GC3B

Global Conference on Cyber Capacity Building

GC3B Summary Report

13–14 MAY 2025

GENEVA
SWITZERLAND

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Foreign Affairs FDFA

GFCE 10 YEARS

TABLE OF CONTENTS

TABLE OF CONTENTS

Foreword

On 13 and 14 May, as part of the Geneva Cyber Week, the second edition of the Global Conference on Cyber Capacity Building (GC3B) took place. Hosted by Switzerland's Federal Department of Foreign Affairs and organized by the Global Forum on Cyber Expertise (GFCE), the conference gathered more than 600 people, including representatives of states from all regions of the world, international and regional organizations, the private sector, NGOs, research institutions, and cybersecurity experts. By bringing together these communities, the GC3B aimed to elevate cyber resilience across international and national development agendas, supporting broader development goals and effectively serving the needs of developing countries.

Building on the momentum of the first GC3B in 2023, which resulted in the Accra Call for Cyber Resilient Development —a blueprint outlining concrete actions to advance cyber capacity building, endorsed by over 90 governments and organizations— this second edition focused on reviewing progress, identifying lessons learned and defining next steps to enhance global cyber resilience.

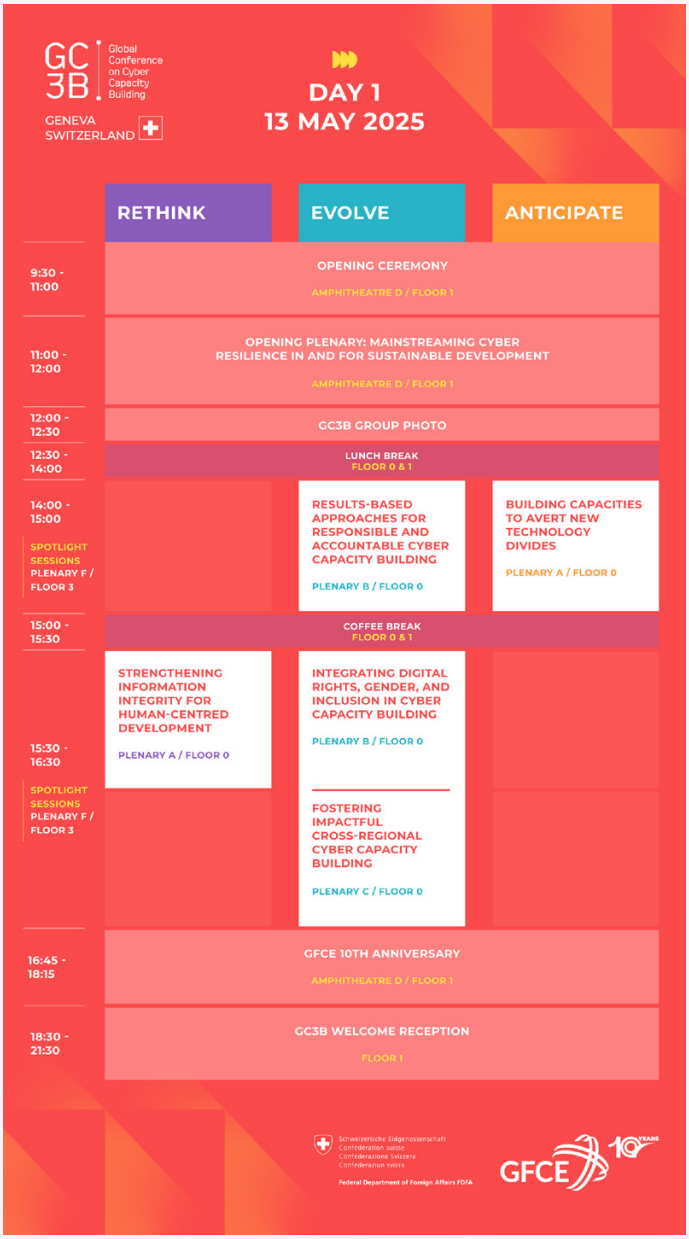
At the conference, participants convened to coordinate strategies, share best practices and resources to support countries in strengthening their digital foundations and pursue the objectives of the Accra Call through their own internal processes and mandates. Based on a comprehensive program structured around pillars 'Rethink', 'Evoke' and 'Anticipate', the GC3B offered dynamic keynotes, thought-provoking panel discussions, and hands-on workshops. In addition, the conference provided great networking opportunities.

On behalf of the Swiss Federal Department of Foreign Affairs and the Global Forum on Cyber Expertise, we thank all attendees, speakers and involved organizations, as well as the GC3B team behind the scenes, who contributed to cyber resilience for development through a shared belief in our mission to ensure a secure and free digital future. We hope you had a most fruitful conference and that this report provides an insightful summary of the discussions that were held at the GC3B 2025.

THANKS TO STRATEGIC PARTNERS & SPONSORS

The second edition of the GC3B would not have been possible without the unwavering support of our **strategic partners and sponsors**. Both the Swiss FDFA as host, and the GFCE as facilitator, express deep appreciation for the crucial role our partners played in shaping the GC3B 2025. Their commitment to advancing global cyber resilience has been pivotal in crafting a forward-looking program and driving our shared mission to embed cybersecurity into broader development agendas. Thanks to their contributions, this edition was not only a meaningful convening, but also **a vital step toward a more secure, open, safe, and sustainable digital future**.

PROGRAM PER DAY



KEY HIGHLIGHTS

HIGH-LEVEL MULTI-STAKEHOLDER REPRESENTATION

GC3B 2025 demonstrated strong institutional commitment to cyber capacity building, with high-level participation from ministers and senior government officials, heads of international organizations officials, and private sector leaders across the world. The opening and closing ceremonies featured impactful statements from high-level representatives, who underscored the urgency of embedding cybersecurity into national development strategies and called for sustained, cooperative action to close global capacity gaps.

This momentum was bolstered by a multi-stakeholder coalition of key strategic partners and sponsors, whose financial support and strategic guidance enabled the conference and shaped its vision. Their engagement, alongside senior representatives throughout sessions on artificial intelligence, infrastructure, regional resilience, and cyber governance, ensured that the conference maintained a high-level, action-oriented character. Their involvement affirms that cybersecurity capacity building is now anchored as a high-level priority across development and security agendas.

High-level group photo at the GC3B 2025, including Ministers from countries across the globe and senior representatives from international organizations and the private sector

GC3B RECEPTION: A SWISS WELCOME TO A GLOBAL GATHERING

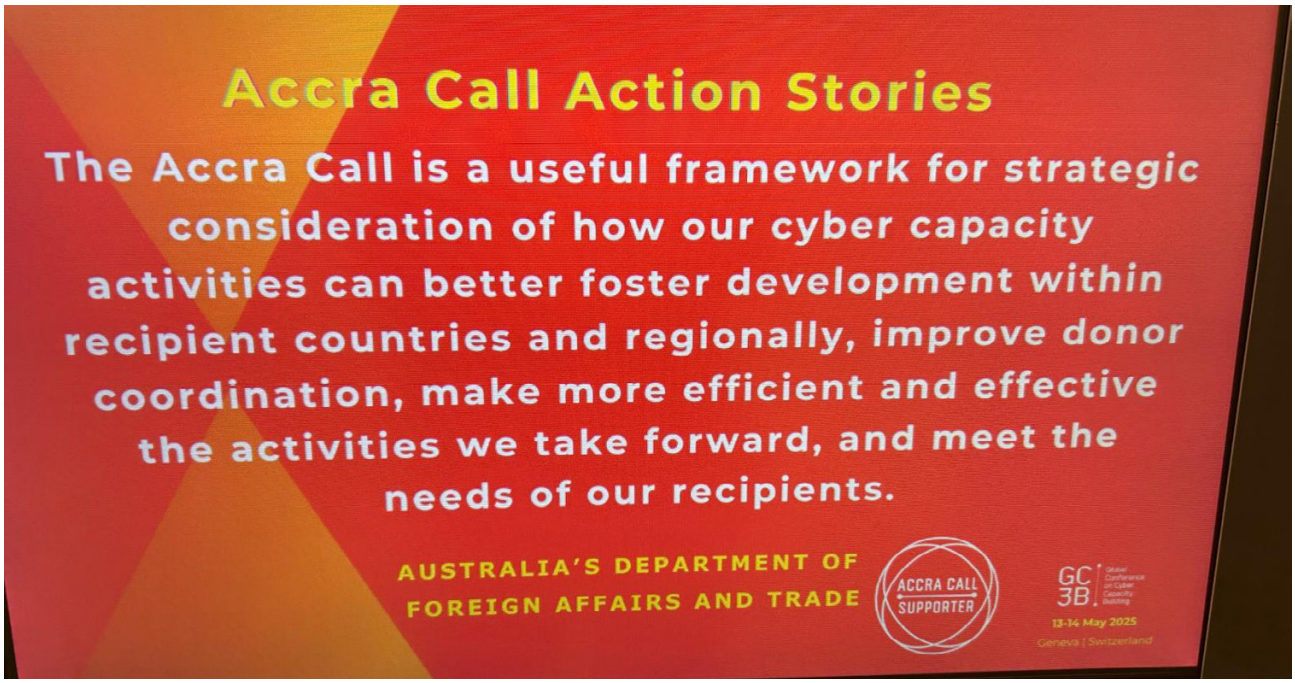
The GC3B 2025 Welcome Reception set the tone for the event, underscoring the conference's unique ability to bring together a diverse global community committed to cyber capacity building. Hosted in the heart of Geneva, the evening offered participants a space to reconnect, forge new partnerships, and reflect on the evolving landscape of cybersecurity collaboration. True to its Swiss setting, the reception featured traditional elements, including an ensemble of alpine horn players and local cuisine, adding a memorable cultural touch that symbolized both international exchange and hospitality. The gathering not only celebrated the growing momentum of the GC3B process but also affirmed its role as a trusted and inclusive platform for advancing shared digital resilience.

CELEBRATING THE GFCE'S 10TH ANNIVERSARY

This session celebrated the 10th anniversary of the Global Forum on Cyber Expertise (GFCE), the facilitator of the GC3B. It highlighted its remarkable growth from a bold idea launched at the 2015 Global Conference on Cyberspace into a cornerstone organization of the international cyber capacity building community. Community members invited on stage reflected on a decade of progress: from fostering early public-private partnerships to becoming a vibrant multi-stakeholder platform that now brings together over 250 members from across the globe.

The session served as both a tribute to the GFCE's achievements and a rallying call for the future. With strong support from regional leaders, governments, civil society, and the private sector, the GFCE was praised for its unique role in harmonizing efforts and elevating trust-based collaboration. The Strategic Steering Committee and Foundation Board were recognized for charting a sustainable, regionally driven path forward. It was reiterated that the GFCE's strength lies not only in its tools, but in its ability to build bridges between sectors, regions, and people, anchored in shared values and a common vision for a more secure and inclusive cyberspace.

Photo of the GFCE 10th anniversary celebration on Day 1 of the GC3B 2025. From left to right, the photo features: Ms. Julia Bauer (GC3B Master of Ceremonies); Mr. David van Duren (GFCE Director); Marjo Baayen (GFCE Director) and Robert Collett (active GFCE community partner)



PROGRESS ON THE ACCRA CALL FOR CYBER RESILIENT DEVELOPMENT

The Accra Call for Cyber Resilient Development, launched at the inaugural GC3B in 2023, served as an inspiration throughout the conference. Referenced in many sessions, including the opening plenary, it serves as a valuable framework to mainstream cyber resilient development. A collection of Accra Call Action Stories, featuring quotes from pledgers, were visible around the venue. The document "From Ghana to Geneva and Beyond: Notes from a Travel Journal" was published in the aftermath of the event, reporting on the progress made by endorsers and pledgers in mainstreaming cyber resilient development. The full Accra Call Action Stories, featuring developments made by key Accra Call stakeholders, have also been published and are available on the GC3B webpage titled "Progress towards the Accra Call". We encourage all stakeholders active in the field and committed to this mission to endorse or make a pledge towards the Accra Call actions. Progress on the Accra Call will be reviewed at the third iteration of the GC3B.

GC3B IN NUMBERS AND MEDIA

GC3B 2025 was more than just a conference: it was a **global convening of actors shaping the future of cyber capacity building**. With over 600 participants and 123 speakers from 130 countries, the event showcased inclusive engagement across regions, genders, and stakeholder groups, underscoring the **scale, global reach, and unique convening power** of the GC3B 2025. This global mosaic of voices enhanced cross-regional dialogue and knowledge-sharing, which is essential to shaping solutions that are effective, equitable, and context-aware. Through valuable networking opportunities and high-level, action-driven discussions grounded in local realities, GC3B 2025 advanced its mission to strengthen global cyber resilience.

WE ARE PLEASED TO SHARE THE FOLLOWING RELEVANT LINKS AND ARTICLES:

GC3B 2025 IN NUMBERS

For a detailed overview of the key figures of the GC3B, please check out **this article**

PHOTOGRAPHY

The main photo album collection can be found **here**

THE AFTERMOVIE

Youtube: GC3B 2025

OPENING CEREMONY

Organized by the Swiss Federal Department of Foreign Affairs (FDFA) and the Global Forum on Cyber Expertise (GFCE)

The Opening Ceremony, moderated by Ms. Julia Bauer, marked the official start of GC3B 2025. The keynote remarks by high-level representatives aimed to set the tone for the days ahead by discussing shared priorities, ongoing efforts, and the need to **RETHINK**, **EVOLVE**, and **ANTICIPATE** in today's rapidly changing digital landscape.

Mr. Gabriel Lüchinger

Assistant State Secretary of Switzerland

Mr. Lüchinger welcomed participants to Geneva and its unique multi-stakeholder community. He celebrated how the Accra Call has expanded its signatory base since its launch in Ghana, emphasizing that *"cybersecurity is the foundation upon which we build our digital house"*. He called for trust, expertise, and cooperation across silos, urging the international community to embed cyber capacity building (CCB) into development.

Mr. Divine Selase Agbeti

Acting Director-General of Ghana's Cyber Security Authority

Mr. Agbeti stressed that *"this is a defining moment: digitalization brings opportunities but also stark threats"*. Ghana is both a leader and a learner, having invested in local cyber skills, especially for youth, while acknowledging the global workforce gap. "GC3B offers an opportunity to move from ideas to strategy, from dialogue to partnerships. The Accra Call has already catalyzed genuine exchanges of needs and experiences among countries".

Ms. Doreen Bogdan-Martin

Secretary-General of the ITU

Ms. Bogdan celebrated ITU's 160th anniversary alongside 10 years of the GFCE. She emphasized that *"when people trust tech, they use it"*. She concluded by urging partners to *"advance capacity building for a cyber-resilient and trusted future for humanity"*.

H.E. Samuel Migal

Minister of Investment, Regional Development and Informatization of the Slovak Republic

The Minister noted that Slovakia is preparing for the regulatory challenges ahead, especially in the areas of quantum computing, AI, and cloud data governance. Cybersecurity, he argued, is now part of national identity and sovereignty. *"We share our experience because we believe common standards make us all safer"*.

Ms. Joanna LaHaie

Director of Capacity Building Office of the U.S. State Department

Ms. LaHaie applauded GC3B's efforts to sustain the multilateral system and looked forward to *"meaningful conversations among the top experts convened here"*.

