GLOBAL CYBER EXPERTISE MAGAZINE

Volume 13, May 2025

Foreword

Welcome to the GFCE's 10th Anniversary Edition of the Global Cyber Expertise Magazine! We are thrilled to present this special edition during the 2025 GC3B in Geneva, hosted by Switzerland's Federal Department of Foreign Affairs. Now is the perfect moment to take stock of GFCE's first decade, and to look forward to the next ten years of community-driven cyber capacity building (CCB) around the world.

Welcome to the GFCE's 10th Anniversary Edition of the Global Cyber Expertise Magazine! We are thrilled to present this special edition during the 2025 GC3B in Geneva, hosted by Switzerland's Federal Department of Foreign Affairs. Now is the perfect moment to take stock of GFCE's first decade, and to look forward to the next ten years of community-driven cyber capacity building (CCB) around the world.

In this edition, we feature the GFCE's community-led working groups. Their wide and varied reports on different technologies, environments and goals all shared a common path over the past ten years; an ongoing evolution to even greater community leadership and cooperation, and ever more practical and localized approaches and tools. This edition reflects how CCB has matured over a decade of cooperation, greater coordination, knowledge-sharing, and relationship building to more effectively share what really works. The GFCE's regional hub directors echoed this community-led change toward a demand-driven approach with greater sensitivity to regional needs.

Looking to the future, some key directions emerge from authors who identify future drivers of change. CCB will respond to the increasing cyber risks of a more fragmented world, as the article "Future challenges and opportunities in cybersecurity" describes, but, as Pavlina Pavlova writes in "Bringing Gender Equality into the Fight Against Cybercrime", we can actively shape more inclusive, responsive, and ultimately effective approaches. How CCB is prioritized globally is changing, too, with unfolding discussions about how to forge stronger international cooperation described by Manon Le Blanc of the EU's External Action Service in the article "Strengthening International Cybersecurity through Global Cooperation".

Exciting and practical new ideas will drive an ever-evolving CCB future. This edition's expert interview is with Yurie Ito, a new member of the GFCE's Foundation Board, and the Founder and Executive Director of the CyberGreen Institute. Yurie's concept of cyber hygiene uses the lens of public health to change how we look at and even feel about cybersecurity, to build a culture of cybersecurity that is both proactive and resilient.

We thank our many guest writers from the GFCE global community for their unique and invaluable insights, and we hope you enjoy reading this very special anniversary edition of the Global Cyber Expertise Magazine.

On behalf of the Editorial Board,

David van Duren, Director, The Global Forum on Cyber Expertise (GFCE)

Marjo Baayen, Director, The Global Forum on Cyber Expertise (GFCE)

GLOBAL FORUM ON CYBER EXPERTISE

CELEBRATING A DECADE OF IMPACTFUL CCB COORDINATION

2015

ESTABLISHMENT GFCE
42 MEMBERS
UK LIAISON / INDIA LIAISON
CYBER SECURITY CAPACITY PORTAL
THE HAGUE DECLARATION

2016

55 MEMBERS; 4 PARTNERS
UK LIAISON / INDIA LIAISON
CYBER SECURITY CAPACITY PORTAL
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD

2017

65 MEMBERS; 8 PARTNERS
UK LIAISON / INDIA LIAISON
CYBER SECURITY CAPACITY PORTAL
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
DELHI COMMUNIQUE

2018

74 MEMBERS; 17 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
CYBER SECURITY CAPACITY PORTAL
CLEARING HOUSE
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS

2019

84 MEMBERS; 28 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK

2020

87 MEMBERS; 41 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
LIAISON: PACIFIC
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD

2021

98 MEMBERS; 57 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
REGIONAL HUB: PACIFIC
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD

2022

107 MEMBERS; 78 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
REGIONAL HUB: PACIFIC
SOUTH-EAST ASIA - LIAISON
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD

2023

120 MEMBERS; 93 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
REGIONAL HUB: PACIFIC
REGIONAL HUB: AFRICA
REGIONAL HUB: SOUTH-EAST ASIA
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD
GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING
ACCRA CALL
AFRICA AGENDA

2024

128 MEMBERS; 110 PARTNERS
UK LIAISON / INDIA LIAISON
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
REGIONAL HUB: PACIFIC
REGIONAL HUB: AFRICA
REGIONAL HUB: SOUTH-EAST ASIA
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
STRATEGIC STEERING COMMITTEE - INTEGRATING ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD

2025

131 MEMBERS; 127 PARTNERS
REGIONAL HUB: PACIFIC
REGIONAL HUB: AFRICA
REGIONAL HUB: SOUTH-EAST ASIA
REGIONAL HUB: LATIN AMERICA AND THE CARIBBEANS
CYBIL KNOWLEDGE PORTAL
CLEARING HOUSE
GFCE RESEARCH COMMITTEE + CCB RESEARCH AGENDA
GLOBAL CYBER EXPERTISE MAGAZINE
STRATEGIC STEERING COMMITTEE - INTEGRATING ADVISORY BOARD
5 WORKING GROUPS
WOMEN IN CCB NETWORK
FOUNDATION BOARD
GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING

UNITING EXPERIENCE AND RESEARCH

TO HELP COUNTRIES STRENGTHEN POLICY AND STRATEGY-DEVELOPMENT: THE ROLE AND ACHIEVEMENTS OF GFCE WORKING GROUP A

Written by:
Szilvia Toth, CBMs, Norms and Cyber-Diplomacy Co-Lead, Carolin Weisser Harris, Topic Leader Strategies & Assessments.

WG A brings together experience, evidence-based research, dialogue, and practical tools to help countries and stakeholders develop effective strategies and, above all, learn from each other.

Since its initiation in 2018, Working Group A (WG A)[1] has served as a platform for dialogue, collaboration, and knowledge-sharing on how countries can develop and implement National Cybersecurity Strategies (NCS), conduct and learn from cybersecurity assessments, and engage in cyber diplomacy to enhance international cooperation.

Growing cyber threats pose significant risks to national security. Evidence-based and integrative NCS and assessment processes that the WG A promoted and supported help countries to identify strengths and gaps in their cybersecurity capacity, enhance cybersecurity frameworks, and

respond effectively to those threats, and so strengthen national security and cyber resilience. National strategies are critical to build the structure for protecting critical infrastructures like finance, healthcare, energy, and transportation from cyber attacks; they are essential for secure digital environments to promote investment, business confidence, and technological innovation.

As cyber threats are global in nature, international cooperation in cyberspace is indispensable to address new and emerging challenges such as ransomware. The GFCE was established at the same time as UN negotiations in cyber diplomacy reached a milestone which resulted in the International Framework of Responsible State Behaviour in Cyberspace. The framework states that international law applies in cyberspace, gives recommendations on cyber norms and confidence-building measures (CBMs) to reduce the risk of cyber conflicts, and highlights the importance of capacity-building to reduce the digital divide and support the implementation of the framework. Working Group A has raised awareness of cyber diplomacy by building understanding and bringing stakeholders together in support of the implementation of the framework.

Over the last seven years, WG A initiated, coordinated and delivered several practically oriented tools that help GFCE partners and CCB actors build their cyber capacity, and has contributed to a global knowledge-base on these topics. The working group has capitalized on the knowledge and expertise of the GFCE multistakeholder community and helped shape national cybersecurity policies and their implementation, strengthened international cooperation, and built trust within the global CCB community.

Key Outputs and Achievements

1. Development of National Cybersecurity Strategy Tools & Resources

- 2020: Released the *"Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle"* to assist countries in designing their NCS. The Catalog was launched as an interactive web-based tool in 2022, supported by the U.S. State Department.[2]
  2021: Published the *"Global Overview of Existing Cyber Capacity Assessment Tools (GOAT)"* for nations, available in four languages.[3]

- 2022: In collaboration with WG C, drafted a white paper *"Towards Identifying Critical National Infrastructures in the National Cybersecurity Strategy Process".*[4]

- 2023: Launch of a research project on *"Cyber Capacity Building Impact Evaluation"* for more resilient development. A white paper was launched in 2023 and the work has been presented at various occasions such as the GC3B 2023. The work is led by the Global Cyber Security Capacity Centre at Oxford, Integrity, and Royal Holloway University.[5]

2. Capacity Building & Stakeholder Engagement

- 2018: Conducted interviews with cybersecurity experts from Norway, Mexico, and Senegal on their experience of developing their national cybersecurity strategies.[6]

- 2019: Supported Sierra Leone in its cybersecurity strategy development through the GFCE Clearing House initiative.[7]
- 2021: Created an internal database tracker for monitoring National Cybersecurity Strategies and Assessments

- 2022: Released a *"Short Guide to Stakeholder Engagement"* for NCS development.[8]

3. Cyber Diplomacy & International Cyber Norms

- 2020 Published an overview of existing capacity building initiatives in international diplomacy.[9]

- 2020: Developed the *"Introduction Paper on Confidence-Building Measures (CBMs) in Cyberspace"* (available in English & Spanish).[10]

- 2021: Published the study *"Improving the practice of cyber diplomacy: A gap analysis of training, tools, and other resources"*.[11]

- 2021: Published *"Putting Cyber Norms in Practice: Implementing the UN GGE 2015 recommendations through national strategies and policies"*.[12]

- 2022: Launched series of online sessions on capacity building & UN processes, in collaboration with WG C, to align cyber capacity building efforts with UN negotiations (GGE, OEWG, AHC).[13]

4. Research & Knowledge Sharing

- Mapped existing cybersecurity initiatives and organized capacity-building workshops at GFCE Annual Meetings since 2018, as well as at the Global Cybersecurity Capacity Building Conference (GC3B) in Accra in 2023

- 2021: Contributed research proposals for the Global CCB Research Agenda, 2022.

> ***"Working Group A's vital work has been foundational to the work of the GFCE and all its working groups. National Strategies are the blueprint for how countries organize and respond to cyber challenges, and efforts to enhance cyber diplomacy and training are the lynchpin for international negotiations and greater cyber stability."*** **- Chris Painter, former President of the GFCE Foundation.**

We extend our sincere gratitude to Chris Painter, Ian Wallace, and Nathalie Jaarsma for their outstanding leadership. We also appreciate Kaja Ciglic, Robert Collett, Qendresa Hoxha, Lea Kaspar, Nicolas Ott, Daniela Schnidrig, Szilvia Toth, and Carolin Weisser Harris for their invaluable contributions in shaping and delivering the WG's outputs. A special thanks to Manon van Tienhoven, Kathleen Bei, and Caterina Morandini from the GFCE Secretariat for their essential role in facilitating the WG. Lastly, we thank each GFCE member and partner whose contributions were instrumental in the WG's success.

INCIDENT MANAGEMENT AND CRITICAL INFRASTRUCTURE PROTECTION:

FROM THE 2015 UNGGE REPORT TO TODAY'S THRIVING, DYNAMIC, AND, ABOVE ALL, LOCAL RESPONSE SYSTEMS

Written by: *Kleé Aiken, Director for Community & Capacity Building at FIRST and Chair of Working Group B.*

By expanding the idea of what's possible, and working with diverse stakeholders, WG B makes meaningful and sustainable impact on global incident management and critical infrastructure protection capacity.

Ten years ago, just as the GFCE was being launched at the 2015 Global Conference on Cyberspace, a group of diplomats and government experts from 20 States were finalizing their consensus report.[1] The 2015 UNGGE report elevated critical infrastructure protection, incident response, CERTs/CSIRTs, and cyber capacity building (CCB) to being central components in the cyber norms discussion and the concept of responsible state behavior in cyberspace. But at that time, if you were to mention the norms discussed in the report to the very same critical infrastructure operators, or head across to a gathering of incident responders, you'd likely have been met with confusion and quizzical looks.

Since then, there has been increasing convergence, conversation, dialogue, and understanding across these worlds, and Working Group B (WG B) has been right at the centre. WG B is a space where policymakers, cyber diplomats, operational practitioners from incident response and critical infrastructure, and those looking to build their capacity have come together to talk shop, coordinate, and collaborate. During the last ten years, the needs, priorities, and aspirations of working group members have evolved, and so has the wider capacity building world for Cyber Incident Management (CIM) and Critical Infrastructure Protection (CIP).

Expansion of the ecosystem

The CCB community is no longer just talking about national incident response teams; we are increasingly receiving requests, sharing lessons learned, and exploring the dynamics of an expanded incident response ecosystem. Whether it's the development of sector CSIRTs, building capacity within individual critical infrastructure organizations, or simply bolstering stakeholder engagement and uplift, our work is increasingly addressing the fuller ecosystem in which we work.

Pushing boundaries

Over the past ten years we have dispelled myths about what's possible, or rather, what people believed was not possible. Whereas many once believed that small countries could not maintain their own national CERTs, we now have thriving ecosystems of incident response in the Pacific, Caribbean, and elsewhere. Instead of looking at resource-intensive global frameworks, we see the proliferation of localized approaches that embrace context and demonstrate what can be done with limited resources. WG B-supported efforts like "Cyber Incident Management in Low-Income Countries"[2] and "Getting started with a National

CSIRT Guide"[3] exemplify this. They share practical, diverse case studies, and shift from top-down, cookie-cutter frameworks toward good practice approaches.

More peer-to-peer sharing

WG B is now less about small groups of experts creating good practice documents, and more about dynamic and ongoing peer-to-peer exchange. This has been driven by the greater presence, confidence, and engagement of our diverse working group and GFCE community. It is particularly evident at our in-person meetings at both the GFCE and FIRST Annual Conferences, where a mix of seasoned experts and newcomers come together to discuss shared challenges and to swap approaches. Building these meetings around informal conversation rather than presentations has encouraged participants to continue their connection offline, realizing many of the principles of the Delhi Communique.

This approach is also proving successful for implementation, where long-term engagement, operationally-focused collaboration, and flexible, community-driven initiatives have made the most meaningful and sustainable impact.

Engaging with policy

While the gulf of perspectives between the policy and technical communities may have seemed unnavigable in 2015, in the years since, the level of engagement and dialogue has grown enormously. There is plenty more to accomplish, but efforts like the IGF Best Practices Forum, Geneva Dialogue, and the promotion of multistakeholder participation at policy discussions such as the UN Open Ended Working Group (UN OEWG) have all helped drive awareness, informed better decision making, and created a stronger enabling environment for cybersecurity practitioners.

WG B has played its role here, too, by providing a platform to convene this multistakeholder community and drive well-defined, policy conscious, and operationally-driven CCB. Working Groups A & B have also collaborated to explore the Geneva Dialogue on Responsible Behavior in Cyberspace. Through the GFCE-UNITAR Women in International Security and Cyberspace (WIC) Fellowship workshops on the sidelines of the OEWG, FIRST Incident Response table-top exercises have explored the complexities of incident response.[4]

There is little in CCB, both operational and policy, that doesn't in some way involve or impact critical infrastructure and incident response. Both fields have seen positive evolution but also face new challenges as we collectively work to strengthen our own, and each other's, capacity to meet them. A working group with one of the strongest practitioner presences in the GFCE community, WG B continues to develop its practice and focus. We remain committed to building trust and engaging across stakeholder groups, and staying grounded through focusing on operational impact.

