



**GC
3B** | Global
Conference
on Cyber
Capacity
Building

29-30 November 2023
Accra | Ghana

GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING

REPORT



Global
Conference
on Cyber
Capacity
Building

Contents

Acknowledgements	i
Acronyms	ii
Background	1
Media Engagements	4
Opening Ceremony and Signing of the Accra Call	5
Remarks from Partners	7
Panel Sessions focusing on the Four Conference Pillars	18
Side Events	39
Closing Ceremony	43
Significance of the Accra Call	52
Conclusion	54
Photo Gallery	58



Acknowledgements

The inaugural Global Conference on Cyber Capacity Building (GC3B) was under the theme “Cyber Resilience for Development”.

The success of the GC3B event co-organised by the Global Forum on Cyber Expertise (GFCE), the CyberPeace Institute, the World Bank, the World Economic Forum (WEF), and the Ministry of Communications and Digitalisation (MoCD) through the Cyber Security Authority was possible due to the invaluable contributions and collaboration of numerous individuals and organisations.

We appreciate the support of the President of the Republic, H.E. Nana Addo Dankwa Akufo-Addo and his Vice, H.E. Alhaji Dr. Mahamudu Bawumia in making it possible to host this conference.

The leadership provided by the Minister for Communications and Digitalisation, Hon. Mrs. Ursula Owusu-Ekuful, was enormous, impacting greatly on the successful execution of the GC3B event. We acknowledge the Governing Board of the Cyber Security Authority (CSA), whose vision and guidance steered the strategic direction of the event.

The Joint Intelligence Committee (JIC), and the Joint Cybersecurity Committee (JCC) provided invaluable insights and expertise towards the success of the event. The significant role of the Ghana Immigration Service in this regard cannot be overemphasised.

A heartfelt gratitude is extended to the Parliamentary Select Committee on

Communications, whose support and advocacy have propelled cybersecurity initiatives forward in Ghana.

Further commendation goes to Dignitaries, including the Senior Presidential Advisor, Hon. Yaw Osafo-Maafo, who represented the President of Ghana at the event, the Deputy Minister for Communications and Digitalisation, Hon. Ama Poma Boateng, the Deputy Minister for Information, Hon. Fatimatu Abubakar, and all other esteemed dignitaries for their presence and varied contributions towards the event.

We are grateful to the State Protocol Department, the GC3B Steering Committee Members (Dr. Albert Antwi-Boasiako - Director-General, CSA; Ing. Dr. Kenneth Ashigbey - CEO, Ghana Chamber of Telecommunications; Mr. Kwame Baah-Acheamfuor - Director, International Affairs, MoCD; Dr. Collins Yeboah-Afari - Director-General, Ghana-India Kofi Annan Centre of Excellence in ICT; Mr. John Awuah - CEO, Ghana Association of Banks; and Mr. Arthur Mills - Deputy Director, Protocol Bureau, Ministry of Foreign Affairs and Regional Integration), the GC3B Work Teams, Sponsors, and all officials who supported the event through various teams for their diligent efforts in coordinating logistics and ensuring the smooth execution of the event.

Gratitude is further extended to the management and staff of the Cyber Security Authority, for their dedication and commitment that made the event outstanding.



Acronyms

AGAMAL	AngloGold Ashanti Ghana Malaria Control
ANCA	Africa Network of Cybersecurity Authorities
AUDA	African Union Development Agency
CBMs	Confidence-Building Measures
CoE	Council of Europe
CICTE	Inter-American Committee against Terrorism
CII	Critical Information Infrastructure
CSIRT	Computer Security Incident Response Team
DPI	Digital Public Infrastructure
GFCE	Global Forum on Cyber Expertise
INTERPOL	International Criminal Police Organisation
ITU	International Telecommunication Union
JCC	Joint Cybersecurity Committee
JIC	Joint Intelligence Committee
LaC4	Latin America and Caribbean Cyber Competence Centre
MoCD	Ministry of Communications and Digitalisation
NEPAD	New Partnership for Africa's Development
OAS	Organisation of American States
OEWG	Open-Ended Working Group
POC	Point of Contact
SDGs	Sustainable Development Goals
SMEs	Small and Medium Enterprises
SOC	Security Operations Centre
UNIDIR	United Nations Institute for Disarmament Research
USAID	United States Agency for International Development
WEF	World Economic Forum
WiCyS	Women in Cybersecurity



Background

Over 800 cybersecurity experts, professionals, high-level leaders, the international development community, and innovators from across the world converged in Ghana from November 29-30, 2023 to participate in the inaugural edition of the Global Conference on Cyber Capacity Building (GC3B), in Accra.

Under the auspices of the Ministry of Communications and Digitalisation through the Cyber Security Authority (CSA), the conference was co-organised by the Global Forum on Cyber Expertise (GFCE), the World Bank, the Cyber Peace Institute, and the World Economic Forum (WEF) under the theme “Cyber Resilience for Development.

The event served as a platform for actionable dialogue and the exchange of innovative ideas

among policymakers and industry leaders to contribute to the advancement of cyber capacity building at the global level.

The Global Conference on Cyber Capacity Building (GC3B) was organised to raise awareness on the need for every nation to have relevant expertise, knowledge, and skills to safeguard their digital future. The event was also used to encourage countries to work together on developing these capabilities to ensure a free, open, and secure digital world.

The event thus focused on common goals and solutions by addressing the need to increase resources for cyber capacity building, which is a key enabler for sustainable development, economic growth, and social progress.



Why Ghana was selected to host the event

The 2020 score of 86.69% on the Global Cybersecurity Index is a major progress from previous ratings in 2017 and 2018 of 32.6% and 43.7%, respectively, placing Ghana's cybersecurity readiness in third place on the African continent behind Mauritius and Tanzania. The rating also placed Ghana on the world map with respect to cybersecurity development.

Ghana was therefore selected to host the GC3B event based on the demonstrable commitment and dedication shown towards the development of a safe and resilient digital ecosystem. The selection was also due to the Ministry of Communications and

Digitalisation's efforts, through the CSA, to secure Ghana's cybersecurity environment through international cooperation.

Having co-organised and hosted several significant conferences like the Freedom Online Conference in 2020, the Africa Cyber Experts Kick-off Committee Meeting, and the Global Internet Forum to Counter Terrorism (GIFCT)-Tech Against Terrorism (TAT) workshop in 2022, and collaborating in various cybersecurity events around the world, the sponsors of the event were confident that Ghana could effortlessly host a successful event and indeed they were not disappointed.

Conference Pillars

The conference sessions were anchored on four pillars:

- Making international development cyber-resilient
- Collaborating to secure the digital ecosystem.
- Cyber capacity building for stability and security.
- Operationalising solutions.

The conference, among other things, catalysed global action to elevate cyber resilience and capacity building in the international development agenda and in national development plans and investments as key enablers of sustainable development, inclusive economic growth, and social prosperity for all.

The Accra Call

A major highlight of the conference was the announcement of the Accra Call for Cyber Resilience Development on November 29, 2023: a global framework for collaborative initiatives to help countries increase their cyber resilience.

The action framework calls on all governments and organisations across all sectors and regions to affirm their willingness to voluntarily promote, pursue and coordinate efforts on sixteen specific actions to elevate cyber resilience across international and national development agendas.

In addition, the Accra Call aims at promoting cyber capacity building which supports broader development goals and effectively serves the needs of developing countries.

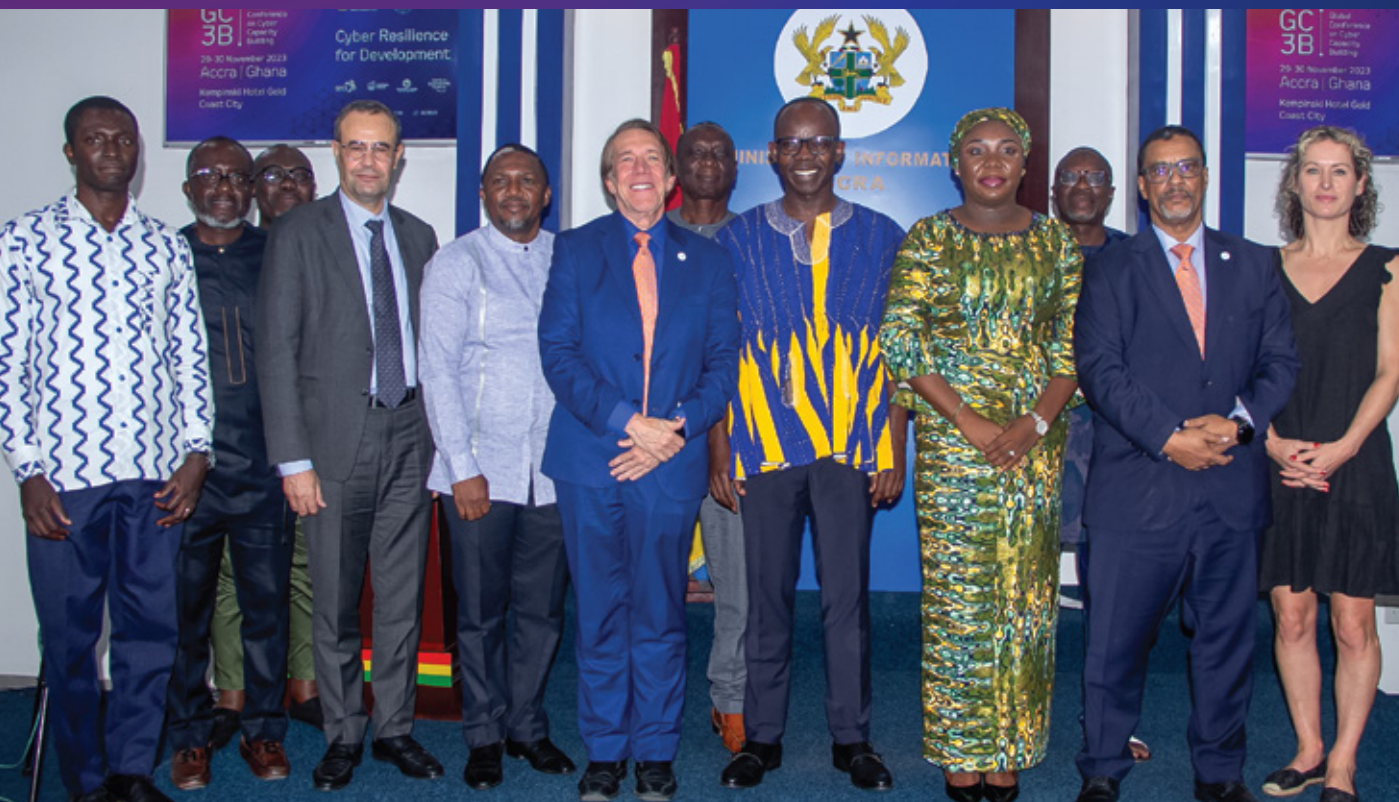


Media Engagements

A media launch to herald the inaugural GC3B event was held at the Ministry of Information, drawing esteemed dignitaries and representatives from renowned media outlets. The press conference garnered extensive coverage on mainstream media channels nationwide, with a live broadcast on the esteemed national channel, GTV.