Mr. Abdurahman Alhassan

CEO of the Global Cybersecurity Forum

Mr. Alhassan called women's empowerment a *"moral and strategic imperative"* for resilience. He shared practical, scaled-up partnerships conducted with IGF and WEF and a new cybersecurity champion initiative in Saudi Arabia to address regional gaps.

Mr. Ewan Smith

Head of Incident Response and Cybercrime Programmes at the United Kingdom FCDO

Mr. Smith reflected on a decade of Cyber Capacity Building evolution, noting that it has broadened to include academia, non-profits, and new partners. He highlighted the increasing threats from hybrid warfare and the dual challenge/opportunity of AI. A joint crime programme is being launched by the UK, and *"the Accra Call guides our next steps toward secure infrastructure in Africa and the Pacific"*.

Ms. Christina Leimoni

EMEA Regional Director at Microsoft

Ms. Leimoni emphasized the importance of investing in a reliable and inclusive AI ecosystem. Microsoft is working with governments, schools, and NGOs to *"equip people with the skills to use AI ethically and safely"*. She also cited the ARCA initiative in Kenya as a best practice in incident reporting and community engagement.

Mr. Magnus Hellgren

Swedish Ambassador to the UN in Geneva

Amb. Hellgren reaffirmed Sweden's commitment to a *"free and open cyberspace"*. The country is integrating digital security into its broader sustainable development agenda, co-leading efforts on the Global Digital Compact and launching a project in Sub-Saharan Africa aimed at connecting and digitizing through local partnerships and capacity building.

Mr. Chris Carter

Account Group Director at BAE Systems

Mr. Carter addressed the tension between digital development and cybersecurity, emphasizing integration rather than trade-offs. He argued that "security enables development, but development also enables security". He stressed the role of threat intelligence, public-private partnerships, and national cybersecurity capabilities to secure the global digital economy. *"We need sovereign capabilities and shared norms to build a safe and open cyberspace"*.

Amb. Diego Brasioli

Italy's Cyber Ambassador

Amb. Brasioli highlighted Italy's national strategy, which views Cyber Capacity Building as *"a strategic tool for sustainable development and peace"*. He reaffirmed support for the Accra Call, especially Call to Action 11 on inclusive and demand-driven initiatives. The Italian approach is reflected in the Mattei Plan, and it is based on a *"non-predatory, locally responsive, and gender-sensitive"* international development agenda.

Ms. Gracita Arrindell

Minister Plenipotentiary of Sint Maarten

Ms. Arrindell reminded delegates that the digital revolution is reshaping the world but also fragmenting it, reminding the participants that *"Cyber Capacity Building is not just technical assistance, it is a cornerstone of our cyber strategy"*. She also highlighted how it reinforces both cyber resilience and human rights, urging continued commitment to multi-stakeholder cooperation, as *"any country that builds cybersecurity contributes to the global commons"*.

Mr. Helmut Reisinger

CISO for EMEA and LATAM at Palo Alto Networks

Mr. Reisinger called for a rethink of the fragmented cybersecurity landscape which requires real-time, AI-driven, automated systems, particularly in healthcare and critical infrastructure. *"We need simplicity, speed, and collaboration across academia, government, and industry"*. He reaffirmed that Palo Alto, celebrating its 20th anniversary, pledges to *"protect for a better tomorrow"*.

Mr. Achim Steiner

UN Development Programme Administrator (via a pre-recorded video)

Mr. Steiner emphasized that cyber threats jeopardize *"hard-won development gains"*. He pointed to the finance sector as especially vulnerable, warning of alarming country-to-country and regional disparities in readiness. UNDP is working on toolkits and regulatory frameworks, advocating for *"demand-driven and inclusive cyber resilience"*.

Ms. Cristina Camacho

Chair of the GFCE Foundation Board

Ms. Camacho closed the ceremony by affirming that "Cyber Capacity Building is no longer a luxury, but a precondition for digital trust", and added that Geneva is the right place to reaffirm multi-stakeholder cooperation. With over 90 endorsers of the Accra Call, the GC3B process shows that follow-through, community, and resourcing now matter more than ever. "Let's remember what brought us here and get to work", she concluded.

Key Takeaways

Cyber capacity building is no longer a technical niche, but it's a strategic imperative. Speakers repeatedly underlined that digital resilience is foundational to development, trust, and peace, with the Accra Call and GC3B framed as key platforms to turn shared ambition into concrete, inclusive action.

Skills, partnerships, and demand-driven approaches are essential to move forward. From Ghana to Italy, countries highlighted initiatives investing in local talent and tailoring support to national contexts.

Multi-stakeholder cooperation is the only way to address global cyber challenges. All speakers converged on the need to break silos and foster collaboration across sectors, and Geneva, as host and hub, was the right place to connect people and advance this agenda.

OPENING PLENARY:

MAINSTREAMING CYBER RESILIENCE IN AND FOR SUSTAINABLE DEVELOPMENT

Organized by the Global Forum on Cyber Expertise (GFCE)

Speakers

- **Moderator – Ms. Nayia Barmpaliou,** GC3B Program Advisor
- **H.E. Stefan Andonovski,** Minister of Digital Transformation of N. Macedonia
- **Ms. Agi Veres, Director,** United Nations Development Programme (UNDP) Geneva
- **Mr. Johan Gerber,** Executive Vice President and Head of Security Solutions, Mastercard

Discussion

The opening plenary began with Ms. Nayia Barmpaliou (GC3B Program team) warmly welcoming participants and recognizing how much effort it has taken to bridge the gap between policy and technical communities. She highlighted that digital development has evolved significantly—it's not only driving growth but also posing real risks. Ms. Barmpaliou emphasized that what once felt like a jumble of buzzwords is now clearly converging under Cyber Capacity Building (CCB). But, she pointed out, to truly benefit from this convergence, investments need to be strategic and aligned with realistic budget constraints. Referring back to the Accra Call launched in 2023, she posed a challenging question: *"Two years later, where are we, especially now that we are at a crossroads, needing to do more with less, and to do it smarter?"*

In response, Ms. Agi Veres (Director of UNDP Geneva), called for a critical shift in how we see cybersecurity: *"Cybersecurity isn't just a technical issue—it's a development issue."* She underscored that digital transformation is now central to UNDP's efforts because safeguarding public institutions and development gains requires digital resilience. Ms. Veres pointed out a harsh reality: many developing countries still lack even basic cyber strategies, making them especially vulnerable, particularly when it comes to critical infrastructure. With digital technologies essential in achieving 70% of the Sustainable Development Goals (SDGs), she stressed that global progress is slowing. To counter this, UNDP is embedding cyber resilience across sectors, building institutional readiness, and helping citizens acquire crucial digital skills. Partnering with the private sector, she added, isn't just about accessing resources; it's about staying ahead of rapidly evolving threats. Cybersecurity must become a standard element of public service delivery and a fundamental pillar of sustainable development.

Sharing a practical perspective, Mr. Stefan Andonovski (Minister of Digital Transformation of North Macedonia), highlighted how his country chose to focus on developmental needs rather than simply meeting donor preferences. *"We built what we needed, based on our comparative advantages,"* he stated. North Macedonia's cyber strategy involved over 40 diverse stakeholders—from ministries and financial institutions to academia and civil society—making sure everyone was included. Specific tasks, clear deadlines, and allocated budgets fostered accountability

and a strong sense of ownership. This broad participation made it a genuinely national strategy, positioning North Macedonia as a regional leader. Importantly, the country intentionally avoided heavy reliance on any single donor, allowing them to continue their initiatives despite recent global funding cuts.

Ms. Barmpaliou then turned to the financial sector for insights, asking Mr. Johan Gerber (Executive Vice President at Mastercard), what could be learned from mainstreaming cyber resilience. Gerber strongly argued that cybersecurity shouldn't be an afterthought following an incident—it should be considered a core enabler of growth. He described how Mastercard views cybersecurity as central to sustainable growth, mentioning significant initiatives, including a USD 10 billion investment and their work with Recorded Future, which monitors threats alongside financial institutions and law enforcement. Mastercard's Community Pass in Africa and the Trust Center for small businesses stood out as strong examples of inclusive digital resilience. However, Gerber expressed concern about growing trends in data and tech nationalism, warning these could fragment efforts and hinder global collaboration. He emphasized the importance of a positive first experience: *"If someone's first encounter with the digital economy is a scam, we've lost them."*

Addressing the fragmented geopolitical context, Mr. Andonovski noted a paradox: increasing investments often go hand-in-hand with declining coherence. He cited examples of overlapping donor-funded projects and siloed government initiatives as sources of fragmentation. Small countries in particular, need strategic resource management—they can't afford inefficiencies. He underscored the need for strong coordination both internally and among international donors, mentioning the ongoing effort in North Macedonia to consolidate multiple tax portals into a single, secure one.

Mr. Gerber reinforced the vital role the private sector plays, highlighting scale, frameworks, and partnerships. Mastercard's cooperation with the World Bank exemplifies embedding trust into digital systems from the outset. *"We're closely collaborating with governments and NGOs because resilience and innovation underpin our business model,"* he emphasized. Ms. Veres then connected the discussion back to development, especially in fragile contexts. She warned that cybersecurity vulnerabilities erode trust not just economically, but also socially affecting critical services like pensions, identity systems, and inclusion initiatives. She encouraged governments to approach cybersecurity as an integrity issue affecting the entire society. Ms. Veres highlighted UNDP's Digital Inclusion Playbook and a new handbook for policymakers as practical tools for embedding cyber resilience across sectors. She framed it as "**the 3 Ps—Protection, Policy, and People.**"

As the plenary wrapped up, Mr. Andonovski reminded everyone that trust and inclusion must remain at the core of all cyber initiatives. *"Citizens need to feel safe. We are building for people,"* he stressed. Mr. Gerber echoed this call to action, pushing for urgency and measurable impact: *"Let's come back next time*

and see the impact." Finally, Ms. Veres cautioned against *"techno-determinism"* and emphasized inclusive cybersecurity, particularly protecting the most vulnerable. Drawing from UNDP's Human Development Report, she listed four priorities: building a complementary economy, aligning innovation with real human needs, closing global skill gaps, and promoting equitable access through policy innovation.

Ms. Barmpaliou closed the session with three remarks: the necessity of co-creation in partnerships, the shift of cybersecurity from being "good for business" to being essential to business, and the importance of intentionally designing programs and investments with people, especially those most vulnerable, at the centre.

Key Takeaways

Cyber resilience is no longer a technical detail but is essential for development and growth. From financial systems to public services, cybersecurity and the resulting trust must be treated as foundational enablers of growth and innovation.

Co-creation is key to building effective partnerships and ensuring ownership. Convening diverse stakeholders with clear roles, timelines, and budgets avoids fragmentation and builds resilient systems that deliver.

People must be at the center of cyber capacity building, especially the most vulnerable. Trust in digital infrastructure starts with inclusion and fairness, not just access: programs need to be designed to serve, protect, and empower users.

HIGH-LEVEL MINISTERIAL CLOSED SESSION

ON CYBERSECURITY CAPACITY BUILDING IN AFRICA AND THE GLOBAL SOUTH

Hosted by the World Economic Forum under the auspices of the GC3B

Organized by AUDA-NEPAD and facilitated by the GFCE

Speakers

- **Moderator: Mr. Amine Idriss Adoum,** Senior Director, AUDA-NEPAD
- **Mr. Moctar Yedaly,** Africa Hub Director, Global Forum on Cyber Expertise
- **Mr. Mamadou Biteye,** Executive Secretary, Africa Capacity Building Forum
- **Mr. Johan Gerber,** Executive Director, Mastercard

Background of the session

In the digital age, cybersecurity has become a cornerstone for national security, economic resilience, and societal wellbeing. Africa, with its burgeoning digital economy and increasing internet penetration faces unique challenges in building cybersecurity capacity. Many African Union (AU) institutions and member states have highlighted the pressing need for enhanced cybersecurity frameworks, infrastructures, and trained personnel to safeguard national assets, critical information, and citizens. Despite ongoing efforts, vulnerabilities to cybersecurity threats remain due to resource constraints, technological limitations, and gaps in policy implementation. These challenges are reflective of broader systematic issues across the Global South.

Discussion

The session highlighted the pressing need for inclusive, strategic and sustainable cybersecurity capacity building (CCB) efforts, particularly across the Global South. Central to the discussion was the notion that in cybersecurity, "we are only as strong as the weakest link," a message reinforced by representatives from the AU, AUDA-NEPAD, and numerous global stakeholders.

By bringing together stakeholders from different regions across different sectors, the session demonstrated that CCB is a shared responsibility and a shared opportunity.

The African Perspective

Representatives from African stakeholders emphasized the importance of leveraging science diplomacy to create inclusive and resilient cyber strategies. While digital transformation poses risks, it also presents a unique opportunity to bridge existing developmental divides. Africa's digital economy is constantly increasing; however, cybersecurity remains a major obstacle as it can divert resources from critical sectors such as education and health. Therefore, without strong CCB initiatives, the digital divide threatens to grow.

Stakeholders highlighted the importance of human-centered approaches, calling for investments in the continent's youth through partnerships, technical support, and capacity development.

Thematic Takeaways

This session brought together many different stakeholders, varying from European and Global South governmental representatives to private sector actors. The session illustrated the growing consensus that inclusive, locally anchored, and globally supported Cyber Capacity Building is not only necessary for cybersecurity but also critical to sustainable development.

1. **Cybersecurity Is Global and Borderless:** Esteemed high-level participants highlighted the shared nature of cyber threats, calling for international frameworks, such as the UN Cybercrime Convention, to include the perspectives and needs of developing countries.

2. **Inclusion and Human-Centered Design:** rather than focusing solely on technological solutions, participants stressed the need to design cybersecurity initiatives around the lived experiences, needs, and capabilities of individuals ensuring no one is left behind in digital transformation efforts.

3. **Moving from Global Knowledge to Local Realities:** a recurring theme was the importance of mutual learning and knowledge exchange between stakeholders. It was stressed that we need to avoid imposing external solutions and rather listen to local stakeholders. Meaningful capacity building must be context-specific, co-created with local actors, and grounded in their realities, priorities and knowledge.

PILLAR: RETHINK

STRENGTHENING INFORMATION INTEGRITY FOR HUMAN-CENTRED DEVELOPMENT

Organized by the CyberPeace Institute and the Government of Albania

Speakers

- **Moderator – Ms. Francesca Bosco,** CyberPeace Institute
- **Ms. Emmanuelle de Foy,** Ministry of Foreign Affairs of Belgium
- **Ms. Manon Le Blanc,** European External Action Service
- **Mr. Franz Zylyftari,** National Agency for Information Society of Albania
- **Ms. Era Gjata,** Albanian National Cyber Security Authority
- **Mr. Mattia Caniglia,** Global Disinformation Index and Co-Chair of FIMI ISAC
- **Mr. Alex Dalessio,** eQualitie

Discussion

This session offered a timely and urgent reflection on the role of information integrity within the broader mission of cyber capacity building. The discussion opened by emphasizing a fundamental shift in understanding resilience: from protecting technical systems alone to defending people, democratic institutions, and public trust. In today's digital age, resilience can no longer be understood solely in terms of hardened infrastructure or encrypted systems. It must be redefined as a human-centered endeavor that defends against not only technical breaches but also narrative attacks, disinformation, and the erosion of civic trust. Speakers agreed that these are interlinked areas requiring hybrid responses to address increasingly complex threats.