WG B's positive dynamic is a testament to its current and previous Chairs, Task Force Leads, Secretariat liaisons, and of course the multistakeholder members. Whether it takes the form of developing good practice materials or simply fostering trusted networks of peers you can turn to, WG B will continue to adapt to new challenges and shape the development of CIM and CIP capacity building for years to come.

ADVANCING CAPACITY BUILDING
FOR CYBERCRIME PREVENTION AND MITIGATION

Written by: *Nnenna Ifeanyi-Ajufo, Chair of the GFCE Cybercrime Working Group C.*

Cooperation and partnerships are the key to addressing cybercrime and building the capacity of countries and regions to mitigate its effects.

GFCE's Mandate on Cyber Capacity-Building (CCB) to Address Cybercrime

The GFCE's commitment to addressing cybercrime is encapsulated within its broader mission to strengthen capacity for cybersecurity globally. As outlined in the Delhi Communiqué, the GFCE identifies cybercrime as one of its five thematic areas, emphasizing the need for collaborative efforts to develop effective legal frameworks, enhance law enforcement capabilities, and foster international cooperation.[1] The GFCE operates on the principle that cybercrime mitigation and prevention should respect human rights and fundamental freedoms, and be gender-sensitive, inclusive, universal, and non-discriminatory. This is based on the GFCE's overall goal to help build an open, free, peaceful and secure digital world. Its work on cybercrime mitigation is non-binding but consistent with the application of the principles of international law in cyberspace.

The Role of Working Group C (WG C)

Within the GFCE, WG C specifically addresses cybercrime and brings together governments, industry, and experts to coordinate CCB work related to cybercrime.[2] The working group is a collaborative platform for stakeholders to share best practices, coordinate CCB efforts, and develop tools to combat cybercrime effectively. WG C focuses on enhancing legal frameworks, strengthening criminal justice enforcement and responses, and promoting formal and informal cooperation mechanisms among countries and regions.

WG C is also a platform for those involved in the prevention, response and assessment of cybercrime to engage with each other and share knowledge and expertise, leading to the development of CCB projects and initiatives that help countries deal with cybercrime. Identifying and sharing best practices in cybercrime mitigation has helped the GFCE and its partners to assess the impact of prevention responses and drive more informed and inclusive activities. As the GFCE also promotes legal harmonization and advocates for the alignment of national cybercrime laws with international standards such as the Budapest Convention, WG C activities have also worked to help countries to develop and implement effective legal frameworks.

In 2021 WG C launched the 'Cybercrime Series', a new initiative to share knowledge and expertise in a structured way. The Working

Group identifies topics, setting the agenda for members to discuss emergent trends, develop a common understanding of developments, and share successful approaches and practices in capacity-building. Session topics have included:

- The current cybercrime landscape; latest trends and developments
- Cryptocurrencies and virtual assets – during this session, ransomware was identified as a priority topic and so a further session was organized.
- The role of CCB in fighting ransomware
- CCB in the context of AHC negotiations: reflections from the LAC Region
- CCB in combatting online child exploitation and abuse
- Harnessing AI regulations for cybercrime prevention; international cooperation and best practices.

These sessions highlighted the respective realities of the global north and global south and worked on identifying commonalities and differences in capacity for cybercrime prevention. The discussions continue to focus on more local contexts and realities through working with regional organizations, and underscoring regional perspectives in the context of south-south cooperation for cybercrime mitigation.[3]

Involvement in United Nations Cybercrime Convention and ICTs Security Processes.

The GFCE was an active stakeholder during the negotiations of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (AHC). It held and contributed to side-events as part of the AHC process, including the WG C event, "Regional perspectives on Cybercrime Capacity Building: Reflections from Africa", held on the margins of the Sixth Session. The GFCE also submitted a contribution to the Sixth Session of the AHC process,[4] and at the Fourth intersessional consultation of the AHC Committee.[5]

Coordinating with GFCE Working Group A (WG A), WG C initiated a series of sessions under the cross-cutting theme of "UN cyber processes and capacity building". This series shared outcomes, experiences, and lessons learned from engaging in both the OEWG and AHC. It is a platform for discussions and exchanges within the GFCE community to highlight the main aspects of the ongoing UN cyber processes, identify the specific needs of countries and stakeholders participating in the dialogues and develop their capabilities, and discuss how the GFCE can engage with these processes and support their outcomes.

The coordinated WG A and C sessions include:

- Capacity-Building and UN Cyber Processes Series on Human Rights Safeguards and Gender Mainstreaming within AHC and the

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG)

- GFCE Capacity-Building and UN Cyber Processes Series: "From agreement to action; implementation of the UN Convention on Cybercrime and synergies with existing frameworks".

GFCE's Multistakeholder Approach and Partnerships for Addressing Cybercrime

The GFCE's multistakeholder approach involves collaboration among governments, international organizations, civil society, academia and private companies. This multistakeholder and partnership-driven approach has ensured diverse perspectives and expertise in mitigating cybercrime and proven essential in addressing the multifaceted nature of cybercrime. This partnership includes stakeholders who are regularly involved in WG C activities such as the United Nations Office on Drugs and Crime (UNODC), Europol, the Global Cyber Alliance, INTERPOL, the Council of Europe, and other organisations, companies and civil society organizations.

Other partnerships and collaborations include:

The Cybersecurity Tech Accord – a partnership to enhance efforts to secure the online environment, which brings together companies committed to improving cyberspace's resilience against malicious activities.[6]

Institute for Security and Technology (IST) - In 2023, the GFCE collaborated with the IST to research public-private cyber partnerships. This research identified effective public-private partnership strategies in the fight against ransomware and was presented at a dedicated session of WG C.[7]

Counter Ransomware Initiative (CRI) - The GFCE officially joined the CRI in 2024, contributing to global efforts to detect, disrupt, and deter cybercrimes, particularly those of ransomware actors. This, and the above project with IST, aim to to assist and provide guidance to countries on establishing, strengthening and leveraging public-private partnerships to combat ransomware.

Partnerships with International Organizations – These include a partnership with the United Nations Institute for Disarmament Research (UNIDIR), integrating the GFCE's Cybil Portal with UNIDIR's Cyber Policy Portal to enhance information-sharing and transparency in CCB.[8] GFCE also works with UNODC, the Council of Europe, INTERPOL, and others. At the INTERPOL Global Cybercrime Conference in October 2023, the GFCE held a session; "Capacity Building for Countering and Combating Cybercrime in the Global South: Best Practices from the Third Sector".

Regional CCB Initiatives

The GFCE has strengthened cybercrime mitigation capacity through various regionally focused initiatives, and supported tailored CCB programs that recognize the diverse challenges faced in different regions. For instance, the Asia-Pacific Cybercrime Capacity-Building Hub (APC-HUB) was

developed in collaboration with the Supreme Prosecutors' Office of the Republic of Korea and the World Bank, and provided specialized training to stakeholders in the Asia-Pacific region.[9] Through the AU-GFCE program, representatives of over 30 African Union (AU) Member States and 25 multi-national African organizations, associations, and Regional Economic Communities (RECs) joined forces to map CCB needs, expertise and priorities across the continent under the theme of "Africa Cyber Experts". The GFCE, in partnership with the AU and supported by the Bill & Melinda Gates Foundation, developed CCB knowledge modules for African countries to better understand and address their needs and strengthen their collaboration with the GFCE community.

Future Directions for WG C

WG C will continue in its mandate to strengthen international cooperation on CCB for addressing cybercrime by connecting needs, resources, and expertise. A key focus is to avoid gaps and duplications in mandate, hence the need for partnerships with other GFCE Working Groups. As WG C continues to evolve, its initiatives remain vital in equipping GFCE members with the tools and expertise necessary to address the complex landscape of cybercrime. WG C is open to new memberships, especially from civil society and academia, to further expand a multistakeholder approach to delivering its mission. The upcoming GC3B conference will be a platform for further conversations on future directions.

CYBER-SECURITY IS NOT JUST A TECHNICAL CONCERN

BUT A CULTURAL PRIORITY ACROSS NATIONS

Written by: *Luanda Domi, Facilitator of the Working Group D on Cybersecurity Culture and Skills, GFCE.*

WG D is building a global community to invest in people and culture, and map skills to jobs, to boost cyber hygiene across all of society and ensure people of different backgrounds can forge cyber security careers.

As the GFCE marks a decade of global collaboration, Working Group D (WG D)on Cybersecurity Culture and Skills reflects on steady, people-centred progress made possible through a growing international community. From raising awareness to encouraging workforce development, WG D has helped facilitate knowledge exchange among diverse stakeholders committed to strengthening cybersecurity capacity where it matters most; with people.

GFCE has earned recognition as a trusted platform for international cooperation. For our partners like Nina Bual, Co-founder of Cyberlite, the value of this collaboration is tangible:

> ***"At Cyberlite, we have witnessed firsthand how GFCE's leadership has shaped the global conversation on cybersecurity education. From facilitating knowledge-sharing platforms to strengthening capacity building initiatives, GFCE has been instrumental in ensuring that cybersecurity is not just a technical concern but a cultural priority across nations."***

Bual's organization has scaled impactful cyber hygiene programs across Bhutan, Maldives, Bangladesh, and India, empowering students, parents, and educators with essential cyber safety skills:

> ***"The collaborative efforts driven by GFCE have enabled organizations like ours to scale impactful programmes. Looking ahead, I believe that GFCE will continue to be a catalyst for change; bridging regional gaps, addressing the cybersecurity talent shortage, and ensuring that digital literacy remains a cornerstone of cybersecurity resilience."***

Cybersecurity starts with culture

Bual's experience is echoed by many in the community, reflecting a shared belief in the value of people-first approaches to cybersecurity. Her story reflects a broader consensus in WG D that cybersecurity resilience starts with informed, empowered individuals. WG D has consistently spotlighted the importance of digital

literacy and basic cyber hygiene across all layers of society.

As former Working Group Chair Tereza Horejsova emphasized:

> ***"Without improving the education of future generations, we would be having a very theoretical and disconnected discussion."***

In 2022, the group helped release a best practice report on cyber education for children and adults, which reinforced that investing early in people's digital understanding is not optional but essential.[1]

Workforce readiness in a rapidly changing field

The importance of investing in people does not stop with awareness. As the digital threat landscape evolves and regulatory demands increase, attention has shifted toward building a cyber workforce that can meet both current and future challenges.

Todd Spires, Chair of WG D and Program Director at CRDF Global, said; *"Our partners have voiced a new appreciation for basic cyber hygiene."* Spires highlighted how workforce development cannot focus only on high-tech solutions in under-resourced regions, but must also prioritize foundational behaviors like using multi-factor authentication and spotting phishing attempts.

Through knowledge-sharing and peer exchanges, WG D has helped identify a key priority; matching cybersecurity education with real-world employment opportunities. Stakeholders across regions consistently raise the need for clearer pathways into cybersecurity careers, greater integration between education providers and employers, and stronger alignment between training content and industry needs.

This is particularly urgent in regions with rapidly growing digital economies and acute talent shortages. As Bual said; *"In the Asia-Pacific region, where digital adoption is skyrocketing, the need for cybersecurity education among youth, educators, and professionals has never been greater."* Her call to action - bridging regional gaps and ensuring that digital literacy remains a cornerstone of resilience - is one echoed throughout WG D's knowledge exchange forums.

Looking ahead: Building the human infrastructure of cybersecurity

Cybersecurity is no longer a niche issue. It is a matter of public safety, economic stability, and global cooperation. As GFCE enters its next phase, WG D will continue supporting communities to embed cybersecurity culture and skills into everyday life.

Looking forward, participants have stressed the importance of improving coordination between education and employment, investing in diversity and lifelong learning, and strengthening regional collaboration. Discussions also emphasize the need to make cybersecurity careers visible and accessible to a broader pool of talent, including to those from non-traditional backgrounds. During a recent session, one participant said; *"We need pathways that are visible, flexible, and open to people from non-traditional backgrounds."*

Ultimately, GFCE's value lies in its ability to convene and connect. As Bual so aptly put it; *"By championing partnerships and fostering a proactive cybersecurity culture, GFCE is setting the stage for a safer and more inclusive digital future."* Through WG D, the voices of educators, practitioners, and innovators will continue to shape how we build the human infrastructure of cybersecurity; one skill, one story, and one partnership at a time.

A SUCCESSFUL TRACK RECORD AND AN AGILE PIVOT

TO MEET EMERGING TECHNOLOGY CHALLENGES: THE ROLE, HISTORY, AND ACHIEVEMENTS OF GFCE WORKING GROUP E

Written by: *Maarten Botterman, Working Group E Chair.*

WG E pro-actively targets and prioritizes CCB responses to emerging technologies, equipping nations with the knowledge and resources they need for the next generation of cyber threats and opportunities.

The GFCE's Working Group E (WG E) is a forum for dialogue, collaboration, and information-sharing on cyber capacity building, particularly on the adoption of Internet and technology standards. It also addresses challenges presented by emerging technologies such as Artificial Intelligence (AI), the Internet of Things (IoT), quantum computing, and blockchain.

WG E History: 2018-2024

WG E was formed in 2018 to meet the need for structured methodologies and assessment tools that underpin the GFCE's practical guidance and frameworks. Since its inception, WG E has been instrumental in shaping the GFCE's approach to CCB. Over time, WG E has expanded its focus to include collaborative research efforts, training programs, and partnerships with key cyber institutions.

Since 2018, the GFCE Internet Infrastructure Initiative (Triple-I) workshops have been exemplary opportunities for regional CCB; they aim to enhance justified trust in the use of the Internet and email in various regions. Until 2024, WG E concentrated on foundational CCB efforts, including the development of maturity models, assessment frameworks, and knowledge-sharing platforms. The working group played a key role in facilitating national and regional cybersecurity assessments and enhancing cooperation among global stakeholders to address cyber threats through best practices and structured research.

Evolution of WG E Since 2024

WG E has now evolved to address emerging technological challenges. Recognizing the rapid advancements in digital technologies, the group has expanded its scope to include research and capacity- building initiatives focused on AI and quantum technologies. WG E has worked to understand the implications of these technologies for cybersecurity, and to develop new frameworks and training programs that equip nations with the knowledge and resources needed to navigate these complex domains.

As AI and quantum computing increasingly shape the global digital landscape, their impact on cybersecurity has become a critical area of focus. AI-driven threats, such as deepfakes and automated cyberattacks, require new defensive strategies, while quantum computing poses potential risks to encryption and data security. WG E is prioritizing these technologies to ensure that CCB efforts remain relevant and proactive in addressing future challenges. By fostering collaboration and knowledge-sharing in these cutting-edge fields, WG E aims to prepare stakeholders for the next generation of cyber threats and opportunities.