Following the launch, GC3B representatives and Cyber Security Authority (CSA) officials actively engaged with various media houses, participating in insightful interviews that provided valuable insights into the objectives and significance of the upcoming event.

The launch not only initiated the momentum for the main event but also generated significant media coverage, setting the stage for widespread publicity of the GC3B event.



**Opening
Ceremony and
Signing of the
Accra Call**

GC3B Official Opening Ceremony and Signing of the Accra Call

To extend a warm welcome to dignitaries and participants, a cultural dance group was stationed at the event grounds to usher guests into the auditorium, offering a vibrant glimpse into Ghana's rich heritage. The opening ceremony commenced with a patriotic performance of the Ghana National Anthem, led with solemnity and pride by members of the Ghana Armed Forces Band. The performance set an impeccable tone for the event, encapsulating the essence of unity and a collective purpose to ensure cyber resilience for development.



Opening Remarks

Hon. Ursula Owusu-Ekuful

Minister for Communications and
Digitalisation

In her remarks, the Minister referenced the theme of the conference as “Cyber Resilience for Development” and underscored Government’s political will to enhance cybersecurity in Ghana to boost Ghana’s emerging digital economy which is supplemented by Ghana’s hosting of the African Continental Free Trade Area (AfCFTA)

Secretariat. As part of Ghana’s agenda in improving digitalisation, the Minister noted the implementation of the rural telephony project that will connect over 4 million unserved and underserved citizens to a shared national platform and network. It was noted that due to Ghana’s intentional and transformational improvement in cybersecurity, the country recorded a higher index in the 2020 ITU Global Cyber Security Index of 86.69% from 32.6% in 2017. Despite these achievements chalked, the challenges that confronted the cybersecurity space are numerous.

For instance, in the first half of 2022 and 2023, Positive Energies reported that the global financial sector was the most hit with cyber-attacks recording 18% followed by telecommunications sector with 13%, Government agencies with 12%, Trade organisations with 12% and the industrial sector with 10%. In the second quarter of 2023, the African Continent experienced an average weekly cyber-attack of 2,164 attacks reflecting a year-on-year increase of 23% compared to the same period in 2022.

The Minister concluded her remarks by calling upon all stakeholders to work together to achieve a safe and robust cybersecurity space and assured stakeholders of Ghana’s commitment to improving cybersecurity.

**Remarks from
Partners**



Mr. Chris Painter

President, GFCE Foundation Board

Mr. Painter expressed excitement and optimism at the changing trends of cybersecurity especially with the introduction and development of Artificial Intelligence (AI). He underscored the importance of technological advancement vis-à-vis the boosting of the national economy, increasing productivity and fostering human and social relations.

He noted that the various vulnerabilities and challenges facing the digital economy impede economic growth and undermine societal trust in the digital environment, hence, it was imperative that stakeholders work together

to ensure that no country is below the 'cyber poverty line'. Furthermore, he stated that cybersecurity is closely entwined with achieving the various Sustainable Development Goals (SDGs). Considering the challenges facing cybersecurity, he noted that the GFCE has built a robust network and has advanced efforts to coordinate globally and mutually. He also noted that the challenges facing the cyber space calls for a paradigm shift, stressing that the GC3B will trigger actions beyond Accra. He highlighted that a key contribution of the GC3B is the multi-stakeholder 'Accra Call' for cyber resilience development.



Mr. Pierre Laporte
World Bank Country Director, Ghana

Mr. Laporte noted in his speech that “development delayed is development denied” also applies to cybersecurity capacity building. He highlighted that economic prosperity and poverty eradication cannot be achieved without cyber resilience. In view of this, the World Bank has provided over \$20m in grants to provide

expert technical assistance to developing countries.

He highlighted that Ghana has one of the best cybersecurity success stories, stressing that the World Bank has been supporting Ghana since 2006 and is committed to continue the collaboration.



Mr. Akshay Joshi

Head of Industry and Partnership,
World Economic Forum

In his remarks, Mr. Joshi informed participants that cybercrime and cyber insecurity continue to feature among the top 10 risks in the World Economic Forum's Global Risk Report.

He further noted that this year's Global Cyber Security Outlook Report indicates that 93% of cyber leaders and 86% of business leaders were of the opinion that geo-political instability was likely to result in catastrophic cyber-attacks over the next two (2) years. He also noted that the changing trends in security, specifically the development of AI has shifted the balance in favour of attackers as opposed to defenders.

Further, he indicated that the World Economic Forum established the Centre for Cybersecurity

in 2018 to provide an independent and impartial platform to reinforce the importance of cybersecurity as a strategic imperative and to foster global public-private collaborations to address some of the systemic cybersecurity challenges. He added that the GC3B presented a unique opportunity to unlock global public-private co-operations and to ensure the benefits of digitalisation can be translated equitably to nations, industries, and individuals alike. In conclusion, he reiterated the Forum's resolve to continuously support the GC3B and its positive impact.



Ms. Francesca Bosco

Chief Strategy and Partnerships Officer,
CyberPeace Institute

Ms. Francesca Bosco in her remarks stated that the conference was one that underscores the crucial role that cyber resilience and capacity building play in advancing the UN 2030 agenda for sustainable development. She emphasised the effectiveness of sustainable and inclusive stewardship of international cooperation for cyber resilience development. She added that the Conference was a unique opportunity to raise awareness of how cybersecurity and cyber capacity building support digital, social, and economic development in line with the sustainable development goals.

There is often an underestimation of the cyber risk and the threats that come with increased use of the ICTs and digitalisation, or these risks and threats are not fully understood and addressed as a systemic challenge. These cyber insecurities

she said can unwind the progress that has been made so far with digitalisation.

She therefore called on Civil Society Organisations, which she was representing, to play a fundamental role in contributing to a safe and secure sustainable development since these organisations are often the ones closest to the people and can better define the cyber capacity building needs of the people. This would enable impactful solutions from awareness raising, training and educational activities that will close the cybersecurity warfare gap and operationalise principles for capacity building in a diverse and inclusive manner.

She further called on donors to make the much-needed commitment that was truly needed for a multistakeholder and impactful approach.



Ms. Alison Treppel

Executive Secretary, Inter-American
Committee Against Terrorism,
Organisation of American States (OAS)

Ms. Alison Treppel in her remarks indicated that the Organisation of American States (OAS) became a founding member of the Global Forum on Cyber expertise (GFCE) because it recognised the value and the need for greater coordination of cybersecurity capacity building both regionally and internationally. Thus, the OAS continues to encourage other countries throughout the Western Hemisphere to join the forum so that they can also benefit from the tools and opportunities that this community of public and private stakeholders, civil society and academia offer. She opined that the most impactful ways to create increased

cyber resiliency was through greater and more coordinated capacity building among the donor community, among implementers and among the beneficiary countries. Commenting on the Accra Call, she indicated that, “it reflects our collective commitment as public and private sector institutions as international organisations academia and civil society to a common goal to strengthen cybersecurity capacity building and resilience across the globe”. The OAS she stated remains committed to supporting these objectives and to coordinating with all within and outside the American region to create a more resilient, safer and secure cyber space.



Mr. Matthew Wong

First Secretary OEWG Digital Corporation
and Cyber Security

Mr. Matthew Wong, in the remarks delivered on behalf of the Chair of the United Nations Open-Ended Working Group on Security, Ambassador Burhan Gafoor commended the organisers for the initiative in bringing the cyber capacity building community together to have a crucial and timely conversation. He stated that in the recent annual progress report of the Open-Ended Working Group, the international community recognised that capacity building as an important confidence building measure, is a topic that cuts across all the pillars of the OEWG's work and that a holistic approach to capacity building is essential. He called on

participants to consider how the cyber capacity building community can work closely with the UN as a platform to amplify the reach and impact of their capacity building work given the universal status of the UN. He proposed that the conclusions of the various conversations be brought to the UN's global round table which comes off on May 10, 2024.

Lastly, he called on participants to consider how ideas that are sparked at the conference could be formulated as specific proposals and recommendations that could possibly garner consensus at the UN to ensure that the discussions at the conference make lasting impact at the Global level.



Ms. Manon Le Blanc

Coordinator for Cyber Issues at the European
External Action Service, European Union

Ms. Manon Le Blanc stated in her address that the development and use of technologies have increased globally, supporting economies and connecting societies.

However, it has created a new reality of an evolving cyber threat landscape with critical infrastructure, supply chains, businesses and citizens being targeted daily in cybercrime and ransomware attacks. She remarked that these

threats must not prevent us from exploring the opportunities that the new digital era brings.

She indicated that the EU has increased its investments in cyber capacity building and is partnering with countries across the globe to ensure a stable and secure cyber space.

She encouraged all stakeholders to invest in people, processes and technologies that are vital to harness the benefits of this new digital reality.



Mr. Orhan Osmani

Acting Head of Cybersecurity Division, ITU

Mr. Osmani outlined that the ITU has been at the forefront of driving digital development since 1988 and in terms of cybersecurity, the ITU has long term involvement in capacity building and strengthening the digital development.

He added that cyber capacity building must start at an early age and that the ITU has been involved in this process since 2007 with the development of the guidelines on Child Online

Protection, and is currently working with other partners to mentor children in cybersecurity. He remarked that the collaboration between the ITU and its partners is based on information sharing to avoid duplication of efforts. He endorsed the Accra Call as a move from words to action on capacity building, and the Call will be a road map for the cyber community to work together in achieving set goals.