The key message was clear: these two domains can no longer be treated in silos, but as two fronts on the same battlefield. The session highlighted practical examples from countries that have faced combined cyber and disinformation attacks. One example illustrated how Albania, following significant cyber incidents and targeted disinformation campaigns that aimed to undermine public trust, introduced comprehensive legal reforms, enhanced CERT capacities across critical sectors, and developed dedicated national disinformation strategies. These initiatives benefited from collaboration with international partners.

The conversation also underscored the critical role of inclusion and co-creation amongst stakeholders in capacity building activities. A case was shared illustrating how governments, civil society, and the private sector collaborated effectively, jointly identifying critical infrastructure and designing proactive response methodologies. Participants noted the importance of genuine participation, transforming traditional consultations into bottom-up, meaningful partnerships.

The session further addressed the broader geopolitical context, emphasizing that information manipulation is now a central tool used by state and non-state actors globally. Participants described detailed examples of how some

nations now dedicate significant resources to strategic information operations, often outsourcing them to private actors. In parallel, he also warned that these actors are also filling the gaps left by diminished international programs, opening space for malign influence in Africa, Southeast Asia, and the Balkans. The discussion stressed that recognizing disinformation as both a security and developmental issue is crucial, advocating strongly for empowering civil society as the frontline of defense through increased funding and building coordinated infrastructures to enhance interoperability.

The metaphor of information manipulation being a slow, relentless tide that erodes things slowly—rather than a sudden wildfire—resonated with participants. The consensus was clear: responses must be systemic, enduring, and anticipatory - integrating digital literacy, media education, and cybersecurity into a unified resilience ecosystem rather than parallel tracks.

Concluding the session, the conversation shifted to practical implementation strategies, emphasizing the importance of user-centric design. It was reiterated that whilst civil society is stepping up, governments remain trapped in short-term, incremental thinking. A call for effective long-term partnerships that foster trust, and usability was highlighted as critical. Participants advocated moving beyond short-term solutions to creating sustainable information ecosystems rooted in local realities and user experiences.

In sum, the session challenged the audience to **RETHINK** both the purpose and practice of cyber capacity building. If digital threats are hybrid, our defenses must be hybrid too by bridging both infrastructure protection with democratic resilience and technical protocols with civic trust. The task is not simply to secure systems, but to secure societies. And that requires investing in a human firewall, one made of critical thinking, institutional safeguards, and community capacity.

Key Takeaways

Information integrity must form the foundation of cyber capacity-building strategies, **recognizing it as both a development and security challenge** that demands a proactive, coordinated response.

Hybrid threats require hybrid solutions, combining technical, societal, and institutional measures.

Civil society, though critically positioned at the frontline, remains underfunded and **must be prioritized** to effectively combat disinformation and protect democratic institutions.

SCALING UP SMART APPROACHES AND FINANCING FOR SUSTAINABLE CYBER CAPACITY BUILDING

Organized by the World Bank

Speakers

- **Moderator – Ms. Anat Lewin,** World Bank
- **Ms. Chinenye Chizea,** Nigeria ID4D
- **Ms. Mariama Yormah,** Cybersecurity Coordination Centre, Sierra Leone
- **Mr. Carlos Leonardo,** National cybersecurity Center, Dominican Republic
- **Ms. Masayuki Furukawa,** Japan International Cooperation Agency

Discussion

The session opened with a call to shift away from traditional models of technical assistance towards comprehensive, sustainable cyber capacity building frameworks. Participants explored diverse national experiences, revealing how different starting points and resources shape strategic pathways.

One country shared its approach to securing a national digital identity ecosystem in the context of institutional fragmentation. Cybersecurity was embedded into a broader security culture, securing biometric data and positioning the national ID as a foundational layer of digital trust, supported by an ecosystem of partners and sustained investments in mentorship and local capacity development. Threat monitoring and tailored security practices that address local needs were also developed alongside the expansion of backend data processing capabilities, frequent staff training, and public awareness campaigns. The establishment of a dedicated CERT for the ID sector also provided critical visibility and responsiveness. A focus was also placed on expanding infrastructure and digital services to underserved communities, positioning inclusion and trust as central to national cyber resilience.

Another intervention focused on countries' efforts to strengthen regional cybersecurity through partnerships in South-East Asia. In 2019, Japan supported workforce development initiatives, including the establishment of regional cybersecurity academies and centers in Indonesia and Thailand, and the organization of regular cybersecurity drills within ASEAN. The strategy emphasized the importance of mobilizing domestic private actors and attracting international investment to ensure sustainability. Collaborations with other countries further enriched training efforts. However, participants noted that direct replication of such approaches are not always feasible in other regional contexts, reinforcing the need for context-sensitive and locally adapted public-private funding models.

Sierra Leone also shared how starting from a low baseline allowed for strategic planning from the outset, instead of dealing with legacy systems. A national strategy and cybersecurity center were developed with support from regional and international partners like ECOWAS and the EU. Despite ongoing infrastructure challenges, the country achieved notable progress in managing cybercrime and digital evidence through institutional and legal capacity building. Partnerships with universities and the integration of cybersecurity education into school curricula were identified as essential enablers, as well as government commitment. Looking ahead, plans include expanding the national center, developing a tiered CERT framework, creating sector-specific protection protocols, and launching multi-lingual awareness campaigns tailored to women and children.

The case of the Dominican Republic illustrated how limited initial resources did not prevent rapid progress when supported

by strong governance and clear strategic alignment. Since 2015, they have strengthened cyber governance, established national cybersecurity requirements, and centralized public-private platforms into a national center. International cooperation has played a key role in building technical capabilities, including threat visibility across over one million IP addresses. The country is now focused on enhancing data-driven decision-making systems and quantifying both the actual and avoided economic costs of cyber incidents to better guide investments and policy decisions.

An audience intervention asked how these initiatives are embedded in national cyber strategies. Responses highlighted the importance of private sector collaboration in raising public awareness and communicating cyber risks effectively—an approach rooted in broader national strategy development and outreach. Throughout the session, participants emphasized the importance of transitioning from one-off projects to integrated and sustainable models that account for technical, financial, and political dimensions. Trust-based partnerships that reflect local contexts and adaptive ambitions were identified as key to long-term success. Even if countries are navigating different pathways, they all recognize that resilient cyber capacity building requires both ambition and adaptability.

Key Takeaways

Build trust through inclusive partnerships that adapt to local realities: Trust-based, context-aware collaboration across sectors and borders underpins effective and sustainable cyber capacity building.

Invest in people: Human capital is the foundation of resilient cybersecurity. Investing in education, mentorship, and cultural awareness ensures long-term institutional readiness.

Prioritize meaningful, continuous training: Cybersecurity training should go beyond technical skills, encompassing critical thinking, adaptability, and real-world threat comprehension, empowering local actors to respond effectively.

SECURE, TRUSTED AND RESILIENT INFRASTRUCTURE AND CONNECTIVITY

Organized by the U.S. Department of State

Speakers

- **Moderator – Ms. Patricia Eke,** Microsoft
- **Ms. Jennifer Bachus,** United States Department of State
- **Mr. Filip Pavlović,** Ministry of Foreign Affairs of Serbia
- **Ms. Cristina Camacho,** Ministry of Foreign Affairs of Ecuador

Discussion

The session brought together perspectives from government, development agencies, and national infrastructure authorities to explore how countries are approaching **risk management for infrastructure security** in complex and evolving threat environments.

Panelists began by framing the multi-dimensional nature of infrastructure threats, emphasizing that risks stem not only from cyber intrusions and supply chain exposure but also from regulatory fragmentation, institutional readiness, and broader geopolitical dynamics. The complexity of the threat landscape requires a **holistic approach,** one that considers **not only technological solutions but also cultural, institutional, and legislative readiness**. Drawing from the United States' experience, the importance of treating cybersecurity as a sustained commitment rather than a one-time investment was emphasized. A continuous and adaptive risk management process was described as essential, particularly in contexts where threat actors evolve faster than the systems protecting against them. The importance of embedding cybersecurity into governance frameworks, processes, and workforce development was emphasized.

Another intervention illustrated Ecuador's national journey from being ranked among the lowest in the Global Cybersecurity Index to substantially improving its cybersecurity posture. Outdated legal frameworks, limited domestic

funding, and a shortage of skilled professionals were cited as common obstacles. Nonetheless, the country had made significant gains through institutional coordination, the creation of the National Cybersecurity Committee, and active participation in international dialogues. It was noted that progress also depends on clearly defining what qualifies as critical infrastructure within the national context to ensure tailored and effective protection strategies. Political willingness, regional collaboration and access to international funding and training were flagged as key accelerators to sustain progress.

The case of Serbia was also shared, which focused on advancing secure infrastructure and cybersecurity resilience in underserved regions. Examples shared included initiatives to **provide secure digital connectivity for schools and developing national cybersecurity standards** aligned with international regulations. Investments were also made in secure data centres, public-private partnerships, and integrating cybersecurity into broader digital literacy programs. Risk management was discussed not only as a policy priority but as a practical necessity at the operator level. Tools such as routine risk assessments and incident response planning were highlighted as foundational.

Throughout the discussion, panelists agreed that resilience must be seen not only as a technical goal but as a societal one. Trust in infrastructure and public services hinges on **sustained, inclusive collaboration between governments, private sector actors, and civil society**. A

recurring theme was the importance of embedding cybersecurity into national development plans, especially as artificial intelligence and emerging technologies both present opportunities and introduce new vulnerabilities.

The session concluded with a collective call **to shift from reactive to proactive strategies**. The path to resilience is built through leadership, political will, and a culture of continuous learning and adaptation that spans all levels of society and infrastructure.

Key Takeaways

Cybersecurity is a continuous, multi-dimensional challenge: Evolving threats require a dynamic approach that integrates technology, legal frameworks, institutional capacity, and cultural readiness.

National progress depends on leadership and tailored strategies: Resilience requires clearly defined infrastructure priorities, political will, and frameworks that reflect national and regional realities.

Resilience is built through inclusive, long-term collaboration: Sustainable infrastructure security relies on cross-sector partnerships, investment in human capital, and a shared commitment to digital trust.

TOWARDS A CYBER AND CLIMATE RESILIENT DIGITAL TRANSITION

Organized by The Kingdom of The Netherlands

Speakers

- **Moderator - Moliehi Makumane,** UNIDIR
- **Ernst Noorman,** Cyber Ambassador of The Netherlands
- **Ms. Gracita Arrindell,** Minister Plenipotentiary of Sint Marteen
- **Mr. Lacina Koné,** Smart Africa
- **Ms. Liina Areng,** EU CyberNet
- **Mr. Juri Nicolaas,** Country of Aruba
- **Ms. Robin Zuercher,** ITU

Discussion

The discussion focused on the intersection of cybersecurity, climate resilience, and inclusive development, emphasizing that both must be treated as **interdependent components of a successful digital transition**.

Panelists underscored that cybersecurity is now recognized as a core pillar of green digital agendas. While digital infrastructure is a strategic enabler, a large portion of global communities remain unconnected, and rising technological demands risk exacerbating environmental stress. The importance of building cyber-resilient infrastructure that is also environmentally conscious was reiterated, highlighting water scarcity and e-waste as pressing concerns. It was emphasized that **sustainability must be embedded from the outset, not added later**. Examples included training programs targeting women in cybersecurity, multi-national drills, and bridging infrastructure investment gaps. Sovereign data control and sustainable infrastructure design were also cited as emerging priorities.

A perspective from the African continent emphasized that

the absence of legacy systems offers African nations a unique opportunity to build sustainable digital infrastructure from the ground up. Innovation hubs and national blueprints are being crafted with **sustainability at their core**. The need to move beyond outdated global cooperation paradigms was highlighted, with calls for **equitable technology transfer and infrastructure investment models** tailored to local contexts.

Moving towards the Caribbean region, it was emphasized that a **shift from siloed to integrated cyber and climate policymaking is underway,** defining national cyber-climate priorities and embedding sustainability from the beginning of any initiative. However, small island nations face unique challenges in aligning development goals with procurement and resilience planning, particularly due to limited human and financial resources. A call was made for context-sensitive, practical frameworks that adapt global standards to national realities.

The experience of The Netherlands in integrating cybersecurity into renewable energy infrastructure was shared, emphasizing the importance of institutional resilience and regional cooperation. National cybersecurity councils, collaborative policymaking, and coordination with multilateral institutions like the World Bank were offered as examples of forward-looking approaches. The importance of **regional cooperation and institutional resilience** was recognized as key to a sustainable twin transition.

Other contributions echoed the importance of **aligning digital and green agendas from the beginning**. Examples included support for SMEs in Czech Republic through targeted programs and partnerships with research networks in Latin America like RedClara (through the Copernicus program). Empowering local actors—like government officials, media, and civil society, was presented as essential to achieving a truly inclusive resilience.

Audience contributions revolved around practical examples. One participant emphasized the urgency of engaging more directly at the policy level with the twin transition agenda. Another described the early adoption of AI impact measurement in workforce development initiatives. It was noted that Aruba's Cyber & Climate Academy, once viewed as unconventional, had proven to be an effective bridge between both agendas. Furthermore, another participant reflected that such events offer valuable learning for all stakeholders, reinforcing the need for active, not passive, engagement.

The session closed with a strong

call to action. Small developing states, which face the twin burdens of legacy systems and resource constraints, require urgent support. Speakers argued that **sustainability and security are not separate goals but must be pursued together**. Integrated planning at the national level, backed by global cooperation frameworks, is essential to ensure no country is left behind in the green digital transition.

Key Takeaways

Beyond technical skills, workforce development must address institutional and coordination gaps: Building cyber resilience in green transitions requires aligning education, infrastructure, and policy across sectors, especially in contexts without legacy systems.

Cooperation must evolve beyond Global North-South binaries and one-size fits all models: Effective partnerships are grounded not in replication, but in mutual learning, investment, and support to countries in developing tailored solutions.

Embed security and sustainability from the start: Infrastructure and policy planning must integrate security and environmental considerations early to avoid costly retrofitting and foster long-term resilience.

MULTI-STAKEHOLDER COLLABORATION FOR CYBER-RESILIENT DEVELOPMENT

Organized by the Global Cyber Alliance, NetHope and Deloitte

Speakers

- **Moderator – Ms. Dianna Langley,** NetHope
- **Ms. Catalina Vera Toro,** Permanent Mission of Chile to the OAS
- **Mr. Giacomo Assenza,** World Bank
- **Ms. Komal Bazaz-Smith,** Global Cyber Alliance
- **Ms. Elizabeth Villarroel,** Deloitte

Discussion

This dynamic session brought together a diverse group of speakers with deep field experience across regions, including small island states, Latin America, and the global donor community, to examine the **transformative potential of multi-stakeholder collaboration** in cyber capacity building. Framed around the urgency of advancing cyber-resilient development, the session underscored that no single sector or stakeholder can deliver sustainable outcomes in isolation.

Speakers emphasized the limitations of siloed or top-down initiatives. These often fail to capture the complexity of local needs, miss opportunities for co-ownership, and face challenges in scaling or sustaining impact beyond short-term project cycles. Several examples illustrated how single-sector approaches, whether donor-led, government-driven, or private sector-led, can falter without **local buy-in, contextual relevance, or multi-actor alignment**.