WG E Achievements

WG E has made significant contributions to the field of CCB, including:

- Development of the GFCE Global CCB Research Agenda: This initiative identifies key research priorities to guide global efforts in CCB.
- Cyber Capacity Maturity Models and Frameworks: WG E has contributed to the creation and refinement of tools that help countries assess their cybersecurity maturity levels and identify gaps for improvement.
- Facilitation of Knowledge- Sharing: By organizing workshops, webinars, and expert discussions, WG E has helped to build a global repository of best practices and lessons learned in CCB.
- Support for Regional and National Cyber Assessments: WG E has played a key role in supporting countries and regions in conducting cybersecurity needs assessments, enabling more targeted and effective CCB efforts.
- Strengthening Multi-Stakeholder Collaboration: The working group has successfully fostered partnerships between academia, the private sector, and government agencies, ensuring a holistic approach to CCB.

Join Us in Shaping the Future of CCB

The achievements of this working group, as with so many GFCE achievements, trace back directly to the generosity, collaborative spirit, and subject matter expertise of community members. I would like to extend my thanks to the many colleagues who have contributed to these discussions over the past eight years.

As we look to the future, GFCE WG E invites stakeholders from governments, the technical community, and industry to actively contribute to our mission. Your expertise, resources, and collaboration are essential in advancing research, frameworks, and training initiatives that address the pressing challenges of AI and quantum technologies in cybersecurity. Together, we can drive impactful solutions, enhance global cyber resilience, and ensure that nations and organizations are well-prepared for the evolving digital landscape. Join us in this crucial effort to shape a secure and resilient cyberspace for all.

WHAT WE'RE BUILDING TOGETHER:

REFLECTIONS FROM THE WICCB NETWORK IN 2024

***Written by:** Luanda Domi, Gender Mainstreaming and Cyber Skills Development Manager, GFCE.*

Making space for women in cyber capacity building is not about numbers, and not just about participation; it's about leadership.

In 2024, something powerful happened within the GFCE's Women in Cyber Capacity Building (WiCCB) Network; not only that we expanded our partnerships, or that we hosted our largest sessions to date,but because the pieces started to fall into place. Stories from Albania to Tonga, Ghana to the UAE, began to connect. Women who had once worked in isolation found each other, and together we began to reimagine what cybersecurity could look like when it reflects everyone.

We were never just trying to close a gap in numbers. We've been working to shift power - toward more equitable, resilient, and diverse cybersecurity ecosystems. WiCCB, *a network of networks* launched by the GFCE in 2019, is now a living tapestry of regional women's communities; from Women4Cyber Foundation in Europe to WiCSME in the Middle East, CyberSafe Foundation in Africa, and TWICT in the Pacific. This year, our collective voice began shaping not just programs, but policy. Now it provides not just opportunities, but leadership.

GFCE Annual Meeting, September, 2024: Our Moment in Washington, D.C.

The 2024 GFCE Annual Meeting in Washington, D.C. produced what many in our community have since called a turning point. The WiCCB Breakfast Session, "Actionable Pathways for Gender Mainstreaming in Cybersecurity", brought together 120 delegates from every corner of the world. What made it extraordinary wasn't just the

impressive speaker lineup—but the intimacy and honesty of the breakout tables led by our community. The conversations were vulnerable, candid, and real:

> ***"Mentorship is not just a tool. It's how we build ladders for women who are already climbing."***

> ***"We're not just talking about attracting women in cybersecurity anymore—we're talking about progressing them into leadership."***

We co-created strategies, not just reports. We mapped mentorship programs, designed processes to track meaningful collaboration, and proposed new models for cyber diplomacy that reflect the lived realities of women from the Global South. These recommendations are now contributing to the United Nations Institute for Disarmament Research (UNIDIR)'s forthcoming global compendium of best practices for gender mainstreaming in cybersecurity policy. As our Director Marjo Baayen said in her opening remarks: *"One of the biggest challenges we face is not just the shortage of people in cybersecurity, but the shortage of diverse perspectives at the table. WiCCB is not just about participation; it's about leadership."*

What We've Learned: Voices from Across the Network

In 2024, our events weren't just sessions. They were mirrors that reflected our collective efforts to build a cybersecurity workforce shaped by inclusion, accessibility, and intentional design. In April, we explored DEIA-informed workforce models and surfaced how frameworks like NICE can guide not only skills development but also the values we embed in our talent pipelines. On Girls in ICT Day, we were reminded that visibility matters. Young

girls seeing themselves in this field can be transformational. In June, Synergy in Cybersecurity catalyzed mentorship pathways that connected women across continents. In our closing session in December, we took on the difficult but urgent topic of online gender-based violence, emphasizing AI accountability, ethics, and digital justice. We examined how inclusion must be built into the very code and systems we develop.

But our biggest insights came not from panel experts, but from community members' contributions:

> ***"Cybersecurity is not gender neutral. When we ignore gender, we ignore vulnerabilities."***

> ***"Bias in AI isn't an accident. It's a reflection of human decisions, and it's time we start holding systems accountable for the harm they reproduce."***

> ***"Women are more connected than ever, but also more targeted. Without safeguards, access can come with exposure."***

> ***"We need to stop asking why women aren't joining, and start asking why our systems weren't built for them in the first place."***

These aren't just reflections; they're roadmaps for change.

The Barriers We Still Face - And How We're Pushing Back

Let's be honest - DEIA efforts globally are underfunded, under-prioritized, and often tokenistic. There's a fatigue around "diversity work", especially in technical fields. Some of the most frequent challenges we hear from our WiCCB members include:

- Limited access to leadership pathways - women may be present but not promoted.
- Lack of mentorship structures - programs often don't reach early-career or mid-career professionals in meaningful ways.
- Fragmented collaboration - many initiatives still operate in silos, without scaling or sustaining.
- Unequal protection - women and marginalized groups face more frequent and severe online threats, with little recourse.
- Intersectional invisibility - most policies don't consider overlapping forms of discrimination from disability to ethnicity to gender identity.

But here's what's changing; we're no longer just identifying problems. We're co-creating solutions. At every session, our community has called for more inclusive, cross-regional mentorship; for policy frameworks that reflect real lives; and for educational ecosystems that support rather thansideline those who don't fit the "traditional" mold.

As one participant put it: "If you want to future-proof cybersecurity, you need to make space for people who see the world differently."

Reimagining the Future: What WiCCB Is Building

WiCCB isn't a campaign. It's a platform for transformation powered by the people who carry it forward.

We are currently working to build mentorship programs with a regional lens, tailoring them to individuals with different kinds of disability. We're supporting twinning models where more established networks mentor newer ones to accelerate mutual learning. We're supporting cyber diplomacy communities to ensure women from underrepresented countries help shape the rules of the digital road. We're doing all of this because we believe cybersecurity isn't just about infrastructure. It's about people. And people shape the systems they're part of:

Institutions aren't fixed—they're human-made and human-sustained. If we want them to evolve, we have to actively reimagine them.

That's what WiCCB is doing; creating space for women from every region to not only enter the cybersecurity field—but to redefine it.We're not just closing the gender gap. We're changing what cybersecurity looks like when everyone is in the room.

And So, We Look Ahead

We're stepping into a new decade with renewed purpose and a powerful milestone. As the GFCE celebrates its ten-year anniversary at the 2025 GC3B in Geneva, the WiCCB Network will host a special session that reflects how far we've come and where we're going next.

"Networks, Not Silos – Co-Creating an Inclusive and Future-Ready Cyber Workforce" is more than a panel. It's a gathering of bold ideas, lived experience, and collective resolve. From inclusive youth training programs to innovative approaches to AI bias and leadership development, this session will spotlight the models already reshaping cybersecurity, and the work still ahead to make these approaches the norm, not the exception.

This moment isn't just about us. It's about what CCB makes possible; a free, open, and secure digital future. The second edition of GC3B is a global call to mainstream cyber resilience in the development agenda, and GFCE continues to serve as the platform where international cooperation turns into coordinated action.

WiCCB is proud to stand at the heart of that mission. We are building the kind of cybersecurity ecosystem the future demands; where talent is diverse, leadership is inclusive, and no one is left behind.

The work continues. And we're doing it - together.

FROM THE ACCRA CALL TO GENEVA, 2025:

HOW GC3B IS PUTTING CYBERSECURITY AND RESILIENCE AT THE HEART OF GLOBAL DEVELOPMENT CONVERSATIONS

Written by: *The Federal Department of Swiss Foreign Affairs (FDFA) and the Global Forum on Cyber Expertise.*

The 2025 Global Conference on Cyber Capacity Building (GC3B), hosted by Switzerland, will sustain the momentum of the 2023 Accra Call with multistakeholder dialogue and knowledge-sharing, and by prioritizing measurable outcomes drive systematic, enduring change.

Cyber capacity building (CCB) is critical to strengthening national and international preparedness, particularly for developing countries seeking to securely harness the transformative economic impacts of digital transformation. Recognizing this, the Global Conference on Cyber Capacity Building (GC3B) was established as a high-level platform to elevate cyber resilience within global governance and development agendas. Following its successful launch in Accra, Ghana, in 2023, the second GC3B is being held in Geneva, Switzerland, on May 13–14, 2025, to drive international collaboration and actionable solutions for cyber capacity challenges.

GC3B: From global platform to the Accra Call

The GC3B was conceived to address critical gaps in CCB by bringing together policymakers, industry leaders, technical experts, and development cooperation practitioners to bridge communities and practices. The inaugural conference in 2023 underscored how cybersecurity is not merely a technical issue but a fundamental enabler of sustainable development. The conference set the stage for long-term commitments through its outcome document, the "Accra Call for Cyber Resilient Development". The Accra Call emphasizes the need for an inclusive, cooperative approach, recognizing that a digitally interconnected world is only as strong as its most vulnerable link.

The Accra Call facilitates more and better knowledge-sharing, donor coordination, and integrating cybersecurity into digital development work. It is a structured action framework to encourage governments, multilateral institutions, private sector entities, and civil society organizations to pro-actively strengthen global cyber resilience. To date, the Accra Call has garnered endorsements from over eighty stakeholders worldwide. Many organizations have also made pledges to implement the Accra Call, ranging from providing technical assistance and funding to fostering public-private partnerships. The 2025 GC3B is an opportunity for participants to measure progress on these voluntary commitments and ensure the Accra Call continues to evolve to meet emerging cybersecurity challenges.

Switzerland's hosting perspective: Cyber resilience is essential for development

The passing of the baton from Accra to Geneva reflects Switzerland's longstanding commitment to international cooperation, multilateralism, and digital governance. As a global hub for diplomacy, and home to numerous international organizations, NGOs and academic Institutions, Geneva is an ideal setting for the next stage of the GC3B journey, helping to bridge the gap between cybersecurity and development stakeholders. Switzerland recognizes the intrinsic link between cybersecurity and sustainable development. In an increasingly digital world, it is vital that nations, especially those in the Global South, can manage cyber risks and ensure their economic stability and social progress. By hosting GC3B 2025, Switzerland aims to facilitate a structured, inclusive dialogue among all stakeholders, reinforcing that incorporating cyber resilience is at the core of modern development strategies. This is crucial to achieving long-term aims such as the sustainable development goals (SDGs).

Objectives and expectations for GC3B 2025

Building on the momentum of the Accra conference, GC3B 2025 seeks to deepen global engagement and drive practical outcomes for CCB. The conference will be a collaborative forum for governments, development agencies, international organizations, NGOs, civil society actors, academia and private sector leaders to share best practices, discuss emerging challenges, and explore innovative solutions for integrating cyber resilience into broader development frameworks.

Key objectives of GC3B 2025 include:

- **Enhancing knowledge-sharing:** Showcasing best practices, tools, and methodologies that have proven effective in different contexts.
- **Fostering multistakeholder cooperation:** Encouraging collaboration between governments, industry, academia, and civil society to develop more holistic cyber capacity strategies.
- **Driving actionable commitments:** Encouraging stakeholders to make concrete pledges that translate into measurable outcomes.
- **Strengthening the development-cybersecurity nexus:** Embedding cybersecurity considerations into development cooperation programs.

The conference will emphasize practical implementation. While discussions will address high-level policy considerations, GC3B 2025 will prioritize translating commitments into tangible actions that benefit countries with the greatest capacity needs.

Looking beyond 2025: The future of CCB

The GC3B is becoming an essential pillar in the international cyber resilience landscape. By fostering a recurring, high-level dialogue that brings together diverse communities, the conference aims to sustain momentum for CCB beyond individual events. The lessons learned and commitments made in Geneva will serve as a catalyst for continuous improvements in cybersecurity governance, funding mechanisms, and international cooperation.

As digital threats evolve, so must the approaches to mitigating them. Future GC3B iterations will need to address the increasing complexity of cyber risks, ensure inclusivity in participation, and expand the reach of capacity-building efforts to more regions and sectors. The conference's long-term success will be measured by its ability to drive systematic, enduring change in how the global community approaches cyber resilience.

GFCE'S REGIONAL HUBS EMPOWER LOCAL STAKEHOLDERS, BUILD REGIONAL KNOWLEDGE, AND STREAMLINE DONOR ENGAGEMENT

Written by: *Tereza Horejsova, GFCE Senior Outreach Manager and Caterina Morandini, GFCE Advisor.*

Working to connect and collaborate with regional organizations, centres, and leaders, the GFCE's regional strategy supports regions to drive their own CCB priorities toward prosperity, development, and resilience.

How the global and regional dynamics of cyber capacity-building inspired the GFCE regional hubs project

The field of cyber capacity-building (CCB) has certainly matured in the last ten years; as the field has grown more complicated, our responses to it also became more nuanced. The GFCE continued to work on supporting greater effectiveness, fostering efficient allocation of resources, and reducing duplication.

A few years into the GFCE's formal activities, it became clear that better coordination efforts required reinforcing a demand-driven approach, and that greater sensitivity to regional needs was essential. The idea of establishing regional nodes or hubs materialized as a way to strengthen coordination and ensure that regions drive their own CCB priorities toward prosperity, development, and resilience. As a result, regional communities now gained more influence over their cyber resilience while contributing to a more cohesive global effort have that bridges the national and global layers.

A regional approach also works better because countries within a region tend to share many of the same priorities, and can reach common understanding, agreement, and ways forward. Regional approaches can be instrumental in improving regional collaboration and knowledge-sharing amongst stakeholders.

To ensure sustainable and long-term impact, capacity-building requires buiding trust between implementers and the beneficiary community. The GFCE is committed to connecting and collaborating with regional organizations, centres, and key leaders. This enables the GFCE to tap into existing platforms with long-lasting, trusting relationships to help the GFCE tailor its approach in each region. In turn, the GFCE is a valuable partner for regional organizations, centres, and key leaders, supporting the realization of their CCB ambitions while avoiding duplication.

