Group D. Spires brings extensive experience from his role as Director of Cyber and Digital Resilience Programs at CRDF Global, where he has been instrumental in implementing cybersecurity initiatives aimed at improving resilience across diverse sectors. With a career dedicated to advancing digital resilience and cybersecurity, Todd's leadership in Working Group D will contribute significantly to GFCE's mission of elevating global cybersecurity standards.

DISCUSSION

- **Integrating Regulations and Standards into Talent Pipelines**

The speakers examined the effective integration of regulatory frameworks, standards, and best practices within cybersecurity workforce development. Roselle Safran emphasized the need for customized cybersecurity guidelines tailored to specific organizational needs, advocating for a centralized strategic focal point within organizations to steer cybersecurity initiatives. Randy Pestana highlighted the NIST Cybersecurity Framework as a critical tool for aligning communication and practices among diverse stakeholders, enhancing cohesion across government, private sector, and civil society. Todd Spires underscored the importance of practical simulations, exercises, and regulatory compliance within workforce pipelines, fostering a resilient culture aligned with the protection of critical infrastructure.

- **Role of Public-Private Partnerships in Workforce Development**

The session addressed the significant role of public-private partnerships in bridging skills gaps within the cybersecurity workforce. Spires noted the complexities of donor coordination, as different donor priorities often complicate workforce alignment. He emphasized that organizations are increasingly seeking professionals with soft skills—such as creativity, intellectual curiosity, and team communication—that complement technical expertise. Pestana identified challenges in assessing cybersecurity needs accurately and aligning workforce training with industry requirements. He recommended partnerships with hiring organizations to provide practical experience, helping bridge the gap between academic training and employer expectations. Safran expanded on these points, stressing the importance of hands-on experience within academic programs and the role of a centralized focal point to guide organizational cybersecurity strategy effectively.

- **Immediate and Long-Term Skill Needs**

The speakers also explored immediate and long-term skill needs essential for building a sustainable cybersecurity workforce. Randy Pestana advocated for a long-term approach that includes diversity initiatives, reaching underrepresented groups and creating pathways to attract a broad talent pool. Todd Spires underscored the need for competencies that encompass both cyber and physical vulnerabilities, which are integral to critical infrastructure protection. Roselle Safran highlighted the importance of structuring short-term skills training within a broader, long-term strategy, with each phase of training contributing to a sustainable cybersecurity program.

- **International Upskilling Initiatives and Case Study: Ukraine**

The session concluded with insights into successful international upskilling initiatives, including those targeting the Ukrainian cybersecurity workforce. Pestana shared a project that trained Ukrainian military officers in cybersecurity, providing them with the necessary skills to transition into civilian cybersecurity roles. Spires highlighted the “Cyberdefenders” program in Ukraine, which trained war veterans in both technical and soft skills, illustrating the value of targeted upskilling initiatives in critical infrastructure resilience.

KEY TAKEAWAYS

The session highlighted the vital role of leadership, strategic coordination, and tailored workforce development in building resilient cybersecurity frameworks.

Customized programs that address specific organizational needs, combined with strong public-private partnerships, form the foundation for effective, real-world cybersecurity training.

Integrating diverse skills and inclusive hiring practices enables organizations to cultivate a versatile workforce equipped to adapt to evolving cyber threats, reinforcing critical infrastructure protection.

Working Group E Breakout Session:

At the Cutting Edge: What Emerging Technologies Mean for Cyber Capacity Building

SPEAKERS

- **Moderator**: **Chris Buckridge**, Senior Strategy Advisor, Global Forum on Cyber Expertise (GFCE)
- **Selvana Gopalla**, Information Security Specialist at the Computer Emergency Response Team of Mauritius (CERT-MU) of the Ministry of Information Technology, Communication and Innovation
- **Sarah Nicole**, Senior Policy & Research Associate, Project Liberty Institute
- **Elizabeth Thomas-Raynaud**, Head of Emerging digital technology unit, Directorate for Science, Technology and Innovation, OECD
- **Martin Koyabe**, Senior Project Manager | Lead AU-GFCE Coordination, Global Forum on Cyber Expertise (GFCE)

BACKGROUND OF THE SESSION

Emerging technologies - artificial intelligence, quantum computing, and more - are at the forefront of today's digital policy discussions. Managing the opportunities and advances made possible by these technologies, while mitigating the inherent risks is a challenge that governments and regulators the world over are grappling with. The need for cyber capacity building efforts to respond to these developments is clear, but that response is still evolving. This session will draw on expertise from across the GFCE community and beyond to understand the changes underway and explore the strategies that will help keep cyber capacity building efforts current and relevant.

DISCUSSION

Chris Buckridge introduced this session, reflecting on the past Working Group E sessions, what can be seen as emerging technologies, and questioned whether emerging technologies can be seen as a useful umbrella term.

Panelists discussed the role of governance and policy making when it comes to emerging technologies and highlighted the dual nature of emerging technologies. This duality was especially significant in sectors such as agriculture and cybersecurity, where the benefits of emerging technologies, such as the increase in job creation, go hand in hand with increased risks.

Sarah Nicole noted that while regulations are necessary, the EU AI Acts – which had to be rewritten multiple times due to the constant updates of technology - is an example of how difficult it is to include emerging technologies in regulations. She also addressed the toolkit developed by Project Liberty designed to help various stakeholders navigate the complexities of blockchain governance, noting that the toolkit has been designed to understand how to design and govern your own community online, in blockchain and beyond.

Elizabeth Thomas-Raynaud highlighted OECD's Framework for Anticipatory Governance as a means to help tackle the challenges of policy-making for emerging technologies. The framework aims to equip governments and stakeholders to anticipate governance needs by leveraging technology for societal benefit and building long-term capacity to manage emerging challenges effectively. The OECD is focused on stakeholder involvement to create such a framework to understand the potential impact of technologies on human lives, considering aspects including human rights and democratic values.

Coming back to the concept of emerging technologies as an umbrella term, Selvana Gopalla highlighted that it is a useful terminology that serves as a catalyst for innovation in many different sectors. However, this innovation comes with challenges, one of which is the scale and speed at which the emerging technologies are evolving. While cyber capacity building approaches are improving, currently they cannot fully keep pace with it, and she noted that, while many regions and organizations have governance frameworks and standards, many countries lack behind on the development and adoption of these technologies. Therefore, creating awareness and providing explanations of these standards and legislation is almost as important as having the legislation to begin with.

KEY TAKEAWAYS

Speakers on the panel emphasized the importance of international cooperation, and inclusive actions to develop and improve regulatory frameworks.

Multistakeholder participation and the prioritization of ethical considerations are crucial in maximizing the benefits of these technologies while managing the associated risks.

It is clear that emerging technologies are reshaping our approach to cybersecurity, and that cyber capacity building must also adapt to match this evolving landscape.

Panel Discussion:

Western Balkans Cybersecurity: Progress in National Cyber Authorities Establishment and Skills Development

SPEAKERS

- **Moderator: Luanda Domi,** Gender Mainstreaming and Cyber Skills Development Manager, Global Forum on Cyber Expertise (GFCE) & Advisor for Western Balkans
- **Stefan Andonovski,** Minister of Digital Transformation, Skopje
- **Lulëzon Jagxhiu**, CTO and Advisor to the Prime Minister, Pristina
- **Era Gjata,** Head of Sector for International Project Coordination, Strategic Development, and Identification, Directorate of International Project Coordination and Strategic Development of Cybersecurity, National Cybersecurity Authority, Tirana
- **Jair H Van der Stelt**, Policy Advisor, U.S. Department of State

BACKGROUND

The Western Balkans session addressed ongoing efforts to enhance cybersecurity resilience in the region, with each participating country sharing its progress and challenges in developing cybersecurity frameworks aligned with the European Union's NIS2 Directive. With the shared goal of fortifying national cybersecurity capabilities, countries in the region are making strategic decisions on how best to align their governance structures with EU requirements, particularly in establishing or strengthening National Cybersecurity Authorities (NCAs).

DISCUSSION

The Western Balkan countries emphasized that cybersecurity remains a top priority, yet highlighted the importance of tailoring programs to fit each country's unique governance structures and developmental stages. While there is consensus on regional collaboration, it was noted that each country has distinct institutional approaches and needs, underscoring the necessity for customized cybersecurity initiatives.

- **Diverse Approaches to Cybersecurity Governance**

Albania, Kosovo, and North Macedonia are each at different stages in establishing or refining their NCAs to manage national cybersecurity responsibilities. Albania has progressed significantly, with a fully operational National Cybersecurity Authority that has passed new legislation aligned with the NIS2 Directive. This advancement underscores Albania's proactive stance on cybersecurity governance and its commitment to comprehensive threat management and resilience within critical infrastructure sectors.

Conversely, Kosovo and North Macedonia are actively developing their cybersecurity frameworks and are taking context-specific approaches. Kosovo has passed the law and all secondary legislation for establishing its NCA, focusing on a "whole-of-society" approach that integrates the private sector as an essential partner in securing critical infrastructure. This model reflects Kosovo's intent to leverage existing national resources and engage a broad range of stakeholders in its cybersecurity efforts.

- **North Macedonia's Integrated Departmental Approach**

North Macedonia stands out in its approach by opting not to create a standalone NCA but instead establishing a dedicated Cybersecurity Department within its Ministry of Digital Transformation. This decision reflects a strategic assessment of national resources and existing institutional structures, where cybersecurity oversight can benefit from the support of established departments, such as human resources and legal services, within the Ministry. North Macedonia's model highlights a pragmatic response to frequent election cycles and limited resources, emphasizing that cybersecurity governance can be strengthened within existing frameworks rather than through new agencies.