In contrast, multi-stakeholder approaches were shown to **enable greater trust, inclusion, and adaptability**. One speaker highlighted a compelling set of examples from Facebook (Meta), where the company successfully supported resilience by partnering with local actors. Among the

initiatives mentioned was the provision of public Wi-Fi access, which was co-developed with community organizations to ensure usability and sustainability. This demonstrated how private sector actors can meaningfully contribute not only by providing technical solutions but also by aligning efforts with the priorities of civil society and local governments.

Another speaker described cyber capacity building efforts in the health, agriculture, and energy sectors in Latin America and the Caribbean. These sectoral initiatives revealed that embedding cybersecurity into broader development goals, such as digital service delivery and infrastructure modernization, was more successful when local stakeholders, including NGOs and academia, were **engaged early on**. For instance, a multi-sectoral effort in the energy sector led to improved cyber resilience among electricity regulators by fostering regional cooperation, joint risk assessments, and tailored training programs.

A strong theme throughout the discussion was the value of civil society and the technical community in driving long-term impact. In small island developing states (SIDS), for example, trust-building among municipal authorities, local providers, and citizens enabled the co-creation of **digital governance frameworks that outlasted external funding cycles**. One speaker shared how they helped build "a network of networks" connecting stakeholders across the public and private sectors to design, implement, and maintain resilient infrastructure for remote communities.

The panel also reflected on the operational challenges of scaling multi-stakeholder efforts: the **need for coordination mechanisms, flexible and sustained financing, interoperable standards, and shared language**. Communication and translation—both literal and cross-sectoral—were noted as vital enablers of effective collaboration. Helping different actors "speak the same language," whether in terms of digital literacy, policy objectives, or technical requirements, was repeatedly cited as a make-or-break factor.

Finally, panelists agreed that multi-stakeholder cyber capacity building efforts must go beyond consultation. Genuine collaboration requires **distributing leadership, resources, and credit**. Integrated approaches

foster mutual accountability and shared value, increasing the chances that cyber resilience becomes embedded in national development strategies rather than treated as a niche technical add-on.

Key Takeaways

Integrated approaches to cyber capacity building foster local ownership and sustainable outcomes, particularly when diverse actors co-develop diagnostics and implementation plans.

Civil society and local technical communities are essential to ensure relevance, inclusion, and continuity beyond donor funding cycles.

Siloed, top-down initiatives risk failure if they do not engage or align with the institutional, cultural, and economic realities of local contexts.

MAINSTREAMING CYBER RESILIENCE: LESSONS AND COLLABORATION MODELS FROM THE PACIFIC (SAMOA)

Organized by WebSafe Samoa

Speakers

- **Moderator – Mr. Leiataualesa Jobenz Manoa,** WebSafe Samoa
- **Mr. Mitchell Dunn,** Department of Foreign Affairs & Trade of Australia
- **Ms. Pua Hunter,** GFCE Pacific Hub
- **Ms. Vui Athena Matalavea,** MCIT Samoa
- **Mr. Esau Tupou,** CERT Tonga
- **Ms. Pateli Vailea,** Tonga Women in ICT

Discussion

This session convened leaders from across the Pacific to reflect on how island nations are embedding cyber resilience into national development strategies. Discussions focused on **leveraging community-driven approaches, regional partnerships, and donor collaboration** to address the specific challenges faced by Small Island Developing States (SIDS). Framed around the lived experiences of Samoa, Tonga, and the Cook Islands, the session highlighted context-sensitive models and actionable insights for broader application.

Speakers emphasized that cybersecurity is no longer a peripheral technical issue but a foundational pillar of sustainable development. As digital transformation accelerates across the Pacific, the cyber threat landscape is expanding, presenting both risks and opportunities. Panelists underlined that **cyber resilience must be co-created through inclusive partnerships**, spanning governments, local communities, civil society, the private sector, and development agencies, and **anchored in local ownership and leadership**.

Samoa shared its national approach to **strengthening cyber readiness throughmulti-sectoralcollaboration**. The government partnered with CERT NZ and other regional actors to bolster cybersecurity capabilities ahead of major international events such as the Commonwealth Heads of Government Meeting (CHOGM). Specific actions included targeted training for small and medium-sized enterprises (SMEs), coordinated exercises with national stakeholders, and capacity-building efforts across government, non-governmental organizations, and the private sector. The development of national awareness campaigns was emphasized as a tool for mainstreaming a cybersecurity culture.

Tonga presented a strong case for **community-level engagement**, underscoring that effective resilience begins with inclusion. The partnership between CERT Tonga and Tonga Women in ICT enabled grassroots outreach through tailored workshops and educational campaigns. These efforts targeted underrepresented groups, particularly women and youth, and succeeded in building digital

trust, expanding local capacity, and improving cyber hygiene practices. Community champions emerged as critical enablers of this success, ensuring sustainability and cultural relevance.

The Cook Islands detailed its strategy to build a sustainable cybersecurity workforce through partnerships between government, education providers, and private sector entities. National initiatives included the publication of a **Cybersecurity Manual to guide public institutions**, and the implementation of workforce development programs designed to build long-term technical capacity. Community engagement and feedback mechanisms were embedded into these programs to ensure that initiatives remained responsive and inclusive.

Representatives from Australia reflected on its support for regional strategies and reiterated the value of **long-term, respectful engagement**. The importance of co-designing solutions with local actors and investing in capacity that stays within communities was stressed. Speakers noted that the Pacific is moving beyond its traditional role as a recipient of capacity-building and is emerging as a contributor to global thinking on cyber resilience. The region is developing **innovative models that bridge traditional knowledge systems with modern cybersecurity strategies**.

Persistent challenges were acknowledged, including financial and human resource constraints, high turnover of skilled personnel, and limited enforcement mechanisms. However, the session also showcased pragmatic solutions. For example, countries are adopting **modular and risk-based approaches** to cybersecurity, such as selectively implementing relevant controls from ISO and NIST frameworks. This flexible approach enables progress despite constrained resources and supports local implementation.

The discussion highlighted the importance of regional knowledge sharing through platforms such as the **Pacific Cyber Security Operational Network (PaCSON)**. These platforms facilitate threat intelligence sharing, peer learning, and harmonized response mechanisms, contributing to a collective regional posture.

Sustainable impact, it was agreed, hinges on early involvement of local experts in project design, co-delivery models that ensure equitable distribution of responsibilities, and investments in infrastructure that serve both economic development and cybersecurity goals. Such investments should aim to **embed knowledge within institutions and communities**, reducing long-term dependence on external actors.

Pacific nations are asserting their role as thought leaders in cybersecurity by integrating resilience into sustainable development strategies. Their efforts underscore that secure digital futures are built through collaboration, respect for local knowledge, and a shared commitment to equity, security, and sustainability.

SYMBOLIC CLOSING

Director Dunn was gifted a **tafesilafa'i**, a symbol of unity and resilience inspired by Samoa's warrior princess Nafanua reminding us that the Pacific's fight in cyberspace is grounded in both **tradition and innovation**.

Key Takeaways

Context matters: Cybersecurity initiatives must align with national realities, including resource availability, institutional maturity, and local priorities. One-size-fits-all models are ineffective.

Empower communities: Inclusion of women, youth, and traditional leadership structures enhances resilience and fosters trust. Community-level engagement ensures that cybersecurity is locally meaningful and sustainable.

Donor collaboration must evolve: Effective donor partnerships require early and ongoing involvement of local actors, mutual accountability, and alignment with national development goals.

Tailor global frameworks to local contexts: Adopting modular controls from international standards such as ISO and NIST allows for practical implementation without overburdening limited capacities.

The Pacific leads by example: The region is creating context-sensitive, innovative models of cyber resilience that are globally relevant and can serve as blueprints for other SIDS.

PILLAR: EVOLVE

RESULTS-BASED APPROACHES FOR RESPONSIBLE AND ACCOUNTABLE CYBER CAPACITY BUILDING

Organized by the Inter-American Development Bank

Speakers

- **Moderator – Ms. Caroline Weisser Harris,** Global Cyber Security Capacity Centre, University of Oxford
- **Maj Gen Luiz Fernando Moraes da Silva,** Institutional Security Cabinet, Presidency of the Republic of Brazil
- **Ms. Anat Lewin,** World Bank
- **Mr. Ariel Nowersztern,** Inter-American Development Bank
- **Ms. Yurie Ito,** CyberGreen Institute / GFCE Foundation Board

Discussion

The session explored how a results-based approach can improve the **effectiveness, accountability, and impact** of cyber capacity building (CCB), particularly in developing countries. With more actors and resources involved in CCB, speakers emphasized the need to move beyond outputs and towards evidence-based measurement of progress and outcomes. The discussion gathered perspectives from multilateral development banks, technical experts, national government representatives, and global CCB networks, and focused on key practices, tools, and institutional frameworks that can enable more meaningful monitoring and evaluation (M&E) in the field.

The conversation opened with a national government perspective, which stressed the need to anchor

cyber M&E in national policies, strategies and plans. In the case of Brazil, their cybersecurity framework is organized around four pillars: infrastructure protection, international and domestic cooperation, sovereignty, and digital governance. To support continuous improvement, the government conducts biannual reviews of its privacy and information security program, and has applied the Cybersecurity Capacity Maturity Model for Nations (CMM) in 2020 and 2023. The latest assessment found that 50% of evaluated areas reached an established level of maturity, while others still require development. The country plans to conduct a new review next year, and plans to design a national model to reflect evolving needs and sovereignty. It also shared plans to expand its national CSIRT's data monitoring network and promote the creation of information sharing and analysis centers (ISACs). A recent comparative review of over 40 national strategies across 17 countries revealed a shift from defense-centered approaches to more holistic cyber policies focused on economic opportunity and inclusion. The importance of aligning with global progress while remaining anchored in national realities was also reiterated.

The discussion moved to perspectives on how development banks are embedding cybersecurity within broader development programs. While only a few projects

are exclusively cyber-focused, over half of its operations in 2024 referenced cybersecurity as a core component. A notable example was a multi-year, nationwide initiative in Uruguay, which increased student participation in cyber education from 50 in 2018 to over 400 in 2023, with women now making up 30–50% of participants. The initiative also strengthened monitoring mechanisms: cybersecurity oversight expanded from 2 to 18 ministries, and Uruguay developed a national maturity assessment tool based on the NIST framework. The development bank used a "pyramid of indicators" ranging from technical to ecosystem-level metrics and funded longitudinal studies to assess direct impact and broader systemic progress over time.

From the World Bank perspective, a key obstacle identified was the lack of reliable, comparable data for effective M&E of cybersecurity outcomes. While many frameworks, such as theories of change, are in use, most countries lack the statistical capacity to collect meaningful indicators beyond basic outputs such as training counts. Outcome-level data is often missing, inconsistent, or not attributable to specific interventions. Sector-specific statistics are often rarely collected, inconsistent, and definitions vary widely across countries, which hinders cross-country analysis. In some cases, informal incident reporting offers more insight than formal mechanisms constrained by legal requirements. The need for global consensus on a core set of cybersecurity indicators, investment in national data systems, and partnerships with private-sector entities that hold valuable, underutilized data was stressed. A recent initiative from the World Bank made use of AI to map cybersecurity incidents in 90 countries, showcasing creative responses to data scarcity required in the absence of official statistics. Building statistical capacity and fostering data-sharing partnerships is essential for data-driven investment and policymaking in cybersecurity.

Furthermore, CCB should mirror public health principles, meaning interventions should be outcome-focused, contextual, and evidence-based. It presented two tools: the Internet Infrastructure Health Metrics Framework (IIHMF), which monitors digital infrastructure health on a weekly basis using technical indicators like misconfigured DNS resolvers, email practices and security protocol implementation; and the Cyber Belief Model (CBM), which recognizes that not all outcomes are technical by tracking behavioral change in risk awareness through indicators like adoption of multi-factor authentication and regularly updating devices. These tools help assess whether awareness and mitigation efforts are having real-world impact. However, large-scale, long-term outcomes remain difficult to measure over short timeframes

Across the discussion, concrete steps to foster a culture of results in cybersecurity capacity building emerged. Transparency and communication were emphasized as critical to making impact more visible, particularly through dashboards and transparent reporting. Incentivizing data use, linking funding to measurable results, and building national statistical capacity was considered key. Strengthening data-sharing partnerships and aligning around a shared set of core indicators measuring impact,

were all identified as necessary next steps. Cybersecurity policy must be grounded in data and aligned with the evolving threat landscape. Together, speakers underscored the need for data, investment, coordination, and shared accountability in driving effective outcomes.

Audience contributions emphasized the need for a global platform to harmonize and compare cybersecurity indicators. Panelists noted that raw incident numbers can be misleading without context, and that real progress lies in understanding behavior change and system-level outcomes. Transparency, public dashboards, and the use of metrics beyond training outputs were seen as vital for accountability and trust. There was broad agreement that while cybersecurity remains largely an art due to data limitations, transforming it into a science requires better data, structured collaboration, and shared commitment to evidence-based development. Overall, the discussion underscored the need for better metrics, more structured collaboration, and a shift toward treating cybersecurity as a public good.

Key Takeaways

Results-based cyber capacity building depends on **reliable, country-level cybersecurity statistics**, yet these remain scarce, inconsistent, and especially limited across the Global South.

To enable data-driven decisions and optimize investment impact, the community must prioritize the development of harmonized cyber indicators: rooted in **consensus-based definitions and supported by sectoral data partnerships**.

Building statistical and institutional capacity at the national level, alongside deeper collaboration with data-holding partners, is essential to ensure accountable, effective, and context-specific cyber development.

INTEGRATING DIGITAL RIGHTS, GENDER, AND INCLUSION IN CYBER CAPACITY BUILDING

Organized by Global Partners Digital and the Government of Mexico

Speakers

- **Moderator: Ms. Rose Payne,** Global Partners Digital (GPD)
- **Mr. Diego Sánchez-Moreno,** Ministry of Foreign Affairs of Mexico
- **Ms. Szilvia Toth,** Organization for Security and Co-operation in Europe, OSCE
- **Mr. Brett DeWitt,** Mastercard
- **Ms. Veronica Ferrari,** Association for Progressive Communications (APC)

Discussion

This session explored how to build inclusive and rights-based cyber capacities, which is essential to ensure no one is left behind in the digital age. A central message emerged early in the discussion: cyber capacity building must be **people-centered**, not solely focused on infrastructure or state capability. Cybersecurity strategies can be **more impactful when they systematically integrate human rights principles, gender mainstreaming, and intersectionality** into their policy design and implementation plans.

The discussion first focused on the importance of **designing practical tools and approaches** that integrate human rights, gender equality and inclusion. Women, LGBTQ+ individuals, and marginalized communities often experience cyber threats in unique ways that require tailored approaches. The Association for Progressive Communications (APC) developed a **gender-responsive cybersecurity policy framework** to support governments and institutions to ensure their responses are inclusive and sensitive to these varying experiences.