The GFCE now has active hubs in the Americas and the Caribbean, Africa, Pacific and South-East Asia. There are also dedicated activities, albeit not in the form of a hub, in the Western Balkans. Our work is ongoing; other regions deserve dedicated regional focus, and the GFCE hopes to be able to extend its support in the near future. The pilot activities of the last four years show that the regional concept works; it brings more regional perspectives to the global discourse, and developing local presence and knowledge creates a very natural point of contact for stakeholders.

From left to right: Martin Koyabe, Senior Manager AU-GFCE Project, Moctar Yedaly, Africa Hub Director and Dominic Sepenu, Regional Liaison, Africa Hub.

The Africa Hub

> ***"The Africa Hub is a catalyst for change: With African stakeholders, we're building a future where African solutions lead the way in shaping global cybersecurity resilience."***
> **- Moctar Yedaly, Africa Hub Director.**

In Africa, it all started with a project in collaboration with the African Union. This led to increased African memberships and partnerships with the GFCE, and the formation of the African CCB Coordination Committee. This coordination committee laid the groundwork for a sustainable, multistakeholder CCB ecosystem to link local initiatives, promote African talent, reduce duplication, and enable direct investments in participating African countries.

The Africa Cyber Experts Community is another example of an initiative that supports and encourages regional leaders in the field. It provides greater opportunities for a more focused and specifically African vision of cyber capacity challenges. We plan to replicate this model in other regions, starting with the Americas and the Caribbean.

The Africa Hub was later officially launched at the inaugural Global Conference on Cyber Capacity Building (GC3B) in Accra, Ghana, in 2023. The hub is led by Moctar Yedaly, with the support of Martin Koyabe, Senior Manager, and Dominic Sepenu, Regional Liaison. The Africa Hub enables Africa's cybersecurity stakeholders to unify their efforts toward a resilient and inclusive cybersecurity ecosystem in Africa. As part of these commitments, the GFCE Africa Hub has joined forces with the African Capacity Building Foundation (ACBF), AUDA-NEPAD, and the African Development Bank (AfDB) to strengthen CCB across the continent through resource mobilization, knowledge-sharing, facilitating access to the international CCB ecosystem, and supporting policy development and sustainable funding models.

The Americas & Caribbean Hub

> ***"The Americas and the Caribbean Hub is committed to enhancing the region's cybersecurity resilience by strengthening the capacity-building community and facilitating dialogue and international cooperation among key stakeholders. With the continued support of the Government of Canada and the Organization of American States, we are on track to making a meaningful and lasting impact."*** **- Carlos Alvarez, Americas and the Caribbean Hub Director.**

The Americas & Caribbean Hub has a unique arrangement as it is hosted by the Organization of American States, in Washington, D.C. This helps it to build much closer relationships between the GFCE and OAS member states.

Some prominent meetings in the region, including in Santo Domingo, San Jose and Washington, D.C., have helped collect inputs on urgent topics for the region. The hub not only supported the participation of different national representatives to these meetings, but gave practical guidance, expertise, and support to communities in the region to strengthen their cyber resilience. Additionally, the hub took a central role

Carlos Alvarez, Americas & Caribbean Hub Director.

in supporting the coordination of the GFCE Annual Meeting 2024, hosted at the OAS Headquarters in Washington, DC. Alongside this meeting, the GFCE Regional Meeting for the Americas and the Caribbean was organized, with the central theme of coordinating --building efforts in the region, with a special focus on emerging technologies.

At the beginning of 2025, a new director of the Americas & Caribbean Hub, Carlos Alvarez, began, following in the footsteps of Kerry-Ann Barret. Thanks to generous support from the Canadian government, the hub will now carry out additional activities, beginning with the establishment of the LAC Cyber Capacity Building Committee which is modelled on the pilot that was successfully tested in Africa.

The Pacific Hub

> ***"The GFCE Pacific Hub is committed to empowering Pacific Island countries by fostering strong collaboration with donors and partners to enhance cybersecurity capacity-building efforts."*** **- Pua Hunter, Pacific Hub Director.**

A pioneer of GFCE hub activities, the Pacific Hub held its first regional meeting back in 2020, and the hub as officially established during the Pacific Cyber Capacity Building and Coordination Conference (P4C) in 2023. Starting with a scoping assessment for how a GFCE Pacific Hub can best support and coordinate CCB in the region, the hub embarked on a journey to support and empower Pacific Island countries. It also

Pua Hunter, Pacific Hub Director.

Cherie Lagakali, Pacific Hub Senior Advisor Cyber Policy & Communications.

advises regional and international donors on Pacific Island needs, and coordinates with existing regional structures and mechanisms rather than attempting to compete with them. In 2023, the GFCE Pacific Hub with the Oceania Cyber Security Centre (OCSC) organized the inaugural Partners in the Blue Pacific (PBP) Pacific Cyber Capacity Building and Coordination Conference (P4C) held in Nadi, Fiji. The report of outcomes is available online.[1] Additionally, the Pacific Hub has taken major steps toward gender mainstreaming in the region.

The Pacific Hub has really progressed on donor alignment. For the last two years, it has regularly brought together all major donors in the region to exchange on their priorities and planning. Such exchanges proved effective in eliminating duplication of efforts. Now, other hubs have begun organising similar meetings, taking inspiration from the Pacific's lead. The hub is headed by Pua Hunter, supported by Cherie Lagakali.

The Southeast Asia Hub

> ***"Cybersecurity is not just an IT function; it is now a pillar of national resilience. Investing in talent is investing in national security and digital sovereignty."*** **- Allan Cabanlong, Southeast Asia Hub Director.**

Another unique hub arrangement is in Southeast Asia, where the Southeast Asia Hub has a home within the ASEAN-Singapore Cybersecurity Center of Excellence (ASCCE).

Allan Salim Cabanlong, Southeast Asia Hub Director.

Headed for the past two years by ASEAN Engineer Allan Cabanlong, the Southeast Asia Hub has increased its visibility in the region and contributed in an advisory function to anti-cybercrime related activities and to a clearing house on cyber standards. The hub often represents the GFCE at regional and national events, both to highlight its work and to share expertise on how to promote a safe and secure digital environment in Southeast Asia. Furthermore, the hub has significantly strengthened its relationships with regional and national stakeholders over the years; now, almost all countries in the region are members of the GFCE community. Finally, the hub regularly shares identified regional needs through the Cybil Portal, as part of its donor alignment efforts to help direct resources effectively.

Regional meetings of the Southeast Asia Hub traditionally take place during the Singapore International Cyber Week (SICW), organized annually by the Cybersecurity Agency of Singapore (CSA). This reflects our ongoing partnership with the agency, which will be further strenghtened in the future.

Activities in the Western Balkans

While not a regular GFCE Hub per se, dedicated activities aimed at six countries in the Western Balkans region are worth mentioning. Based on several requests from the GFCE community, this region presented particular challenges in terms of coordination of CCB efforts. The GFCE stepped in to regularly align donors and implementers, in close coordination with the recipient countries.

Future Directions and Challenges

> ***"Shifting the attention of the GFCE towards regional perspectives of cyber capacity building has certainly been a step in the right direction. It is exciting to watch the hubs take more and more ownership in facilitating key stakeholders in the region with their CCB efforts. It is reassuring to see key stakeholders in the regions finding the contributions of the hubs useful for their work."*** **- David van Duren, GFCE Secretariat Director.**

To ensure the sustainability and the long-term viability of all these efforts, the GFCE needs to maintain a fixed presence staffed by recognized regional leaders and local cyber security experts. We will continue to support the hubs, who we anticipate will increasingly act more and more independently, with them feeding into the Secretariat, rather than vice versa.

The hubs must further solidify as trusted and credible access points for CCB in their respective regions; for beneficiaries, implementers and donors. This has been a clear advice and instruction from the GFCE Strategic Steering Committee, and the GFCE will continue to support and implement this successful regional strategy:

> ***" While our hubs already contribute to day-to-day coordination, their true potential lies in becoming regional centres of gravity for cyber capacity building. This evolution is essential for the GFCE to deliver on its global mandate."*** **- Marjo Baayen, GFCE Secretariat Director.**

Finally, as important as it is to favor a regional approach to CCB, it is equally important to ensure an inter-regional transfer of best practices and lessons learned. The GFCE prioritizes exchanges among the hubs, recognizing that these exchanges improve efficiency and efficacy, and lead to greater impact, supporting the ultimate goal to strengthen CCB globally and enhance cyber resilience for all.

FUTURE CHALLENGES AND OPPORTUNITIES IN CYBERSECURITY

***Written by:** Dr. Malcolm Shore, Technical Director, Kode-1.*

Future challenges and opportunities in cybersecurity will be driven by AI, quantum computing, immersive technology, and digital sovereignty. On the ten-year anniversary edition of the magazine, we reflect upon the past decade and anticipate the challenges and opportunities of the decade to come.

Huge progress from 2015 to 2025

The GFCE was launched at the Global Conference on Cyberspace held in the Hague on 16-17 April, 2015. It was an eventful week, also including cyber attacks on Ryanair and Lufthansa, and the Operation Russian Doll campaign which exploited vulnerabilities in Adobe Flash and Windows. That year, 2015, about 6,500 Common Vulnerabilities and Exposures (CVEs) were published, and the ITU Global Cybersecurity Index showed an average cybersecurity maturity for the top ten nations of 75%, with over 90 nations having a maturity of less than 20%. There was clearly more work to do in the developed nations, and significant support required for the developing nations.

As the GFCE reaches its 10th anniversary, let's take a look at where we are now and what we can expect as we navigate the next decade.

Growing fragility and emboldened adversaries

In September 2024, the ITU released its fifth version of the Global Cybersecurity Index. Now, the top ten nations have 100% maturity, and only 14 nations in the lowest tier are at less than 20% maturity. This is a significant improvement in overall cybersecurity maturity, for which the GFCE can take some of the credit. However, in the decade leading up to April 2025, cyber crime and state-sponsored attacks have continued to leverage a growing number of vulnerabilities, with over 40,000 CVEs being published in 2024. Even in the role model nations at full maturity, adversaries continue to exploit targets ranging from individual ransomware victims to critical infrastructures. An example is the Salt Typhoon campaign of 2024 which leveraged vulnerabilities in Microsoft Exchange, Sophos Firewalls, and Ivanti VPN software, and achieved a massive infiltration of a number of US telecommunications providers. In addition to malicious activity, there are signs that the growing consolidation and interdependence of technologies has increased the fragility of our global digital environment. A key example is the 2024 Crowdstrike incident which caused a massive global outage of Microsoft systems, due to a flawed Crowdstrike update. Also of concern were the unconnected global outages of Azure and Amazon Web Services (AWS) which occurred soon after.

As we head into the next decade, we start with a fragile and vulnerable digital environment in which adversaries are developing faster than our cybersecurity capabilities. There are, in addition, several key themes which will shape the cybersecurity landscape and the GFCE's mission.

1. Balkanization of technology

The first theme is the balkanization of technology. Over the last decade we've seen increasing fragmentation of the internet as governments continue to establish localized or regional controls over online spaces to limit the free flow of information. In addition, the imposition of sanctions and exploitation of supply chains are leading to a growing divide between east and west technologies. This is exemplified by Huawei's development of an indigenous Chinese operating system, Harmony OS, and China's investment in its own semiconductor industry. These profound and growing changes in market access and influence will shape the technology industry and global collaboration over the next decade.

2. Generative AI brings both challenges and benefits

A second theme is the rapid growth of generative AI in 2024 which will drive a second wave growth of action-capable AI agent technology from 2025 onwards. While still in the early stages of its hype cycle, AI will dominate many aspects of the offensive and defensive cybersecurity landscape over the next decade. Already we are seeing new players such as Hug-

gingface, OpenAI, and Nvidia emerge in the big tech space to add to and supplant existing players.

AI is already presenting new and significant challenges. Nations are grappling with the balance between innovation and safe and responsible use of AI, and individual businesses scramble to innovate or be left behind. These challenges will continue as agentic AI becomes ubiquitous. On the upside, AI offers the potential to significantly accelerate cybersecurity maturity in developing countries through automation of governance and use of AI-enhanced architectures. However, achieving those benefits will require a trained workforce that understands and can deliver and secure AI applications. For many nations, the need to develop capacity and capability in safe and responsible AI over the next decade is arguably greater than their need for cybersecurity was over the last decade.

3. Growing regulatory demands will drive improvement

Another theme is the increasing weight of regulatory demands for cybersecurity. On top of this, Chief Information Security Officers (CISOs) face increasing personal liability for failures that occur on their watch. Over the last decade we've seen a significant increase in national guidance and legislation on cybersecurity, with GDPR being one of the most far-reaching both in its demands and penalties. The European Union Network and Information Security Directive (NIS2) came fully into force in October 2024, and more recent legislation such as the EU Artificial Intelligence Act, the European Union Cyber Resilience Act (CRA), and the financial sector Digital Operational Resiliency Act (DORA) continue the trend of increasing oversight. In 2024, Singapore enacted the Operational Technology Cybersecurity Masterplan to deliver the cybersecurity needed to underpin a modern economy. Over the next decade, this is likely to become the blueprint for other nations to adopt as part of their digital economies. We expect to see new legislation continue to be enacted and implemented, bringing an overall improvement in cybersecurity posture across all critical sectors.

4. Broad impacts of quantum and immersive technologies

Quantum technology continues to make progress, but real world deployment is still some years away. Quantum technology will be an effective solution for high computational workloads, including cryptography and AI. The US National Institute of Standards and Technology (NIST) is already proactively working to standardize quantum-resistant algorithms. Some of the early application projections for quantum technology such as drug design are already using AI technologies, and we'll likely see quantum and AI become increasingly intertwined.

The immersive technology market has grown from $10B in 2022 to $40B today, and is projected to quadruple over the next five years. Early targets include education, emergency services, and product development. The use of techniques such

as virtual reality may provide benefits for cybersecurity monitoring, while the use of immersive spaces for business will almost certainly attract criminals. The Information Technology and Innovation Foundation has submitted its insights on augmented and virtual reality to NIST, and notes that the technology presents unique cybersecurity and privacy concerns. Despite little current focus or guidance, this field will have a significant impact on both offensive and defensive cybersecurity going forward.

5. Trust itself is under threat

The final theme is trust. Over the next decade, cybersecurity will become less about protecting confidentiality and more about ensuring correctness, protecting integrity, and identifying the provenance of information. Misinformation and social engineering by influencers, cyber-spies and criminals could fracture regional and global cooperation. The use of AI to present fabricated information in text, audio and visual forms will exacerbate the problem. If we are to avoid losing trust in our digital infrastructures entirely, we'll need more than just moderators and guardrails; we'll need technology futurists who can envisage the digital architecture of the future – one which enables privacy, integrity and cooperation.