- **Challenges and Regional Coordination Needs**

All countries agreed on the importance of regional coordination to combat cyber threats effectively. However, the session underscored that while regional cooperation is essential, it must also accommodate the specific institutional and developmental realities of each country. This tailored approach will require flexibility in cybersecurity capacity-building programs, particularly as countries like Kosovo and North Macedonia move toward full implementation of cybersecurity regulations and structures.

- **Public-Private Partnerships and Talent Retention**

Each country recognized the need to address workforce shortages in cybersecurity, a persistent challenge due to competitive global markets and the migration of skilled professionals. The Western Balkans aim to bridge this gap by fostering public-private partnerships, with both Kosovo and Albania placing a strong emphasis on private sector collaboration in national cybersecurity efforts. By engaging private companies and educational institutions, the countries aim to create robust pipelines for cybersecurity talent, develop sustainable career paths, and retain professionals within the public sector through salary increase for technical roles.

- **Role of International Support and Knowledge Sharing**

The U.S. Department of State plays a key role in supporting the Western Balkans' cybersecurity development, particularly through initiatives focused on establishing and strengthening National Cybersecurity Authorities (NCAs). By sharing its expertise in cybersecurity governance, workforce development, and diversity, the U.S. provides valuable resources and best practices that Western Balkan countries can adapt. Emphasizing digital literacy and diversity as foundational elements, the U.S. promotes a comprehensive workforce strategy that includes training frameworks and initiatives to bring underrepresented groups, such as women and minorities, into cybersecurity roles. This collaborative support aligns with the region's goals of protecting critical infrastructure and closing workforce gaps, reinforcing a strong, unified cybersecurity posture tailored to local governance and resource needs, particularly in light of recent geopolitical events.

Launching of the Project titled: "Coordination of Cyber Security and Capacity Building Efforts in the Western Balkans" - Presented by Velimir Radičević (GFCE Program Coordinatior)

Project Objectives

- Enhanced Efficiency in Capacity Building: To support funders active in the Western Balkans, enabling more efficient cyber capacity building.
- Proactive Communication and Resource Matching: The GFCE Western Balkans Group will actively communicate needs and priorities, matching them with available resources, and create joint regional capacity building programs.

Activities

- Regular Meetings and Capacity-Building Travel: Facilitation of more frequent meetings for the Western Balkans Group and enabling travel to regional events for capacity-building purposes.
- Multi-Stakeholder Conference in 2025: Organize a regional conference to align perceptions, provide updates, and coordinate efforts among members and donors.
- Clearing House Programs: Facilitate two regional Clearing House programs, responding to priorities from the Western Balkans Group (e.g., legislative development, youth capacity building, technical support).
- Decision-Making Tools for Donors: Create online tools to aid decision-making and streamline communication between donors, implementers, and local partners.
- Virtual and In-Person Meetings: Provide support for ongoing efforts to deconflict and align CCB initiatives across the region.

KEY TAKEAWAYS

The Western Balkans cybersecurity session highlighted a strong commitment to enhancing regional cyber resilience through tailored governance models, regional cooperation, and support from international partners. The GFCE's capacity-building project, combined with U.S. backing, ensures a collaborative approach that considers each country's unique institutional landscape while supporting the collective goal of a resilient, secure Western Balkans.

OPENING CEREMONY

SPEAKERS

- **Masters of Ceremony: Tereza Horejsova,** GFCE Senior Outreach Manager
- **Mr. Nestor Mendez**, Assistant Secretary General of the Organization of American States (OAS)
- **Ms. Maartje Peters**, Former GFCE Co-Chair, new SSC member
- **Mr. Chris Painter,** GFCE Foundation Board Former President and Member
- **Ms. Cristina Camacho,** GFCE Foundation Board Chair & Minister, International Cooperation & Partnerships, Mission of Ecuador to the EU
- **Mr. Richard Harris,** Advisory Board, new SSC member

BACKGROUND OF THE SESSION

The Opening Ceremony of the GFCE Annual Meeting 2024 welcomed the GFCE global community to the 9th edition of the event. The Ceremony was hosted in the memorable Hall of the Americas at the Organization of American States (OAS) headquarters, where the 1st GFCE Annual Meeting took place.

DISCUSSION

The Master of Ceremonies, Tereza Horejsova, opened the GFCE Annual Meeting 2024 by highlighting the significant time at which this meeting is held, given the introduction of key governance structures. She introduced the keynote speech of Nestor Mendez, the OAS Assistant Secretary General, who highlighted the rapid pace of digitalization, describing it as a double-edged sword in many regions, especially in Latin America and the Caribbean. While the Latin America and the Caribbean region have made great strides in embracing technology, they continue to incur new and complex risks. Data from the EY Global Cybersecurity Leadership Insight Study concluded that 91% of Latin American companies recorded a cybersecurity incident last year, while 62% had suffered a data breach. Checkpoint Research, a cyber threat intelligence entity, concluded that there had been a 30% yearly increase in cyber attacks globally, reaching 1,636 attacks per organization per week.

***Mr. Nestor Mendez**, Assistant Secretary General of the Organization of American States (OAS)*

Cyber threats have a strong impact since they can disrupt essential services, erode public trust, and have far reaching economic consequences. Mendez emphasized the need to continue to embrace international cooperation as a way forward, one in which nations work together, share information, and build collective resilience against cyber threats. He conveyed OAS's vision on cybersecurity, which is to achieve a level where there are known rules for what is or isn't acceptable to do in cyberspace. The OAS aims to promote responsible state behaviour and accountability in cyberspace by adhering to international laws and norms, respecting state sovereignty, and refraining from conducting malicious cyber activities.

In his statement, Mendes also emphasized his belief that the Foundation Board and the new GFCE Strategic Steering Committee (SSC) will facilitate a more formal, empowered, inclusive and transparent mechanism to represent multiple stakeholders in cyberspace. As the SSC comprises representatives of each stakeholder group, including donors, civil society and the private sector, and have a regionally balanced community, it will help positively shape the strategy and direction of the future of the GFCE and the global cyber capacity building progress. He welcomed the start of a new structure of the GFCE and opened the GFCE Annual Meeting 2024 to the audience.

The second keynote speech was given by Maartje Peters, who introduced the exciting results and the growth that the GFCE has accomplished over the past year. First, she highlighted the Women in Cyber Capacity Building (WIC) Fellowship, which has rightfully gained significant attention. Under this Fellowship, the GFCE has facilitated the participation of 77 female diplomats in UN cyber processes. She emphasised that this has not only significantly increased the visibility, participation, and interventions of female diplomats in UN discussions, such as the OWEG and the Ad-Hoc Committees, but it also meant the strong and meaningful engagement and collaboration of a variety of countries all over the world in UN discussions on cyberspace. Furthermore, she stated that the GFCE helped effectively connect national cyber capacity building ecosystems with their receptive regions, and in turn these regions to the international community through the network of regional hubs in Africa, the Americas & Caribbean, the Pacific and South-East Asia. She exemplified this through the GFCE Africa Hub, which facilitated the creation of the first African Cyber Capacity Building agenda, involving key stakeholders from the region. In November 2023, the GFCE co-organized the inaugural Global Conference on Cyber Capacity Building (GC3B) in Ghana, bringing together a high level, diverse and multi-stakeholder community to discuss solutions, share results and mobilize resources for cyber capacity building. Furthermore, she emphasised that the SSC has been formed to provide a broader scope in cybersecurity, maintaining and strengthing the growth, network, resources, and trusted relationships the GFCE has cultivated over the years. Peters reminded the audience that the members have been carefully selected taking into account geographical representation, gender balance as well as expertise from governments, CSOs, and private sector. She also explained that the rationale behind the transition of the Co-Chairs and Advisory Boards structures into the SSC is to streamline and enhance the governance of the organization.

Horejsova went on to introduce the key address from Chris Painter, who reminded the audience that the GFCE has grown with a very a global (and continuously growing) network, which are key in contributing tot the field. He went on to state how over these years, the GFCE has faced challenges, celebrated successes, and most importantly, grown from an organization into a community, from 99 members and partners when the Foundation Board was created in 2019 to over 230 members and partners in 2024. He highlighted how the GFCE has seen the establishment of the regional hubs, creating communities in their regions and developing regional networks, such as the Cyber Capacity Building Coordination Committee in 2021. This has provided oversight and feedback on key cybersecurity capacity building projects and ensured great coordination and effective use of resources across the African continent. Furthermore, Painter stated that the GFCE developed and sustained a number of critical tools and mechanisms, such as the Civil Knowledge Portal and the Clearing House mechanism, as well as Cyber Capacity Building Knowledge modules and a catalogue of options for establishing national cyber strategies. Moreover, he emphasized how the community had worked with Microsoft Sweden and the International Telecommunications Union (ITU) to develop a compendium for mainstreaming cybersecurity into the digital development agenda. As THE GFCE sees exciting and significant structural changes, he strongly urged community members to stay connected and be active in the GFCE's work. As he closed his speech, he symbolically passed the mic to Cristina Camacho for a brief introduction to the community.

Cristina Camacho introduced herself and stated that the community will have some cyber challenges ahead. However, she is thrilled to work with the Foundation Board, the Strategic Steering Committee and all of the community to new ideas and efforts forward, bringing the GFCE to a new phase.

Richard Harris, representing the Advisory Board, welcomed the new structure of GFCE. He stated that the primary purpose of the Advisory Board was to reflect the voices of civil society in the GFCE. The huge growth in the number of partners and members, the increasing importance of cyber capacity building in the globe's complex technological and geopolitical environments among other things are important reasons why the GFCE decided to improve their governance structure. The Advisory Board was in agreement about the governance structure changes, particularly the creation of the SSC. He highlighted past contributions of the Advisory Board, which included formulating GFCE inputs to the OEWG, encouraging civil society participation in the working groups, and helping the community understand where they could find the best value from the GFCE. Harris emphasized that civil society organizations remain vital to the GFCE and they will have a strong voice on the SSC and the Foundation Board. He called upon all of the community to renew shared commitment to helping nations, regions, and people create a secure and safe digital future for everyone.