Hon. Yaw Osafo-Maafa

Senior Presidential Advisor, Ghana

Hon. Yaw Osafo-Maafa, who delivered remarks on behalf of the President of the Republic of Ghana stated that the digitalisation of economies, governments and societies has been a transformative process that has led to numerous benefits which has in turn contributed significantly to our social economic development. He added that the advancement of technology comes with the development of cyber threats making it imperative for state and non-state actors to build the relevant skills, knowledge and infrastructure needed to safeguard the digital assets, investment, Information Communication Technologies and other digitalisation initiatives, emphasising that GC3B is the best platform to share ideas.

He mentioned that cyber resilience and capacity building plays a pivotal role in advancing the UN 2030 agenda for sustainable development

which underscores the collective commitment to harnessing the power of digital technologies in driving progress and development.

Due to the increased internet penetration, cybercriminals are threatening digital development. The threat landscape has become increasingly volatile and hence the need for governments, businesses, and stakeholders within the cyber ecosystem to collaborate and cooperate with integrity or listening strategies that will address these complex threats.

He stated that the the “Accra Call” will outline concrete actions that will strengthen cyber resilience in enabling and accelerating sustainable development and it is expected to promote cyber capacity building that effectively serves the needs of developing countries, as digital transformation is being embraced as a cornerstone.

Signing of the Accra Call

As part of the opening ceremony, the Senior Presidential Advisor, Hon. Yaw Osafo-Mafo, was joined by the Honourable Minister for Communications and Digitalisation, Mrs. Ursula Owusu-Ekuful and the Director-General of the Cyber Security Authority, Dr. Albert Antwi-Boasiako, to sign the 'Accra Call' on behalf of the Government of Ghana. This was an indication of Ghana's willingness to voluntarily promote, pursue and coordinate efforts to elevate cyber resilience across international and national development agendas.



**Panel Sessions
focusing on the
Four Conference
Pillars**

Pillar 1

Making International Development Cyber Resilient

This pillar focused on justifying the essence of mainstreaming cyber resilience into the international development agenda as a core enabler of digital, economic, and social development. It sought to define the benefits of embracing cyber resilience as an integral part of development cooperation and fostered a better understanding of the benefits of incorporating cyber resilience across the strategic priorities of developing countries.

Investing in Cyber Resilience to Enable Sustainable Development

The Global Program Manager, Digital Development of the World Bank, Mr. Casey Torgusson introduced the panel session, and highlighted the impact of cyber-attacks on Critical Information Infrastructure (CII) of developing countries and how it affects their GDP. He emphasised the importance of developing innovative ways to bridge the speed and scale that deliver better results in terms of cybersecurity.

The six member-panel were made up of the following personalities.

- Hon. Mrs Ursula Owusu-Ekuful, Minister for Communications and Digitalisation
- Mr. Chris Burns, Agency Chief Digital Development Officer, and Director Technology Division
- Mr. Osama Manzar, Founder & Director, Digital Empowerment Foundation, Miss Dianna Langley, Chief Operating Officer, Nethope
- Dr. Kanwaljit Singh, Bill and Melinda Gates Foundation, Digital Public Infrastructure
- Mr. Brett DeWitt, Vice President, Global Cyber & Technology Policy, Mastercard.

Recommendations

- Developing countries should develop their capacities to manage their own digital infrastructure, to reduce the overreliance on external or foreign consultants.
- Local and international cooperation and partnerships are relevant and must be improved to grow the cybersecurity ecosystem globally because cybercrimes are borderless.
- Capacity-building programmes should focus on the social, cultural, and behavioural patterns of digital users.

- Cybersecurity digital capacity building must be need-driven, customised to the country context, globally coordinated, and focused on Digital Public Infrastructure (DPI).
- Cybersecurity must be integrated as the lifeblood of digital infrastructure.
- Public and private sectors need to bridge in the growing cyber talent gap by investing in

young people and mid-level professionals to upskill and train.

- Private and Public sector partnerships, including policymakers, regulators, NGOs, academia, law enforcement, and standard body organisations are to be added to capacity building programs.



Pillar 2

Collaborating to Secure the Digital Ecosystem

Discussions under this pillar centred on scaling public-private collaboration and multi-stakeholder cooperation to address systemic challenges and vulnerabilities critical to securing the digital ecosystem. Two critical areas where such collaborations are needed are: (1) narrowing the cybersecurity workforce/skills gap, and (2) protecting critical infrastructure and essential services. The sessions below were held to address the issues.

Panel 1

Closing the Cybersecurity Skills Gap in Developing Countries: Developing an Action Agenda

The focus of this session was how to address the skills gap in the cybersecurity sector globally and how countries can collaborate to collectively combat cyberthreats.

Opening the session, the Ambassador for Cyber Affairs in the Netherlands' Ministry of Foreign Affairs, Mr. Ernst Noorman, stated that in his country there are hundreds of cybersecurity experts leaving their universities with most of the students from abroad. This, he indicated contributes to capacity building in cybersecurity for other countries thus creating a skill gap in his country.

The moderator for the session was Ms. Anat Lewin, Global Lead, Digital Safeguards, World Bank with panellists, namely:

- Ms. Kaja Ciglic, Senior Director, Microsoft
- Mr. Orhan Osmani, Acting Head, Cybersecurity Division, International Telecommunication Union (ITU)
- Mrs. Alison August Treppel, Inter-American Committee against Terrorism(CICTE) Organisation of American States (OAS))
- Ms. Oyinye Iruoma Nwaneri, Chief Executive Officer, Afrika Tikkun Services

Recommendations

- Countries with strong cybersecurity infrastructure should assist weaker countries to level up in the global fight against cyberattacks.
- Donors should support the Global Forum on Cyber Expertise to ensure countries in need of strengthening cyber skills receive assistance from countries with advanced cybersecurity architecture.

- Public-private sector partnerships to conduct a deeper dive into the issue of skills gap in cybersecurity and insufficient training opportunities.

Panel 2

Strengthening the Resilience of Critical Information Infrastructure

Strengthening the cyber resilience of Critical Information Infrastructure (CII) is essential to enabling social and economic development and to meeting the Sustainable Development Goals (SDGs). It is also essential to maintaining international security and stability. The session brought experts together to exchange information on existing approaches, lessons and good practices to incorporate at national and international levels to improve the resilience of CIIs.

Madam Manon Le Blanc, Coordinator for Cyber Issues, European Union, European External Action Service was the moderator for the session and had the underlisted experts as panellists.

- Ambassador Claudio Miguel Peguero Castillo, Ambassador for Cyber Matters, Ministry of Foreign Affairs, Dominican Republic.
- Dr. Hoda Al Khzaimi, Director, Director of Center for Cyber Security, NYU Abu Dhabi Center for Cyber Security / Co-Chair of the Global Future Council for Cyber Security, World Economic Forum / Director, Emaratsec.
- Mr. Jadet Khunakongkit, Assistant Secretary General, National Cyber Security Agency, Thailand
- Dr. Paul Timmers, Researcher, University of Leuven / Oxford University.

Recommendations

- Call for the development and implementation of a risk management framework.
- A global equitable access to all the necessary tools that would allow for the development of advanced cyber competencies.
- Ensure the design of fit-for-purpose regulations to protect critical information infrastructure.

Panel 3

Sharing Success: Lessons for Developing Effective Cyber Capacity Partnerships

The session highlighted the importance of adopting a partnership approach to cyber capacity building with emphasis on the need to bridge gaps between governments and the private sector. It also noted the significance of region-specific and context-sensitive models of collaboration in implementing cybersecurity projects and strengthening cyber-resilience in developing countries.

The discussion was moderated by Madam Yasmine Idrissi Azzouzi, Cybersecurity Project Officer at ITU. The panellists were:

- Mr. Regine Grienberger, Cyber Ambassador, German Federal Foreign Office Berlin, Germany
- Mr. Christopher Banda, Head of Malawi CERT, Malawi
- Ms. Rebecca Stewards, co-SRO, Cyber Capacity Building Programme, Home Office, United Kingdom
- Mrs. Vanessa Copetti Cravo, Cybersecurity Technical Group, ANATEL, Austria

- Mr. Samuel Tew, Principal Consultant, AXON Partners Group, Spain Yasmimi Idrissi Azzauzi, International Telecommunication Union (ITU)

Recommendations

- Criteria for selecting partners, should focus on alignment of objectives, effective absorption capacity, a favourable governance environment, robust reporting, and potential short-term and long-term impacts.
- Cyber Capacity Partnership approaches should shift from isolated activities to collaborative initiatives with organisations like the International Telecommunication Union (ITU)

Panel 4

Staying Ahead of the Curve: Cybercrime in the Era of New Tech

The discussions centred on the rapid advancement of new and emerging technologies including Artificial Intelligence and their associated opportunities and challenges. While these innovations offer various benefits, the panellists unanimously admitted to emerging technologies and cited how these have become tools used by malicious actors to perpetuate cyber-attacks.

The session mentioned proactive measures to stay ahead of cybercriminals when utilising these new technologies.

Panellists for the session were:

- Mr. Stephen Cudjoe-Seshie – Lead, National Computer Emergency Response Team, Cyber Security Authority
- Ms. Pei Ling Lee, Head of Cyber Strategy and Capabilities Development, INTERPOL

- Mr. Ahshay Joshi, Head of Industry and Partnerships, Centre for Cybersecurity, – World Economic Forum
- Ms. Laura Temesi. Head, Cyber Partnerships and Communications, – Standard Chartered Bank
- Ms. Komal Bazaz Smith, Chief Business Officer, Global Cyber Alliance was the moderator.

Recommendations

- Deepen capacity building and awareness creation strategies targeted at children, the public, government, and businesses.
- Enhance collaboration between governments agencies and, civil society organisations for effective global fight against cyberattacks.
- Develop tools to combat cybercrimes.
- Build capacity of law enforcement agencies and academia about current cyber trends.
- Adopt information sharing between governments and private institutions.