Cybersecurity will evolve rapidly, creating opportunity and improving practices and architectures

The last decade has seen improvements in our approach to cybersecurity management. With some prompting from national authorities, we've seen an evolution from legacy and largely outdated cybersecurity architectures based on perimeter firewalls and passwords to more modern approaches. Microsoft and Google are championing password-less solutions, multi-factor authentication has become the norm, zero trust architectures are being increasingly adopted, and software bills of materials are helping reduce the risk of supply chain attacks. These changes are helping developed nations to improve their cybersecurity, and can be the norm for developing nations as they ramp up their cybersecurity programs.

Nevertheless, adversaries continue to penetrate our digital infrastructures. Threats in cyberspace will continue to be an issue for nations and their communities, but the emergence of new approaches to cybersecurity will bring many opportunities for innovative individuals and businesses to deliver better cybersecurity management paradigms through the next decade. Initiatives such as the Cybersecurity Futures 2030 simulations, run by the World Economic Forum in collaboration with the Center for Long-Term Cybersecurity, will help inform cybersecurity strategic plans and enable practitioners to understand impacts and prepare for the future of digital security. The GFCE will continue to play a critical role, bringing together cybersecurity-mature nations and those with evolving cybersecurity practices to realize the digital architectures of the next decade.

STRENGTHENING INTERNATIONAL CYBERSECURITY

THROUGH GLOBAL COOPERATION

Written by: *Manon Le Blanc, Coordinator for Cyber Issues at the European External Action Service.*

The EU has been a leading force in promoting capacity building through policies, funding, and partnerships. However, the global nature of cyber threats means we need to forge stronger international cooperation, including in the United Nations (UN). The UN's role in building a stable environment for cooperation, and bring countries together to discuss, implement, cooperate, and build capacities in the cyber domain is key to achieving this.

To ensure that the international community can reap the benefits of digital technologies, cyber capacity building (CCB) is of the essence. Better cybersecurity reduces system vulnerabilities to cyber threats with a potential global impact, so it is essential to strengthen global cyber resilience and advance international security by investing in the people, processes, and technologies vital to harness the benefits of our new digital reality.

The need for CCB

In light of rapid global digitalisation, CCB is a priority for many countries and a central issue in multilateral, regional, bilateral, and multi-stakeholder discussions. Systematic efforts with partner countries and relevant organisations to enhance national, institutional, and organisational capacities are needed to improve cybersecurity and resilience.

For developing and emerging economies, CCB is particularly crucial. Many of these countries lack the technical expertise, financial resources, and institutional frameworks necessary to address cyber threats effectively. Without a strong foundation in cybersecurity, these nations are vulnerable to malicious cyber activities which not only undermine their digital transition and development goals but also impact international security and stability.

CCB is essential to bolster states' capabilities, both at the technical level, such as incident response and threat landscape monitoring, and through the development of necessary national legal frameworks and policies. CCB efforts should therefore be as multifaceted as the threat is. They should focus on a range of issues, notably on how to enhance cyber resilience and protect critical infrastructure and essential services, how to manage and respond adequately to incidents, and how to implement the UN framework for responsible state behaviour in cyberspace, including in building confidence between states. Additionally, it is essential to promote awareness about cyber threats among the general public, enhance cybersecurity skills and competencies, and advance cooperation with relevant stakeholders, particularly the private sector, in order to build a whole-of-society approach in tackling cyber challenges.

The European Union's efforts in building global cyber capacities

The EU has been at the forefront of building the cyber capacities of partners; the respective EU Cybersecurity Strategies emphasize CCB as a core priority of our cyber diplomacy efforts. Along with significant

investments by the European Commission and Member States, the EU has stepped up, partnering with countries around the globe. Today, the EU runs a portfolio of approximately one hundred million euros and is committing to new programmes in all regions. The EU's investments in CCB activities aim to foster a secure, interconnected, and resilient global digital ecosystem by supporting partners in achieving their development goals. In response to rapid digital development, the EU also helps partners transition towards a resilient and sustainable digital economy, promoting the mainstreaming of cybersecurity from the outset.

Need for enhanced international cooperation

The demand for CCB is strong and increasing, and rightly so. In recent years, CCB efforts have grown significantly, both in number of donors and implementers, and in the number of resources and projects made available. Moreover, a growing number of actors are mainstreaming cyber resilience across development programmes and funds. This is exemplified by joint initiatives such as the Accra Call for Cyber Resilient Development.[1] Coordination of these efforts is vital to meet partners' needs effectively. Strong coordination and cooperation between states, with international organizations such as the Global Forum on Cyber Expertise (GFCE), and with other stakeholders, including industry, civil society and academia is key to meaningful allocation of scarce resources and also to deliver effective and sustainable CCB activities which take account of the often limited absorption capacities of beneficiaries.

A United Nations Cyber Programme of Action to build global capacities

The UN plays an essential role in advancing CCB efforts. In the current UN Open-Ended Working Group on the security of and in the use of information and communications technologies, 2021–2025 (OEWG), CCB is a central focus. In the OEWG discussions, states recognize the UN's role as an inclusive platform to continue exchanging views, ideas, and best practices related to CCB. The UN can help to leverage existing initiatives to support states in developing the institutional strength and capacity needed to enhance their resilience and implement the UN framework for responsible state behaviour in cyberspace.

The proposal to establish a UN Programme of Action (UN PoA) to advance responsible state behaviour in cyberspace was presented by the EU and a cross-regional group of dozens of co-sponsors in February 2020, places a needs-based and collaborative approach to CCB at the heart of the discussions in the UN.[2] In addition to ongoing deliberations on CCB in the plenary, the UN PoA would include CCB as a standing item of the programmes of work of the envisaged cross-cutting dedicated thematic groups.[3] Furthermore, an action-oriented roundtable on CCB could complement the efforts by bringing together experts on CCB to discuss and identify opportunities for further international,

regional, and bilateral cooperation in this area.

The proposal for the UN PoA therefore integrates ongoing reflections and discussions on CCB as a key pillar of the UN framework for responsible state behaviour, with action-oriented discussions in cross-cutting thematic groups and a roundtable that would systematically identify needs and solutions, facilitate the exchange of best practices, and respond to the capacity-building priorities of states.[4] This approach will ensure that the UN continues to strengthen its role in galvanizing the capacity-building ecosystem, while avoiding duplication of existing delivery mechanisms. The UN PoA would also foster stronger cooperation with stakeholders and facilitate discussions that are more comprehensive, concrete, and aimed at knowledge transfer and practical cooperation.

The Global ICT Security Cooperation and Capacity-Building Portal could in addition be a key opportunity to link state-led discussions to CCB outcomes. An open and transparent platform to facilitate exchanges, and the sharing of expertise of businesses, NGOs, and academia, would provide states and the multi-stakeholder community with a much needed hub under the future mechanism.

Conclusion

As digitisation continues to evolve, so do the cyber threats that accompany it. CCB is essential to reduce the 'digital attack surface' and strengthen international stability. Developing countries that lack the necessary resources and expertise to combat cybersecurity challenges should be at the core of shaping global CCB efforts. The EU has been a leading force in promoting CCB through policies, funding, and partnerships. However, the global nature of cyber threats requires stronger international cooperation in order to enhance global resilience and achieve the Sustainable Development Goals. Building a stable environment within the UN is essential to foster international cooperation on cybersecurity, and bring countries together to discuss, implement, cooperate, and build capacities in the cyber domain. The proposal to establish a UN PoA as the future permanent mechanism would bring the international community closer to reaching this objective. It would put cyber CCB at the heart of the discussions, whether in plenary, the dedicated thematic groups, or between experts at a roundtable. Our core common goal should be to tackle the cyber threats harming our economies, societies, and democracies; by working together we will strengthen international security and stability.

SYNERGY VERSUS CYBERCRIME:

HOW TO BUILD SOUTHEAST ASIA'S REGIONAL CAPACITY THROUGH PUBLIC-PRIVATE PARTNERSHIPS

Written by: *Helena Yixin Huang, Associate Research Fellow with the Executive Deputy Chairman's Office at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.*

Public-Private Partnerships (PPP) can strengthen Southeast Asia's regional cybercrime-fighting capacity, but to unlock the full potential of PPPs harmonization of rules and information-sharing protocols, and better resources are needed.

Southeast Asia's rapid digital expansion has unfortunately coincided with a surge in cybercriminal activity which threatens the region's economies. Varied levels of digital development across Southeast Asian countries create vulnerabilities which can be exploited by cybercriminals. While some of these countries have more robust digital defences, others have limited resources and nascent cybersecurity infrastructures. This disparity can potentially facilitate cross-border cybercrime as perpetrators exploit the region's interconnectedness. Cybercriminal activities such as ransomware attacks, sophisticated phishing campaigns targeting newly online populations, and large-scale online fraud schemes preying on the growing e-commerce sector are increasingly common. These crimes not only cause significant financial losses but can also undermine trust and hinder the region's growth.

Yet much can be and is being done to address these challenges. INTERPOL runs the Cyber Capabilities & Capacity Development Project aimed at strengthening the ability of Southeast Asian countries to combat cybercrime and work together as a region.[1-2] Additionally, public-private partnerships (PPPs) are an essential component in the region's fight against cybercrime.

How PPPs Build Anti-Cybercrime Capacity

PPPs can facilitate crucial initiatives such as joint training programs, technology-sharing, and collaborative curriculum development, all of which enhance regional capabilities in combating cybercriminal activities.

Joint training programs

Joint training programs led by industry specialists to build cybercrime investigation skills are a cornerstone of effective PPPs. These programs provide hands-on experience in critical areas such as digital forensics, incident response specific to criminal activity, and threat intelligence analysis focused on identifying and disrupting cybercriminal networks. In Malaysia, the CyberSecurity Malaysia Collaboration Program aims to "bridge the gap between public and private sectors".[3] When implemented effectively, this approach fosters a deeper understanding of cybercriminal tactics and strengthens the capabilities of participating

organizations to respond to and mitigate cyber threats. By providing practical, skill-based training, similar PPP arrangements could strengthen Southeast Asia's overall ability to address sophisticated cybercriminal operations.

Technology-sharing

Technology-sharing to combat cybercrime is another critical component of effective PPPs. These partnerships can facilitate access to cutting-edge tools and platforms from the private sector to aid cybercrime investigations and prevention. These tools and platforms might otherwise be beyond the reach of the public sector due to budget constraints and bureaucratic processes which impede timely installation and access. In Thailand, a collaboration between the National Cyber Security Agency (NCSA) and Microsoft Thailand uses advanced AI-powered cybersecurity solutions to strengthen Thailand's cybersecurity standards, *"empowering both cybersecurity professionals and the general public with the skills to navigate a secure digital landscape"*.[4-5] This partnership is designed to enhance Thailand's cybersecurity capacity through both technology transfer and skills development, and to improve threat intelligence capabilities and enable more efficient detection, analysis, and responses to sophisticated cyber threats. This approach could accelerate Thailand's and the region's ability to keep pace with the rapidly evolving tactics of cybercriminals.

Cybersecurity Malaysia Collaboration Programme (CCP) Launching Ceremony, April, 2019.
Source: CyberNews, the quarterly cybersecurity newsletter of the Ministry of Communications and Multimedia, Malaysia.

Collaborative curriculum development

Collaborative curriculum development between educational institutions and private cybersecurity firms can help to enhance long-term educational capacity in cybercrime investigation. In Singapore, global cybersecurity company Kaspersky has signed Memorandums of Understanding with three tertiary institutes; Singapore Institute of Technology, Republic Polytechnic, and Temasek Polytechnic. Kaspersky will "provide support in curriculum development, consultancy in the areas of digital forensics, malware analysis, threat intelli*gence, threat hunting and incident response, as well as student and staff training opportunities along with student internship programmes".*[6] These initiatives incorporate industry-relevant case studies and practical exercises to focus on real-world cybercrime scenarios, ensuring graduates are well-prepared for careers in cybercrime investigation and prevention. This approach strengthens human capital and fosters a culture of continuous learning, ensuring that professionals across Southeast Asia remain adept at countering evolving threats.

The positive effects of PPPs go beyond the operational stage. PPPs can also significantly enhance cybercrime investigations and reduce investigative time. Private sector entities possess unique insights into digital infrastructure and threat actors, both of which are invaluable to law enforcement. Secure information-sharing platforms facilitated by PPPs can enable a secure and rapid exchange of threat intelligence and digital evidence. In the case of collaborative investigations where private sector experts assist and support law enforcement, the improved investigative capabilities and access to different forensic tools and techniques can open the door to more efficient and effective prosecution of cybercrime cases.

Challenges; legal fragmentation and resource constraints

However, there is a significant challenge to the successful implementation of PPPs in the Southeast Asia region. The region's diverse regulatory landscape, with varying legal definitions of cybercrime and disparate procedural laws, creates complexities for cross-border investigations and prosecutions. This fragmentation allows cybercriminals to exploit jurisdictional loopholes, hindering the effective pursuit and conviction of perpetrators. Resource constraints in some Southeast Asian nations can also limit the scope, scale, and effectiveness of PPP initiatives.

To address these challenges, the region must prioritize the harmonization of cybercrime legislation and the establishment of common procedural standards. This will facilitate smoother cross-border collaboration and ensure that cybercriminals cannot evade justice by exploiting legal differences. Secondly, the development of clear and secure information-sharing protocols, specifically for cybercrime-related data,

NCSA, led by AVM Amorn Chomchoey, Secretary General (centre), collaborates with Microsoft Thailand, represented by Mike Yeh, Regional Vice President of Corporate, External and Legal Affairs (third from right), and Supahrat Juramongkol, AI National Skills Director (far right), to advance AI-powered cybersecurity in Thailand.
Source: Microsoft.[7]

is crucial. This will enable law enforcement agencies and private sector partners to rapidly exchange crucial evidence and intelligence, improving the speed and effectiveness of investigations. Finally, incentive structures, such as grants for specialized cybercrime training and funding for advanced forensic technology can encourage greater private sector participation in law enforcement initiatives. By tackling these challenges head-on, Southeast Asia can unlock the full potential of PPPs to create a more robust and effective regional response to cybercrime.

Conclusion

The direct impact of PPPs on building regional capacity is undeniable. PPPs remain a potent mechanism to fortify Southeast Asia's defences against the escalating threat of cybercrime. By strategically leveraging joint training, technology transfer, and collaborative curriculum development, PPPs can significantly enhance the region's anti-cybercrime capabilities. These partnerships facilitate the rapid dissemination of expertise and resources, equipping law enforcement and professionals with the necessary tools to combat evolving cyber threats. Moving forward, sustained investment and focused collaboration through PPPs will be crucial in creating a robust and resilient anti-cybercrime infrastructure across Southeast Asia.