The final part of the opening ceremony, which shifted into the next session on the SSC, consisted of a video presentation of Strategic Steering Committee members.

Plenary Session:

The Future of the GFCE: Open Discussions with the Strategic Steering Committee

SPEAKERS

- **Master of Ceremonies: Dr. Tereza Horejsova**
- **Rick Harris,** Former Advisory Board, new SSC member
- **Louise Marie-Hurel,** Former Advisory Board, new SSC member

BACKGROUND

This interactive session allowed the GFCE Community to directly engage with the new Strategic Steering Committee. The roundtable format enabled participants to brainstorm and express their thoughts, concerns and ideas on GFCE developments directly with the Steering Committee, who will use it as an opportunity to reflect and assess the future direction of the GFCE and how we can better support the needs and ambitions of our global community.

DISCUSSION

The session focused on improving knowledge sharing, platform usability, and strengthening the role of regional hubs in cyber capacity building. The session began with participants discussing the challenges posed by the Cybil portal, a key GFCE knowledge-sharing platform. Many agreed that Cybil's usability could be significantly enhanced by revamping its user interface, making it easier for users to navigate and access critical information. Currently, users struggle to find relevant resources unless they know exactly what to look for. To address this, there was a recommendation to reorganize the platform's layout, simplifying how information is updated and accessed to encourage broader community engagement. Streamlining these processes would allow members to share knowledge more effectively.

Another central theme of the session was the need to improve interoperability among knowledge repositories, as many valuable resources are siloed across different think tanks, academic institutions, and organizations. Participants emphasized the potential of integrating these sources with Cybil to enable more effective cross-referencing and collaboration. Using emerging technologies like AI to analyze data from these sources could allow for more informed decision-making across the community. Furthermore, it was suggested that regional hubs play a more proactive role in disseminating local insights through Cybil, helping to provide the GFCE community with region-specific information and perspectives.

Inclusivity and diversity within the GFCE framework were also highlighted as priorities. Participants pointed out the importance of representing different regional needs, such as those of the Caribbean, Pacific, and the Americas, to ensure balanced global representation. Inclusivity should also span cultural and demographic lines, with a special emphasis on encouraging input from underrepresented groups, including women.

The role of regional hubs in supporting cyber capacity-building initiatives was another major focus. The session underscored that hubs should prioritize local needs and act autonomously from the GFCE Secretariat to better reflect the interests of their specific regions. Using tools like the National Cybersecurity Index, hubs can assess the cybersecurity posture of member countries, tailoring their initiatives to address those unique needs. Additionally, it was recommended that hubs support cross-collaboration by sharing lessons learned, such as those from the Pacific hub, with other regions facing similar challenges.

When discussing the GFCE's Clearing House mechanism, participants expressed concerns about its current limitations. Many felt that the Clearing House creates unrealistic expectations as it can be slow to respond to requests from countries in need. A more flexible model, potentially transitioning from a match-making service to one focused on planning and networking support, was proposed to better manage expectations. By facilitating conversations and helping countries refine their requests, the Clearing House could better connect countries with suitable donors and implementers. To address delays, there was a proposal to establish a dedicated GFCE trust fund, which would provide immediate financial resources while awaiting longer-term donor assistance. However, participants acknowledged that the current donor climate might make this difficult to implement.

Regional hubs were also encouraged to take on a more active role in the Clearing House process by helping countries align their requests with donor priorities. This would involve assisting in the planning and proposal stages, ensuring that the requests resonate with donors' long-term strategic goals. Better donor coordination was also advised to prevent overlap and ensure assistance reaches areas most in need. Participants stressed that by aligning regional hub activities with both local and global cybersecurity objectives, GFCE could achieve a more unified, impactful approach to cyber capacity building.

The session concluded with an acknowledgment of the GFCE community's growth, announcing the addition of new members, including the Italian Republic, Chad, Namibia, and Aruba. As the community expands, the GFCE is increasingly focused on fostering collaboration, refining strategic priorities, and actively listening to its diverse stakeholders. The session ended on an optimistic note, with participants invited to continue the dialogue informally over the coffee break and at the official reception that took place subsequently, emphasizing the GFCE's commitment to building an inclusive and responsive global cybersecurity community.

KEY TAKEAWAYS

The community emphasized the need to improve the interoperability and usability of GFCE platforms, like the Cybil Knowledge Repository. AI tools were proposed, as well as improving the process of updating content.

Enhancing the Clearing House mechanism was also reiterated, including involving the GFCE Regional Hubs more.

Empowering the Regional Hubs was also emphasized, with a focus on addressing local challenges and strengthening inclusivity and diversity of representation.

Plenary Session

GC3B: Catalyzing Action for Cyber Resilient Development

SPEAKERS

- **David van Duren,** GFCE Director
- **Vincent Barras**, Embassy of Switzerland in the USA
- **Nayia Barmpaliou**, Cyber Lab International

BACKGROUND OF THE SESSION

The Global Conference on Cyber Capacity Building (GC3B) 2023 was a key gathering that helped secure and improve decision makers' awareness on cyber capacity building by bringing the cyber and development silos together, strengthened coordination of efforts on a global scale and widened the pool of resources available. The 2025 edition will build on these successes to further bridge the gap between the cyber and development silos, helping bring cyber resilience to the forefront of national and international agendas.

In line with this, the session explored the importance and the need for cyber resilient development and how the Accra Call can enable more concrete best practices to align the development and cyber security community. In addition, this session was open, allowing participants to come up with possible outcomes to make the Accra call concrete and constitute an opportunity to share concrete lessons learned for conducting CCB (projects).

DISCUSSION

- **Overview of the GC3B and its strategic importance**

The meeting commenced with a comprehensive overview of the Global Conference on Cyber Capacity Building (GC3B), which has grown into a pivotal event for advancing international dialogue and action on cyber resilience and sustainable development.

David van Duren underscored the GC3B's role in bridging the gap between the cybersecurity and development sectors. He emphasized how cyber resilience is not merely a technical concern but a crucial component for advancing global sustainable development goals (SDGs). The conference has become a cornerstone in the global effort to operationalize cyber resilience for development .

Referring to the Accra Call for Cyber Resilient Development, David highlighted that the document, launched during GC3B 2023 in Accra, Ghana, has garnered widespread support with endorsements from more than 70 governments and organizations. This call to action provides a framework for mainstreaming cyber resilience into broader development agendas. He noted that the next GC3B in Switzerland (2025) would build upon the successes of the Accra event, further advancing this mission.

- **Cyber resilience as a driver for development**

Mr. van Duren elaborated on the growing understanding that cyber resilience is foundational for enabling sustainable economic and social progress, particularly in an increasingly digital world. In this context, he noted that digital threats continue to evolve and pose significant risks to both national and international development efforts. He stressed that ensuring the security of digital ecosystems is vital for safeguarding critical infrastructure, protecting sensitive data, and fostering trust in digital systems, which are integral to development outcomes. Without robust cybersecurity, development goals such as the SDGs could be jeopardized, as disruptions in digital infrastructure can lead to economic losses, social instability, and setbacks in achieving long-term development objectives.

- **Reflections on the first GC3B (2023) and its outcomes**

The inaugural GC3B 2023 in Accra brought together over 600 participants, including government representatives, international organizations, civil society, and private sector actors. Over the course of 95 sessions, the conference served as a platform to share knowledge, build partnerships, and discuss solutions to enhance global cyber resilience. The **Accra Call for Cyber Resilient Development,** a major outcome of the 2023 conference, was highlighted as a catalyst for coordinated global action. This framework aims to align efforts across various sectors, ensuring that cyber resilience is embedded into global and national development strategies. The GC3B's emphasis on multi-stakeholder participation, including inputs from diverse geographical regions and sectors, was seen as a critical factor in its success. The discussions during the 2023 conference laid the groundwork for more robust global cooperation on cyber capacity building (CCB) and set the stage for the next conference in Switzerland.

- **Preparations for the GC3B 2025 in Switzerland**

Vincent Barras, representing the Embassy of Switzerland, introduced plans for the upcoming GC3B 2025. He noted that Switzerland's commitment to hosting the conference is rooted in the country's broader approach to international development and cybersecurity. Mr. Barras emphasized the need for strong security measures in digital systems to protect critical infrastructure and enable trust in the digital economy. Without these measures, development initiatives can be undermined by cyber threats, leading to widespread consequences such as economic losses and disruptions in essential services. The second GC3B in Switzerland aims to continue fostering international cooperation, with a particular focus on safeguarding infrastructure, protecting data, and promoting CCB for sustainable development. Switzerland's role as a host reflects its long-standing commitment to multilateralism and cyber diplomacy.

- **Promoting diversity and inclusion in CCB**

A key topic raised during the session was the importance of promoting diversity and inclusion within the CCB community. Participants stressed that efforts to build global cyber resilience must include the perspectives and contributions of women and minorities, who are often underrepresented in the cybersecurity field. Nayia Barmpaliou emphasized the need to actively involve these groups in future conferences and capacity-building projects, not just as beneficiaries but as leaders and contributors. This aligns with the GFCE's commitment to mainstreaming gender inclusivity and ensuring that all stakeholders have equal opportunities to participate and contribute.

- **Operationalizing the Accra Call for cyber resilient development**

There was an in-depth discussion on how to operationalize the Accra Call to make it more actionable and impactful. David van Duren urged participants to explore concrete steps that could be taken to align their national and organizational strategies with the Accra Call's objectives. These steps include strengthening public-private partnerships, enhancing international coordination, and securing financial resources to support CCB at scale. By mainstreaming cyber resilience into development programs, governments and organizations can better address emerging challenges while contributing to broader sustainable development goals.