Furthermore, Mastercard emphasized the role of private actors in advancing practical, scalable solutions, particularly for small and medium-sized enterprises (SMEs)

in underserved markets. Several of their programs have developed **tools to help SMEs assess cyber risk, improve digital security and build resilience**. With nearly half of small businesses facing cyberattacks and one in five going bankrupt after such incidents, these accessible tools are crucial in addressing economic vulnerability and digital inequity.

Lessons from Mexico showcase that effective capacity building must also include **context-specific tools**, particularly for indigenous communities. This includes developing **cybersecurity awareness materials in native languages** and adapting methodologies to reflect local cultural, social, and linguistic realities. Such an approach is critical to making cyber capacity building inclusive in both intent and impact, ensuring digital rights are upheld even in remote or historically excluded regions.

The discussion then moved to **lessons and strategies for inclusive, equitable cyber cooperation**. At the heart of next-generation cyber cooperation lies the principle that capacity building must be systemic, participatory, and inclusive by design. Mastercard's work in emerging markets reflects this by coupling technical support with community-centered partnerships. Their initiatives are grounded in the belief that inclusion is not a corporate social responsibility checkbox, but a core ingredient of sustainable security and market stability.

From a regional and multilateral perspective, it was noted that the OSCE has integrated **gender-sensitive approaches into its work with national cybersecurity institutions**. For example, it brought practical experience by hosting workshops in Sarajevo and Astana. Participants from across Central Asia, the South Caucasus, and Mongolia **explored OSCE's 16 Cyber Confidence-Building Measures (CBMs) through a gender lens**. These sessions helped translate policy into practice, offering participants the tools to assess and reshape cybersecurity frameworks to better include and empower women.

Panelists further emphasized that inclusive **cyber cooperation must be embedded structurally and systemically**. It was noted that Mexico has advocated at the UN's Open-Ended Working Group (OEWG) for the inclusion of **human rights and non-state voices in cyber norms discussions**. The government has also supported the development of cyber norms that align with fundamental freedoms such as privacy and access to information. The OSCE further reiterated the importance of promoting confidence-building measures that reduce the risk of inter-state conflict in cyberspace. By examining CBMs through a gender lense, they make a deliberate effort to ensure these measures are not gender-blind, **surfacing the often invisible barriers that women and underrepresented groups face** in both cyber workforce development and diplomatic representation.

APC further supports this direction by championing **multi-stakeholder models for cyber governance**. They argue that inclusive cybersecurity must go beyond state actors and include civil society, academia, and grassroots voices in shaping policies. Their research demonstrates how policies that fail to recognize gendered dimensions of online threats, such as online harassment, doxxing, or digital exclusion, can

inadvertently reinforce existing inequalities.

It was reiterated that inclusion should be **both structural and intentional**. Mastercard described investing in local cyber champions, who are individuals involved in local communities that are equipped to lead digital security initiatives, with support from partners like the CyberPeace Institute and UNDP who help scale impact inclusively through public-private collaboration. These champions play an important role in raising awareness in populations disproportionately affected by scams and online fraud, such as women and the elderly. APC also highlighted that simply inviting diverse stakeholders to the table is not enough; inclusion is almost about ensuring those most affected can meaningfully influence solutions. Without addressing the intersectional impacts of cyber harm, cybersecurity efforts risk replicating the very inequalities they seek to address.

Key Takeaways

Design Context-Specific Tools to Support Inclusion and Digital Rights in CCB: Effective CCB must include the development of tools that are adapted to local realities, including those tailored to indigenous communities, developed in their native languages. This ensures that cybersecurity is accessible and meaningful to all populations, respecting cultural, linguistic, and social diversity.

Adopt a Human Rights-Centered Approach in CCB: A human rights approach ensures that cybersecurity is not treated as gender-neutral but acknowledges and addresses its disproportionate impacts, including on women and marginalized groups.

Integrate the Gender Dimension into Confidence-Building Measures (CBMs): Bringing a gender lens to CBMs not only strengthens inclusion but also enhances the overall understanding and design of these measures. Incorporating gender into CBMs is an effective way to ground these efforts in real-world situations, making them more impactful and relevant.

FOSTERING IMPACTFUL CROSS-REGIONAL CYBER CAPACITY BUILDING

Organized by the European Union (EU) and the Organization of American States (OAS)

Speakers

- **Moderator - Ms. Mariana Cadorna,** Organization of American States (OAS)
- **Mr. Abdul Hakeem Ajijola,** African Union
- **Mr. Hamilton Vagi,** Government of Papua New Guinea
- **Ms. Alison August Treppel,** Organization of American States (OAS)
- **Ms. Camille Lalevee,** European Commission (EC)

Discussion

The session explored **cross-regional strategies for advancing effective, sustainable, and inclusive cyber capacity building**. Panelists from Africa, Latin America, the Pacific, and Europe reflected on the shared challenges of fragmentation, duplication, and limited coordination among actors in the global cyber capacity building ecosystem.

It was emphasized that **stronger mutual understanding** between donors and implementers is essential to reduce fragmentation. The importance of coordination not only among implementation partners but also among donor institutions themselves was underscored. **Peer exchange mechanisms** such as CSIRT Week were mentioned as effective platforms for connecting technical experts with policymakers and facilitating knowledge transfer across regions. Furthermore, the European Commission's Digital for Africa programme was cited as a model that promotes more effective division of labour among actors. As part of the Global Gateway, such initiatives seek to **ensure sustainability beyond the funding period** through inclusive partnerships and local ownership.

Perspectives from the Pacific region highlighted shared challenges with the African region regarding duplication and fragmentation of efforts, noting that existing strategies in Africa, such as the Malawi Convention, are underused. It was proposed that **Clearing House mechanisms could streamline**

coordination and clarify roles across national, regional, and continental levels. In addition, shared curricula were identified as a means of ensuring consistency across countries and regions.

The value of **self-assessment tools**, such as those developed by the University of Oxford, were highlighted as driving countries to identify their own needs and progress on their own terms. **Progress does not mean full uniformity**; it should be coordinated and contextually appropriate. Regional frameworks were also presented as effective bridges to local practices, making high-level strategies more relevant on the ground.

There was caution against "**helicopter support models**" that overlook local contexts when delivering capacity building. The importance of using **existing regional instruments and developing operational curricula** tailored to local realities was underlined. For cyber resilience to be sustainable, it must be embedded into institutions and supported by local mentorship structures, as externally imposed models often fail because they lack contextual sensitivity.

Key Takeaways

Stronger coordination is crucial: Fragmentation and duplication remain prevalent across regions. Institutionalized coordination mechanisms are necessary to enhance efficiency and effectiveness.

Ownership and local adaptation drive sustainability: Successful cyber capacity building must be grounded in local realities, leveraging regional instruments and enabling capacity development within institutions.

Building trust and fostering multi-stakeholder collaboration: Trust between political and technical communities, and across public, private, and academic sectors, is essential. Peer learning mechanisms and regional leadership play a vital role in enabling inclusive, meaningful cooperation with support from international partners.

NOT ANOTHER WORKSHOP! THE MISSING POLICY PIECE TO TRANSFORM ACTIVITIES INTO CAPACITIES

Organized by the Forum of Incident Response and Security Teams (FIRST) & the Geneva Centre for Security Sector Governance (DCAF)

Speakers

- **Moderator – Ms. Franziska Klopfer,** DCAF - Geneva Centre for Security Sector Governance
- **Mr. Domingo Kabunare,** Digital Transformation Office, Kiribati Government
- **Ms. Zana Djurovic,** Psychologist and HR specialist
- **Mr. Klée Aiken,** FIRST
- **Ms. Martina Calleri,** Deutsche Gesellschaft für Internationale Zusammenarbeit (GiZ)

Discussion

The session opened with a recognition of the growing frustration around workshops and short-term training programs in cyber capacity building, particularly when these initiatives fail to deliver sustained and tangible outcomes. It focused on the importance of **understanding the political and institutional context**, as well as the need for **motivated individuals and local champions**, in ensuring that capacity building efforts lead to real, long-term outcomes.

In the Pacific, it was emphasized that even individuals who have access to high-quality trainings are often unable to apply their knowledge due to a **lack of institutional readiness**. There is a common disconnect between individual learning and systemic change, where institutions have not been restructured to accommodate or implement the new skills and knowledge gained. A call was made to rethink one-size-fits-all approaches and to prioritize targeted trainings towards individuals and organisations who are receptive to change.

Furthermore, the discussion emphasized the crucial role of **political will and community trust**

in sustaining cyber capacity building efforts. Policymakers often operate in silos, but real progress requires them to work closely with technical experts and local communities. An example from Tonga illustrated how political support can enable rapid progress. High-level commitment from the Prime Minister enabled the swift creation of a national CERT two months after a workshop with FIRST. This case demonstrated how political buy-in can unlock cross-sector collaboration, mobilize national resources, and generate momentum. The role of **community trust and locally embedded networks** was also emphasized, citing local communities such as Women in ICT Tonga, exemplifying how mentoring and shared purpose can support long-term resilience.

The discussion moved towards emphasizing the importance of **agility, local ownership and sustained application of knowledge**, particularly in volatile or rapidly changing environments. In the context of Ukraine, priorities shift rapidly, and staff are often too engaged in emergency response to attend formal training. Donors and implementing partners were urged to adopt flexible programming that responds in real time to evolving conditions, with efforts focusing not just on structure, but also on empowering local actors.

This intervention was echoed by another panelist who focused on the psychological dimensions of capacity building. She emphasized that while individual motivation is vital in achieving behavioural change, it is rarely enough. When training is not quickly followed by institutional support, **knowledge decay** sets in. Moreover, leadership changes, often result in rejection of prior efforts, making it difficult to build long-term capacity or maintain a development-oriented mindset.

Furthermore, a call was made for the development of **better Key Performance Indicators (KPIs) that go beyond short-term outputs**. It was proposed that donors and

practitioners adopt industry-agreed KPIs over a 10-year period, capable of measuring not only whether training was delivered, but whether it had a positive impact on people's lives. This would allow for a more accurate assessment of systemic and behavioural change.

The importance of **measuring trust-based networks and informal mentoring arrangements** was also discussed. Although difficult to quantify, these relationships often form the backbone of effective cyber capacity building. Suggestions included introducing train-the-trainer models through targeted ad hoc mentoring of officials in key roles within institutions, based on assessed needs. Lastly, embedding cybersecurity standards into policy and law can be effective, but often lags behind technological change. **Financial incentives** could be explored to encourage services that embed adaptability and flexibility.

Key Takeaways

Workshops must be embedded in context: The effectiveness of cyber capacity building depends not only on training quality but on the institutional, political, and cultural context into which they are delivered.

Trust and collaboration are critical: Sustainable change stems from building trusted relationships across stakeholders, between technical experts, policymakers, communities, and donors. Informal mentoring and local champions play an essential role.

Motivation must be supported by systems: Even highly motivated individuals cannot succeed without institutional backing, opportunities to apply new knowledge, and mechanisms that reward long-term impact.

Agility and local relevance matter: Programs must be adaptable to local contexts, especially in conflict-affected or rapidly changing environments. There is no one-size-fits-all solution.

Better metrics are needed: Existing KPIs often fall short. There is a need for more thoughtful, long-term indicators that measure systemic and behavioural change, not just training delivery.

PUBLIC-PRIVATE PARTNERSHIPS FOR CYBER RESILIENT SOCIETIES

Organized by the German Federal Foreign Office

Speakers

- **Moderator – Mr. Patryk Pawlak,** GC3B Program Advisor
- **Mr. Divine Selase Agbeti,** Cyber Security Authority (CSA), Ghana
- **Ms. Larissa Schneider Calza,** Ministry of Foreign Affairs of Brazil
- **Mr. Anton Demokhin,** Ministry of Foreign Affairs of Ukraine.
- **Mr. Bertie Kerr,** BAE Systems
- **Ms. Yvonne Nasshoven,** Federal Foreign Office, Germany
- **Mr. Simon Melchior,** Cyber Defense Africa

Discussion

The session opened by acknowledging the centrality of public-private partnerships (PPP) in cyber capacity building. Given the growing complexity of cyber threats and the dynamic nature of geopolitical and technological landscapes, the discussion focused on evolving **PPP models and how to structure them to drive scalable, sustainable cyber resilience**.

Effective PPPs must be grounded in inclusive policy-making. Brazil has advanced a multi-stakeholder model through its National Cybersecurity Council, which advises the presidency and includes representatives from government, academia, civil society, and the private sector. This model **fosters collaborative regulation**, where the private sector is not just consulted but often leads in calling for stronger standards, reiterating that inclusive dialogue increases buy-in and effectiveness. Moreover, Ghana's National Cybersecurity Strategy was emphasized as a strong foundation for public-private partnerships. By clearly defining the roles and responsibilities of all actors, the strategy fosters legal clarity, builds trust, and reduces the risk of misunderstandings.

This structured approach not only encourages collaboration but also enables financial incentives that attract private investment, ensuring partnerships align with national priorities and regulatory frameworks.

Shifting the conversation towards operational models of PPPs, Togo offered a compelling example of how PPPs can work effectively, even in resource-constrained settings. Through a co-investment model supported by a loan mechanism, Cyber Defence Africa helped establish a Security Operations Centre (SOC) – a critical capability for national cybersecurity. This initiative reflects a broader vision of cybersecurity not only as a public necessity, but as a viable market opportunity, too. This approach, which blends public investment with private sector expertise, illustrates how practical, sustainable cyber infrastructure can be built through strategic partnerships.

The importance of strategic alignment between public and private actors was also emphasized. While companies are increasingly willing to support national strategies, fragmented regulations and data protection laws can create legal and financial risks for multinational firms. Regulatory harmonization at the regional level was highlighted as a crucial enabler for cross-border collaboration. Nevertheless, it was noted that PPPs have evolved over time, as twenty years ago private sector involvement was minimal. As cyber threats multiplied, governments and businesses alike have recognized the need for deeper, more structured partnerships. Today, what is needed is a clearer articulation of roles and responsibilities as well as better incentives for investment, encouraging the private sector to engage meaningfully and sustainably in national and international cybersecurity efforts.

Ukraine's experience underscored the importance of resilient digital infrastructure in conflict contexts. Since 2014, and especially during active hostilities, Ukraine has relied heavily on private sector support to maintain operational continuity. Cyberattacks frequently preceded physical strikes, turning cybersecurity into a frontline defense. The Tallinn Mechanism emerged as a key tool for coordinating support between governments, donors, and private actors. It helps match Ukraine's needs with private sector capabilities, ensuring a timely and targeted response. The mechanism has become a strong model for global cybersecurity cooperation, which builds on PPPs. Focused on civilian infrastructure and EU-wide coordination, the mechanism drives innovation, sets standards, and aligns regional approaches. Germany also emphasized that cybersecurity is a

shared responsibility, as no one is safe unless everyone is. Institutionalizing the mechanism ensures there is a ripple effect of strengthened global resilience.

Furthermore, legal and institutional frameworks must be both adaptable yet protective. Some shared how initial focus on operational capacity (SOC) sometimes preceded legal structure or suggested the use of performance indicators and donor coordination to align PPP efforts more closely with measurable outcomes. States highlighted their efforts to partner with international firms in navigating complex legal contexts. A three-layer approach to effective PPP development was proposed by Germany, where a) funding mechanisms are accessible and responsive; b) stakeholder environments are mapped for legal flexibility; and c) continuous dialogue is needed to match capabilities with evolving legal contexts.