Panel 5

Stronger Together: Cross-Regional Approaches to Cooperation in Cyber Capacity Building

The panel session was organised by the Organisation of American States (OAS), it began with opening remarks on fostering communication and exchanging information, especially through cyber resilience. The panel advocated the strong belief in fostering cross-regional knowledge, experience, and expertise as a catalyst for advancing sustainable global cybersecurity solutions. Moreso, the discussion also explored cross-regional

approaches to cyber capacity building particularly from the Americas and Asia.

The moderator Mr. Randy Pestana, Associate Director for Cybersecurity Policy, Florida International University sought to explore and discuss cross-regional approaches to cyber capacity building from the Americas and Asia. Notable cybersecurity experts for the discussion included:

- Mrs. Gordina Hector-Murrell, Director of Cyber Security, Ministry of Information and Communication Technologies of Antigua and Barbuda.
- Mr. Alan Cabanlong, Regional Director for South-East Asia, Global Forum on Cyber Expertise (GFCE).
- Mr. Carlos Leonardo, Director, Dominican Republic CSIRT.

Recommendations

Some solutions for cross-regional and regional cooperation proposed during the session included.

- Organisation of joint-training activities, the sharing of cyber policies and strategy documents.
- Identification of national points of contact (POC) to facilitate the application and adaptation of confidence-building measures (CBMs).
- The facilitation of dialogue among various stakeholders. The need for effective capacity-building cooperation to avoid duplication.



PILLAR 3

Cyber Capacity Building for the Stability and Security of the Digital Environment

This pillar entailed sessions that sought to address and support the role that cyber capacity building plays in strengthening the links between international security and sustainable development, and in contributing to an open, secure, stable, accessible, and peaceful ICT environment. Information on ongoing work at the UN relevant to the framework for responsible state behaviour and protecting the digital environment, including the expansion of capacity building efforts was discussed.

Panel 1

Connection In Progress: Cyber Resilience, Development, and International Security

Although capacity building and international cooperation are recognised as key pillars of the framework for responsible state behaviour, its associated risk receives little attention amidst other competing developmental needs such as access to food, water, or eradication of poverty. The call for a clear roadmap was evident in the deliberations to bridge existing divides between different policy communities and ensuring a mutual international security regulation. Relatedly, the discussion further centred on how international cooperation mechanisms can be used to promote the implementation of the framework for responsible state behaviour in cyberspace.

The panel session was moderated by Ms. Francesca Bosco, CyberPeace Institute and had notable speakers such as:

- Amb. Nathaniel Fick, U.S. Department of State
- H.E. Tingika Elikana, Associate Minister for Telecommunications and ICT, Government of Cook Islands
- Ms. Towela Nyirenda-Jere, Head of Economic Integration, AUDA-NEPAD
- Ms. Lefaoali'i Meremine Auelua, Programme Director Pacific Partnerships, CERT New Zealand

Recommendations

Countries should:

- Prioritise the development and implementation of comprehensive national cybersecurity strategies that integrate seamlessly with broader development programmes.
- Establish and participate in international collaboration frameworks that facilitate

information sharing, intelligence exchange, and joint efforts to address cyber threats.

- Support and invest in capacity building initiatives, including educational programmes to enhance cybersecurity expertise at both national and global levels.
- Advocate and implement a holistic approach to technology topics, recognising the convergence of digital policy, infrastructure issues, and emerging technologies in cybersecurity strategies.
- Encourage the integration of artificial intelligence in cybersecurity efforts, particularly in "secure by design" principles, to enhance the development of secure software and systems.
- Prioritise the establishment of trusted networks and infrastructure, ensuring that the technological backbone of a country's communication systems is secure and reliable.
- Promote bottom-up initiatives by involving local communities and businesses in cybersecurity efforts.

Panel 2

Back to the Future: Lessons for Cyber Capacity Building

The session proceeded to provide a comprehensive overview of the progress made and elaborated a clear vision and direction from other government or counterpart institutions. Countries cited how they successfully institutionalised cyber development initiatives. Costa Rica's Criminal Justice Sector was named to have enhanced priority with a multi-faceted strategy that combines training, collaboration, and technology integration. Additionally, the Philippines explained why it prioritises inclusivity and accessibility in training programs, implementing measures to reach marginalised groups, such as women, indigenous peoples, and persons with

disabilities. Ghana shared how it took steps to raise awareness and educate stakeholders in each sector about the importance of cybersecurity by conducting workshops and training sessions to help industry players understand the potential risks and vulnerabilities they face in the digital age.

The session was moderated by Ms. Nayia Panagiota Barmaliou, a consultant on Cyber Policy, Diplomacy and Capacity Building at Cyber Lab International. Panellists for the session included:

- Dr. Albert Antwi-Boasiako - Director-General, Cyber Security Authority, Ghana.
- Ms. Lolita Lomanta - Senior Assistant Provincial Prosecutor, Department of Justice, Philippines.
- Mr. Juan Carlos Cubillo - Deputy Prosecutor, Attorney General's Office, Costa Rica.
- Mr. Alexander Segger - Head of Cybercrime Division and Executive Secretary of the Cyber Crime Committee, Council of Europe.
- Ms. Gill Thomas - Director of Engagement, Cyber & Resilience, Global Cyber Alliance.

Recommendations

- Emphasise the importance of continuous monitoring, information sharing.
- Adopt and implement a proactive measure approach to stay ahead of emerging threats.

Panel 3

Applying a Principles-Based Approach to Cyber Capacity Building

The session encapsulates how cybersecurity experts engaged with the public on the application of a principles-based approach to cyber capacity building. The panel explored the growing consensus regarding the importance of such an approach, sharing their experiences and practical lessons derived from applying principles in practice. The focus of the

discussion similarly revolved around identifying and exploring principles that have been implemented by countries for cyber capacity building, economic development, cybersecurity and human rights. Finally, panellists proffered solutions to the changes associated to the implementation of these principles.

The Executive Director, Global Partners, Ms. Lea Kasper from Croatia moderated this session with the underlisted panel members.

- Ms. Joyce Hakmeh, Deputy Director of the International Security Programme at Chatham House.
- Mr. Moctar Yedaly, GC3B special envoy from Mauritania.
- Ms. Amy Clark, Head of Resilience, Foreign Commonwealth & Development, United Kingdom
- Mr. Juan Diego Castañeda, Acting Director Karisma Foundation, Colombia

Recommendation

- Prioritise and value the human element in order to bring about meaningful and transformative change.
- The use of multistakeholder approach will foster the development of local talents.
- Combine the three pillars of training, collaboration, and technology for continuous capacity training and enhancement of the performance of the justice sector.
- Comprehensive monitoring and evaluation system will aid in effective implementation.
- Involve civil society to bring unique insights and perspectives during the formulation of principles.

Panel 4

Levelling the Playing Field: How International Law Expertise Can Strengthen Cyber Resilience

The session was essential because of the insights, interpretations and the consensus building regarding broad multilateral frameworks. To begin, panellists admitted that although the internal law covers the cyberspace there is need for countries to generate interest towards understanding the geopolitical context of these frameworks and apply them accordingly. This, if effectively implemented will lead to inclusive and transparent cyber resilience processes.

The session was moderated by Dr. Patryk Pawlak – Visiting Scholar Carnegie Europe and Chair of the GC3B Program Advisory Team. Speakers include.

- Dr. Nnenna Ifeanyi-Ajufo, Chair Working Group C of the Global Forum on Cyber Expertise.
- Ambassador Ricardo Otarola Pacheco, Legal Advisor at the Office of Deputy Minister for Foreign Affairs of the Republic of Costa Rica.
- Ms. Kristine Leilani Salle, Philippines Permanent Mission/Deputy Permanent Representative
- Ms. Liis Vihul, Chief Executive Officer of the Cyber Law International
- Mr. Christian Ranger, Deputy Director for Cyber Foreign Policy of Global Affairs Canada.

Recommendations

- Ensure international law equally applies to the cyberspace and not only on subjects of sovereignty and human rights.
- Countries should be actively involved in

creating jurisprudence.

- Advocacy for Africa academic writing and research in international law to be an open source for reference.

Panel 5

Integrating Cybersecurity in Development Lending Operations

The discussion highlighted the challenge of underestimating and underfunding cybersecurity initiatives in developing nations, particularly due to limited resources and competing priorities. International institutions like the World Bank were cited for their support to provide resources and technical assistance in addressing this issue.

The moderator for the session was Mr. Oleg Petrov, Programme Coordinator, World Bank, United States of America.

The six member-panel was made of personalities like.

- Dr. Albert Antwi-Boasiako, Director-General, Cyber Security Authority Ghana
- Mrs. Mariama Yormah, National Cybersecurity Coordinator, Sierra Leone
- Mr. Andrew Toimoana, Director, Digital Transformation Department, Government of Tonga
- Mr. Tawhidur Rahman, Senior Technical Specialist (Digital Security), CERT, BCC (Bangladesh)
- Mr. Carlos Leonardo, Director, National CSIRT (Dominican Republic)
- Ms. Anat Lewin, Global Lead, Digital Safeguards, World Bank

Recommendations

- Foster partnerships with development institutions like the World Bank and Council of Europe to establish cybersecurity agencies and align national strategies with global standards.
- Governments should focus on developing a Security Operations Center (SOC) team

to ensure the security of interconnected government systems.

Panel 6

Volunteerism and Other Innovative Approaches to Building Skills in Cyber-Poor Environments

The session identified the challenge of how cyber-poor environments affects both public and private entities making them struggle to combat cyber threats due to a lack of expertise and resources. Scaling up volunteering initiatives was cited as crucial to meet the needs of vulnerable communities.

The panellists comprised:

- Ms. Francesca Bosco, Chief Strategy Officer at CyberPeace Institute
- Mr. Derek Asamoah-Ameyaw, Senior IT Infrastructure at Anglogold Ashanti (GH) Malaria Control (AGAMAL)
- Ms. Silja-Madli Ossip, Community Lead at EU Cybernet
- Ms. Laura Temesi, Head of Cyber Partnerships & Communications at Standard Chartered Bank
- Mr. Maurice Kent, Deputy Cybersecurity at USAID.

Recommendation

- Foster partnerships with development institutions like the World Bank and Council of Europe to establish cybersecurity agencies and align national strategies with global standards.
- Prioritise addressing Critical Information Infrastructure (CII) at national and sectoral levels, focusing on raising awareness among CII owners and children.
- Strengthen cybersecurity measures through continuous awareness creation, skills development, and implementing

cybersecurity bills.