- **Future focus: workshops and practical solutions**

There was a consensus among participants on the need to expand practical workshops and training programs as part of future GC3B events. These workshops should focus on real-world applications of cybersecurity, such as protecting critical infrastructure and responding to cyber incidents. Platforms like Cybil, which match needs with solutions, were recognized as vital tools in ensuring efficient knowledge sharing and avoiding duplication of efforts in capacity building. Increased use of digital platforms and social media to disseminate best practices and enhance visibility of CCB initiatives was also encouraged.

- **Engagement and communication strategies**

The session also touched on the importance of effective communication strategies to promote cyber resilience initiatives. Participants discussed leveraging social media platforms such as LinkedIn and Twitter to reach a broader audience, especially in the lead-up to the 2025 GC3B in Switzerland. It was recommended that short promotional videos and regular updates be posted on the GC3B website and other communication channels to keep stakeholders engaged and informed.

KEY TAKEAWAYS

Enhance diversity and inclusion: Actively promote the involvement of women and minorities in all CCB efforts and future GC3B conferences, ensuring diverse representation in decision-making roles.

Develop promotional content: Produce and disseminate short videos and promotional materials on the GC3B website and social media platforms to raise awareness and engage stakeholders in the lead-up to GC3B 2025.

Organize practical workshops: Plan and execute practical, hands-on workshops focused on cybersecurity, cyber resilience, and development, enabling participants to develop critical skills applicable in real-world contexts.

Organize practical workshops: Plan and execute practical, hands-on workshops focused on cybersecurity, cyber resilience, and development, enabling participants to develop critical skills applicable in real-world contexts.

Strengthen public-private partnerships: Encourage collaboration between governments, private sector, and civil society to operationalize the Accra Call and integrate cyber resilience into broader development strategies.

Expand use of digital platforms: Leverage platforms like Cybil to enhance coordination, share knowledge, and match resources with identified needs, improving the efficiency of CCB efforts globally.

Breakout Session:

Africa Cyber Capacity Building Initiatives - Enhancing Cyber Resilience and Capacity Building in Africa

SPEAKERS

- **Moderator: Dr Martin Koyabe**, Senior Manager, GFCE Africa
- **Mr Amine Idriss Adoum**, Senior Director, Infrastructure and Energy, Industrialisation, Trade and Regional Integration (AUDA-NEPAD)
- **Mr Moctar Yedaly**, Director, GFCE Africa
- **Mr Ghislain de Salins**, Senior Digital Development Specialist, World Bank Group
- **Major Gbota Gwaliba**, Director General (DG), Agence Nationale de la Cybersécurité (ANCy), Togo (Republic of Togo Representative)
- **Mr Samuel Asiyanbola**, Associate Director, Cyber and Privacy Advisory, KPMG, Nigeria
- **Mr Malik Arnold Geraldo**, Agence Nationale de la Cybersécurité (ANCy), Togo
- **Mr Palakiyem Assih**, Chief Technology Officer (CTO), Cyber Defense Africa (CDA), Togo
- **Mr Simon Melchior**, Director General (DG), Cyber Defense Africa (CDA), Togo.

BACKGROUND

Digital transformation in Africa is a dynamic and rapidly evolving process that is reshaping economies, societies, and governments across the continent. This session highlighted two selected initiatives that aim to enhance cyber resilience and capacity building in the continent. The selected initiatives include the Africa Agenda on Cyber Capacity Building (AA-CCB). It was developed to enhance coordination and identification of successful policies, practices, and ideas for cyber capacity building in Africa. The second initiative to be presented encourages Africa cooperation on cybersecurity resilience, through establishment of the African Centre for Coordination and Research in Cybersecurity (ACCRC) in Togo.

The session was hosted by project partners: AUDA-NEPAD for AA-CCB, and KPMG, GFCE, World Bank, UNECA and Republique Togolaise for the ACCRC project.

DISCUSSION

- **Mr Moctar Yedaly:**

Highlighted the importance of the Africa Session during the GFCE Annual Meeting. He emphasized the impact of the two initiatives in enhancing CCB at the national, regional and global levels. GFCE Africa, which is GFCE's Africa regional hub, in partnership with AUDA-NEPAD and Africa CCB Coordination Committee members, developed the AA-CCB agenda.

- **Mr Amine Idriss ADOUM:**

Highlighted the activities undertaken by AUDA-NEPAD and GFCE in the formulation of the implementation plan for the AA-CCB agenda in Africa. He emphasized that cybersecurity is not merely a technical issue but a matter of national security and economic stability and that AUDA-NEPAD, in collaboration with the GFCE, has made significant strides over the past two years. These achievements include the formation of the African Cyber Experts (ACE) Community, the Cyber Capacity Building Coordination Committee (CCB-CC), and the African Agenda on Cyber Capacity Building (AA-CCB).

- **Dr Martin Koyabe:**

Highlighted the need and benefits of establishing the centre, including providing the opportunity to enhance cyber resilience and coordinate cybersecurity research in the African continent. He also emphasised that ACCRC will provide potential access to relevant cybersecurity services and exchange ideas, knowledge, and information with cybersecurity experts within and outside Africa.

- **Mr Ghislain de Salins:**

Informed the participants of World Bank commitment to the project and support to the Republic of Togo. He emphasized the need for more regional cooperation and integration on Cybersecurity and related focus areas, to better empower cybersecurity practitioners in Africa.

- **Major Gbota Gwaliba:**

He appreciated the support from the World Bank Group and project consortium members. He assured participants of the government of Togo's full support for the project. The government of Togo welcomes potential partners from both private and public sector, and funding agencies, in supporting the establishment of ACCRC.

- **Mr Samuel Asiyanbola:**

Provided a breakdown of why participants and potential partners should support the establishment of ACCRC. He emphasized the need for cooperation and coordination of Cybersecurity in Africa.

- **Mr Simon Melchior, Mr Palakiyem Assih and Mr Malik Arnold Geraldo:**

Provided an account of the efforts made by the government of Togo to establish ACCRC. They both stressed the need to develop a business model that will support the operations and sustainability of the centre.

KEY TAKEAWAYS

Capacity Building: the participants expressed the essential need to develop both technical know-how/expertise and the willingness to engage stakeholders in CCB initiatives in Africa.

Demand-Driven CCB: CCB initiatives must respond to the specific needs of African nations and empower them to use the knowledge effectively.

Consistency and Complementarity of CCB: CCB initiatives need to ensure consistency across the various initiatives emerging on the continent, especially on regional cooperation and coordination in Cybersecurity.

Data Collection: There is a need for better data collection on cybersecurity incidents in Africa to inform policymaking. Once established, ACCRC is well placed to support such initiatives in Africa.

Collaboration: All stakeholders emphasized the importance of building trust and coordination at national, regional, and global levels.

Plenary Session

Women in Cyber Capacity Building (CCB) Breakfast: Actionable Pathways for Gender Mainstreaming in Cybersecurity

OPENING REMARKS AND KEYNOTE SPEECHES

- **Marjo Baayen**, Director of the Global Forum on Cyber Expertise (GFCE)
- **Luanda Domi**, Gender Mainstreaming and Cyber Skills Development Manager, GFCE
- **Melissa Hathaway**, President of the Hathaway Global Strategies LLC, and Former Cybersecurity Policy Advisor to the White House
- **Cristina Camacho-Terán**, Minister, International Cooperation & Partnerships, Mission of Ecuador to the European Union Embassy to Belgium and Luxembourg & Chair of the GFCE Foundation

BACKGROUND

Building on previous GFCE's Women in Cyber Capacity Building Network (WiCCB) events focused on developing diverse cyber career pathways and fostering global impact, this interactive follow-up session translated insights into actionable strategies to enhance gender diversity in cybersecurity. Featuring speakers from GFCE's WiCCB network, the session provided resources for women's career advancement. Through collaborative group work involving over 120 participants worldwide, attendees tackled structural barriers, mapped successful inclusion initiatives, designed mentorship programs, and developed strategic engagement plans for stakeholders. This collective input will guide WiCCB's strategic direction, driving tangible progress in building a diverse, inclusive cybersecurity workforce that empowers women globally.

Summary of keynotes

The session opened with a powerful address from Marjo Baayen, who spotlighted the urgent need for diversity to address the cybersecurity workforce shortage. "Our challenge isn't just a lack of people in cybersecurity—it's a lack of diverse perspectives," she stated, underscoring the importance of women's leadership in shaping the field. She associated the Women in Cyber Capacity Building (WiCCB) Network as a crucial force for breaking barriers and fostering global collaboration. "WiCCB is about leadership, not just participation," Marjo emphasized, highlighting its role in building pathways for women into leadership through mentorship and cross-regional collaboration.

Building on Marjo's call to action, Luanda Domi framed WiCCB as the heart of this transformative effort. "Today's event is about action, about showing what happens when women are given opportunities," she declared. Luanda stressed that WiCCB is pivotal to advancing cross-regional collaboration and sustaining investment in Diversity, Equity, and Inclusion (DEI), positioning it as a catalyst for lasting change. "We're shaping a cybersecurity future as diverse as the challenges it faces," she added.

Continuing this momentum, Melissa Hathaway discussed the importance of self-awareness, preparation, and resilience for women leaders in cybersecurity, reminding participants that leadership requires more than technical expertise; it demands integrity and resilience. Cristina Camacho-Terán highlighted the need for diverse voices in global cybersecurity frameworks, drawing from Ecuador's experience in adapting global policies to local needs. "Resilient frameworks must reflect the voices of all regions," she noted, advocating for a cybersecurity diplomacy that embraces regional perspectives and inclusivity.