Ukraine stressed the importance of digital sovereignty, aiming to build internal capacities while still benefiting from private sector expertise. Ghana reaffirmed that effective partnerships at both the national and international level, enable real progress.

Key Takeaways

PPPs are essential but evolving: Cybersecurity threats have made PPPs a necessity rather than a choice. Stakeholders must continuously redefine their roles, expectations, and contributions.

Regulatory clarity and trust matter: Clear frameworks that establish roles, legal certainty, and financial incentives are fundamental to successful and scalable partnerships.

Coordination mechanisms like the Tallinn model are effective: Structured platforms that align private sector resources with national needs offer a replicable model for crisis and long-term resilience.

BUILDING LOCAL CYBER INDUSTRY ECOSYSTEMS: LESSONS AND GOOD PRACTICES

Organized by CREST International

Speakers

- **Moderator – Ms. Joyce Hakmeh,** Chatham House
- **Mr. Nick Benson,** CREST International
- **Mr. Divine Agbeti,** Cyber Security Authority
- **Mr. James Kimuyu,** National Computer and Cybercrimes Coordination Committee of Kenya
- **Mr. Ewan Smith,** UK Foreign, Commonwealth & Development Office
- **Ms. Zoja Antuchevič,** Solutions Lab
- **Mr. Abdallah Toutoungi,** Cyber Shield Ghana

This session explored CREST Camp, a program designed to accelerate the development of local cybersecurity industries by pairing emerging companies with seasoned international providers. The idea was born out of a challenge: traditional models only worked for the most mature ecosystems, leaving many nations struggling to build foundational capabilities.

CREST International shared how the concept was first shaped in Accra, aiming to bridge the gap by fostering mentorship and collaboration. The UK's Foreign Commonwealth Office emphasized the program's cost-efficiency and strategic value, advocating for sustainable investment in local expertise.

National authorities from the African continent showcased how CREST Camp aligned with their cybersecurity strategies. Ghana used it to strengthen its regulatory framework and protect critical infrastructure, while Kenya saw it as a way to close the skills gap and enhance threat response capabilities.

The private sector described the program as a transformative "boot

camp" that built trust and credibility. A camp mentor further highlighted the importance of ethical community building and knowledge sharing, stressing that sustainability comes from collaboration, not competition.

The program's structure was built on voluntary participation, multi-stakeholder engagement, and rigorous self-assessment. With mentoring support and a focus on local capability, companies could reduce their readiness timeline from years to months. Over 10% of CREST's member companies volunteered as mentors, targeting middle-tier firms ready to grow.

Working groups tackled key challenges like brain drain, resource constraints, and scalability. They recommended starting small, fostering genuine partnerships, and embedding long-term planning. The emphasis was on building trust, sharing knowledge, and maintaining high professional standards.

As one participant put it: "Maturity is not a destination, it's a journey."

CREST Camp is paving that journey: one partnership, one country, one company at a time.

LEVERAGING NETWORK EFFECTS: INFORMATION AND THREAT INTELLIGENCE SHARING FOR CYBER CAPACITY BUILDING

Organized by CI-ISAC International, ECOWAS, Global Humanitarian ISAC, Shadowserver Foundation

Speakers

- **Moderator – Ms. Anastasiya Kazakova,** DiploFoundation
- **Mr. Tob Eberle,** The Shadowserver Foundation
- **Ms. Folake Olagunju,** Economic Community of West African States (ECOWAS)
- **Mr. Scott Flower,** CI-ISAC International
- **Mr. Nino Hares,** NetHope

Discussion

The session explored the vital role of **Information Sharing and Analysis Centers (ISACs)** and similar cooperative platforms in enhancing global cyber resilience. As cyber threats grow more sophisticated and interconnected, particularly due to supply chain dependencies and shifting geopolitical dynamics, timely, trusted, and actionable information exchange becomes an indispensable element of **collective cybersecurity**. The discussion underscored how ISACs are instrumental not only in enabling early warning and coordinated response, but also in **fostering trust across sectors and regions**, especially where infrastructure is privately owned and threat intelligence tends to be fragmented.

The conversation began by examining the evolution of ISACs and their function as trusted communities for the exchange of threat intelligence. One example highlighted the importance of secure channels for cross-sector collaboration, noting that sector-specific models are increasingly insufficient given the complexity of contemporary cyber risks. In this context, it was noted that trust must be built not just between individuals, but between institutions, and that

achieving this requires more than technical infrastructure: it demands governance models, anonymization techniques, and shared expectations.

The discussion then turned to challenges and innovations in the non-profit sector. A prominent initiative was the creation of **an ISAC dedicated specifically to non-governmental organizations and humanitarian actors**. Given that cybersecurity threats to NGOs often go underreported and uncoordinated, this ISAC creates a space for these groups to pool resources and threat intelligence while maintaining mission integrity. By integrating shared knowledge into operational environments and tailoring alerts to specific organizational contexts, this approach enhances not only cyber defence but also operational continuity for actors serving vulnerable populations.

Another example emphasized **the global reach and technical depth** required to make threat intelligence accessible to all. One foundation offers free, subscription-based data feeds that include reports of compromised systems, indicators of compromise, and known vulnerabilities. These are made available to hundreds of national and sectoral CERTs around the

world. Their open-data philosophy ensures that even organizations with limited technical or financial resources can benefit from world-class threat intelligence. The model also **empowers proactive action** by equipping teams with the tools and context needed to identify and address risks before they escalate.

In West Africa, efforts to strengthen regional information-sharing mechanisms face distinct institutional and political challenges. Frequent turnover among **cybersecurity personnel, inconsistent prioritization by governments, and a general culture of denial** around cyber incidents all complicate efforts to create sustainable sharing frameworks. Despite these barriers, efforts are underway to define data classification protocols and response mechanisms. Building trust among stakeholders remains a core challenge: one that requires not only technical solutions but cultural change, political will, and clear follow-through procedures.

Throughout the session, the need for **sustainable, context-sensitive, and cost-effective information-sharing models** was a recurring theme. It was acknowledged that in many developing regions, regulatory constraints, lack of technical infrastructure, and funding gaps limit the effectiveness of traditional ISAC models. Therefore, scalable alternatives must be adapted to local capacity while maintaining alignment with global norms.

The importance of **appropriate legal and governance frameworks** was also raised. Without these, information sharing remains fragmented and occasionally inhibited by fears of legal liability or reputational harm. One solution proposed was the broader use of non-disclosure agreements, coupled with anonymization technologies and standardized taxonomies to ensure consistent interpretation of cyber threat data. However, speakers cautioned that overly stringent or poorly harmonized regulatory environments could suppress cooperation rather than foster it.

Several interventions reinforced that the success of ISACs hinges on their ability to foster a sense of shared purpose. This requires an understanding that not all value comes from rapid data exchange as some of the most effective results arise from **relationship-building, co-investment in shared tools, and alignment of threat reporting standards** across sectors. Informal communities and mentoring networks were also acknowledged as vital complements to formal structures, particularly where trust in institutions remains limited.

The session closed with a reminder that collective cybersecurity depends on inclusion. Whether it be non-profit actors, under-resourced governments, or small and medium-sized enterprises, all stakeholders benefit from, and must be included in, the development of resilient information-sharing ecosystems.

Free and open access to cyber threat intelligence, paired with pragmatic governance and long-term investment, is **not a luxury but a necessity in today's interconnected threat landscape**.

Key Takeaways

Collaborative approach is fundamental: Effective cybersecurity relies on cooperation among diverse sectors, including public, private, non-profit, and regional actors.

Trust is essential: Institutional trust, reinforced by technology and governance, underpins all successful information sharing practices.

Tailored and sustainable models are needed: ISACs must be context-specific and financially viable, especially in developing and resource-constrained environments.

Political will and governance matter: Clear governance frameworks and sustained political commitment are essential for enabling actionable, cross-sector collaboration.

Accessibility of intelligence empowers all: Free and low-cost access to high-quality threat intelligence strengthens cyber readiness for organizations of all sizes and mandates.

CLOSING THE CYBER TALENT GAP: THE ROLE OF PUBLIC-PRIVATE PARTNERSHIPS IN THE GLOBAL SOUTH

Organized by the World Economic Forum

Speakers

- **Moderator – Mr. Akshay Joshi,** World Economic Forum (WEF)
- **Eng. Abdulrahman Al Hassan,** Global Cybersecurity Forum (GCF)
- **Ms. Thelma Quaye,** Smart Africa Secretariat
- **Mr. Rob Rashotte,** Fortinet
- **Ms. Jacky Fox,** Accenture Ireland

Discussion

As cyber threats escalate in complexity and global reach, the shortage of qualified cybersecurity professionals poses a significant risk to both digital security and economic development. This session convened voices from international organizations, regional alliances, and the private sector to examine how public-private partnerships (PPPs) can address the global cyber workforce shortage - currently estimated to range from 2.8 to 4.8 million professionals worldwide. The discussion highlighted the **importance of national coordination, inclusive hiring practices, and long-term, locally embedded strategies** that support skill development across diverse contexts.

The session opened with a global framing of the challenge. It was noted that the cybersecurity talent shortage should not be viewed merely as a human resources issue but as a **pressing strategic vulnerability**. Without the workforce necessary to secure digital infrastructure and respond to evolving threats, even the most advanced policy frameworks or technologies fall short. In response to this, several organizations have begun to develop new strategies and tools to reshape how talent is recruited, trained, and retained.

A recent framework developed by a global multi-stakeholder initiative proposes four pillars to address the gap: **attracting new talent, increasing awareness of cybersecurity career pathways,**

scaling training efforts, and embedding inclusion in recruitment and hiring. This model aims to offer a systemic approach, moving beyond ad hoc skilling programs to build long-term, results-driven ecosystems. A complementary white paper released in parallel identifies three preconditions for successful PPPs: inclusive stakeholder engagement, measurable impact metrics, and shared project governance. Together, these efforts underline the need for deliberate, coordinated action to transform talent pipelines.

From a national policy perspective, experiences shared from the Middle East emphasized the critical role of central governance structures in managing cyber talent strategies. Standalone efforts by government or private actors, while valuable, are insufficient to address the scale and urgency of the shortage. National cybersecurity frameworks must incorporate **centralized oversight, policy coherence, and defined standards for training and certification**. A recent workforce report shows that 43% of global employers prioritize certification in hiring, pointing to the importance of harmonized and recognized benchmarks.

In response, new multi-stakeholder initiatives have emerged that align national priorities with international cooperation. One such program, developed in partnership with the private sector and academic institutions, is rolling out scalable, long-term cybersecurity training. Parallel efforts to advance cyber workforce economics, such as the **co-creation of a Center for Cyber Economics**, seek to generate evidence-based insights that guide investment and capacity planning.

Regional perspectives from Africa further highlighted the challenges of **institutional fragmentation and limited political prioritization of cybersecurity**. In many contexts, cybersecurity remains framed as a purely technical issue, siloed from broader digital transformation or economic policy agendas. Only a minority of countries across the region have dedicated cybersecurity agencies, limiting the visibility and coordination needed to attract and sustain private sector engagement.

To address this, stakeholders are advocating for a "**cybersecurity by design**" approach, where security considerations are integrated from the outset into all digital development strategies. This shift requires elevating cybersecurity to a political priority, on par with digital inclusion or economic competitiveness. Without policy

clarity, national coordination, and a clear talent pipeline, the private sector is unlikely to make long-term training investments. However, where governments demonstrate commitment through coherent strategies and regulatory frameworks, public-private cooperation becomes not only possible but productive.

Throughout the discussion, it was acknowledged that **the workforce gap cannot be closed through short-term skilling alone**. Instead, systemic change is needed: national frameworks that link cybersecurity to broader development goals, inclusive hiring practices that expand the talent pool, and cross-border cooperation that enables knowledge sharing. The cyber workforce of the future must be diverse, agile, and embedded in national and regional digital ecosystems. In this context, PPPs are not simply a means of implementation: they are core to defining the cyber resilience agenda itself.

Key Takeaways

Partnerships are no longer optional: Governments and the private sector must co-create long-term, inclusive training ecosystems to close the cyber workforce gap - an urgent issue for both economic development and national security.

Governance enables sustainability: Effective strategies depend on national coordination, measurable standards, and cross-sector alignment. Fragmentation and duplication must be avoided through shared planning and oversight.

Cybersecurity must be politically prioritized: Integrating cybersecurity into national development agendas signals commitment and creates the enabling environment necessary for investment in skills and institutional resilience.

CYBERSECURITY FOR CITIES: NAVIGATING THE CHALLENGES OF URBANIZATION AND TECHNOLOGICAL TRANSFORMATION

Organized by the World Bank

Speakers

- **Moderator – Mr. Hagai Mei-Zahav,** World Bank
- **Mr. Alessandro Ortalda,** Expire Strategy & Advisory
- **Ms. Jessica Carolina Grisanti Bravo,** World Bank
- **Mr. Matheus Oggioni Lima Beninca,** State of Espirito Santo, Brazil
- **Mr. Rafal Rohonzinski,** SecDev
- **Mr. Ishan Khokar,** World Bank

Discussion

As urbanization accelerates and digital transformation reshapes how cities function, cybersecurity is becoming an indispensable element of urban resilience and public governance. While national strategies have traditionally dominated the cybersecurity landscape, this session emphasized that cities now stand at the forefront of both vulnerability and opportunity. Their growing dependence on digitally integrated infrastructure, ranging from public transportation to utilities and citizen services, demands **tailored, localized cybersecurity responses** that go beyond national oversight.

Representatives from Brazil, Japan, and Canada illustrated how city governments are beginning to internalize this shift. In Brazil's Espirito Santo state, the development of a **centralized government data center** was framed not only as a technological upgrade but as a resilience measure to safeguard critical services against disruption. The project set an example for how subnational actors can design forward-looking digital infrastructure while embedding

cyber resilience into administrative routines.

Japan's experience reflected a long-standing commitment to human-centered smart city development. Drawing on lessons from preparations for the 2021 Olympic Games, the **national cybersecurity strategy emphasized the role of cities** as active nodes in the digital security ecosystem. Investments in cyber risk identification, scalable technological solutions, and institutional coordination were presented as key enablers for integrating cybersecurity into long-term urban planning, particularly in ecological and disaster-prone areas where the resilience of digital systems intersects with broader safety and development goals.

Meanwhile, Canadian insights drew attention to the funding and human resource constraints that often hinder municipal cybersecurity. Cities like Ottawa face challenges in recruiting and retaining qualified professionals, especially given global competition for cybersecurity talent and the absence of stable budget lines for long-term investments. Despite housing the majority of global population and GDP, many cities lack dedicated strategies or technical expertise to address growing cyber risks. **Public-private partnerships and practical toolkits** were identified as essential mechanisms to support local governments, both in terms of expertise and resourcing.

Across all regions, the session identified a **clear gap between digital ambition and cybersecurity preparedness** at the municipal level. Cities are increasingly digitized but often under-prepared, particularly when it comes to assessing cyber maturity, planning strategic investments, or aligning with national cybersecurity frameworks. The complexity of urban infrastructure, characterized by cyber-physical systems, legacy technologies, and fragmented service delivery, compounds these challenges.