EMPOWERING COMMUNITIES

THROUGH DIGITAL LITERACY AND CYBER SAFETY AWARENESS

Written by: *Debra Popa, Executive Director of KnowledgeFlow Cybersafety Foundation, with contributions from the KnowledgeFlow team.*

As cyber-attacks grow more sophisticated, they increasingly target vulnerable communities with limited cybersecurity awareness and access to training. Nonprofit organizations, such as libraries, victim services, immigrant support centers, and community hubs, serve as crucial pillars of support for these communities. However, they often lack the resources necessary to protect themselves and those they serve from cyber threats.

By equipping nonprofit organizations with essential cybersecurity knowledge and cyber safety principles, we can significantly reduce cybercrime and protect those most at risk. This article explores the cyber threats facing nonprofits and their clients, the challenges nonprofits encounter in implementing cybersecurity measures, and how accessible education can bridge the gap between vulnerability and resilience. By making cybersecurity education approachable and providing free, high-quality resources, we can empower nonprofits and their communities to navigate the digital world safely.

Cyber safety vs. Cyber security

One of the biggest barriers nonprofits face in addressing cyber threats is

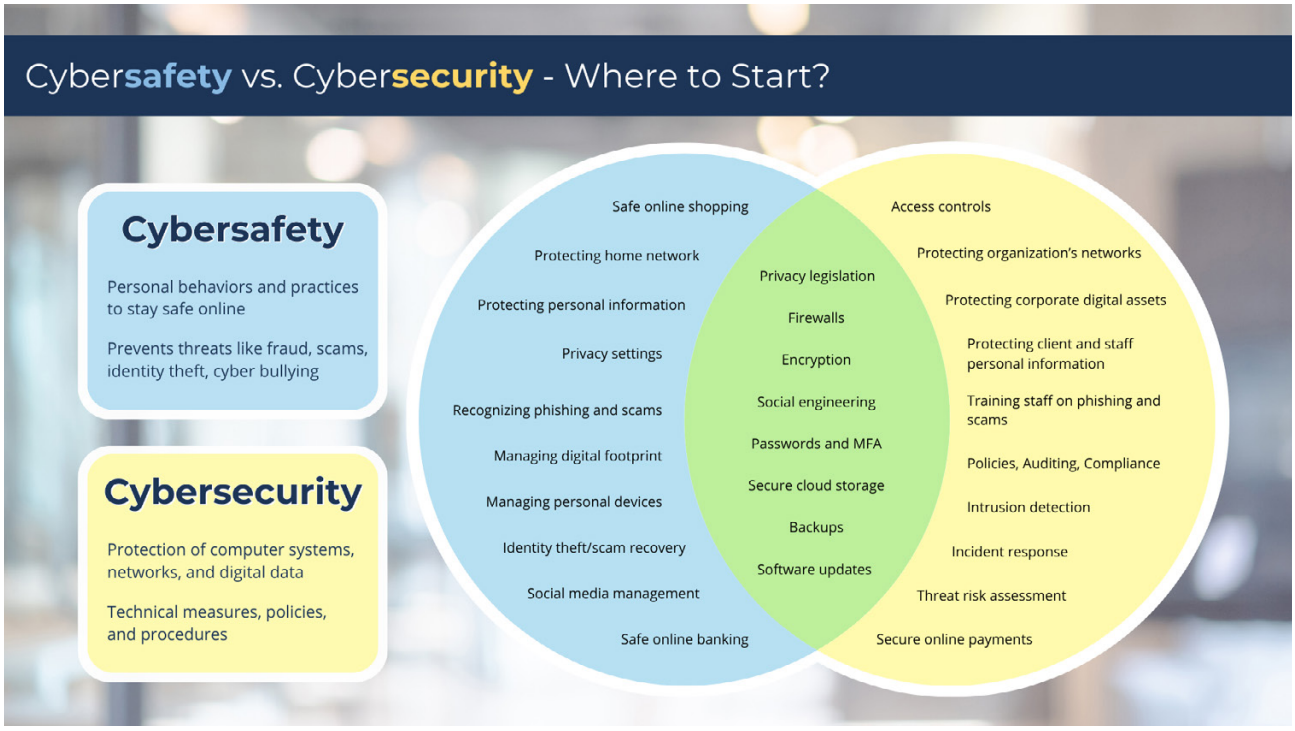

Figure 1: "Understanding the distinction between Cybersafety and Cybersecurity".
Image created by KnowledgeFlow Cybersafety Foundation.

the misconception that cybersecurity is exclusively a technical discipline requiring expensive solutions. To bridge this gap, we introduce cyber safety as a fundamental digital literacy skill.

Cyber safety focuses on individual behaviors and best practices, such as recognizing phishing attempts, managing digital footprints, and safeguarding personal information. Cyber security, on the other hand, involves more technical defenses, such as implementing security controls, encrypting sensitive data, and securing networks. By integrating cyber safety into nonprofit training, organizations can strengthen their security posture while also empowering staff and clients to protect themselves from cyber threats in their personal lives.

The Role of Nonprofits and Their Cyber security Challenges

Nonprofits play a critical role in serving vulnerable communities, yet they remain some of the most under-resourced organizations when it comes to cyber security. Canada alone has over 86,000 registered nonprofits, with millions more worldwide. Many of these organizations operate on limited budgets, lacking dedicated IT personnel, security expertise, or resources to implement cyber security policies and training programs.

Despite their financial constraints, nonprofits are entrusted with sensitive client data, including personal, financial, and health-related information. Cybercriminals recognize these vulnerabilities and exploit them, launching phishing campaigns, data breaches, and financial fraud schemes. A single cyber-attack can disrupt nonprofit operations, compromise client trust, and cause lasting harm to the communities they support.

The impact extends beyond the nonprofit itself. When an organization is breached, attackers may gain access to donor records, client data, and volunteer contact lists, information that can be used for identity theft, financial scams, or other fraudulent activities. Given this landscape,

it is critical that nonprofits have access to affordable and accessible cybersecurity education and tools.

Cyber Threats Facing Vulnerable Communities

Nonprofits and their clients are frequent targets of cyber-attacks, particularly those leveraging social engineering tactics. Some of the most common threats include:

- **Financial fraud:** Phishing scams targeting beneficiaries of public assistance programs have resulted in millions of dollars in stolen funds. In 2022 alone, Electronic Benefits Transfer (EBT) card fraud led to over $2 million in losses, a 2100% increase from the previous year.[1]
- **Data breaches:** Nonprofits store sensitive client information that, if compromised, can lead to widespread harm, particularly for vulnerable populations such as survivors of domestic violence or recent immigrants.
- **Identity theft:** Personal data exposed in breaches can be used to commit fraud, access financial accounts, or steal medical benefits.

By strengthening both nonprofit security practices and community awareness of cyber safety, we can reduce the success rate of these attacks and protect individuals from exploitation.

How Cyber safety Enhances Overall Cybersecurity

For many nonprofits, cybersecurity can seem overwhelming. It is often perceived as expensive, complex, and unattainable. However, implementing cyber safety practices can serve as a gateway to a more secure nonprofit environment.

When staff, volunteers, and clients adopt simple cyber safety behaviors, such as using strong passwords, enabling multi-factor authentication, and recognizing common online scams, they contribute to a more secure digital ecosystem. Creating a culture of cyber security awareness within nonprofits not only reduces risk at the organizational level but also benefits the communities they serve.

Moreover, cyber safety should be inte-

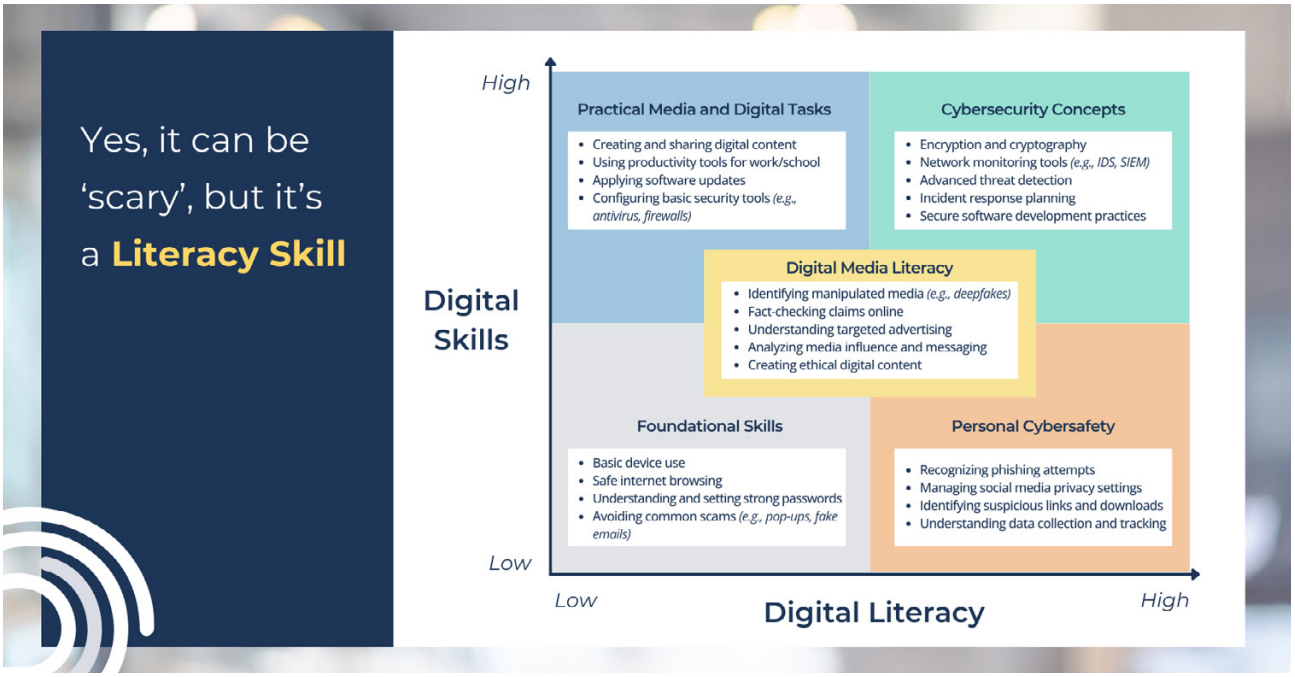

Figure 2: "Cybersecurity as a Digital Literacy Skill".
Image created by KnowledgeFlow Cybersafety Foundation.

grated into nonprofit community outreach efforts. Because these practices are actionable, free, and widely applicable, they provide a scalable approach to increasing cyber security awareness among vulnerable populations. By emphasizing cyber safety as an everyday habit rather than a reactive measure, we can create lasting behavioral change that strengthens nonprofit resilience.

Bridging the Gap with Free Cyber security and Cyber safety Education

As a fellow nonprofit organization, KnowledgeFlow Cybersafety Foundation understands the unique challenges that nonprofits face in terms of funding, staffing, and cyber security preparedness. We understand that many nonprofits operate with limited resources and little to no dedicated IT support, making it difficult to prioritize cybersecurity. Our team includes professionals with industry certifications in cyber security and privacy, allowing us to provide expert guidance tailored to the nonprofit sector. We recognize that nonprofits require accessible, high-quality training to strengthen their digital security posture. Our **free online cyber security and cyber safety courses** provide tailored support for nonprofits, covering both corporate cyber security fundamentals and personal cyber safety best practices.

- **The Cybersecurity Catalyst Course:** Designed for nonprofit organizations, this course provides **actionable cyber security strategies** that any organization can implement, even with no dedicated IT team. It includes guidance on security audits, monitoring, patching, strong authentication policies, phishing simulations, and cyber incident response planning.

- **CAPE: Cybersafety Awareness for Public Educators:** This course extends cyber security education to **nonprofit staff, volunteers, and the public**, focusing on cyber **safety best practices** that can be integrated into nonprofit outreach programs. It equips organizations with the knowledge to educate their clients about online threats, scam prevention, and digital literacy.

In addition to these courses, KnowledgeFlow provides **cyber safety tipsheets translated into multiple languages**, ensuring that cyber security awareness is accessible to diverse communities. Nonprofits are welcome to use these resources in their own programming, incorporating them into workshops, training sessions, and community outreach initiatives.

By offering these resources at no cost, we help nonprofits develop **both an internal cyber security framework and a community-focused cyber safety education model**, ensuring that digital resilience extends beyond the organization to the populations they serve.

For more information and to access our free resources, visit www.knowledgeflow.org. Nonprofits are encouraged to take advantage of these tools and integrate them into their existing programming to strengthen both their internal security posture and their community outreach efforts.

Conclusion

Cyber-attacks against nonprofits have wide-reaching consequences, disrupting essential services and putting vulnerable communities at further risk. Without accessible cyber security education, these organizations remain prime targets for cybercriminals. However, by integrating cyber safety into nonprofit operations and outreach, we can build a foundation of digital resilience that benefits both organizations and the communities they serve.

Free resources like those provided by **KnowledgeFlow Cybersafety Foundation** offer nonprofits a clear path to strengthening their security without requiring significant financial investment. Through proactive training, open discussions about digital threats, and community-driven cyber safety initiatives, we can transform cyber security from a daunting challenge into an attainable goal for all nonprofits.

Cyber security is not just a technical issue; it is a community issue. By equipping nonprofits with the right tools and training, we empower them to protect themselves, their clients, and their communities, creating a safer digital world for everyone.

BRINGING GENDER EQUALITY INTO THE FIGHT AGAINST CYBERCRIME

Written by: *Pavlina Pavlova, Lead of the Stakeholder Working Group on Cybercrime, Alliance of NGOs on Crime Prevention and Criminal Justice.*

The new United Nations Cybercrime Convention creates momentum to tackle gender-based online violence against women and girls, but only if it is implemented with focus, consideration, and sufficient resources.

Women are disproportionately targeted by cybercrime, experiencing higher rates of online threats compared to men. As technology-facilitated gender-based violence continues to rise, the United Nations (UN) Cybercrime Convention can either support or undermine gender equality. The convention provides an opportunity to integrate critical gender concerns into development initiatives to strengthen institutions, enhance justice systems, and support victims, but it will only work if states implement the treaty responsibly and build the necessary cyber capacities.

Cybercrime creates new forms of victimization

In much of the world, gender is a basis for discrimination, mistreatment, and the targeting of vulnerable populations. These power dynamics are amplified in online spaces. Gender, age, and digital gaps are tightly connected; almost half the world's population - 3.7 billion people, most of them women in developing countries - remain offline. In low-income countries, nine out of ten adolescent girls and young women aged 15-24 do not have access to the Internet.[1] The impact of this disparity is palpable. The lack of technology access and digital skills makes women and girls more susceptible to certain types of cyber offenses, including hacking and surveillance, phishing and online fraud, stalking, and social media impersonation.