Together, these keynote addresses set the session's tone as a platform for tangible progress in advancing gender mainstreaming in cybersecurity. The session the continued with a panel discussion to further deep dive on topic foci above.

PANEL SPEAKERS

- **Moderator: Luanda Domi**, GFCE
- **Nina Olesen**, Chief Operating Officer of Women 4 Cyber Foundation, and Head of Skills and Human Factors Sector at the European Cyber Security Organisation (ECSO)
- **Confidence Staveley**, Founder of the CyberSafe Foundation
- **Priyanka Chatterjee,** Co-Founder and Board Member at WiCSME
- **Anne Marie Mills**, the U.S. Department of State, Bureau of Cyberspace and Digital Policy

KEY CONTENT FROM PANEL DISCUSSION

- **The Evolving Role of Women in Cybersecurity**

The discussion kicked off with an acknowledgment of the growing yet insufficient presence of women in cybersecurity roles. While there has been progress, the cybersecurity workforce shortage remains acute, with women representing a fraction of the talent pool. Speakers emphasized that the narrative surrounding DEIA must evolve. The conversation has shifted from justifying the need for diversity to understanding how women can drive innovation in cybersecurity through their unique perspectives and skills. Panel emphasized that women's lived experiences allow them to identify cybersecurity vulnerabilities that may be overlooked by their male counterparts, making their participation critical to the sector's growth and effectiveness.

- **Challenges in Diversity, Equity, Inclusion and Accessibility (DEIA) Messaging and Investment**

One of the session's central themes was the disparity in DEIA funding and focus, with speakers noting a global reduction in investment in DEIA initiatives. There was a consensus that despite the increasing awareness of diversity's importance, organizations are still underfunding programs that are essential to retaining women in cybersecurity. The DEIA narrative needs to be reframed—from a "nice to have" to a business-critical necessity. The discussion also stressed the importance of data-driven advocacy, where demonstrating the tangible benefits of DEAI through evidence and metrics can compel stakeholders to make sustained investments.

- **The Role of Cyber Diplomacy**

Speakers underscored the growing significance of cyber diplomacy as a critical field where women can excel and lead. The Women in Cyber Fellowship, discussed during the session, serves as an example of empowering women in cyber diplomacy, preparing them to navigate complex international negotiations. Through this fellowship, women from the Global South are given the tools to shape cybersecurity policy at the UN level. The discussion highlighted the importance of scaling such initiatives globally, as cyber diplomacy not only strengthens international cyber policy but also creates leadership opportunities for women.

- **WiCCB as platform for Cross-Regional Collaboration and Mentorship**

A major theme was the need for cross-regional collaboration to break down silos between cybersecurity initiatives. The WiCCB Network has been instrumental in fostering global partnerships among women-led cyber initiatives, ensuring that best practices are shared across regions. The speakers proposed that cross-regional mentorship programs should be adaptable and flexible to meet the needs of women at different career stages and in different cultural contexts. These programs should focus not only on technical skills development but also on leadership pathways, ensuring that women have the support to rise to decision-making positions. WiCCB as network of networks, ought to serve, as an advocacy tool for regional women's networks working in cybersecurity capacity building for global impact.

Breakout Group Discussions:

At the WiCCB Breakfast Session, approximately 120 participants from around the globe gathered to share experiences and strategies for advancing gender diversity in cybersecurity. Expert-led breakout groups focused on practical solutions for both global and regional challenges to shape WiCCB's future direction. Key discussions emphasized strengthening global collaboration among women's cybersecurity initiatives, enhancing mentorship programs with a global perspective, and leveraging cyber diplomacy for gender mainstreaming. Participants also explored increasing regional investment in DEI initiatives, supporting women in leadership through targeted upskilling and reskilling, attracting and retaining women in cybersecurity roles, and scaling impactful educational initiatives. Together, these insights provided a foundation for WiCCB's strategic direction, fostering a more inclusive cybersecurity landscape worldwide.

BREAKOUT DISCUSSION FACILITATORS

- **Dr. Towela Nyirenda-Jere**, GFCE Foundation Board
- **Irene Corpuz,** Co-Founder and Board Member of Women in Cyber Security Middle East (WiCSME)
- **Cristina Camacho-Terán**, GFCE Foundation Board Chair & Minister, International Cooperation & Partnerships, Mission of Ecuador to the EU
- **Priyanka Chatterjee**, Co-Founder and Board Member, Women in Cyber Security Middle East (WiCSME)
- **Confidence Staveley**, Founder and Executive Director, CyberSafe Foundation
- **Nina Olesen**, Chief Operating Officer, Women4Cyber Foundation
- **Floreta Faber,** Deputy Director, National Cyber Security Authority, Albania
- **Era Gjata**, Head of Sector, International Projects Coordination and Strategic Development, Albanian National Cyber Security Authority
- **Randy Pestana**, Director of Cybersecurity Policy, Jack D. Gordon Institute for Public Policy, FIU
- **Sorene Assefa**, Cybersecurity and Digital Governance Expert, UNECA
- **Klée Aiken**, Director of Community & Capacity Building, Forum of Incident Response and Security Teams (FIRST)
- **Rick Harris,** Principal Cyber Security and Privacy Engineer, MITRE

KEY TAKEAWAYS

The session concluded with each facilitator sharing three key outcomes from their respective breakout groups, highlighting the diverse insights and actionable steps discussed. These summaries provided a clear roadmap for WiCCB's future efforts:

Reframe DEI as a Core Business Strategy: Facilitators emphasized that WiCCB should encourage organizations to embed Diversity, Equity, and Inclusion (DEI) into their core strategies. By showing the economic and security benefits of including women in cybersecurity, WiCCB can drive sustained investment in DEI initiatives.

Develop Global Mentorship and Leadership Programs: A key outcome from many breakout groups was the importance of mentorship and leadership training. Facilitators stressed that WiCCB should lead the development of scalable, flexible mentorship programs that support women at all career stages and are tailored to regional needs, with a focus on long-term sustainability.

Leverage Cyber Diplomacy for Gender Mainstreaming: Several facilitators highlighted the importance of cyber diplomacy as a tool for advancing gender equality. WiCCB was encouraged to integrate cyber diplomacy into its strategic initiatives, helping women from underrepresented regions participate in international cyber policy discussions.

Strengthen Cross-Regional Collaboration: Facilitators also stressed the need for WiCCB to continue fostering cross-regional collaboration. By acting as a bridge between women's initiatives in different parts of the world, WiCCB can promote global cooperation, helping women share resources, best practices, and strategies.

Create a Leadership Pipeline for Women: Building a leadership pipeline for women in cybersecurity was a recurring theme. Facilitators encouraged WiCCB to focus on helping women advance from entry-level roles to leadership positions through targeted upskilling and mentorship programs.

Advocate for Sustained Investment in DEI Initiatives: Finally, facilitators noted the need for WiCCB to push for sustained investment in DEI initiatives, particularly in under-resourced regions. By highlighting the long-term benefits of a diverse workforce, WiCCB can help secure the funding needed to support these initiatives.

Plenary Session

Navigating the Web of International Cyber Processes

SPEAKERS

- **Moderator**: **Pavlina Pavlova, UN external expert on cybercrime & #ShareTheMicInCyber Fellow, New America**
- **Tracy Hackshaw**, Chef d'Entreprise, .POST Business Management Unit, Universal Postal Union (UPU)
- **Liina Areng**, Director, EU CyberNet
- **Robert Collett**, Director, Developing Capacity Ltd
- **Louise Marie Hurel**, Cybersecurity Researcher, Royal United Services Institute (RUSI)

BACKGROUND

As cyber issues have gained prominence and urgency over the past decade, efforts to coordinate collective, global responses have led to a myriad of processes, venues, and structures spread across the United Nations, international organisations, and multinational private sector entities. This session will help untangle the current state of play, the developments to watch out for, and explore the question of how such processes can most effectively help meet the cyber capacity needs of governments and stakeholders the world over.

DISCUSSION

This session kicked off with a consideration of the ongoing work in the Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG). Louise Marie Hurel noted that discussions around peace and security in the digital space have been going on for more than two decades, including the development of norms of state behaviour in cyberspace, and the implication that states should undertake best effort to implement these norms draws cyber capacity building (CCB) into the discussion. However, she noted the tension this can create, as some states see peace and security as very distinct from development activities.

Pavlina Pavlova gave some insight on the work underway to develop a UN treaty on cybercrime, which has also been linked (again, somewhat contentiously) to CCB efforts. Robert Collett highlighted that CCB activities (like the Women in Cyber fellowships) have enabled the active participation of a lot of countries that were disengaged from these processes, and that has made the UN processes better, producing outcomes more reflective of global views of cybersecurity. But he also noted the risks, particularly when new mechanisms are proposed that duplicate existing efforts, such as a trust fund (similar to that managed by the World Bank), a CCB portal (similar to portals maintained by UNIDIR, the ITU, or the GFCE's Cybil Portal), and global coordination activities (work that the GFCE has been very active in).

Liina Areng emphasized the potential for CCB to builds bridges between different communities and skillsets, and in particular the role that regional networks can play in developing these links. Tracy Hackshaw noted the opportunities that have been created in recent years for UN agencies to work more closely with CCB partners, stressing the importance of working cooperatively to develop effective CCB strategies. He also stressed the need for a real-time, "living" inventory of global, regional, sub-regional, national, and sectoral CCB initiatives if we wish to optimize multistakeholder collaboration within and with the UN system (as well as other IGOs and INGO.

KEY TAKEAWAYS

There was strong agreement that all stakeholders should seek to coordinate in support of the existing mechanisms and structures. This is especially vital as international cyber processes inspire the creation of new projects or initiatives that can duplicate or detract from existing work.