To close this gap, participants advocated for several actionable measures. Municipalities need **localized maturity assessments, capacity-building tools tailored to urban settings, and frameworks that integrate cybersecurity** from the inception of any smart city initiative. Embedding cybersecurity into critical sectors such as energy, transport, and healthcare must become standard practice. Importantly, cybersecurity needs to be communicated in human terms, not merely as a technical risk but as a matter of **public safety, trust, and daily service continuity**. Framing cybersecurity in this way can help local leaders secure political support and citizen engagement.

Ultimately, the session underscored the need for a more intentional alignment between city-level innovation and national cybersecurity priorities. As digital infrastructure becomes more distributed, the role of municipalities in global cyber resilience will only grow. Without a strategic shift in resources, coordination, and framing, **cities risk becoming the weakest link** in national cybersecurity ecosystems, even as they drive much of the world's digital and economic progress.

Key Takeaways

Cities Are the Frontlines of Cybersecurity: Urban areas are central to global economic and social life yet remain under-prioritized in cybersecurity planning despite their increasing reliance on complex digital systems.

Local Governments Face Unique Capacity Gaps: Municipalities often lack stable funding, planning tools, and cyber talent, making public-private partnerships and practical guidance essential.

Cyber Resilience Is Core to Sustainable Urban Development: Resilience must include cybersecurity from the outset, on equal footing with infrastructure, climate adaptation, and public health.

Human-Centered Framing Improves Engagement: Communicating cybersecurity as a citizen issue, linked to services, trust, and safety, can increase local buy-in and political prioritization.

Strategic Alignment Is Essential: Urban cybersecurity must align with national and regional strategies to avoid fragmentation and ensure effective coordination of resources and responsibilities.

PILLAR: ANTICIPATE

BUILDING CAPACITIES TO AVERT NEW TECHNOLOGY DIVIDES

Organized by the United Nations Institute for Disarmament Research (UNIDIR)

Speakers

- **Moderator – Ms. Andrea Gronke,** UNIDIR
- **Ms. Thelma Quaye,** Smart Africa
- **Ms. Larisa Galadza,** Global Affairs Canada (GAC)
- **Mr. Haider Pasha,** Palo Alto Networks
- **Ms. Lauren Conroy,** IBM

Discussion

As the global uptake of artificial intelligence (AI), quantum computing, blockchain, and virtual environments accelerates, the session examined how cyber capacity building must evolve to ensure these technologies are both inclusive and secure. Rather than framing the issue as one of technological deficit in the Global South, speakers emphasized the need to recalibrate cooperation models, placing local leadership, inclusive innovation, and fit-for-purpose strategies at the center of future efforts. The session brought together diverse voices from governments, regional organizations, and the private sector to explore what inclusive and sustainable cyber capacity building should look like in the face of technological transformation.

The discussion began with a reframing of traditional models of capacity building. Canada emphasized the shift in global discourse, **from capacity building to capacity enhancement**, particularly within G7 circles. This shift

acknowledges that many countries already possess foundational digital infrastructure and technical know-how; the challenge now lies in strengthening and scaling those ecosystems in ways that are self-directed and sustainable. In the field of AI, for example, Canada's approach focuses on supporting local talent pipelines and innovation ecosystems in the African and Indo-Pacific regions, moving away from dependency models in favor of equitable partnerships.

A central example cited was the **Tallinn Mechanism**, implemented in support of Ukraine. This mechanism allowed the Ukrainian government to **lead its own cybersecurity needs assessment**, map out national priorities, including emerging technology threats, and match those priorities with targeted donor support. The demand-driven nature of the model enabled alignment between what the country needed and what partners could offer, creating a replicable model for countries navigating complex cybersecurity challenges stemming from new technologies. Panelists noted that this mechanism offers a practical framework for integrating donor contributions into national strategies while preserving local agency and accountability.

Turning to the African context, perspectives from regional organizations stressed that **equitable access to emerging technologies remains constrained by structural barriers**, particularly disparities in digital infrastructure, affordability, and policy readiness. While mobile network coverage has expanded to reach around 85% of Africa's population, actual usage of internet-enabled services remains disproportionately low. Factors such as the cost of data, limited access to devices, and gaps in digital literacy inhibit meaningful participation in digital transformation. As a result, the benefits of AI or blockchain-based services remain largely out of reach for many.

In response, **public-private partnerships were presented as a vital pathway to accelerate access and bridge the infrastructure divide**. Governments were encouraged to focus on enabling environments, through policy clarity, spectrum

regulation, and digital inclusion strategies, while the private sector is best placed to drive scalable training, localized innovation, and affordability initiatives. In this model, governments act as conveners and enablers rather than direct service providers, facilitating investments that respond to real user needs.

The conversation also addressed the **persistent cybersecurity talent gap**, which continues to undermine progress in both the public and private sectors. Participants noted that despite significant investment in training programs globally, the gap between skills supply and demand continues to grow. Three main reasons were identified: training often does not reflect actual job roles in cybersecurity; human resources departments struggle to assess technical skills effectively; and potential professionals frequently lack visibility into clear career pathways. Without correcting these mismatches, talent development programs risk measuring success by the number of training sessions delivered rather than by employment outcomes or resilience metrics.

Efforts to address this disconnect were illustrated through initiatives at regional innovation centres, such as the **Smart Africa Cybersecurity Innovation Centre**, which integrates mentorship, market access, and demand-side coordination to align training with industry needs. Speakers underscored that building cybersecurity capacity requires more than delivering courses; it demands the creation of pipelines, role models, and employment ecosystems that link talent to long-term opportunities. This requires coordination between ministries of education, industry bodies, and private employers, supported by donor frameworks that prioritize job creation over training outputs.

Discussions on **AI** emphasized the dual role of the technology in cybersecurity: both **as a threat vector and as a capacity multiplier**. AI systems were not originally designed with security in mind, making them vulnerable to misuse. Yet when responsibly integrated, AI can strengthen cyber capacity building by supporting **Security Operations Centers (SOCs)**, automating repetitive tasks, and enabling more efficient threat detection and response. To realize this potential, cybersecurity must be embedded by design, from procurement processes to policy frameworks.

Examples from the Middle East highlighted successful localization of cybersecurity frameworks. The UAE was cited as a positive case where national cybersecurity policy had been adapted to reflect local risk profiles and cultural considerations, rather than applying generic global standards. This adaptability was seen as essential in emerging technology governance, particularly in sensitive sectors such as healthcare, financial services, and critical infrastructure, where trust and context are paramount.
The private sector further emphasized the need for **transparency, ethical governance, and inclusive design** in emerging technology deployment. Trust was repeatedly cited as a prerequisite for both technology adoption and effective capacity building. This includes transparency around data handling, open dialogue with civil society, and clear standards for accountability in AI systems.

In discussing quantum computing, panelists warned that current encryption protocols are likely to

be compromised within the next few years as quantum capabilities mature. Organizations and governments were urged to begin post-quantum readiness activities now, mapping their cryptographic assets, identifying vulnerabilities, and planning for phased upgrades to quantum-resilient standards. Delaying this process could leave sensitive data exposed for decades to come.

The conversation closed with reflections on measurement and impact. Defining success in cybersecurity capacity building remains challenging, as progress often looks like the absence of failure. Speakers agreed that traditional development metrics may not adequately capture resilience or institutional change. Instead, programs should co-develop benchmarks with beneficiaries and donors from the outset, defining what success looks like in that context, whether improved coordination, employment outcomes, or reduced attack surface. Only then can meaningful monitoring and evaluation systems be designed.

Key Takeaways

Partnerships Must Center on Beneficiary Needs and Enable Capacity Transfer: Effective collaboration must reflect the priorities of local actors and aim to build autonomous ecosystems, not prolonged dependency.

Local-Led Talent Mapping and Donor Alignment as a Model for Cyber Workforce Development: Ukraine's experience shows how national needs assessments can effectively guide international support through mechanisms like Tallinn.

Emerging Technologies Should Be Integrated into Capacity Building: AI and other tools offer opportunities to improve cyber operations and should be treated as enablers, not obstacles.

Quantum Threats Require Urgent Preparedness: The post-quantum era is imminent; proactive asset mapping and transition planning must begin immediately.

Define Success Together and Early: Impact must be measured against shared and locally meaningful benchmarks, not just training statistics or donor outputs.

CYBER RESILIENCE IN THE AGE OF AI

Organized by Microsoft

Speakers

- **Moderator – Dr. Robin Geiss,** United Nations Institute for Disarmament Research
- **Mr. Nemanja Malisevic,** Microsoft
- **Mr. Hadi Anwar,** CPX
- **Dr. James J Kimuyu,** NC4 Kenya
- **Ms. Mariana Cardona,** Cybersecurity Program Officer, Organization of American States

Discussion

The session explored the rapidly evolving relationship between artificial intelligence (AI) and cybersecurity, **recognizing AI as a transformative force**. As AI capabilities become more accessible and integrated into our daily lives, understanding what the AI revolution means for cyber capacity building efforts and how it can make these more effective and sustainable becomes imperative. The discussions also underscored how to **build partnerships between the Global North and Global South** to ensure AI systems and services meet the specific needs of Global Majority countries.

Panelists underscored that AI is no longer a "nice to have" but a fundamental element of modern cybersecurity ecosystems. AI agents are deployed to **reinforce resilience, improving risk assessment, incident detection, and threat intelligence**. Examples from across regions highlighted how AI is already being deployed to strengthen national and institutional cyber defence. In several countries, AI agents are assisting in the real-time assessment of risk and aggregation of threat intelligence, which is then used to inform both public and private sector responses. In contexts with limited cybersecurity resources, such as parts of Latin America, AI is also being applied to filter and triage threat reports, helping national CERTs manage information flows and increase responsiveness.

At the same time, it was acknowledged that AI intensifies existing challenges. AI can serve

as both “blessing and curse”, enhancing security capabilities but also enabling attackers to scale operations with greater speed and precision. With AI now embedded in the cloud layer, questions around data sovereignty, ethics, and shared infrastructure are becoming more pressing. Speakers emphasized that **data fed into AI systems often has a sovereign character**, requiring strong protection measures and clearly defined governance frameworks. Ongoing collaboration between states, industry actors, and cloud providers was seen as vital to **ensuring data integrity across jurisdictions**.

The discussion also returned to the cyber workforce gap, with AI presented as a potential solution to alleviate some of the pressure. Participants noted that AI can assist with burnout, support under-resourced teams, and enable faster analysis of complex threat environments. However, this promise depends on foundational investments in infrastructure, trusted digital ecosystems, and human capital. **Training and continuous upskilling** were repeatedly described as essential, not only to harness AI effectively, but to reduce misconfigurations, which remain one of the top cybersecurity vulnerabilities worldwide.

Comparisons were drawn to military training strategies: capacity building must be continuous, realistic, and resistant to budget cuts. Yet many countries still struggle to align cybersecurity training with real-world job roles or to provide clear entry points into the field. While various programs have emerged to train youth and underrepresented groups, there was a strong call to connect training to employment pathways, ensuring that cyber capacity building does not stop at awareness, but translates into measurable job placement and institutional readiness.

The conversation also turned to the risks of bias and discrimination embedded in AI systems. Participants stressed that **early language models reflected deep cultural and linguistic inequities**, and that future systems must do better. Examples were shared of efforts to develop AI tools tailored to users of underrepresented languages such as Arabic and Hindi, as part of broader commitments to inclusive innovation. There was agreement that AI governance frameworks must guide both the development and use of AI technologies, grounded in ethical principles and inclusive access.

Finally, the link between AI and cloud infrastructure was revisited. While some called for greater sovereignty in AI systems, others noted that the full functionality of AI depends on integration with cloud

environments. There was recognition that with the right safeguards in place, **shared infrastructure and trusted partnerships can provide the scalability and resilience** needed to meet evolving threats. Still, capacity building efforts must remain alert to uneven access, resource limitations, and the risk of dependency, especially in lower-resourced contexts.

Key Takeaways

AI strengthens cyber resilience but also scales threats, requiring **robust governance**.

Inclusive, ethical frameworks are needed to **address bias and ensure equitable access**.

Despite technological advances, **human error and misconfiguration remain significant vulnerabilities**, underscoring the need for continuous cyber capacity building and training.

NAVIGATING TECHNOLOGY CHOICES FOR CYBER INCIDENT RESPONSE

Organized by NRD Cyber Security & International Telecommunication Union (ITU)

Speakers

- **Moderator – Mr. Vilius Benetis,** NRD Cyber Security
- **Mr. Orhan Osmani,** International Telecommunication Union
- **Mr. Bader Al-Sada, Cyber Threat Department,** Qatar
- **Mr. Ghislain de Salins, Global Lead for Cybersecurity,** World Bank
- **Mr. Matt Palmer, Director,** Jersey Cyber Security Centre

Discussion

The session addressed the growing complexity faced by national cybersecurity teams, particularly CERTs and SOCs, as they navigate a landscape crowded with open-source and commercial tools. It explored how national teams with differing levels of maturity and resources can make strategic, sustainable technology choices that align with their operational needs and broader institutional readiness. The conversation emphasized that the success of cyber incident response hinges less on the availability of tools and more on **clear objectives, strategic planning, and sustained capacity building**.

Participants acknowledged the appeal of automation and artificial intelligence (AI) in enhancing incident response but cautioned against seeing such tools as silver bullets. While open-source tools offer important opportunities for customization and accessibility, they also raise concerns around data sensitivity, integration complexity, and operational security. Several panelists stressed the importance of **establishing a clear national strategy and legal framework** before adopting technologies, particularly in contexts where staff capacity and financial resources are limited.

Lessons were drawn from practical experiences. In Botswana, for example, CERT development was guided by technical assistance and a progressive, needs-driven implementation model supported

by international partners. Rather than attempting to build everything at once, national efforts began with foundational assessments, followed by the gradual layering of services and tools. This step-by-step approach was seen as essential for ensuring that national teams are equipped not just with technologies, but with the **human and institutional capacity to use them effectively**.

Poll responses from the session revealed that the most important factors influencing technology adoption include **cost, local requirements, and peer recommendations**. However, panelists noted that challenges persist with limited budgets, integration difficulties, and insufficient staffing continue to hinder progress in many countries. Importantly, decision-makers often prioritize brand recognition or hype over long-term suitability and sustainability.

To address these gaps, organizations such as the World Bank and ITU are working with governments to develop tailored roadmaps for CERT establishment, build capacity through training programs, and provide access to practical guidance. The **World Bank's Cyber Academy** was cited as one such initiative aimed at cultivating long-term communities of practice in cyber capacity building. At the same time, speakers cautioned that growing costs associated with international engagement, such as conferences and memberships, risk excluding countries most in need of support. There was a strong call

to reduce duplication, promote resource sharing, and ensure that collaboration mechanisms remain inclusive and accessible.

The discussion also touched on the risks of misuse associated with the same technologies that promise to improve resilience. As malicious actors adopt AI and other advanced tools, national teams must remain **proactive and anticipate future threats**. Several speakers underscored that without ongoing training and a culture of continuous learning, even well-resourced teams will struggle to keep pace.

Ultimately, the session reinforced a clear message: tools alone do not drive impact. Success in cyber incident response requires a **deliberate and strategic approach**, grounded in local realities and bolstered by sustained investment in human capacity and community collaboration.