- Enhance regional cooperation and external partnerships to collectively address cybersecurity challenges, leveraging shared expertise and resources.
- Emphasise the importance of legal frameworks and ongoing projects in sectors like health and energy, while advocating for research collaboration to address evolving cyber threats effectively.

Panel 7

Sharing is Caring: Strategic Role of Information Sharing in the African CERT Community.

This session focused on the strategic importance of information sharing within the African CERT community. It addressed key themes such as the necessity for a strong legal framework, national cyber crisis management plans, and proactive preparedness measures to enhance resilience against cyber threats. Panellists shared insights on various aspects of information sharing, including collaborative efforts, regulatory frameworks, and the importance of a National Cyber Crisis Management Plan.

Mr. Jean-Robert Hountomey from Africa CERT served as the moderator for the panel discussion, which included panellists such as:

- Ms. Brenda Atoa from CERT Tonga
- Mr. Mustafa Hazem from OIC-CERT, Organisation of the Islamic Cooperation
- Ms. Sithembile Songo from Public Investment Corporation
- Mr. Koichiro Komiyama from Asia Pacific CERT, Japan CERT
- Mr. Kaleem Usmani from CERT Mauritius.

Recommendations

- Establish clear policies and procedures governing information sharing to ensure reliability, capability, and credibility of

shared data.

- Leverage automation and implement effective filtering mechanisms to enhance information systems resilience against cyber threats.
- Encourage regional collaboration among CERTs to address common cybersecurity challenges, balancing decisions based on the needs and aspirations of various stakeholders.
- Develop and implement National Cyber Crisis Management Plans to facilitate coordinated responses to cyber incidents and ensure effective information sharing among different sectors and organisations.
- Promote cross-country sharing of threat intelligence, tools, and repositories to enrich cybersecurity knowledge and enhance collective cybersecurity efforts.

Panel 8

It Takes a Village! The Community Behind Successful Technical Capacity

The session focused on the importance of building robust technical capabilities, organisational structures, and a skilled workforce for effective cyber capacity building. It further emphasised the need for comprehensive strategies beyond skills training, including policy development and implementation plans. Additionally, it addressed the challenges posed by the informal nature of cybersecurity communities.

The panel discussion was moderated by Mr. Kleen Aiken, Director of Community and Capacity Building at the Forum of Incident Response and Security Teams (FIRST) in New Zealand moderated the discussion. The panellists were:

- Ms. Audrey Mnisi Mireku, FIRST Board Member and WiCyS West Africa Vice President
- Mr. Alwell Mulsid, President of PH Cyber Units in the Philippines

- Ms. Sametria McKinney, Director of Bahamas' National Computer Incident Response Team (CIRT-BS)
- Ms. Letitia Masaea, Board Member of the Global Forum on Cyber Expertise (GFCE) Advisory Board.

The panellists during the session recommended that, to address cybersecurity challenges effectively, it's crucial to adopt a multifaceted approach. This involves implementing a combination of regulatory measures, technological innovations, and capacity-building initiatives.

Recommendations

- Advocate for a multifaceted approach to resolving cybersecurity issues, rather than relying solely on a single strategy.
- Recognise the diverse nature of cybersecurity threats and vulnerabilities, emphasising the importance of adopting a comprehensive toolkit of strategies.

Panel 9

Not All About the Money: How Low-Income Countries Can Strengthen Their Cyber Resilience.

The discussion sought to contribute to two key areas.

- How PPPs can be used to support the development of effective cybersecurity services, including well-resourced national CERTs and cutting-edge SOCs?
- Lessons from countries like Togo regarding institutional, legal, and financial arrangements that are relevant for public-private partnership in other low-income countries?

Submissions from the panel members cited Togo's efforts in cyber resilience. This includes the establishment of efficient and sustainable cybersecurity ecosystem through innovative public-private partnership and highlighted the innovative financing arrangement by the ECO Bank Group for the Cyber Defence Africa project.

The panellists included:

- Mr. Gbota Gwaliba - Director General of the National Cybersecurity Agency of Togo.
- Mr. Simon Melchior - Co-Founder & General Director, Cyber Defense Africa
- Mr. Souleymane Toure - Managing Director, Ecobank, Togo
- Ms. Anat Lewin - Global Lead for Cybersecurity, World Bank

Recommendations

- Develop tailored cybersecurity products and services for developing nations, focusing on modularity and scalability.
- Emphasise the role of public-private partnership in delivering training programs and establishing cyber academies in countries with limited capacity.
- Advocate for quality assurance in cyber defense services through government regulations and technical audits.
- Replicate successful cybersecurity models across African nations, fostering collaboration to fortify cybersecurity protocols and safeguard businesses.
- Prioritise incident response, risk management, skills development, and ecosystem and industry development in cybersecurity initiatives.
- Adopt affordable solutions, participatory partnerships, and robust governance mechanisms to bolster cybersecurity frameworks in low-income countries.

Launch of Outcome Document on Ghana and World Bank Collaboration in Cybersecurity

During panel session 5 (Integrating Cybersecurity in Development Lending Operations) under Pillar 3 of the event, an outcome document on Ghana and the World Bank's collaboration in Cybersecurity was launched. This document explores how Ghana has become a regional leader for cybersecurity, focusing on the key milestones and decisions made by Ghana's government, the results delivered to Ghana's economy and society, and the lessons learned that could be applied by other countries seeking to strengthen their cyber resilience.



PILLAR 4

Operationalising Solutions

This cross-cutting, horizontal pillar focused on advancing practical solutions that are of immediate assistance to those working in the field, protecting their development work from digital risks and threats. The outcomes showcased more demand-driven cybersecurity and capacity building solutions or practical initiatives.

Panel 1

Banking on Financial Inclusion: How to Make Africa's Digital Financial Services Cyber Resilient

The session, moderated by Ms. Nanjira Sambuli, a Fellow in the Technology and International Affairs Programme, Carnegie Endowment for International Peace, revolved around enhancing cooperation and information exchange among diverse stakeholders, focusing on pinpointing obstacles to resilience and gleaning valuable insights from the financial services sector that could be extrapolated to other industries.

Featuring a distinguished panel comprising:

- Mr. Brett DeWitt, Vice President of Global Cybersecurity and Technology Policy at Mastercard
- Ms. Laura Temesi, Head, Cyber Partnerships and Communications, Standard Chartered Bank
- Mr. Mark Koulibali, Bank National Invest Small, Ivory Coast
- Mr. Jean-Louis Perrier, Programme Director, Africa Cyber Security Resource Centre Programme

The discussion delved into strategies to bolster collaboration and knowledge sharing in the realm of cybersecurity.

Some recommendations from the session were.

- Emphasise the importance of digital financial inclusion in Africa, driven by mobile banking platforms, but highlight the need for robust cybersecurity measures.
- Address barriers such as unauthorised access to clients' funds and advocate for procedures to handle such incidents, as well as the protection of client information.
- Advocate for effective regulatory frameworks ensuring the accountability

of Financial Service Providers offering electronic services and stress the importance of supervisory authorities in monitoring, enforcing cybersecurity standards and compliance within the financial sector.

- Encourage financial service providers to educate customers about fraud prevention measures and raise awareness about identity theft and social engineering schemes.
- Advocate for transparent reporting mechanisms for cybersecurity incidents within the financial sector, promoting accountability and facilitating collective learning from past incidents.
- Support initiatives that foster collaboration and information sharing across borders to strengthen cybersecurity resilience regionally and globally.

Panel 2

Powering Up Against Cyber Threats: Cyber Resilience in the Energy Sector

The session focused on the potential of distributed energy systems to improve system resilience, emphasising the critical need for robust cybersecurity planning. With the digitalisation of electricity distribution companies and the vast consumer data they manage, the energy sector faces increased vulnerability to data breaches and cyberattacks. As nations advance towards renewable energy generation and modernise transmission infrastructure, ensuring cyber preparedness emerges as a pressing concern for energy stakeholders. Insights gleaned from challenges, practices, lessons, and solutions in the energy sector offer valuable guidance applicable

to sectors like water and transport, and to cybersecurity experts seeking to enhance system resilience overall.

The panel for this session had Mr. Anders Pedersen, Senior Energy Specialist, serving as the moderator, along with

- Mr. Prince Wiredu Darfour, SCADA | ICS Engineer
- Mrs. Jamila Amodeo, Senior Energy Advisor
- Mr. Gulakhmadov Aminjon, Deputy Head of Energy Department
- Mr. Hagai Mei-Zahav

Recommendations

- Establishment of cybersecurity governance within the energy sector to oversee and manage cyber risks effectively.
- Conduct sector-wide risk assessments encompassing all entities within the energy sector, including power generators, transmission, and distribution entities, to ensure comprehensive cybersecurity preparedness.
- Formulate a comprehensive cyber resilience framework tailored to the energy sector's unique needs, incorporating preventive measures, incident response protocols, and recovery strategies.
- Include cybersecurity clauses in contracts with service providers to ensure adherence to security standards and protocols, enhancing overall cyber resilience.
- Conduct regular vulnerability assessments of energy grid systems, including Supervisory Control and Data Acquisition (SCADA) systems, to identify and address potential weaknesses before they can be exploited by cyber threats.
- Implement continuous monitoring protocols for Internet of Things (IoT) devices deployed within energy grids to detect and prevent cyberattacks in real-time.
- Align cybersecurity efforts with broader developmental activities and government agendas to ensure sustainable and integrated approaches to cyber resilience.

Panel 3

Driving a Change from Within: Bottom-Up Approaches in Criminal Justice Capacity Building

The session stressed the vital role of criminal justice authorities in managing cybercrime and electronic evidence for economic growth and democratic governance. Despite significant international investments in capacity enhancement, externally facilitated initiatives often lack sustainability. Locally driven capacity-building efforts offer a more promising avenue for lasting change.