There remains a strong need to mobilise funds for CCB efforts, especially if we hope to ensure such efforts reach all the necessary regions and stakeholders.

Regional initiatives are an essential element in this discussion, and a collective effort to strengthen these networks and initiatives is imperative.

Breakout Session

Bridging Gaps in Cyber Capacity Building: Approaches and Tools for Better Results

SPEAKERS

- **Nayia Barmpaliou** (Cyber Lab International)

BACKGROUND

The significant growth in the complexity of the cyber capacity building ecosystem in the last decade, primarily due to the broader scope and increased financing of actions on cyber cooperation combined with the larger number of stakeholders involved, has also increased the diversity in CCB approaches and practices. While the methodological frameworks underpinning CCB implementation vary significantly, there has been long-standing consensus on the need to focus on results- and evidence-based approaches to CCB. To support this maturity trajectory with concrete recommendations and methodological tools for CCB decision-makers and practitioners, the GFCE has commissioned a research project on "Results-Based Approaches to CCB".

This roundtable discussion offered a platform to discuss initial findings of the GFCE research and invite participants to share their views and reflections on key recommendations, approaches, and tools that would support the CCB community in maximising results and measuring change across the project cycle.

Discussion

Within the scope of the GFCE Research Agenda created in 2021 to address knowledge gaps and research needs identified by the CCB community, a roundtable at the Annual Meeting presented initial findings from the GFCE research project "Bridging Gaps in Cyber Capacity Building: Approaches and Tools for Better Results" and invited input from the GFCE stakeholders to inform concrete recommendations and methodological tools for CCB decision-makers and practitioners.

While there has been long-standing consensus on the need to focus on results- and evidence-based approaches to CCB, from the commitments in the 2017 GFCE Delhi Communique to pursuing a results-based and action-oriented approach, to the 2021 consensus report of the UN Open-ended working group on developments in the field of information and telecommunications in the context of international security (OEWG) that articulated the results focus as one of its CCB principles, and more recently in the Accra Call for Cyber Resilient Development calling to accelerate efforts to improve the measurement of CCB results, the research identifies a range of CCB implementation approaches in pursuing results which is characterized by divergent methodological frameworks as well as an uneven professionalization.

While there is no "one size fits all" approach, given that organizations operate in varying environments and under different governing processes, a systematic integration of results-based approaches in CCB interventions that apply a more streamlined typology can contribute to pursuing and measuring results more effectively, to improving return on investment, and to increasing mutual accountability and transparency between partners and among the stakeholders.

To this end, key concepts of a results-based approach were presented, including the main elements of results frameworks, how they offer a structured way to articulate a project's cause-and-effect sequence from inputs, to outcomes, to impact. Against this background, when mapping the CCB landscape, the research found that existing results approaches to CCB can be categorized in three groups: (a) CCB results frameworks designed and used: for specific project-level interventions; for large cyber initiatives and programs; in line with the results design of their financing instrument; or more rarely to be integrated in national statistics; (b) development cooperation results frameworks used for cyber interventions at the project level; covering the whole cyber portfolio as a sector; incorporating cyber in the institution-wide/corporate results reporting; or addressing cyber as a cross-cutting issue (mainstreaming), while there is no anecdotal evidence of finding cyber included in nation-wide development strategies; and finally (c) activity-focused CCB that makes use of no results frameworks.

The shift to a more consistent results-based approach to CCB can enhance the evidence-base generated by projects with more timely and reliable data, as well as improve the overall definition, monitoring, and assessment of the performance and impact of projects. To achieve that, key high-level recommendations for the development of a CCB results approach include: (a) ensure they are fit-for-purpose by having a clearly defined purpose on the results information from the outset; (b) develop realistic attribution chains from standardized indicator sets; (c) foster a learning culture by enhancing incentives for results-based management and embedding results advisers in CCB programs, as well as building bridges between results and evaluation.

The roundtable included a discussion on reflections for key recommendations and tools that the CCB could use collectively to improve working methods towards maximizing results and measuring change across the project cycle.

Breakout Session

Building Cyber Resilience: Leveraging Public Tools for Global Cyber Resilience

SPEAKERS

- **Moderator**: **Velimir Radicevic,** Program Coordinator, GFCE
- **Pavlina Ittelson,** Executive Director, DiploFoundation US
- **Robert Collett,** Independent Research and Consultancy, Developing Capacity Ltd
- **Komal Bazaz-Smith,** Chief Business Officer, Global Cyber Alliance

BACKGROUND

Public tools on cyber capacity building are crucial resources designed to enhance the cybersecurity capabilities of states, organizations, and individuals. They play a vital role in enhancing global cybersecurity by promoting best practices and providing free access to information and resources . These public tools can be leveraged to fill in cyber capacity gaps, helping build a more secure and resilient cyberspace. Tools and initiatives such as the Cybil Knowledge Portal, the Geneva Dialogue or Common Good Cyber were discussed in the session, illustrating the way in which they can be utilized to support the development of resilient cyber infrastructures and communities, contributing to a safer and more secure digital world for all.

Discussion

The discussion centered around the critical role of freely accessible public tools in enhancing cybersecurity capabilities across states, organizations, communities and individuals. These tools encourage adherence to best practices, knowledge sharing, and skill development without barriers, which is essential for bolstering security in a rapidly evolving cyber threat landscape. The discussion was enriched by representatives from organisations who procure these essential public tools, gathering key insights on the benefits, as well as challenges that these organizations face.

- **Flexibility and Accessibility**

Public tools offer a flexible framework for countries at different stages of cyber maturity, enabling tailored approaches that can be adapted to local needs while fostering a unified global standard for cyber resilience. Robert Collett emphasised how open platforms such as the Cybil Knowledge Repository serve as a primary access point for cyber capacity-building resources. The portal aims to make research and data on CCB accessible, allowing stakeholders to directly contribute data by uploading projects or events, enhancing community engagement and resource sharing.

Pavlina Ittelson discussed DiploFoundation's DigWatch, a comprehensive digital policy observatory that houses over 1,000 resources related to internet governance and digital policies. It offers current developments and data on topics like cybersecurity, legal frameworks, and more. However, a significant challenge in maintaining such resources is funding gaps, which can limit the development of these resources and access for states and organizations unable to afford such tools. Robert illustrated the role of artificial intelligence (AI) in simplifying research processes by using data-sharing connectors to streamline access to information access. This can aid stakeholders in finding specific cyber capacity building projects or events in a certain areas (for example Pacific islands) as well as collect data from multiple portals. This reflects an evolution in the accessibility and usability of public tools. Komal Bazaz-Smith also emphasized how the Global Cyber Alliance's cybersecurity toolkits provide practical resources for communities to implement basic security measures. These cybersecurity toolkits provide basic security steps like secure passwords, multi-factor authentication, and updated software to reduce cyber risk, making them vital for reducing vulnerabilities and enhancing overall digital safety.

Komal Bazaz-Smith highlighted the Global Cyber Alliance's user-centered approach in creating toolkits, tailored to various audiences like small businesses and election officials, to enhance cyber safety through practical actions. Toolkits are translated into numerous languages and have seen extensive global use, although ongoing challenges include funding gaps and limited staffing. The Common Good Cyber initiative underscore the importance of developing long-term funding models to support cybersecurity as a public good, allowing cybersecurity programs to develop and maintain effectiveness.

- **The Role of Civil Society**

Civil society's role in cybersecurity was also a focal point of the discussion. The speakers emphasized the importance of engaging non-state actors in the implementation of cybersecurity norms. By involving a diverse range of stakeholders, including researchers and community organizations, the cybersecurity landscape can be strengthened through shared knowledge and resources.

The Geneva Dialogue on Responsible Behaviour in Cyberspace was highlighted as a platform for fostering these discussions. It encourages collaboration among various actors to develop and implement effective cybersecurity practices. The dialogue aims to create a unified approach to addressing cyber threats and promoting responsible behavior in the digital space by facilitating dialogues that encourage cooperation between state and non-state actors. It culminated in the **Geneva Manual on Responsible Behaviour in Cyberspace**, detailing five key cyber norms. While it offers a neutral platform for discussing peace and security, the Geneva Dialogue faces challenges such as compliance issues and participation restrictions that can strain relations between governments and non-state actors.

- **Challenges**

The speakers addressed the complex task of measuring the success and impact of these tools. As Komal noted, while tools like the GCA's have seen extensive usage, quantifying their impact is challenging. Metrics often capture access numbers but fall short of reflecting long-term behavioral change. Pavlina pointed out that it can be difficult to demonstrate the four-year impact of CCB investments, which complicates donor evaluation and commitment. Furthermore, Velimir Radicevic highlighted the importance of community feedback in understanding how these tools are used, ensuring that they meet real-world needs and foster a culture of resilience.

KEY TAKEAWAYS

This session underscored the vital role of public cyber capacity-building tools in supporting global resilience and security. Despite funding and operational challenges, tools like DigWatch, Cybil Portal, and GCA's cybersecurity toolkits are instrumental in making cybersecurity accessible. Through ongoing community input, innovation, and sustainable funding, these tools can effectively bridge cyber capacity gaps, contributing to a secure and resilient cyberspace for all.

BREAKOUT SESSION

Why do Civil Society Organizations (CSOs) play a key role within CCB? Hearing from experiences of the GFCE community and looking ahead

SPEAKERS

- **Moderator: Louise-Marie Hurel,** Former Advisory Board, new SSC member **and Jessica Walton, CyberPeace Institute**
- **Phil Sheriff. Royal Holloway University of London**
- **Yuri Ito, CyberGreen**
- **Letitia Masaea,** GFCE AB/Women in ICT Solomon Islands

BACKGROUND

This panel discussion did a deep-dive into the key role that various CSOs organizations play within the cyber capacity building landscape. By hearing from different stakeholders working in the field, the panel provided practical steps in which CSOs working on cyber capacity building and beyond can work better together, increase visibility and deliver impactful results on a local, regional and global scale.

