THE GLOBAL CONFERENCE ON CYBER CAPACITY BUILDING (GC3B): MAKING 2023 THE YEAR OF CYBER RESILIENCE FOR DEVELOPMENT

Written by: CyberPeace Institute; Global Forum on Cyber Expertise (GFCE); World Bank; World Economic Forum.

Although digital transformation and connectivity have boomed in the past decade, digital development programs have not always been accompanied by adequate consideration of digital threats and corresponding investments in cybersecurity and cyber resilience. As such, many countries are now experiencing new risks, greater vulnerabilities, and a rise in malicious activities that are threatening the security of their digital services and critical infrastructure – all while eroding trust in the digital environment and institutions. In order to bridge the gap and move toward cyber resilient development, the inaugural Global Conference on Cyber Capacity Building (GC3B) will bring together decision-makers, practitioners, and experts to catalyze global action on mainstreaming cybersecurity, cyber resilience, and cyber capacity building (CCB) across the international development agenda as well as raising awareness of how cybersecurity and cyber resilience are key enablers of sustainable development, economic growth, and social prosperity.

Co-organized by the CyberPeace Institute, the Global Forum on Cyber Expertise (GFCE), the World Bank, and the World Economic Forum, the Global Conference on Cyber Capacity Building (GC3B) is gearing up to host its inaugural event in 2023.

The theme of the first-annual GC3B is "Cyber Resilience for Development."

The conference emerged from a recognition that cybersecurity, cyber resilience, and cyber capacity building (CCB) are critical enablers of digital transformation and social and economic development. Over the past decade alone, the number of Internet users has more than doubled from around 2.25 billion to over 5 billion people worldwide, largely driven by growth in developing countries – many of which are prioritizing digitalization and connectivity. By embracing and embedding information and communications technologies (ICTs) into their networked environments and infrastructure, countries around the world seek to improve productivity, foster economic growth, enable skills development, and much more.

The Importance of Cyber Resilient Development

While each country's development requirements may be unique, some common technological building blocks include, at minimum, a national digital identifier layer, a digital payments layer, and a data protection layer. Their application to vital services, like the healthcare sector, is critical to the success of countries' digital transformation.

Yet, digital development programs and robust digitalization in developing countries have not always been accompanied by adequate consideration of digital threats and corresponding investments in cybersecurity and cyber resilience. Coupled with the rapid proliferation of new threats and an ever-changing security landscape, many countries are now experiencing new risks, greater vulnerabilities, and a rise in malicious activities that are threatening the security of their digital services and critical infrastructure, all while eroding trust in the digital environment and institutions.

Cybersecurity and cyber resilience must therefore be mainstreamed into all development programs, modern infrastructure projects, and national digital transformation strategies. Not doing so can undo decades of progress related to countries' digital development due to the accumulating risks that are not always fully considered or mitigated, but also because of the debilitating impact that the lack of such resilience has on the ultimate beneficiaries of digital development: the people who use and rely on these systems.

To adequately support and safeguard their digital and economic development, countries must make cyber resilience a key priority. Realizing this goal demands multi-stakeholder engagement and cooperation, clear policy focus, and increased investment in managing cybersecurity risks, building cyber capacity, and ultimately ensuring public trust in digitally enabled systems. Doing so is paramount to realizing the digital transformation objectives of states and other actors across the globe as well as the United Nations' Agenda 2030, particularly since each of the 17 UN Sustainable Development Goals (SDGs) either include digital components or can be augmented and realized via digital technologies ranging from monitoring to implementation.

The field of international cyber capacity building has emerged over the last decade to share knowledge and assistance for strengthening national cyber resilience. This work is being advanced by a multi-stakeholder community, and there is great potential for deeper cooperation, collaboration, and connection between this field and the international development community, to the benefit of both. Realizing this potential and avoiding duplication of efforts, while also maximizing resources, will be a central aim of the conference.

Figure 1. Global Conference on Cyber Capacity Building (GC3B).

Aims, Objectives, and Expected Outcomes

Built upon four pillars – (1) Making International Development Cyber Resilient; (2) Collaborating to Secure the Digital Ecosystem; (3) Cyber Capacity Building for the Stability and Security of the Digital Environment, and (4) Operationalizing Solutions for Safeguarding Development from Digital Risks and Threats – the GC3B will bring together decision-makers, practitioners, and experts to catalyze global action on mainstreaming cybersecurity, cyber resilience, and cyber capacity building across the international development agenda as well as raise awareness of how cybersecurity and cyber resilience are key enablers of digital, social, and economic development and critical to achieving the SDGs.