Cybercrime can be committed along gendered lines, and is especially pronounced in the form of revenge pornography, sexualized deepfakes, and sextortion.[2] Image-based abuse is startlingly common; surveys indicate that one in seven adults have been threatened with exposure of intimate images.[3] Research on intimate image abuse crimes showed that nine out of ten female callers to the United Kingdom-based Revenge Porn Helpline suffered threats to non-consensually disclose their images.[4] Conversely, the same proportion of male victims was targeted by sextortion schemes for financial gain. Women, representing 73% of victims overall, reported much longer-lasting social and emotional impacts than men. Young adults are disproportionately targeted and extremely vulnerable; high numbers of adolescent women report having received unsolicited explicit images or being pressured to send them.[5] There is a striking gender disparity in AI-enabled intimate image abuse as well. A report on deepfakes found that 98% of deepfake videos online were pornographic, and 99% of those targeted were women and girls.[6]

Including Gender in the United Nations Cybercrime Convention

Negotiations on the newly agreed UN Cybercrime Convention reflected a growing awareness of the gender dimension, with many countries arguing for gender mainstreaming the entire treaty and spelling out a strong commitment to gender equality. The final text falls short on

fully recognizing these considerations. However, it includes language acknowledging that different genders may face distinctive threats and emphasizing the importance of addressing online gender-based violence. Despite its many shortcomings, the convention can create a platform for unified international cooperation in combating cybercrime, and for empowering national law enforcement agencies. Its effectiveness in addressing gender issues now depends on how the treaty is translated into national frameworks. Impactful implementation will require states to build capacities to respond to gendered crimes, ensuring that gender sensitivity and other intersectional issues are considered.

The inclusion of non-consensual dissemination of intimate images in the convention's criminalization chapter creates an international framework for preventing, investigating, and prosecuting image-based abuse.[7] Often referred to as 'revenge porn' laws, similar provisions already exist in some domestic legislation. However, most states lack comprehensive legal frameworks or address the crime inadequately - and unjustly - by blaming or punishing the victims. This outlook is deeply concerning because extortion schemes, whether carried out by individuals or international criminal groups, exploit those in positions of vulnerability, such as women and girls from targeted or marginalized communities, whose risk is heightened by laws that penalize victims.[8] The convention builds impetus to revise these punitive laws in order to comply with international frameworks.

Beyond the limited case law on technology-facilitated gender-based violence, law enforcement and justice systems frequently lack the capacity and resources to counter and respond to such criminal offenses effectively. Technical assistance included in the convention can address these shortcomings if it is subject to a human-rights impact assessment that informs and guides these activities, their scope, consequences, and the exchanged and employed tools. Similarly, victim assistance services, also touched upon in the treaty, should be systematically funded, and with states increasing domestic capacity to provide gender-sensitive and responsive assistance that prioritizes a victim-centered approach to redress and reparations.

Innovative approaches to tackling image-based crimes are largely driven by stakeholders, with collaborative partnerships redefining victim support. For instance, the StopNCII (Stop Non-Consensual Intimate Image-Sharing) initiative led by the United Kingdom charity South West Grid for Learning (SWGfL) partners with online platforms to provide a free tool that detects and removes harmful images from online spaces.[9] In another example, Report Remove, operated by Childline and the Internet Watch Foundation in the United Kingdom, is a service designed for young people to confidentially take down sexual images or videos of themselves from the internet.[10] By working closely with affected individuals and collecting anonymized statistics, victim-centered organizations develop real-life insights. Their work enables tailored support for some of the most vulnerable groups, such as adolescent boys and girls, young adults, and individuals who might otherwise face significant financial and legal barriers to seeking recourse. These initiatives can be scaled up and provide a model for states implementing the convention.

Improving responses to cybercrime one stakeholder at a time

Gendered crimes target individuals, but they also traumatize whole communities and threaten societal resilience, particularly in developing regions. Despite the gravity of these offenses, support for victims remains fragmented, relying on a patchwork of civil society organizations and social justice groups. These coalitions are insufficiently funded to provide the needed assistance, such as access to reporting mechanisms, legal counsel, psychological support, and effective remedies that prevent revictimization. As part of implementing the convention and building criminal justice capacities, states must increase their support for and cooperation with victim-centered organizations and create specialized cyber victim support units within law enforcement agencies.

The criminal justice system needs a substantial capacity to gather evidence, investigate and prosecute cybercrimes, and sensitize responsible agencies to be gender responsive. Victims often have low confidence that law enforcement will assist them; they experience shame, embarrassment, fear of reputational harm, or may not even realize that it is a crime or know how to report it. This increased vulnerability reflects larger societal issues of gender discrimination and digital disparities in many countries. For this reason, successful implementation of the convention requires that cyber capacity efforts go hand in hand with development initiatives to build resilient and accountable institutions through law enforcement and judicial capacities promoting equal access to justice.

The convention's agreed technical assistance measures will set norms, establish new or improved powers for the state, facilitate collaboration between countries and the private sector, and provide a unique opportunity to address gender-based issues. They can help ensure that law enforcement, prosecutors, and judges have the technical capacity and expertise to secure and verify evidence, conduct thorough investigations, and prosecute offenders in a manner that upholds justice and protects victims' rights. Technical assistance supporting criminal justice systems will directly impact communities and must be driven responsibly, regarding how the technology is acquired and deployed. This will require careful consideration and consultation on how resources are mobilized, and how to support and sustain the sharing of best practices with stakeholders while strengthening local expertise.

Gender equality in the fight against cybercrime does not seek to benefit a single group. Rather, this approach acknowledges that certain individuals and communities face distinct and heightened challenges. Understanding the evolving nature of cybercrime and its profound impact on victims and, concurrently, the strategies and tools for effective prevention and mitigation, can support the employment of emerging technologies for better protection of victims. Innovative, cooperative, and voluntary cyber capacity building is essential to ensuring states fully recognize and address these concerns. The new convention creates an opportunity to significantly ramp up these efforts.

"CYBERSECURITY ISN'T JUST AN INDIVIDUAL RESPONSIBILITY; IT'S A SHARED ONE."

An interview with Yurie Ito

Whether it's improving personal security habits, strengthening infrastructure resilience, or shaping policies that encourage collective defense, we all have a stake in securing our shared cyber ecosystem.

Biography

Yurie Ito, a new member of the GFCE's Foundation Board, is the Founder and Executive Director of the CyberGreen Institute, a global non-profit dedicated to advancing the science of Cyber Public Health.

Q: Yurie, you've worked at the intersection of policy, technology, and international cooperation. Where does your passion for cyber affairs and your continuous drive stem from? And how has the field changed since you began?

My passion for cyber affairs and my drive stem from a deep-seated belief in the power of technology to foster global connections and advance human progress. From early in my career, I was captivated by the potential of the internet and cybersecurity to bridge diverse cultures and economies, thereby promoting a more inclusive global dialogue. This commitment has been at the core of my work at CyberGreen, where we focus on enhancing the "public health" of the global cyber ecosystem.

The field of cybersecurity has evolved dramatically since I started in 2002 at JPCERT/CC. Initially, the focus was predominantly on defending against isolated threats and securing perimeters. However,

today we face a complex landscape where cyber threats are dynamic, sophisticated, and intricately linked to our physical world. This shift has necessitated a transformation towards more holistic approaches that prioritize resilience and the collective health of networks.

The necessity of international cooperation has been underscored by our experiences during the COVID-19 pandemic, which highlighted how collective approaches are vital when addressing interdependent risks. This realization led to the development of the Cyber Public Health framework, emphasizing that cyber threats, like pandemics, do not respect national boundaries. Global collaboration is thus essential for devising effective defenses and informed policies. My journey has been profoundly influenced by these insights, driving me to champion stronger global partnerships and forward-thinking solutions that tackle the complex challenges of our interconnected world.

Q: As someone who has worked in CCB for many years, what's the most valuable lesson you've learned in trying to bring systemic change to cybersecurity?

A crucial lesson I've learned is the importance of recognizing and addressing the unique blockages that hinder systemic change in cybersecurity. Understanding these blockages involves delving into the specific challenges that each community or organization faces. We've developed a framework at CyberGreen called the Cyber Belief Model to better understand these challenges. This model helps us assess how beliefs about cybersecurity risks and benefits can influence the adoption of protective behaviors.

There's also a lack of comprehensive data on the effectiveness of various cybersecurity measures. This gap can impede our ability to demonstrate the real value of robust cybersecurity practices and thus slow down the implementation of necessary changes. Addressing all these issues requires a tailored approach that not only presents the data but also aligns with the specific beliefs and values of those involved. It's about building a case that resonates on both a rational and a personal level, which is key to fostering a culture of cybersecurity that is both proactive and resilient.

Q: What advice would you give to young professionals starting in the field of cyber affairs?

My advice is anchored in the principles of continuous learning and critical inquiry. Always question the status quo and seek evidence through data to support your cybersecurity measures and decisions. This approach not only enhances your understanding but also ensures that your contributions are grounded in empirical evidence.

Moreover, it's crucial to understand the ramifications of your systems and behaviors on others. Cybersecurity is not just about protecting systems but also about safeguarding communities and individuals from harm. Consider the broader impacts of your work, and strive to develop solutions that prioritize ethical considerations and the well-being of all stakeholders.

Finally, be kind to yourself. The field can be demanding, so ensuring you maintain a healthy work-life balance is crucial. Cultivate hobbies and interests outside of work to keep your mind and body refreshed and energized. Embrace challenges as learning opportunities and remember that resilience is built over time through experiences both inside and outside the workplace. Your personal well-being is just as important as your professional achievements.

Q: You've recently joined the GFCE's Foundation Board. What do you hope to achieve from this position and how do you envision the role of the GFCE in the global CCB landscape?

I aim to advocate for and implement a metrics-based approach to our capacity building efforts. This involves establishing clear benchmarks for success and employing rigorous data analysis to continuously assess and refine our strategies. By systematically tracking progress against these metrics, we can not only measure the effectiveness of our programs but also demonstrate their value in enhancing global cyber resilience.

To ensure the long-term sustainability and impact of GFCE, we must explore innovative operational models, including membership schemes and public-private partnerships. Strengthening our community through collaboration and shared responsibility will reinforce GFCE as a resilient platform that delivers lasting value to its members.

My vision for GFCE is to lead in shaping a resilient and inclusive cyberspace, where strategic, evidence-based capacity building empowers nations and organizations to navigate and thrive amid evolving digital threats. By implementing targeted metrics, we can clearly demonstrate the tangible impact of our initiatives, solidifying GFCE's role as a cornerstone in the global cybersecurity landscape.

Cyber Public Health

Q: You've been a key advocate for applying public health principles to cybersecurity, often saying; "My security depends on your security, and your security depends on mine". How would you explain what cyber hygiene/public health is to the non-expert, what led you to this principle, and why it's important?

Cyber hygiene, much like personal hygiene, involves simple, everyday practices - using strong passwords, updating software, and recognizing phishing attempts - to keep individuals and organizations safe online. But just as handwashing alone can't stop a pandemic, individual cybersecurity efforts aren't enough to protect society from systemic digital threats. This is where Cyber Public Health comes in.

Cyber Public Health applies public health principles - prevention, collective responsibility, and evidence-based interventions - to cybersecurity. Rather than treating cyber threats as isolated incidents, it focuses on building resilience across entire digital ecosystems. This means identifying risk factors, designing scalable interventions, and ensuring cybersecurity is both accessible and equitable, just as public health does for disease prevention and healthcare.

What led me to this principle is the realization that cybersecurity isn't just a technical challenge; it's a societal one. Cyber threats, like infectious diseases, spread rapidly across borders, disrupting critical infrastructure, economies, and lives. Yet, traditional cybersecurity often remains reactive - fixing vulnerabilities after an attack rather than preventing them in the first place.

Public health offers a proven framework

for understanding, mitigating, and preventing cyber risks at scale. Just as vaccines and sanitation protect communities from outbreaks, we need scalable, evidence-driven cybersecurity strategies - including baseline security standards, automated protections, and cross-sector collaboration - to safeguard digital ecosystems.

Additionally, just as healthcare is a human right, basic cybersecurity protections should be accessible to all, not just those who can afford them. Bridging the digital divide is essential to ensuring that security measures benefit everyone, not just the privileged few.

By adopting a Cyber Public Health mindset, we can move beyond simply defending against threats to proactively shaping a safer, more resilient digital world. This means embedding cybersecurity into policies, infrastructure, and daily life, just as we do with public health measures. The future of cybersecurity isn't just about stopping attacks; it's about creating a healthier, more secure cyber ecosystem for all.

Q: If we apply this thinking today, what is the equivalent of a serious disease or even a global 'pandemic' in cyberspace? And what would be the cure?

If we apply a public health perspective to cybersecurity, a global cyber pandemic would be a systemic threat that spreads across interconnected networks, destabilizing entire sectors and nations. A prime example is supply chain attacks like the SolarWinds incident, where a single compromised software update infected thousands of organizations globally. Similarly, critical infrastructure vulnerabilities - such as weakness in global internet routing, misconfigured DNS, or open resolvers - can create cascading failures, much like how a pathogen exploits weaknesses in an immune system.

The Cure: A Multi-Layered Approach

There is no single cure, but a coordinated, systemic defense model is essential:

- Prevention – Secure-by-design infrastructure, zero-trust architecture, and stronger DNS/BGP security measures
- Early Detection & Containment – Real-time monitoring, data-driven risk assessment, and enhanced global threat intelligence sharing
- Resilience & Recovery – Building a cybersecurity public health framework that tracks systemic risks, enforces accountability, and fosters collective action.

At CyberGreen, we focus on measuring systemic cyber risks, similar to how public health identifies the risks that harm to societal level and measures them. Without data and metrics, we cannot assess the scale of cyber risks or gauge the effectiveness of interventions. By quantifying cyber hygiene at a global level, we can provide the intelligence needed to prevent, contain, and recover from cyber crises before they escalate into full-scale pandemics. Cybersecurity is no longer an individual effort; it requires collective, data-driven action.

Q: CyberGreen's roadmap envisions a future where Cyber Public Health becomes an academic discipline. What are the biggest barriers to getting there, and how do we overcome them?

First, cybersecurity has traditionally been framed as a technical or national security issue rather than a societal one. On the other hand, public health is rooted in a systems-based approach; measuring risk at scale, developing interventions, and prioritizing prevention. Bridging these perspectives requires a shift in mindset, and that takes time.

Another challenge is the lack of standardized metrics and methodologies for assessing systemic cyber risks. Unlike public health, where we have well-defined indicators for disease control, cybersecurity lacks universally accepted measures for cyber risk at the population level. Developing these standards is critical for legitimizing Cyber Public Health as a field of study.