The meeting was opened by Louise Marie Hurel, co-chair of the GFCE Advisory Board (AB), who welcomed participants and emphasized the importance of discussing the role of civil society organizations (CSOs) within the CCB landscape. She highlighted that while CSOs play crucial roles, their space in this domain is often limited. A key objective of the meeting was to explore how to create more opportunities for CSO involvement and map their contributions across various regions. Efforts to facilitate a dialogue on this began together with CyberPeace Institute during the Global Conference on Cyber Capacity Building (GC3B) in Ghana, with a focus on CSOs from Africa, and have since continued through virtual meetings.

Jessica Walton from the CyberPeace Institute introduced the roundtable, inviting participants to share their experiences. Yuri Ito of CyberGreen highlighted how CSOs, through data-driven approaches, contribute to cybersecurity efforts beyond national security concerns, ensuring societal well-being. She advocated for stronger metrics and statistics to guide efforts.

Letitia Masaea (GFCE AB/Women in ICT Solomon Islands) discussed the positive impact of CSOs on education and community engagement in the Pacific. She emphasized the role of GFCE Regional Hubs in coordinating activities and raising awareness. Phil Sheriff (Royal Holloway, University of London) stressed the importance of sustainable evaluation practices, local ownership, and avoiding "quick wins" in CCB initiatives.

Rob Davidson (ICT Council, Canada) suggested creating an inventory of CSOs working in cyber to enhance collaboration and break down silos. He and others noted the importance of connecting CSOs with open-source solutions, following the example of Nonprofit Cyber. Several participants underscored the need for coordinated efforts to secure funding and build sustainable, long-term projects.

Discussion from Pacific regional representatives such as Manoa Jobenz (Websafe Samoa) and Pateli Valea (Tonga Women in ICT) highlighted the need for more visibility and creating these spaces. They also explored the grassroots, unique role of CSOs in reaching underserved communities and victims of cyber incidents and mentioned the potential role of GFCE Regional Hubs in connecting these efforts. Letitia and Yuri both emphasized the importance of creating safe spaces and mentorship opportunities. Participants agreed that events like these are essential for CSOs to share knowledge and build partnerships across regions.

The session concluded with calls for a joint strategic paper to address sustainability, knowledge gaps, and the challenges CSOs face. Louise Marie Hurel and Jessica Walton highlighted the need to rethink how impact is measured for CSOs, noting that new metrics and approaches are crucial for their success.

PLENARY SESSION:

Regional Approach to Cyber Capacity Building: A Reality Check

SPEAKERS

- **Moderator: Caterina Morandini,** Advisor, GFCE
- **Kerry-Ann Barrett**, Cybersecurity Program Manager and Section Chief of the Cybersecurity Section within the Inter-American Committee Against Terrorism of the Organization of American States (OAS/CICTE)
- **Moctar Yedaly,** GFCE Africa Hub Director
- **Cherie Lagakali**, GFCE Pacific Hub Senior Advisor Cyber Policy & Communications
- **Allan Cabanlong**, GFCE Southeast Asia Hub Director

BACKGROUND

Regional approach to cyber capacity building is a priority for the GFCE, supported by four regional hubs (Africa, the Americas and the Caribbean, Pacific and South-East Asia). After testing this approach for the last few years, this session shared several best practices and lessons learned as well as highlight concrete challenges, such as those pertaining duplication of efforts.

DISCUSSION

The GFCE establishes a network of regional hubs and liaison offices that facilitate cyber capacity building discourse while ensuring unique local and regional cyber security cultural, both institutional and developmental characteristics, are reflected. As multi-stakeholder hub communities, members of the hubs come from government sector, technical community, civil society, private sector, representing dimensional perspectives in the CCB practices being implemented as well as voices in discussions. This session highlighted each hub's best practices as well as challenges and future suggestions for sustainable and self-built and managed CCB practices.

GFCE Americas and Caribbean Hub's Best Practices and Challenges

- Since the establishment of the Americas and Caribbean Hub, with the support of OAS, coordination amongst various implementors and donors in the region has been valued and prioritized in order to create holistic and effective cyber capacity building approaches. Easy access to CCB tools or resources has also been a core value. The Americas and Caribbean has translated resources on Cybil to different languages, including Spanish, English, French, Portuguese, and made them more relatable, allowing the region to identify their needs and solutions more broadly.
- Current challenges for the Hub are A) finding the right place and audience to gather 34 countries together and B) balancing different interests and views amongst countries, implementors, and donors.

GFCE South-East Asia Hub's Best Practices and Challenges

- The South-East Asia Hub was just established in 2023, supported by the Cybersecurity agency in Singapore. The Hub has built trusted relationships with donors and countries, which is highly valued – a culture different from other regions.
- As the South-East Asia Hub matures in the region, more people are needed to enable coordination amongst ASEAN member states or publishing Cybil resources to align solutions. Currently, 7 members out of 10 countries are involved in the hub and they recognize the importance of cybersecurity providing expertise, especially when ASCCE is conducting CCB programs for the region.
- Since many established and upcoming projects are interregional, the South-East Asia Hub works closely with the Pacific Hub.

GFCE Pacific Hub's Best Practices and Challenges

- The Pacific Hub has a trusted network, allowing them to information and knowledge sharing.
- One of the challenges that the Pacific Hub faces is that the responses to incidents has not come from the procedures in place but help from outside of the region, connections and relationships putting the network. Additionally, a lot of experts in the region don't get asked for help with incident responses. The Pacific Hub requests that instead outside resources come into help, more training on the ground should be practiced. Thus, community members should be increased so that the hub can tailor CCB procedures for each country.

GFCE Africa Hub's Best Practices and Challenges

- The Africa Hub, officially established in November 2023, collaborates with the 55 members of the AU and 22 other relevant institutions, making the hub supported by a diverse community. The Africa Hub ensures that the activities and implementations for cyber capacity building need to be, ensuring that everyone involved in these measures sees and understands the needs and advantages of the opportunities. For example, by establishing the African Cyber Experts, supported by Microsoft, Bill Gates Foundation, and the African Union Development Agency, knowledge models that hub members can refer to were introduced. To build the safety and capacity properly, objectives are constantly set, and the hub uses means available to African countries for their cyber legislation and strategies, aiming to create a sustainable national cyber ecosystem among themselves.
- Africa is huge and the needs vary a lot. The challenge is that the funders may have their own agendas with their interests that collapse with GFCE's objectives. To prevent confusion, donors must know the regional strategy visions, which the Africa Hub already sets, while making donor alignment meeting transparent to implementors and countries.

KEY TAKEAWAYS

Each hub has different needs and paces of CCB. Thus, respecting each region's strategies is actually leveraging their resources and talents, creating a sustainable flow of capacity building.

Community members must understand the importance of funding a focal point in the hub or community that understands the region so the objectives and means the hub holds are communicated to every stakeholder effectively.

Build expertise within its community as CCB procedures must address each country's local needs and be understood by the people who use them.

Breakout Session:

Protecting the future: Exploring GFCE role(s) in disrupting internet-enabled child sexual exploitation (WG D)

SPEAKERS

- **Moderator: Richard Harris**, Principal Cyber Security and Privacy Engineer, MITRE
- **Leslie Anderson,** Chief Strategist, Cyber Operations Integration, MITRE
- **Abdul-Hakeem Ajijola,** African Union, Chair, African Union Cyber Security Expert Group (AUCSEG)
- **Dr. Nnenna Ifeanyi-Ajufo,** Chair of GFCE Working Group on Cybercrime, Professor Leeds University Law School
- **Orhan Osmani**, Head of Division Digital, Networks and Society Department, Telecommunication Development Bureau, ITU
- **Nina Bual**, Co-Founder Cyberlite

BACKGROUND

In recognizing the widespread impact of online child sexual exploitation, recent reports, including the 2024 analysis by the Stanford Internet Observatory Cyber Policy Center and UNICEF, emphasized the pressing need for collaborative action. MITRE, supported by GFCE's Working Group D on Cybersecurity Culture and Skills, aimed to explore opportunities for public and private sector collaboration to disrupt internet-enabled exploitation. Significant challenges were noted, such as the under-resourcing of global law enforcement, the complexity of assessing criminal activity scale, and the need for mutual recognition of legal frameworks, highlighting the importance of globally aligned strategies.

The session gathered GFCE members and partners to explore potential roles for the international community in addressing these crimes, focusing on insights into the current threat landscape, investigative practices, legislative approaches, and educational efforts to enhance online safety. GFCE provided a neutral platform for diverse perspectives, fostering knowledge-sharing and identifying pathways for impactful engagement within its mission to advance cybersecurity expertise globally.

DISCUSSION

The session explored potential role the Global Forum on Cyber Expertise (GFCE) could play in this area to foster collaboration and knowledge -sharing. Speakers highlighted the severe and far-reaching impact of online child sexual abuse, stressing the need for constant vigilance and adaptation as new technologies emerge. A key challenge discussed was the limited resources available to law enforcement agencies (LE), which struggle to keep up with the vast scale of exploitation online. This is further complicated by the difficulty of quantifying the true extent of the problem, as much of the illicit activity remains hidden, and companies often lack the incentive or infrastructure to fully address it.

The discussion also touched on the fragmentation of legal frameworks across different countries, making it difficult to create unified responses. For example, issues such as age of consent, prosecution policies, and the definition of child exploitation vary widely, making international cooperation challenging. The session identified the need for more comprehensive and consistent legal frameworks, improved use of reporting tools like MITRE, and a shift from reactive law enforcement to proactive prevention efforts.