The GC3B 2023 is anticipated to:

- Develop a demand-driven and international Global Cyber Capacity Building Agenda for cyber resilient development;
- Enhance CCB efforts by accelerating current multi-stakeholder cooperation and public-private partnerships;
- Mobilize global action, promote coordination mechanisms for CCB at the global and regional levels, and encourage funding of CCB;
- Advance good practices and tools for the protection of critical infrastructure; and
- Showcase examples from developing countries, particularly across the Global South, that have effectively incorporated cybersecurity and resilience into their development strategies and infrastructure projects and successfully coordinated external CCB funding and activities.

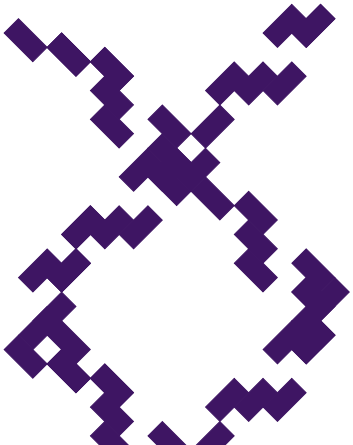
Elevating Global, Multi-stakeholder Perspectives

To showcase the urgent need for this conference, the GFCE and the Permanent Mission of Germany to the United Nations (UN) successfully co-hosted a side event luncheon on 27 July 2022 during the UN Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies (OEWG). This side event highlighted the genesis and purpose of the GC3B, focusing on elevating middle- and low-income country and donor perspectives to emphasize why CCB should be seen as a fundamental element of digital development.

The event featured many speakers from across the development and governmental sectors. Constance Malomo, representing the Botswana Ministry of Communications, Knowledge and Technology, was the first speaker to take the floor, reflecting on why CCB is critical to Botswana's digital development. She emphasized that the Government of Botswana is prioritizing CCB so that their citizens understand that ICTs are not something to be feared but to be understood.

Kerry-Ann Barrett, the Organization of American States' (OAS) CyberSecurity Program Manager, highlighted the role of cyber resilience in development efforts across Latin America and the Caribbean. Specifically, she noted how it is not enough to merely transform governments and manifest online services. On the contrary, she underscored, it is also fundamental that governments ensure they are cyber resilient and have sufficient cyber capacity – including but not limited to human expertise and resources – to respond when attacks occur. Crucial to realizing this is coordination, which she affirmed is difficult to achieve both globally as well as regionally within Latin America and the Caribbean given the varied starting points and resources of different countries. Thus, managing to avoid duplication, collaborate, and share efforts is critical.

Joanna LaHaie from the United States Department of State reiterated the U.S. Government's support for CCB as it pertains to development and creating a more secure cyberspace. Specifically, LaHaie stressed the importance of ensuring that, while everyone should be able to benefit from technology, we must also recognize the need to defend from and respond to the threats those technologies foster.



Isaac Morales from the Ministry of Foreign Affairs of Mexico focused on the relationship between cybersecurity and resilience regarding Mexico's sustainable development efforts – and how they are intrinsically linked. Drawing from their experience, he echoed Barrett's remarks by emphasizing the high value and importance of building capacity internationally and regionally, while also including CCB and cyber resilience within the innovation agenda of countries at the national level.

Tupou'tuah Baravilala, representing the Ministry of Communications of Fiji, underscored why cybersecurity and digital development go hand-in-hand among small island developing states (SIDS), such as in Fiji, where they are also contending with other challenges and threats to their resilience and development, notably climate change and natural disasters. She also reiterated how the main goal of building cyber capacities is to close the digital divide and ensure a level playing field among all countries as much as possible.

Lastly, Laura Burr, representing the Department of Foreign Affairs and Trade of Australia, highlighted her government's commitment to and interest in making the conference a success, especially as it relates to involving more women around the world in cyber-related discourse, empowering them to be cyber resilient, and expand their cyber capabilities.

Figure 2. The GC3B side event at the UN OEWG, in Conference Room 8, UN Headquarters, 27 July 2022.

Bridging Communities and Catalyzing Global Action

In recognition of the importance of and building capacity for cyber resilient development, as highlighted by various members of the global multi-stakeholder community, GC3B 2023 will bring together decision-makers and experts to catalyze global action on mainstreaming CCB and cyber resilience across the international development agenda as a key enabler of sustainable development, economic growth, and social prosperity.

For more information or to get involved, please visit GC3B.org, follow us on Twitter, LinkedIn, or Facebook, or email at: contact@gc3b.org.