Key Takeaways

Strategic planning, not tools alone, determines the success of incident response; **readiness assessments and clear national objectives** must guide technology adoption.

A hybrid approach using both open-source and commercial tools is common, but **decisions must account for data sensitivity, integration complexity, and sustainability**.

Community-building, inclusive collaboration, and continuous capacity development are essential to ensuring that tools enhance rather than overwhelm national CERTs and SOCs.

ADAPTING CAPACITIES OF CYBERCRIME FIGHTERS TO NEW TECH CHALLENGES

Organized by Council of Europe & INTERPOL

Speakers

- **Moderator - Mo Dong Uk Kim,** Specialized Officer, Cybercrime Directorate, INTERPOL Global Complex for Innovation
- **Ms. Tatiana Cesario,** Assistant Prosecutor, Public Ministry, Paraguay
- **Ms. Thokozani Chimbe,** Director of Legal Services, Malawi Communications Regulatory Authority (MACRA), Malawi
- **Mr. Enrique Hernandez Gonzalez,** Assistant Director, Cyber Operations, INTERPOL
- **Mr. Virgil Spiridon,** Head of Operations, Cybercrime Programme Office, Council of Europe

Discussion

This session examined **the complex challenge of building future-proof cyber capacity in an environment where criminals are quick to exploit emerging technologies** such as blockchain, cloud computing, and artificial intelligence. Criminal justice and law enforcement authorities, partners, and donors are under increasing pressure to design programs that are effective amidst the rapid technological change we are experiencing. The challenge is especially acute for countries and organizations with limited resources, since research, innovation, and the development of tools that can support the work of law enforcement are often concentrated in wealthier ecosystems. As these complexities contribute to widening the cyber capability gap, it is essential to assess which strategies demonstrably produce outcomes that are adaptive to these technological changes and contribute to a safer cyberspace.

A key theme running through the discussions was the importance of moving beyond traditional training

approaches and exploring models of capacity building that are adaptable, inclusive, and sustainable. The panelists highlighted the need for **complementary and non-traditional strategies** that empower local practitioners to take ownership of innovation within their organizations and ecosystems. Building resilience requires programs that are both fit-for-purpose and fit-for-future. This means having from the outset the strategic vision for flexible-by-design capacity building that allows for smart evolution, in line with technological shifts while grounded in local realities.

To deliver on this, several aspects and approaches were emphasized. First, the development of **tech-neutral international legal standards and guidelines** is vital. By focusing on legislation and policies that are not tied to specific technologies, countries can establish frameworks that remain relevant as technology changes. The Budapest Convention on Cybercrime was highlighted as an excellent example of this, considering it has stood the test relevance for two decades due it its tech-neutral language while it is complemented by guidance notes that allow practitioners understand and apply its provisions within the technological context they operate in.

Moreover, **learning through self-codification** of international good practices and standards in the local context and systems was stressed as a powerful way for practitioners to internalize knowledge, institutionalize best practices and ensure the capacity building process is locally-led. Panelists noted that true change comes from within, and internal generation of knowledge and skills is a key strategy in ensuring the sustainability of local expertise. The question of tools and equipment was also a central one in the discussion. Building **vendor-neutral skills** in areas such as digital forensics, blockchain analysis, OSINT, and AI is a must for to equip practitioners with capabilities that are widely applicable and less dependent on proprietary tools. Finally, fostering **capacity through systematic public-private collaboration** between law enforcement and industry was stressed as a way to create synergies, build expertise, and accelerate innovation.

Building on these principles, several practical recommendations emerged. **Public-private partnerships** can provide law

enforcement with access to cutting-edge expertise, tools, and real-time threat intelligence. **Open-source and shared tools** lower costs and enable local adaptation, ensuring that innovation is not limited to resource-rich contexts. **Peer-to-peer learning models** allow practitioners to exchange practical knowledge across borders, building networks of resilience. Programs should also **embed flexibility** so that training content and curricula can evolve alongside emerging technologies. Finally, supporting **local innovation hubs** was highlighted as a way to empower practitioners to develop context-specific solutions that meet their own unique challenges.

The session concluded that future-ready capacity building must combine legal, technical, and institutional dimensions. It should not only transfer knowledge but also foster environments where criminal justice practitioners are not merely recipients of knowledge, but can grow as leaders of change and innovation.

Key Takeaways

Promote public-private partnerships to harness expertise and real-time insights from industry.

Invest in open-source and shared tools that reduce costs and enable local adaptation.

Adopt peer-to-peer learning models to encourage cross-border exchange of practical solutions.

Embed flexibility in training programs so that skills evolve alongside technology.

Empower local innovation hubs that are key in fostering sustainable context-specific responses.

ADDRESSING THE AI-CYBERSECURITY NEXUS: PRIORITIES FOR NATIONAL CAPACITY BUILDING

Organized by the Global Cyber Security Capacity Centre (GCSCC), University of Oxford

Speakers

- **Moderator – Mr. Michael Goldsmith,** Global Cyber Security Capacity Centre (GCSCC), University of Oxford
- **Ms. Caroline Troein,** International Telecommunication Union (ITU)
- **Mr. George Michaelides,** Digital Security Authority, Cyprus
- **Mr. Masayuki Furukawa,** Director, Japan International Cooperation Agency (JICA)
- **Ms. Joanna Pawelek-Mendez,** Ministry of Foreign Affairs, Poland

As artificial intelligence accelerates digital transformation, its integration into cybersecurity systems is altering both the nature of threats and the strategies required to defend against them. This session explored how AI's dual-use nature, supporting both defensive capabilities and malicious activities, raises new challenges for national cybersecurity efforts. While AI can improve threat detection and response, its integration expands the attack surface and creates less visibility into compromises, prompting urgent questions about **how national strategies and capacity building initiatives should adapt**.

AI-readiness must be assessed through a national lens, with strategies developed and owned by domestic stakeholders. A strong emphasis was placed on ensuring that national AI strategies are not generated by automated systems or external actors alone, but rather built through participatory processes that engage technical experts, policymakers, and civil society. One speaker noted the **risks of "vibe coding" and misinformation enabled by AI**, which require not only technical safeguards but a broader societal understanding of AI's implications.

Several interventions addressed the importance of **aligning national strategies with internationally recognized norms and standards**. With AI advancing faster than policy can often keep pace, concerns were raised about hastily developed regulations. Instead, a call was made for close coordination between governments, standards bodies, and technical experts to promote thoughtful regulation that protects human rights and promotes trust. Ongoing efforts in the UN, EU, Council of Europe, and Japan's G7 presidency were cited as examples of how international dialogue can support convergence on shared norms while respecting national contexts.

Existing tools such as **Oxford's pilot AI-readiness assessment, the ITU Global Cybersecurity Index, and the Capacity Maturity Model (CMM)** were discussed as helpful starting points, but in need of updates to reflect AI-specific risks. A systems-thinking approach was recommended to integrate AI considerations into existing capacity-building frameworks, with the ITU noted as already applying this model in the Americas. Drills and scenario-based exercises were recommended not only for operational readiness but also as a means of building cross-sector relationships at national and regional levels.

In response to questions on what should be prioritized over the next 12 months, speakers proposed the development of dynamic, accessible best practice guidance to help countries adopt AI securely. A **sandboxing approach**, similar to the EU's 5G toolbox, was suggested to allow governments to test and verify the security of AI-enabled platforms. Other priorities included updating national actor mapping to better understand gaps, expanding access to multistakeholder platforms such as the AI for Good Summit, and ensuring that lessons from AI factories and local innovation hubs inform international standards-setting.

Ultimately, the discussion concluded with a shared call for **coordinated, forward-looking action** from the international cyber capacity building

community. Building on trusted frameworks, enhancing cross-border partnerships, and embedding AI into every layer of cyber strategy, technical, legal, institutional, and societal, were all seen as necessary steps to ensure readiness in a fast-evolving digital landscape.

Key Takeaways

Clear and accurate assessment of national considerations is essential in developing effective strategies for responding to AI cybersecurity threats.

Norms and standards developed at the global level are important, but there is a need to **build capacity and best practices in implementing those at the national level.**

National strategies for AI and cybersecurity need to **engage the whole of society**, drawing on expertise from all stakeholder groups.

CLOSING PLENARY:

CYBER CAPACITY FORWARD - POWERING MEANINGFUL AND SUSTAINABLE RESULTS

Organized by the International Telecommunications Union (ITU)

Speakers

- **Moderator – Mr. Orhan Osmani,** Head at the Cybersecurity Division for Telecommunication Development Sector, ITU
- **Ambassador Václav Bálek,** Ministry of Foreign Affairs of the Czech Republic
- **Ms. Alison August Treppel,** Organization of American States
- **Mr. Lacina Koné,** Smart Africa
- **Ms. Jennifer Bachus,** Department of State, United States
- **Mr. Geoffrey Harris,** Secretary of ICT, Nauru

Discussion

Mr. Orhan Osmani opened the session by underlining the **value of the GC3B as a moment of opportunity** not just to exchange updates, but also to observe what is truly possible when partners align towards implementation. This point resonated with all panelists, who stressed that **the time to move from talk to action is now**.

Mr. Geoffrey Harris shared the journey of Nauru, a small island state that adopted a Cybersecurity Act as early as 2015. Yet Mr. Harris noted that threats evolve rapidly and **digital systems need constant adaptation**. With only 18 IT graduates in the country, capacity gaps are real, which makes outsourcing a necessity, and "security by design" a default approach.

Ms. Alison August Treppel reminded the audience that Latin America and the Caribbean face many of the same cyber capacity building challenges as elsewhere, although with some regional nuances. She outlined the **OAS's "Three Rs" framework focusing on resilience, response, and recovery**, which provides a practical model guiding both strategy and implementation of OAS' efforts. From national cyber strategies to cyber-ready workforces and incident response teams, she emphasized the need to "*track progress, but also acknowledge how far we've come*", while stressing the importance of stronger norm-building and cross-sectoral trust.

Ms. Jennifer Bachus added a **fourth "R", standing for risk**. Risk management, she stressed, cannot be siloed, as it requires a **whole-of-society approach** that includes governments, civil society, and especially the private sector. With this, she echoed other panelists in calling for more inclusive, holistic workforce development that is not attainable by governments alone.

When asked how the global community can better coordinate efforts and avoid duplication when supporting Africa's cyber landscape, Mr. Lacina Koné emphasized that the continent should not be treated as "*the battlefield of rivalry, but it should be the architect of its own future*". Through a coalition-of-the-willing approach, Smart Africa aims to **amplify African Union-led strategies and coordinate cyber efforts across borders**. With the continent's young population and the continent's digital needs quickly outpacing its own capabilities, Africa is in a situation of banking without banks, healthcare without hospitals, AI and cyber readiness are being leveraged into Africa's core development strategy. "*We don't see capacity gaps*", Mr. Koné said, rather "*we see blank canvas without*

legacy systems from which we can build smart from the start."

When asked how efforts across regions can be better coordinated to meet local needs more effectively, Ambassador Václav Bálek of the Czech Republic highlighted his country's focus on **localised, tailored development cooperation, bridging engineering-related know-how with regional needs**. From Eastern Europe to later Latin America and Africa, Czech-supported initiatives are anchored in practical, scalable deliverables. He emphasized the need for a "*common language*" across stakeholders, given the challenge of disconnect between policymakers and experts. As he urged: "***Let's not just keep talking, let's walk the talk***".

On **duplication**, Ms. Bachus called it "*the ultimate question of the conference*",warningthatwithlimited money, time, and people, redundant efforts are not just inefficient but also counterproductive. She suggested a "*parallel play*" approach, allowing **coordinated action across different fora**, with donors, implementers, and local stakeholders working in complementary ways. She also stressed that digital skilling is often more effectively delivered by the private sector, and therefore governments must open up the table to multistakeholder cooperation.

Looking ahead, the panelists all agreed on the **need for adaptive planning**. Ms. Treppel noted that the OAS is working on five-year strategic plans that remain flexible and realistic in the face of rapid change.

Ms. Bachus reinforced the preventive argument that investing before incidents occur is far cheaper than scrambling afterward. Meanwhile, Mr Koné warned against the common perception that cybersecurity is a periphery of the digital economy instead of the core digital economy, stressing that it is in fact the core of the digital economy that enables everything else, and needs a change of mindset that would eventually "*solve the problem of funding*", he said.

Closing the session, Amb. Václav Bálek reminded everyone to keep listening and to take advantage of the "good weather outside" to act, while Ms. Treppel reminded participants about the shared motivations that brought them to GC3B. In his final remarks, Mr. Harris concluded warning that "*a 10-year plan risks becoming obsolete. We should not wait. Now is the time to make things happen*".

Key Takeaways

Cyber capacity building must be locally owned and context-specific to be sustainable. Tailored approaches, like those of the Czech Republic and Smart Africa, demonstrate that practical, small-scale deliverables and regional ownership are critical for long-term impact.

Coordination is the most urgent challenge facing duplication in the CCB community. With limited resources, speakers called for inclusive, multistakeholder cooperation and "parallel play" to ensure that efforts are complementary, especially in workforce development and digital skilling.

Cybersecurity must be treated as a foundational element of digital development and not a peripheral concern. Lacina Koné and others stressed the need to shift mindsets and integrate "security by design" into national digital strategies, while investing now, rather than reacting later, was a recurring theme who reminded participants that the cost of inaction grows with every delay.

CLOSING CEREMONY

Speakers

- **Ambassador Jürg Lauber,** Permanent Representative of Switzerland to the United Nations and other Organizations in Geneva
- **Ms. Marjo Baayen,** GFCE Secretariat Director
- **Ms. Cristina Camacho,** GFCE Foundation Board
- **Ms. Julia Bauer,** GC3B 2025 Master of Ceremonies

From left to right: Marjo Baayen (GFCE Secretariat Director), Marina Wyss Ross (Swiss FDFA), Amb. Jürg Lauber and Irene Grohsmann (Swiss FDFA)

The Closing Ceremony of the Global Conference on Cyber Capacity Building (GC3B) brought together participants to reflect on the key insights, outcomes, and commitments that have emerged over the course of the event. With closing remarks from Ambassador Jurg Lauber and Ms. Cristina Camacho the ceremony reiterated the urgent need to catalyze action for cyber resilient development. It highlighted major themes discussed during the conference, including sustainable capacity building, multistakeholder cooperation, and the importance of aligning cyber resilience efforts with broader development goals. The conference closed with the GFCE extending its heartfelt gratitude to the Swiss Federal Department of Foreign Affairs (FDFA) for its **generous hospitality and unwavering support** in hosting the second edition of the GC3B in Geneva. **Switzerland's belief in the GC3B's mission** of mainstreaming cyber resilience and their commitment to fostering high-level, multi-stakeholder dialogue has marked a **global milestone** in advancing international cooperation in cyber capacity building.

Together, the GC3B has become an **action-oriented space** where global progress in cyber resilience can thrive. Because in the digital age, we are only as strong as our weakest link.

Our gratitude to everyone who believes in this mission and continues to push it forward.

GC 3B Global Conference on Cyber Capacity Building

GENEVA SWITZERLAND

Contact Us

If you are interested in learning more about the Global Conference on Cyber Capacity Building, please reach out to us at **contact@gc3b.org** or stay tuned for updates on our **website**.

Follow us on **LinkedIn**

Follow us on **YouTube**