AI and the Future of Cyber Capacity Building

Friday, 31 May 2024

Summary Report

The GFCE Working Group E on Emerging Technologies held its second meeting of 2024 within the schedule of the WSIS+20 Forum High-Level Event, organised in Geneva by the International Telecommunication Union. Maarten Botterman, moderator and Chair of the working group introduced the session, noting that while the working group focuses on a range of emerging technologies including (but not necessarily limited to) Artificial Intelligence (AI), quantum computing, and the Internet of Things, this session focuses specifically on AI and its impact on cyber capacity building.

Maarten introduced the four speakers for the session:

- Dr. Daniele Gerundino, Research Associate, Institut de Gouvernance de l’Environnement et Développement Territorial (GEDT), University of Geneva
- Mr. Jon France, Chief Information Security Officer, ISC2
- Mr. Moctar Yedaly, Africa Regional Director, Global Forum on Cyber Expertise
- Ms. Katharina Frey Bossoni, Deputy Head, State Secretariat, Digitalisation Division, Federal Department of Foreign Affairs, Switzerland

“The rapid acceleration in the development of artificial intelligence (AI) poses significant potential for society along with large scale risks. The transformative potential of AI cannot be realised without the protection of fundamental human rights and dignity and the principles of transparency and fairness.” This quote from the recent G7 Policy brief on Towards Safe, Secure, and Trustworthy AI neatly identifies the global policy challenge. As one of the authors of this document, Dr. Gerundino noted the extraordinary development of AI over recent decades. While AI is not a new technology, it is newly in the public eye and the number of users that are now adopting AI applications to enhance their work is exploding. This also comes with an exploration of possible regulatory frameworks around the world. He noted that technical standards are important adjuncts to regulatory efforts, ensuring the ability to engage with specific operational aspects. He also suggested that standards can assist different stakeholders to coalesce around common understanding of key terms and concepts. The first steps are made: the challenge is to find a balance between building in guardrails to avoid irreversible damage and creating space to allow innovation to thrive.

Mr. France was noted that, with the adoption of AI, ensuring security is key to avoid tampering and unauthorised access. Safe and secure AI requires well-informed practitioners, but will benefit efficiency and capacity, while alleviating workforce pressures. He reported on a recent ISC2 survey of security professionals, which indicated optimism about what AI will facilitate, but agreement that current approaches to capacity building will need to evolve, and there is hunger for capacity building activities. AI opens new threats and challenges, and on the adversarial side, AI is being used to enhance phishing activities, and may evolve new forms of attack. He raised the issue of available capacity and capacity development keeping up with the speed of developments.
In discussing the impact on the Global South, Mr. Yedaly noted that the data underlying AI models is a primary issue of concern, which is often skewed away from users in the Global South. AI models are trained with data sets that are predominantly available in English and are developed within specific (often Western) cultural environments - therefore, they may contain important biases in their training and deployment when rolled out in other regions in the world. The degree of awareness at the highest levels of government and leadership in these countries and regions is also concerning - there is no broad, clear understanding on the issues to be addressed, yet. However, he stressed that AI represents a massive opportunity for the Global South, particularly Africa - and action is needed in capacity development, as well as in African stakeholders stepping up to help develop standards at global level.

Ms. Frey Bossoni agreed that there are pros and cons for capacity building, but emphasized that it can enhance the capacity building offerings we currently have, allowing us to reach more people with deeper content. She noted that the Global Conference on Cyber Expertise (GC3B, which will take place in Geneva in May 2025) is an important opportunity to share experience and insight on how to further develop such approaches.

Discussion with participants in the room and online highlighted the need to focus on the basics, including data governance, algorithm standards setting and auditing, and a holistic culture in cyber capacity building efforts. It was concluded that there is a need for a “whole of society” approach to managing safe and secure AI adoption. It was observed that different countries and regions are approaching the institutionalisation of AI safety differently, with varying areas of focus. However, there is a common need to agree on global standards, share data, expertise, and other information, and to achieve this cooperation while understanding and respecting cultural differences. Speakers noted that in many cases we are still at the phase of declarations and early steps towards regulation, like the EU AI Act and the US Executive Order on the safe, secure, and trustworthy development and use of artificial intelligence. There is a need to move quickly to identifying and implementing practical steps to mitigate the risks of a fragmented landscape when building guardrails to ensure responsible AI adoption around the world.

In closing, speakers noted the importance of working in cooperation with the universities and public research centers from which many new technologies emerge. There are incentives to move fast in development and adoption (with the private sector generally taking the lead), but there is a need to protect the public interest. It was also suggested that we can learn from experience of Internet governance, which evolved alongside and in response to rapid development and deployment, dealing with the global, cross-border nature of the technology.

In closing the meeting, the Chair noted the importance of continuing work in this area - AI has clearly changed the landscape for many users, opening new opportunities and risk vectors - the value and necessity of linking cyber capacity building efforts with AI adoption, highlighted by the insights and experiences shared in this meeting, are evident. The GFCE, and specifically Working Group E, will provide the space and expertise to develop this linkage (while leveraging experiences across other emerging technologies), whether through
further research and studies, community discussion, or integration with other collaborative initiatives.