The panellists included:

- Dr. Alexander Seger, Cybercrime Division of the Council of Europe, France
- Ambassador Claudio Miguel Peguero Castillo, Ambassador for Cyber Matters, Ministry of Foreign Affairs, Dominican Republic
- Ms. Tatiana Cesario, Assistant Prosecutor, Public Ministry of Paraguay
- Mr. Athul Harilal, Head of Threat Intelligence Research, Uppsala Security, Singapore
- Mr. Sêvi Rodolphe Adjaigbe, Legal Advisor, Information Systems and Digital Agency, Benin
- Mr. Dong Uk Kim, Specialised Officer, Cybercrime Directorate, INTERPOL

Recommendations

- Sustainable cyber capacity building strategies through development, implementation training programmes that inure to capacity building.
- Enhanced collaboration and inter-agency cooperation recognise and address matters relating to capacity building.
- Ensure training programs are inclusive and practical.
- Adopt a gradual approach to capacity building through initiatives such as GLACY+ and INTERPOL IDC programs.

- Equitable access and collaboration with both public and private sectors.
- Policy support and budget allocation for sustainable criminal justice development.
- Legislative support for sustainability of training programs.

Panel 4

Hope for the Best, Prepare for the Worst: Developing National Cyber Crisis Management Plan

The panel discussion, held by NRD Cybersecurity, addressed the escalating frequency and complexity of cyber incidents, which pose potential crises impacting national security, economy, and foreign relations. With investments in cyber incident management institutions like CERTs and SOCs, the current emphasis is on crafting comprehensive national incident and cyber crisis management plans. Understanding how states define cyber crises and delineate key responsibilities at strategic and operational levels is crucial for fostering international cooperation. Two key considerations were.

- Essential capabilities and resources required for effective national cyber crisis management plans.
- Pertinent lessons from managing major cyber incidents and crises, especially relevant for developing countries.

Panellists included:

- Mr. Sanusi Drammeh, Director of Cybersecurity, Ministry of Communications and Economy, Gambia
- Mr. Tarique Mosaddique Barkatullah, Cybersecurity Expert and former Director of BGD eGov CIRT, Bangladesh
- Ms. Sametria McKinney, Manager of Bahamas National CERT
- Mr. Carlos Leonardo, Director of CSIRT, Dominican Republic

Dr. Tadas Jakstas, NRD Cyber Security Senior

Expert was the moderator for the session.

Recommendations

- Emphasise the importance of National Cybersecurity Emergency Response Teams (CERTs) in managing cyber crises. Countries should focus on developing and strengthening these teams to effectively respond to cyber incidents.
- Recognise resource constraints, especially in small island states, and leverage existing frameworks like the National Emergency Management Agency to enhance cyber crisis response capabilities.
- Establish clear cyber crisis thresholds and definitions to facilitate effective crisis management. Foster transparent communication and coordinated responses among stakeholders to mitigate cyber threats effectively.
- Strengthen cooperation between strategic and operational levels in crisis management governance. Define rules and procedures for stakeholder engagement and ensure effective capabilities to mitigate cyber crises.
- Encourage collaboration and information sharing among government agencies, international organisations, and critical infrastructure representatives to address large-scale cyber incidents effectively.
- Prioritise capacity-building efforts to nurture local talent and expertise in cybersecurity.

Panel 5

Think Global, Build Local: The Role of Regional Cyber Capacity Centres

This session focused on the importance of regional cybersecurity centre. It explored some of the different aspects models that government, civil society and industry have put in place to dive capacity building on a regional level.

The six-member panel comprised individuals such as

- Mr. Siosaia Vaipuna, Director of the Global Forum on Cyber Expertise (GFCE) Pacific Hub
- Ms. Liina Areng, Director of the European Union (EU) Cybernet/Latin America and Caribbean Cyber Competence Centre (Lac4)
- Ambassador Tadej Rupel, National Coordinator for External Efforts of Digitalisation, AI & Cybersecurity, Slovenia
- Mr. Giacomo Assenza, Digital Development Specialist at the World Bank
- Mr. Gilles Schwoerer, Cyber Project Manager for the Government of France

The session was moderated by Ms. Kaja Ciglic, Senior Director at Microsoft.

Recommendations

- Recognise the pivotal role of regional capacity centers in enhancing local, regional, and international ownership, particularly in cybersecurity efforts.
- Advocate for the establishment of cybersecurity centers to share knowledge from existing projects globally and foster collaboration among stakeholders.
- Conduct assessments of specific regions and their cybersecurity needs to tailor solutions, accordingly, considering the diverse challenges across regions.
- Ensure adequate funding and transparent decision-making processes.
- Aim to support the host country and prioritise regional ownership.
- Develop training programs tailored to regional needs.
- Acknowledge the World Bank's financing mechanisms for digital development programs and cybersecurity projects.
- Highlight the World Bank's engagement with national governments and regional entities to coordinate capacity-building efforts.
- Emphasise the importance of political commitments from host nations for the sustainability and effectiveness of regional hubs.
- Advocate for impactful programs targeting specific capability gaps in the region.

- Promote collaboration among various stakeholders, including private sector, academia, regional organisations, and NGOs, to avoid duplication of efforts and ensure regional ownership.

Panel 6

Sharing the Success: Lessons for Developing Effective Cyber Capacity Partnerships

The aim of this session was to highlight the importance of a partnership approach to cyber capacity building, emphasising the need to bridge gaps between governments, the private sector, and other actors.

The panellists for the session were:

- H.E Regine Grienberger, Cyber Ambassador for German Federal Foreign Office, Berlin
- Mr. Christopher Banda, Head of Malawi CERT
- Ms. Rebecca Stewards, co-SRO Cyber Capacity Building Programme, United Kingdom Government - Home Office,
- Mrs. Vanessa Copetti Cravo, Cybersecurity Technical Group, ANATEL, Austria
- Mr. Samuel Tew, Principal Consultant, AXON Partners Group, Spain
- Yasmimi Idrissi Azzauzi, ITU who doubled as the moderator.

Recommendations

- Cyber capacity partnerships approach must shift from isolated activities to collaborative initiatives with organisations like the ITU.
- Collaboration should be prioritised to ensure efficient resource use and avoidance of duplication.
- Clarity on goals, mapping benefits, senior sponsorship and government commitment are essential components of successful cyber capacity partnerships.
- Criteria for selecting partners should focus on alignment of objectives, effective

absorption capacity, a favourable governance environment, robust reporting, and potential short-term and long-term impacts.

Panel 7

Thinking Out-Of-The-Box to Inspire a New Generation of Cybersecurity Talent

The Head of Industry and Partnerships Centre for Cybersecurity World Economic Forum, Mr. Akshay Joshi, the moderator for the panel discussion highlighted the urgent need to take steps to the massive shortage of cybersecurity talent.

Panellists include:

- Ms. Apisada Suwansukroj Communications and Digital Technology Programs Manager for Digital Asia Accelerator
- Mr. Adnan Rahman a Bangladeshi Consultant and researcher
- Ms. Danielle Santos, Lead for International Engagement for the National Initiative for Cybersecurity Education at the National Institute of Standards and Technology in the USA
- Mr. Byers Stanley
- Mr. Akshay Joshi, Head of Industry and Partnerships Centre for Cybersecurity World Economic Forum

Recommendations

- The key to designing any approach to a program is to ascertain how the target audience understands the issue as it helps determine the strategy to implement.
- Society should adopt and apply the ABC theory to make the job of cybersecurity professionals easier.
- Cybersecurity career campaigns must be more contextualised, and the messaging should resonate with the target audience.
- Aspiring cyber professionals must strive

to demonstrate innovation, proactiveness in problems, and a high level of integrity and responsibility. Government and stakeholders should reach out to young children, educate them, and create awareness on the various career paths in cybersecurity.

- Cybersecurity experts should act as role models so they can share their experiences and journey with the younger ones.

Panel 8

Hacking the Gender Gap: Unconventional Strategies for Women's Inclusion in Cybersecurity

This session as part of the GC3B was organised to seek the opinions and inputs of experts particularly women in bridging this persistent gender gap.

The panel was made up of:

- H.E Slavica Grkovska, Deputy Prime Minister of North Macedonia
- H.E Brendan Dowling, the Ambassador for Cybersecurity, Australia
- Mrs Manjusha Marar, Cybersecurity Associate, ACPL Systems PVT Ltd and Cybershikshaa Alumni
- Ms. Confidence Staveley, Founder of Cybersafe

Recommendations

- Initiatives specifically targeting women should be implemented, such as the Cyber Pathway for young girls and women funded by the USAID.
- Foster inclusivity by considering women with disabilities, socially and economically vulnerable girls and women, showcase role models and mentors to provide inspiration and guidance to girls and women seeking to delve into the profession.
- Developing and promoting skills academies that are designed to favour women returning to work or looking for a career

change.

- To address the gender gap, infrastructural needs must be met to provide access to devices and internet connections to girls and women to aid learning.
- Industry leaders must refrain from gender stereotypes against women in the field of cybersecurity.
- Introduce more cybersecurity scholarships like the Cybershikshaa program for rural areas.
- There is a need to create end-to-end programs for girls who are not knowledgeable in cybersecurity.
- Social media leveraged as a “tool for evangelism”, to tell the stories of women in cybersecurity.
- The private sector should play a more leadership role in promoting cybersecurity by collaborating with universities to attract a pool of females into the field.

Panel 9

Stars, Clouds and Deep Seas; Improving Secure Access to Communications Technology

The deliberations focused on the technical aspects of cybersecurity and most especially the physical Infrastructure and the functions necessary to enhance their resilience.

Ms. Melanie Garson, Cyber Policy & Tech Geopolitics Lead at the Tony Blair Institute for Global Change moderated the discussion and introduced the distinguished experts as:

- Ms. Towela Nyirenda-Jere, Head of Economic Integration, African Union Development Agency (AUDA-NEPAD)
- Ms. Manon Le Blanc, Coordinator for Cyber Issues, European Union - European External Action Service
- Mr. Giacomo Persi-Paoli, Head of Security and Technology Programme, United Nations Institute for Disarmament Research (UNIDIR)

- Ms. Patricia Ephraim Eke, Director, Global Cybersecurity Policy, Microsoft.

Recommendations

- Submarine cables should be designated as Critical Information Infrastructure, and invest more into the protection, maintenance, and recovery of submarine cables.
- Cybersecurity preparedness should extend beyond technical readiness to include regulatory preparedness, for example, the 1967 space treaty and the 1974 and 1976 registration convention as relevant to cloud regulation.
- Policy developers should utilise international, risk-based policies, standards, and regulations such as the ISO/IEC to leverage consensus.
- Countries with limited resources should prioritise strengthening submarine cables, crucial for connectivity.
- Effective collaboration among cybersecurity governance makers and technology owners to understand evolving cyber-attacks and threats and enhancing the advantage of cyber defenders.