To overcome these barriers, we need interdisciplinary collaboration. We must bring together cybersecurity researchers, data scientists, public health experts, policymakers, and economists to build a shared framework. Investment in academic programs, funding for research, and integration into university curricula will also be essential. Ultimately, recognition from institutions and governments - treating Cyber Public Health as a core component of national and global cyber resilience - will drive its adoption as a formal discipline.

Cyber Governance & The Next Decade

Q: Many cybersecurity initiatives focus on high-level policy but change often happens at a grassroots level. How can we bridge the gap between policy and on-the-ground action?

Bridging the gap between high-level cybersecurity policy and grassroots action requires translating policy into measurable, actionable steps that organizations and individuals can implement. Too often, policies are drafted without clear pathways for real-world adoption or without considering the practical constraints faced by those on the ground.

A key priority in cybersecurity is ensuring that cyber risk data is accessible and understandable, enabling organizations and individuals to take informed action. Just as public health initiatives use epidemiological data to guide interventions, cybersecurity efforts should leverage data-driven insights to help local organizations, small businesses, and governments prioritize actions that have the greatest impact.

Another approach is ensuring policies are designed with implementation in mind. This means involving technical practitioners, local organizations, and industry stakeholders early in the policymaking process to ensure feasibility and buy-in.

Q: For people reading this who want to help build a more resilient, healthy cyberspace, whether they're policymakers, security professionals, or everyday users, what's the most impactful action they can take?

The most impactful action anyone—policymakers, security professionals, or everyday users—can take to build a more resilient and healthy cyberspace is to recognize that cybersecurity is a shared responsibility and take proactive steps within their sphere of influence.

For technical and service providers, the priority is to embed security into products and services by default. This means implementing strong default security settings, automated patching, and user-friendly authentication to reduce the burden on users. A secure-by-design approach ensures that individuals and organizations can operate safely without requiring deep technical expertise.

For security professionals, mitigating systemic cyber risks is critical. Strengthening DNS security, implementing BGP route validation, and improving real-time threat intelligence sharing helps prevent cascading failures across interconnected networks.

For everyday users, the key is to support and advocate for stronger security from providers. This includes:

- Choosing secure products with built-in protections like automatic updates and multi-factor authentication
- Demanding better security from vendors by providing feedback on security defaults and privacy policies
- Staying informed and adopting safe practices, using available security tools to reinforce their digital safety.

For policymakers, the goal is to establish evidence-based regulations that incentivize systemic risk reduction and promote industry-wide accountability.

The most impactful thing we can all do is recognize that cybersecurity isn't just an individual responsibility; it's a shared one. Whether it's improving personal security habits, strengthening infrastructure resilience, or shaping policies that encourage collective defense, we all have a stake in securing our shared cyber ecosystem.

REFERENCES

p6. Uniting Experience and Research

1. GFCE: Cybersecurity Policy and Strategy, https://thegfce.org/theme-gfce/cyber-security-policy-and-strategy/

2. GFCE, "The Activity Catalog for Cybersecurity Strategy Design", https://cyberstrategyactivities.org/

3. GFCE, "Global Overview of Existing National Cyber Capacity Assessment Tools (GOAT)", https://cybilportal.org/wp-content/uploads/2021/08/Global-Overview-of-Assessment-Tools_CLEAN_17Aug.pdf

4. GFCE, "Towards Identifying Critical National Infrastructures in the National Cybersecurity Strategy Process", https://thegfce.org/tools/towards-identifying-critical-national-infrastructures-in-the-national-cybersecurity-strategy-process/

5. Global Cyber Security Capacity Centre, "Cyber Capacity Building Impact Evaluation; Facilitating Impact Evaluation Efforts for More Resilient Development", https://gcscc.ox.ac.uk/cyber-capacity-building-impact-evaluation-bringing-solutions-life

6. GFCE, "National Strategies: Interviews Behind the Cover", https://thegfce.org/wp-content/uploads/2020/09/GFCE-2018-National-Strategies-small.pdf

7. GFCE, Clearing House, https://thegfce.org/clearing-house/

8. GFCE, "A Short Guide to Stakeholder Engagement on National Cybersecurity Strategy Development", https://cybilportal.org/wp-content/uploads/2022/08/GFCE-NCS-Development-Stakeholder-Engagement-Paper.pdf

9. GFCE, "Overview of existing capacity building initiatives", https://thegfce.org/wp-content/uploads/2024/06/gfce-overview-of-existing-ccb-initiatives-2020.pdf

10. GFCE, "Overview Of Existing Confidence Building Measures As Applied To Cyberspace", https://cybilportal.org/publications/overview-of-existing-confidence-building-measures-as-applied-to-cyberspace/

11. GFCE, "Improving the practice of cyber diplomacy: A gap analysis of training, tools, and other resources", https://cybilportal.org/wp-content/uploads/2021/12/GFCE-study-2021-Full-study-December-2021.pdf

12. GFCE, "1 PUTTING CYBER NORMS IN PRACTICE: Implementing the UN GGE 2015 recommendations through national strategies and policies", https://cybilportal.org/wp-content/uploads/2021/11/Putting-Cyber-Norms-in-Practice.pdf

13. GFCE, "Report on the "Capacity Building and UN Processes" Session, 2020", https://thegfce.org/events/annual-meetings/global-regional-meetings/report-on-the-capacity-building-and-un-processes-session/

p9. Incident management and critical infrastructure protection

1. UNGGE, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security", 2015, https://digitallibrary.un.org/record/799853?ln=en&v=pdf

2. GFCE, Jean-Robert Hountomey, Hayretdin Bahsi, Unal Tatar, Sherif Hashem & Elisabeth Dubois, "Cyber Incident Management in Low-Income Countries", 2022, https://cybilportal.org/publications/cyber-incident-management-in-low-income-countries-part-1-a-holistic-view-on-csirt-development/

3. GFCE, TNO (Netherlands Organisation for Applied Scientific Research), https://cybilportal.org/publications/getting-started-with-a-national-csirt-guide/

4. GFCE, "Women in International Security and Cyberspace Fellowship", https://thegfce.org/project/women-in-international-security-and-cyberspace-fellowship/

p12. Advancing Capacity Building

1. "Delhi Communiqué on a GFCE Global Agenda for Cyber Capacity Building", 24 November, 2017, https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

2. GFCE Cybercrime theme: https://thegfce.org/theme-gfce/cyber-crime/

3. GFCE Annual Report, 2023, https://thegfce.org/wp-content/uploads/2025/01/Final-GFCE-Annual-Report-2023.pdf

4. GFCE, "Contribution to the Sixth Substantive Session of the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information Technologies for Criminal Purposes, 2021 - 2024 (AHC)", https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Submissions/Multi-stakeholders/GFCE_submission_6thAHC.pdf

5. GFCE, "Presentation at the Fourth intersessional consultation of the Ad Hoc Committee Vienna, 6 and 7 March 2023", 2023, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Fourth_intersessional_consultation/Panel_2_Horejsova_GFCE_Remarks.pdf

6. GFCE, "Cybersecurity Tech Accord announces partnership with GFCE", 2018, https://thegfce.org/news/cybersecurity-tech-accord-announces-partnership-with-global-forum-on-cyber-expertise-gfce/

7. GFCE, "IST Partners with the Global Forum on Cyber Expertise to Research Public-Private Cyber Partnerships", 2023, https://securityandtechnology.org/blog/ist-partners-with-the-global-forum-on-cyber-expertise-to-research-public-private-cyber-partnerships/

8. GFCE, "UNIDIR and GFCE Joined Forces to Enhance Knowledge and Information on Cyber Capacity Building Globally", 2023, https://thegfce.org/news/unidir-and-gfce-joined-forces-to-enhance-knowledge-and-information-on-cyber-capacity-building-globally/

9. GFCE, "The Asia-Pacific Cybercrime (APC) Capacity-Building Hub", 2022, https://thegfce.org/news/the-asia-pacific-cybercrime-apc-capacity-building-hub-an-initiative-of-the-supreme-prosecutors-office-of-the-republic-of-korea-the-world-bank-and-the-global-forum-on-cyber-expertise/

Further references

10. Council on Foreign Relations. (2015). The Global Forum on Cyber Expertise: Its Policy, Normative, and Political Importance. Available at The Global Forum on Cyber Expertise: Its Policy, Normative, and Political Importance | Council on Foreign Relations

11. DELHI COMMUNIQUÉ ON A GFCE GLOBAL AGENDA FOR CYBER CAPACITY BUILDING 24 November C2017 available at DelhiCommunique-1.pdf

12. Global Forum on Cyber Expertise. Cybercrime. Available at Cybercrime - The GFCE

13. DGFCE Annual Report 2023- Available at Final GFCE Annual Report 2023

14. Global Forum on Cyber Expertise. About GFCE. Available at About GFCE - Cyber Capacity Building Globally

15. Global Forum on Cyber Expertise. Working Groups. Available at Working Groups - The GFCE - Community Driven

16. The Hague Declaration on the GFCE- 16 April 2015. Available at Microsoft Word - The Hague Declaration on the GFCE - Final

p17. Cyber-security is not just a technical concern

1. GFCE, University of Kent and Institute of Cyber Security for Society iCSS); Krysia Emily Waldock, Vince Miller, Shujun Li and Virginia N.L. Franqueira, "UK Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people", 2022, https://cybilportal.org/wp-content/uploads/2022/08/GFCE-report-20220731.pdf

p30. GFCE's regional hubs empower local stakeholders

1. OCSC, "The Partners in the Blue Pacific P4C Outcomes Report, https://ocsc.com.au/wp-content/uploads/2024/08/P4COutcomesReport.pdf, 2024

p42. Strengthening International Cybersecurity

1. "The Accra Call for Cyber Resilient Development" is the outcome document of the inaugural Global Conference on Cyber Capacity Building (GC3B) which took place in November 2023 in Accra, Ghana, under the theme "Cyber Resilience for Development. https://gc3b.org/the-accra-call-for-cyber-resilient-development/

2. The UN Office for Disarmament Affairs, Office of the United Nations Secretariat (UNODA), "Working paper for a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security", 2021, https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf

3. UNODA, "Open-Ended Working Group on Information and Communication Technologies – Proposal for dedicated thematic groups of the RID future mechanism – PoA for consideration of the OEWG", 2021, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Proposal_for_dedicated_thematic_groups_of_the_RID_future_mechanism_-_PoA_for_consideration_of_the_OEWG_(FR).pdf

4. UNODA, "OEWG Working Paper: Action-oriented thematic groups to advance responsible State behaviour in cyberspace", 2021, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Action_oriented_thematic_groups_(FR)_-_OEWG_working_paper.pdf

p46. Synergy Versus Cybercrime

1. INTERPOL, "C3DP: Fostering regional cooperation against cybercrime in Southeast Asia", , Cyber Capabilities & Capacity Development Project, https://www.interpol.int/Crimes/Cybercrime/Cyber-capabilities-development/Cyber-Capabilities-Capacity-Development-Project

2. INTERPOL, "Public Private Partnerships", Public-private partnership, https://www.interpol.int/en/Crimes/Cybercrime/Public-private-partnerships

3. CyberSecurity Malaysia, "About CyberSecurity Malaysia Collaboration Program (CCP)", https://ccp.cybersecurity.my/about/ccp

4. Huang, H. Y. (2024), "Cybercrime in ASEAN: Fostering Regional Collaboration", Home Team Journal, https://www.mha.gov.sg/docs/hta_libraries/publications/home-team-journal-issue-14e328589e-c671-4cc2-90ae-4d221f9a7297.pdf?sfvrsn=4efe400_1

5. Microsoft, "NCSA and Microsoft's Visionary Collaboration Ushers in a New Chapter in AI-Powered Cybersecurity for Thailand", https://news.microsoft.com/th-th/2024/11/04/ncsa-and-microsofts-visionary-collaboration-ushers-in-a-new-chapter-in-ai-powered-cybersecurity-for-thailand-en/

6. Singapore Institute of Technology, "Kaspersky and SIT Renew Partnership", https://www.singaporetech.edu.sg/news/kaspersky-and-sit-renew-partnership

7. https://news.microsoft.com/th-th/2024/11/04/ncsa-and-microsofts-visionary-collaboration-ushers-in-a-new-chapter-in-ai-powered-cybersecurity-for-thailand-en/

p51. Empowering Communities

1. Tisdale, N. "The Hidden Injustice of Cyberattacks", 12 February, 2024, https://www.wired.com/story/cybersecurity-marginalized-communities-problem

p55. Bringing Gender Equality

1. UNICEF, "Bridging the Gender Digital Divide: Challenges and an Urgent Call for Action for Equitable Digital Skills Development", 2023, https://data.unicef.org/resources/ictgenderdivide/#:~:text=Key%20findings&text=Especially%20in%20low%2Dincome%20countries,do%20not%20use%20the%20internet

2. Pavlina Pavlova, "Gendered Harms of Data Weaponization Historical Patterns, New Battlefields, and the Implications for Democracy and National Security", New America, 2024, https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/

3. RMIT University, "Study finds 1 in 7 adults have experienced someone threaten to share their intimate images", Phys.org, 2024, https://phys.org/news/2024-06-adults-experienced-threaten-intimate-images.html#google_vignette

4. SWGfL, "Research reveals gendered trends in revenge porn crimes", 2019, https://swgfl.org.uk/magazine/revenge-porn-research-2019/

5. University College London, Faculty of Education and Society, "Understanding and combatting youth experiences of image-based sexual harassment and abuse", 2022, https://www.ucl.ac.uk/ioe/research-projects/2022/apr/understanding-and-combatting-youth-experiences-image-based-sexual-harassment-and-abuse

6. Security Hero, "2023 STATE OF DEEPFAKES Realities, Threats, and Impact", 2023, https://www.securityhero.io/state-of-deepfakes/

7. Centre for Feminist Foreign Policy, "Intersectional Feminist Perspectives on Cybercrime Law", 2025. https://centreforfeministforeignpolicy.org/2025/02/24/intersectional-feminist-perspectives-on-cybercrime-law/

8. ibid.

9. Stop Non-Consensual Intimate Image Abuse, https://stopncii.org/

10. Report Remove, Internet Watch Foundation, https://www.iwf.org.uk/our-technology/report-remove/

Global Cyber Expertise Magazine Volume 13, May 2025

Colophon

Artwork & Design:

Roguer Restrepo Estrada (Nieuw Licht Grafisch Ontwerp)

Publishers

African Union, www.au.int,
contact@africa-union.org, @_AfricanUnion

European Union, www.europa.eu,
SECPOL-3@eeas.europa, eu, @EU_Commission

Global Forum on Cyber Expertise, www.thegfce.org,
contact@thegfce.org, @theGFCE

Organization of American States, www.oas.org/cyber,
cybersecurity@oas.org, @OEA_Cyber

Disclaimer

Global Cyber Expertise Magazine

AU • EU • GFCE • OAS

contact@thegfce.org

Submit an article/idea for issue 14
by September, 2025