In terms of action, speakers emphasized the importance of educational campaigns and raising awareness among children, parents, and educators to build a culture of online safety. Culturally sensitive, victim-centered approaches were also highlighted as crucial to addressing the socio-economic and cultural factors that can drive CE, particularly in regions where early marriage or family honor may play a role in exploitation.

GFCE's role as a neutral platform was recognized as a unique strength, enabling member states and organizations to engage in candid discussions and share strategies without political or commercial pressure. The GFCE facilitates partnerships, capacity building, and the sharing of best practices, with an emphasis on localized solutions that align with the realities on the ground. The session called for greater coordination among stakeholders, from governments to the private sector, to create a unified front against CE. This includes leveraging technologies like AI for monitoring and detection, fostering a culture of accountability among tech companies, and ensuring that all initiatives are underpinned by robust data and evidence. GFCE's potential role to facilitate targeted capacity-building projects and enhance collaboration across regions was discussed, with the aim on fostering sustainable, long-term strategies to disrupt internet-enabled child sexual exploitation.

KEY TAKEAWAYS

Complexity of child exploitation: internet-enabled CE is multifaceted and varies across regions, requiring a coordinated global response.

Need for preventative measures: prevention through education and shifting societal behavior is critical, especially in addressing normalized behaviors around child exploitation content.

Technological and legal challenges: law enforcement is under-resourced, and legal frameworks differ significantly across countries, creating gaps in effectively tackling CE.

Culturally sensitive approaches: Solutions must be adapted to local realities, especially in communities with strong socio-cultural dynamics, such as early marriage in rural or nomadic areas.

Role of private sector: Tech companies need to collaborate on proactive measures, with frameworks like MITRE providing guidelines, though adoption remains limited.

Youth-centered interventions: Children and youth are integral to driving societal changes, as they are often more tech-savvy than adults, and interventions should consider their role.

Synthetic media and emerging threats: The rise of synthetic images presents new challenges, especially in targeting young women and families. Addressing these requires new technical and legal tools.

Breakout Session:

Projects & Programmes Showcase

SPEAKERS

- **Moderator: Velimir Radicevic**, Program Coordinator, GFCE

BACKGROUND

The GFCE Foundation has, since its inception in 2019, concluded or is currently running over a dozen short-term projects and multi-year programmes on behalf of its growing donor community. These programmes and projects, managed through the Foundation, exist to promote coordination, alignment and best practice exchanges, form and convene networks of cyber security experts, and enable opportunities for the GFCE community. As a facilitator of cyber capacity building efforts, the GFCE projects and programs (PnP) team is committed to growing the scope of its services in both running its projects in the interests of its community and providing additional help to grow out other programmes. These services can include participation as consortium partners, providing advice and information when new programmes are launched, working to actively align ongoing projects and bolster M&E efforts.

During the session, the GFCE PnP team presented the major milestones and characteristics of its previous projects, its current ongoing programmes and discussed opportunities for co-operation with community-run initiatives.

DISCUSSION

In this session, GFCE Program Coordinator Velimir Radicevic outlined the GFCE's Programmes and Projects (PnP) pillar, which plays a critical role in managing and implementing cyber capacity-building initiatives at a regional and global scale. Velimir emphasized that the PnP pillar ensures effective allocation and management of funds, quality control, and continuity of cyber capacity-building (CCB) initiatives. The PnP's mission is to amplify the GFCE's impact by enhancing the availability, quality, and sustainability of services offered to its global community.

- **Quality Control in Project Implementation**

The PnP pillar provides monitoring, evaluation, and reporting services to maintain high standards across projects. It also intervenes in project implementation to address any potential risks or delivery challenges, ensuring that CCB initiatives meet their objectives.

- **Supporting the GFCE Hubs and Regional Initiatives**

By resourcing GFCE hubs, the PnP pillar aims to empower local stakeholders, enabling the growth and maturation of these hubs into self-sustaining entities that can continue to drive CCB efforts independently.

- **Key GFCE Projects and Initiatives**

The PnP pillar is currently engaged in multi-year, multi-donor initiatives, as well as specific, short-term projects:

- Multi-Donor Programs: The U.K. Foreign, Commonwealth & Development Office (FCDO) Memorandum of Understanding with GFCE is a key program, along with initiatives like the Women in International Security and Cyberspace Fellowship, supported by several countries (e.g., the Netherlands, U.S., U.K., Australia, and Germany). These programs emphasize strategic capacity-building on a global scale.
- Single-Donor and Regional Projects: Examples include the GIZ-supported confidence-building project in the Western Balkans and the U.S.-backed CCB alignment efforts in this region, demonstrating PnP's adaptable approach to regional needs.

- **Expanding Community Services**

Radicevic highlighted the PnP's commitment to scaling its support by providing resources to enable community members to participate in essential gatherings like the GFCE Annual Meeting. He also highlighted how the PnP supports tool creation, such as National Cybersecurity Strategy catalogues, which enhance member resources and knowledge sharing.

KEY TAKEAWAYS

The PnP pillar helps maximize donor resources, maintaining project quality, and supporting regional hubs. Through these efforts, the GFCE strengthens its community services and visibility, reinforces global coordination in cyber capacity building, and enhances cyber resilience.

PLENARY SESSION:

At the Cutting Edge: What Emerging Technologies Mean for Cyber Capacity Building

SPEAKERS

- **Moderator: Chris Buckridge,** Senior Strategy Advisor, Global Forum on Cyber Expertise, GFCE
- **Selvana Gopalla**, Information Security Specialist at the Computer Emergency Response Team of Mauritius (CERT-MU) of the Ministry of Information Technology, Communication and Innovation
- **Sarah Nicole,** Senior Policy & Research Associate, Project Liberty Institute
- **Elizabeth Thomas-Raynaud**, Head of Emerging digital technology unit, Directorate for Science, Technology and Innovation, OECD
- **Martin Koyabe**, Senior Project Manager | Lead AU-GFCE Coordination, Global Forum on Cyber Expertise (GFCE)

BACKGROUND

Emerging technologies - artificial intelligence, quantum computing, and more - are at the forefront of today's digital policy discussions. Managing the opportunities and advances made possible by these technologies, while mitigating the inherent risks is a challenge that governments and regulators the world over are grappling with. The need for cyber capacity building efforts to respond to these developments is clear, but that response is still evolving. This session will draw on expertise from across the GFCE community and beyond to understand the changes underway and explore the strategies that will help keep cyber capacity building efforts current and relevant.

DISCUSSION

Moderator Chris Buckridge introduced this session, reflecting on the past Working Group E sessions, what can be seen as emerging technologies, and questioned whether emerging technologies can be seen as a useful umbrella term.

Panelists discussed the role of governance and policy making when it comes to emerging technologies and highlighted the dual nature of emerging technologies. This duality was especially significant in sectors such as agriculture and cybersecurity, where the benefits of emerging technologies, such as the increase in job creation, go hand in hand with increased risks. Sarah Nicole noted that while regulations are necessary, the EU AI Acts – which had to be rewritten multiple times due to the constant updates of technology - is an example of how difficult it is to include emerging technologies in regulations.

She also addressed the toolkit developed by Project Liberty designed to help various stakeholders navigate the complexities of blockchain governance, noting that the toolkit has been designed to understand how to design and govern your own community online, in blockchain and beyond.

Elizabeth Thomas-Raynaud highlighted OECD's Framework for Anticipatory Governance as a means to help tackle the challenges of policy-making for emerging technologies. The framework aims to equip governments and stakeholders to anticipate governance needs by leveraging technology for societal benefit and building long-term capacity to manage emerging challenges effectively. The OECD is focused on stakeholder involvement to create such a framework to understand the potential impact of technologies on human lives, considering aspects including human rights and democratic values.

Coming back to the concept of emerging technologies as an umbrella term, Selvana Gopalla highlighted that it is a useful terminology that serves as a catalyst for innovation in many different sectors. However, this innovation comes with challenges, one of which is the scale and speed at which the emerging technologies are evolving. While cyber capacity building approaches are improving, currently they cannot fully keep pace with it, and she noted that, while many regions and organizations have governance frameworks and standards, many countries lack behind on the development and adoption of these technologies. Therefore, creating awareness and providing explanations of these standards and legislation is almost as important as having the legislation to begin with.

KEY TAKEAWAYS

Speakers on the panel emphasized the importance of **international cooperation**, and **inclusive actions** to develop and improve **regulatory frameworks.**

Multistakeholder participation and the **prioritization of ethical considerations** are crucial in maximizing the benefits of these technologies while managing the associated risks.

It is clear that emerging technologies are **reshaping** our approach to cybersecurity, and that cyber capacity building must also **adapt** to match this evolving landscape.

GLOBAL CYBER EXPERTISE MAGAZINE

The 12th issue of the Global Cyber Expertise Magazine was launched during the cocktail reception on the 10 November. It was presented by Chris Buckridge (GFCE Senior Strategy Advisor).

This edition reflects our ongoing dedication to equipping cyber policymakers and stakeholders with unparalleled insights into global cyber capacity building.

Read the Magazine

Want your article to be featured in the next edition of the Global Cyber Expertise Magazine?

Submit a form with your ideas by scanning the QR code below!

GLOBAL FORUM ON CYBER EXPERTISE

OAS

Contact Us

For more information about GFCE or Annual Meeting sessions or if you have any questions, please reach out to the GFCE Secretariat through our email: contact@thegfce.org

To stay updated about the GFCE projects, activities and initiatives, check out our website and follow us on our social media channels.

Sponsored by

BAE SYSTEMS

thegfce.org @thegfce #GFCEAM24

contact@thegfce.org