Panel 10

What it Takes! Scaling Cybersecurity Tools and Solutions

Ms. Komal Bazaz Smith, the event's moderator, identified four specific areas were for focus: cultural and socio-economic indicators, scalability, impact, and collaborative partnership models.

Speakers at the event were:

- Ms. Komal Bazaz Smith, Chief Business Officer at Global Cyber Alliance
- Ms. Audrey Mnisi Mireku, First Board Member and WiCyS West Africa Vice

President

- Ms. Toni Friedman, Assistant Director, Digital Technology, Policy and Innovation at Asia Foundation
- Mrs. Elizabeth Vish, Senior Advisor, International Cyber Engagement at Institute for Security and Technology
- Mr. Osama Manzar, Founder & Director, Digital Empowerment Foundation
- Mr. Ernest Dugbatey Opare, Security Strategist and Cyber Diplomacy Specialist at the Cyber Intelligence and Security Aid Bureau
- Ms. Terdoofan Agber, Product Owner, Global Anti Scam Alliance
- Ms. Jordan Mathews, Cyber Specialist, KPMG, UK.

Recommendations

- Cultural nuances should be addressed when advising individuals to behave responsibly in the digital realm.
- Prioritise face-to-face communication for sustainable and scalable models before transitioning to digital solutions.
- Small Medium Enterprises (SMEs) should be incentivised to invest time in implementing cyber toolkits.
- Customise foreign cybersecurity initiatives to align with the local environment, aligning foreign strategies to yield results.
- Governments must prioritise cybersecurity and allocate resources tailored to their specific environment.
- Resources like the GCA toolkit can serve as effective alternatives for organisations facing financial constraints, to carry out activities and create awareness in their communities.
- Qualitative approaches like confidence in reaching out for assistance, actual usage of assistance, and the impact of information provided by entities such as the CERT should be used to evaluate impact of initiatives.



Side Events



The Cyber Security Authority organised two side events as part of scheduled activities for participants of the Global Conference on Cyber Capacity Building (GC3B).

The first event was a tour to selected cybersecurity establishments in both government and private sectors and some historical sites in Ghana. The primary goal of the visits to the cybersecurity establishments was to showcase Ghana's success in implementing a decentralised approach to information sharing and incident response through the establishment of Sectoral CERTs. Also, it was to give participants an insight into the daily operations, technologies, and strategies employed for monitoring and

responding to cybersecurity threats. In all, three establishments were visited namely the National Communications Authority CERT, National Information Technology Agency - Security Operations Centre (SOC) and ODUMA Solutions - CERT. The tour was preceded by a debrief session at the Cyber Security Authority.

The second was a visit to selected historical sites in the Greater Accra and Central regions of Ghana. Places visited in Accra included the W.E.B Du Bois Centre, National Museum of Ghana, Jamestown Lighthouse, Accra Arts Centre, Independence Arch and Black Star Gate. For Cape Coast it was the Elimina Castle. Participants expressed a lot of sentiments for the nostalgic moment spent after a very packed conference.

CSA

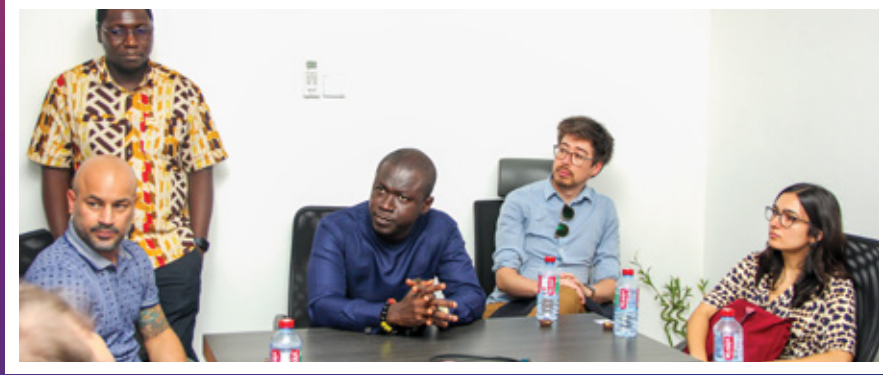
Cyber Security Authority



NCA

National Communications Authority







Closing Ceremony

Closing Ceremony

Introduction

The Global Conference on Cyber Capacity Building (GC3B) ended in Accra on a positive note with the delegates endorsing the Accra Call for a global cyber resilience. Hundreds of delegates from more than 100 countries participated in the maiden event held on the theme “Cyber Resilience for Development.”

Speakers

Mr. Daren Smith,
Expert in CERT

Mr. Smith called on industry players to help with social progress in realising the Accra Call. He added that “we need to work as cyber security professionals not to have biases but to work towards a more diverse future and keep striving for a safer digital future.”

Mr. Sanjay Vayas,
Ministry of Electronics and IT, India

He said digital infrastructure was the sine qua non of bridging the digital connectivity gap. According to him, users of digital tools ought to be empowered to maximise the benefits of the internet. He stated that India was making use of Digital Public Infrastructure (DPI) as a key area to provide innovative solutions to users. He added that India had adopted DPI as a global recognition of its approach to development.

“The success of DPI can serve as a blueprint for digital payment in other countries like the UAE and Singapore. DPI holds potential for achieving the SDGs,” he added.

Mr. Mocta Seck
Chief of Section, Technology and
Innovation, United Nations Economic
Commission for Africa (UNECA)

He said the global digital economy was expected to hit US\$180 billion by 2025, as cybersecurity costs ten percent of Africa’s gross domestic product (GDP). He stated that the UNECA worked with GFCE to build the capacity of African countries and other civil society institutions on cybersecurity.

He said currently, there is a gap of 3.5 million cybersecurity professionals in Africa, coupled with the fact that about 500 million people on the continent are without internet access or social services.

“So, there is a need to develop a cybersecurity architecture in Africa to protect our citizens. Our member states must make an input in this regard,” he stressed.

Madam Pei Ling Lee

Head of Cyber Strategy and Capacities Development, INTERPOL

She underscored the need for capacity-building in the effort to ensure cyber resilience. She said INTERPOL believed in cooperation based on the values of human rights and sovereignty, adding that capacity building must be sustainable.

She remarked that INTERPOL believed capacity building must lead to operational outcomes, for

which reason the organisation had embarked on initiatives to build the capacity of some African countries, including Tanzania, for citizens to undergo training in cybercrime investigations and the takedown of malicious activities and malware sites, among other nefarious cyber activities.

“Capacity building requires cooperation by states and stakeholders with the aim of narrowing the digital divide. We are looking forward to further cooperation. We are supportive of open working groups through a tailored capacity-building process,” Madam Lee added.

Mr. Claudio Peguero

Cyber Ambassador, Dominican Republic

He said his country attached importance to capacity building and the Council of Europe’s Global Action on Cybercrime. He stated that the Dominican government was considering including cybersecurity training programmes in its school curricula. While endorsing the Accra Call, he added that diplomats in the Dominican Republic would equally have the benefit of receiving training in cyber diplomacy.

Mr. Chris Gipson

Executive Director, Forum of Incidence Response and Security Teams

Mr. Gipson described global coordination as key to achieving results, along with building a network of computer emergency response teams across the world. He advocated for a global language to help incident response teams speak the same language within the context of having a common understanding of situations. “Having a global community of incident response is what we aspire to achieve. There’s a lot to reach out to. The Accra Call is a miracle that I am excited to endorse,” he indicated.

Ms. Francesca Bosco

Chief Strategist and Partnership Officer,
CyberPeace Institute

She urged action rather than words if the Accra Call and the fight against global cybercrime are to be realised.

She stated that the CyberPeace Institute would launch a few initiatives, such as a CyberPeace Watch and an internet platform for cyber capacity building. He indicated that the

CyberPeace Institute would increase its cyber capacity building programmes to promote cyber preparation and ensure needs-driven methods to prepare for disruption convergence.

Madam Philis Camal

Head of Visa, Sub-Saharan Africa

She said Visa processes about 14 trillion transactions each year and that the institution has invested US\$10 billion in technology.

She said this was the time to build cyber security resilience, and Visa stood ready to build the resilience to fight fraud and pursue best practices and standards to build cyber security

and resilience, as it was always at the heart of Visa to lead those initiatives.

“Capacity building for our consumers, regulators, and policymakers is key, and Visa is willing and happy to sustainably move forward in cyber resilience and to support the Accra Call,” she added.

Madam Thelma Quaye

Director, Digital Infrastructure,
Smart Africa

She said Smart Africa has a membership of 39 countries with more than 60 stakeholder members. She explained that the organisation’s approach is multi-stakeholder collaboration and that it has set up a cyber security innovative centre in Cote d’Ivoire to train 1000 youth in cyber security and to develop cybersecurity talents.

Madam Quaye announced Ghana’s assumption of the chairmanship of the Africa Network of Cybersecurity Authorities (ANCA), with the Director-General of the Cyber Security Authority at the helm.

Speech by Mr. Chris Painter, President, GFCE



Mr. Painter extended his sincere gratitude to the Government of Ghana, for graciously hosting the conference and showing its warm hospitality and sharing Ghana's beautiful culture.

He equally extended appreciation to the GC3B co-organising partners – the CyberPeace Institute, the World Bank, and the World Economic Forum, who he said have been on this journey with the GFCE since 2021.

“I also wanted to give a special shoutout to the US State Department and the Netherlands Ministry of Foreign Affairs and the UK government for providing additional financial support, giving us the final push”.

Mr. Painter was full of praise to the speakers for

their dedication that had made the GC3B a resounding success, noting the energy, passion, and expertise they brought to Accra and that made the conference a truly impactful and memorable one.

“The Accra Call, a product of our collaborative efforts, stands as a beacon of our shared commitment to advancing cyber capacity building. It serves as a high-level roadmap with clear actions that address the needs and priorities of developing countries in their journey towards improved cyber resilience,” Mr. Painter said.

According to him, the Accra Call was not just a document but a pledge, a covenant, a testament to a dedication to a safer digital future and added that the call remained open for further endorsements.

Remarks by Hon. Minister of Communications and Digitalisation, Mrs. Ursula Owusu-Ekuful



The Minister, in her concluding remarks, urged all to make the Accra Call a reality, saying that the declaration was meant to be an actionable item to build a resilient cybersecurity framework for Africa.

She spoke about the relationships that have been shared and expressed the hope that the network of contacts that took place at the GC3B would be kept and sustained.

She congratulated the participating schools in the National Cybersecurity Challenge and said

the winners were champions who would serve as role models for others.

“We are determined to make Ghana the digital blackstar in Africa, and we are working actively towards that, hoping it will be another milestone to build a resilient online experience,” Mrs. Ursula Owusu-Ekuful added.

According to her, cybersecurity was both a technical and societal concern and must become a way of life in a world that is digitally interconnected.

National Cybersecurity Challenge

The 2023 National Cybersecurity Challenge was won by the OLA Girls' Senior High School (SHS) from Ho in the Volta Region, after defeating Prempeh College, Wesley Girls' High School (Wey Gey Hey), and Navrongo SHS (NAVASCO).

OLA Girls' SHS finished with 45 points, Prempeh College and Wey Gey Hey tied for second place with 38 points each, and NAVASCO finished third with 34 points.

OLA Girls' SHS received a GH¢7,000 cash reward, a trophy, a laptop, branded souvenirs and certificates of participation as its prize. Prempeh College and Wey Gey Hey each received GH¢3,500, branded souvenirs, a laptop and certificates of participation.

The Navrongo SHS earned GH¢2,000, a laptop, branded souvenirs and certificates of participation.

The competition was held at the Cedi Conference Centre at the University of Ghana, and the awards were presented at Kempinski Hotel as part of activities marking the closing ceremony of the GC3B.



Dinner Night

To culminate the GC3B event, a gala dinner was organised, featuring a vibrant cultural showcase and musical performances celebrating the diverse heritage of Ghana. The dinner followed the opening ceremony and was graced by esteemed guests from various prominent organisations including the Ministry of Communications and Digitalisation, the World Bank, the World Economic Forum, CyberPeace Institute, and GFCE. The dinner was attended by over 500 participants.

As part of the evening's event, the GFCE Africa Hub was launched. The regional hub, which is a result of a collaboration between the African Union and the GFCE, aims to support African Union member states in developing their cyber capabilities.







The Accra Call

The Accra Call and its Significance to Cybersecurity Development in the Country and the World at Large

The Accra Call for Cyber Resilient Development: An Action Framework, is the outcome document of the inaugural Global Conference on Cyber Capacity Building (GC3B) that was held on November 29-30, 2023 in Accra, Ghana, under the theme: “Cyber Resilience for Development”.

It aims to stimulate action and voluntary commitments to elevate cyber resilience across international and national development agendas as well as promote cyber capacity building that supports broader development goals and effectively serves the needs and priorities of developing countries.

By signing the Accra Call, governments, development donors and partners, multilateral and bilateral financial institutions, international and regional organisations, the private sector, the technical community, civil society, academia, and philanthropic institutions, and organisations across all sectors and regions affirm their willingness to voluntarily promote, pursue and coordinate efforts on sixteen specific actions to elevate cyber resilience across international and national development agendas through the actions below.

- Strengthen the role of cyber resilience as an enabler for sustainable development.
- Advance demand-driven, effective, and sustainable cyber capacity building.
- Foster stronger partnerships and better coordination.
- Unlock financial resources and implementation modalities.

Progress towards fulfilling the Accra Call will be assessed during the subsequent meetings of the GC3B. Between each conference, the Global Forum on Cyber Expertise will foster the multi-stakeholder ‘Accra Call’ community bringing together all its endorsers and pledging organisations, along with any other interested stakeholder. Endorsers will share their experiences from their pursuit of the Call’s actions within their respective mandates. Insights from lessons learned, successes achieved, and challenges faced, will inform collective efforts in following up on the Accra Call at the next GC3B gathering.

By signing the Accra Call, Ghana can leverage partnerships with other nations, international organisations, and private sector stakeholders to bolster its cybersecurity infrastructure, develop cybersecurity policies and strategies, and enhance cybersecurity awareness and education among its citizens.

Furthermore, it has provided a platform for Ghana to participate in global discussions on cybersecurity governance, norms, and regulations, ensuring that its voice is heard and its interests are represented on the international stage ultimately contributing to shape the future of cybersecurity both regionally and globally, and enhancing cybersecurity resilience and safeguarding of digital assets and citizens' privacy in the increasingly interconnected world.



Conclusion

Conclusion

In conclusion, the inaugural Global Conference on Cyber Capacity Building (GC3B) marks a significant milestone in the collective efforts to fortify digital infrastructure and promote cyber resilience worldwide.

The conference ended on a note of optimism from delegates who pledged to make cyber resilience a reality in their respective countries to break free from the escalating cyberattacks.

Switzerland was named the next country to host the GC3B in 2025.

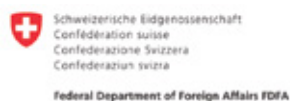
The Accra Call, endorsed by a diverse array of countries and organisations, demonstrates a

shared commitment to fostering a secure and inclusive digital environment for all. The momentum generated by this conference must be leveraged to drive concrete actions and collaborations that strengthen cyber capacity building initiatives globally. Furthermore, the list of endorsing countries and organisations provided in this report reflects the breadth and depth of the collective commitment to this endeavour.

Countries and organisations are hereby invited to endorse the Accra Call through the official website of the Global Conference on Cyber Capacity Building (GC3B).

Endorsers







Ministry of Foreign Affairs
of the Czech Republic



REPUBLIC OF ESTONIA
MINISTRY OF FOREIGN AFFAIRS



REPUBLIC OF SLOVENIA
MINISTRY OF FOREIGN
AND EUROPEAN AFFAIRS



REPÚBLICA
DEL ECUADOR



TRUESEC



Uruguay
Presidencia



UNODC
United Nations Office on Drugs and Crime

VALU*

VISA



**GC
3B**

Global
Conference
on Cyber
Capacity
Building



Photo Gallery

Photo Gallery









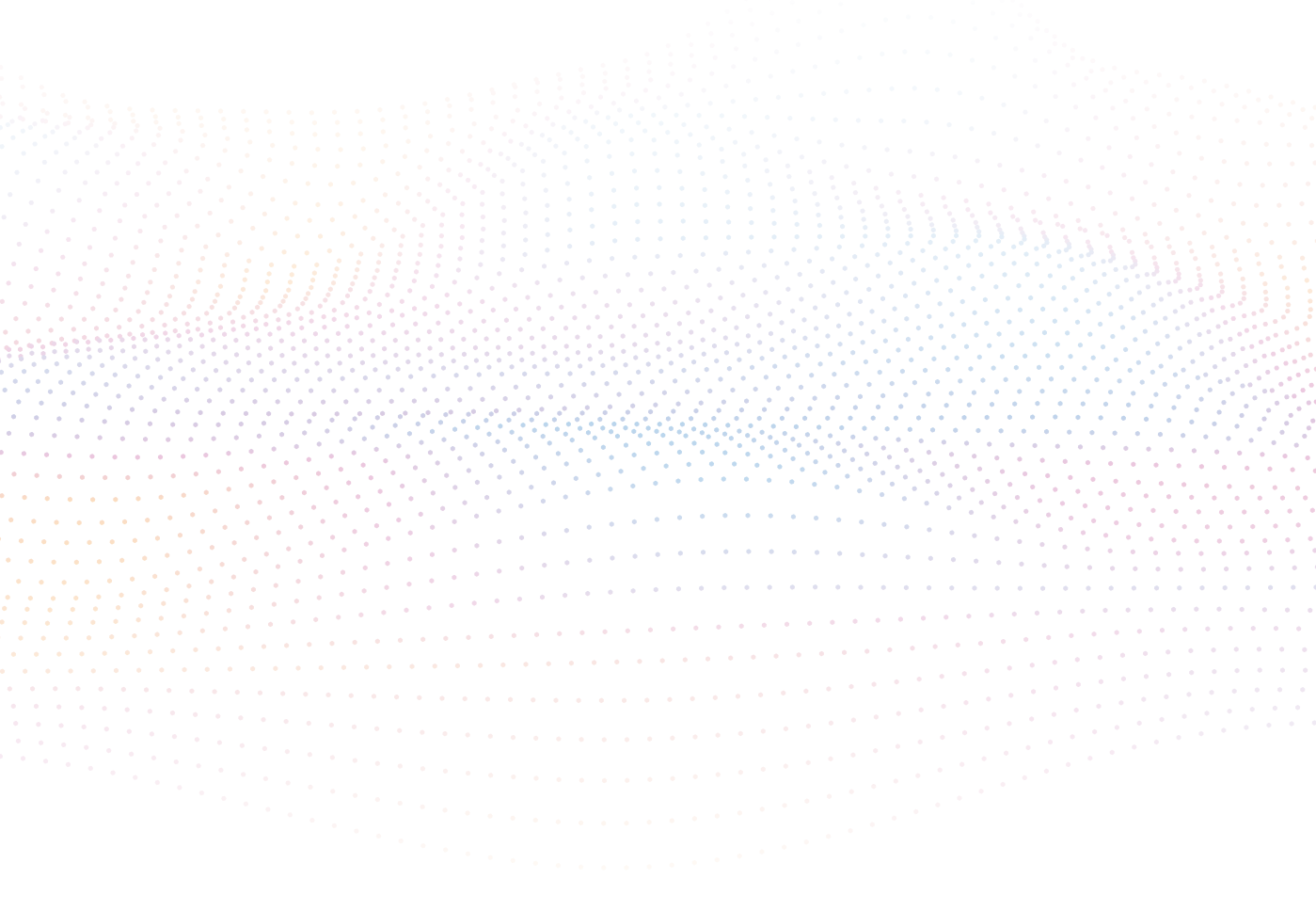




GC
3B



Global
Conference
on Cyber
Capacity
Building





MINISTRY OF
COMMUNICATIONS &
DIGITALISATION



CyberPeace
Institute



THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP

WORLD
ECONOMIC
FORUM

