



ISTOCK/TRAITOV

Strengthen Cybersecurity to Safeguard Positive Global Connectivity

Recommendation: Strengthen cybersecurity through international cybercrime centers, international cybercrime expert rosters, and a global campaign to promote end-user cyber hygiene.

Global Challenge Update: In 2019, the number of internet users in the world passed the four billion mark. With more than half of the world's population connected to the internet, the potential for cybercrime has also increased. Cybercrime has been estimated to cost the world almost U.S. \$600 billion per year, “or 0.8 percent of global GDP.”¹ The rapid adoption of new technologies by criminals, rising numbers of new internet users, the emergence of “cybercrime-as-a-service,” and easier monetization through enhanced financial sophistication among cybercriminals are some of the main reasons for this staggering amount and its continual rise.²

UN Secretary-General Guterres has made addressing “the dark side of the digital world” one of his priorities for 2020. In May 2020, he presented the “Roadmap for Digital Cooperation,”

which covered developing human and institutional capacity, protecting human rights, and promoting digital trust, security and stability.³ Among the Roadmap's recommendations is the appointment of a UN Envoy on Technology by the Secretary-General, an overarching statement on common elements of understanding on digital trust and security, and the creation of a strategic and empowered multi-stakeholder high-level body.

A range of organizations and initiatives have already been working towards securing global connectivity over the past years, despite ideological differences in particular between Russia and China on one side and Western countries on the other. The UN is pursuing international cooperation through its Group of Governmental Experts on Developments in the Field of Information and

Telecommunications in the Context of International Security.⁴ This group examines potential cooperative measures to avoid inter-state tensions in cyberspace.

In addition, since 2015, the Global Forum on Cyber Expertise has brought together stakeholders to share know-how and best practices on countering cybercrime. It now has eighty-six partners, including the United States, intergovernmental organizations, and large private companies.⁵ Its work contributes to building a healthy foundation for global governance in cybersecurity, including a campaign to raise cybersecurity awareness. Furthermore, in November 2019, the Global Commission on the Stability of Cyberspace launched its final report in which it put forward a set of norms and principles, as well as guide

responsible state and non-state behavior in cyberspace.⁶

However, despite the wealth of expertise and technical resources in the international community, cybersecurity still lacks effective international coordination. According to the International Telecommunication Union (ITU), in 2018, there was “still a visible gap between many countries in terms of knowledge for the implementation of cybercrime legislation, national cybersecurity strategies (NCS), computer emergency response teams (CERTs), awareness and capacity to spread out the strategies, and capabilities and programmes in the field of cybersecurity.”⁷ A year later, the UN Secretary-General’s High-level Panel on Digital Cooperation confirmed that, “as technological change has accelerated, the mechanisms for cooperation and governance of this landscape have failed to keep pace.”⁸ And, in December 2019, the UN General Assembly stressed “the need for enhanced coordination and cooperation among States in combating the criminal misuse of information technologies.”⁹

Innovation Proposal: The Albright-Gambari Commission recommended several steps to better tackle cybersecurity as a matter of global governance.¹⁰ Progress has been made on some of them, especially with regards

to the global harmonization of cybersecurity frameworks and standards under the aegis of the UN. This includes the development of principles for responsible state behavior and Member State capacity-building thanks to, among others, the Global Forum on Cyber Expertise mentioned above.

To close the capacity coordination gap highlighted by the ITU, this paper makes two recommendations to the UN membership, regional organizations and the new UN Envoy on technology. Firstly, an international roster of cybercrime experts should be created to assist countries for the development of critical cybersecurity capabilities. These rosters could be managed by a UN-affiliated global network of cybercrime centers under the auspices of regional organizations. They can draw on the experience and best practices of, for instance, Europol’s European Cybercrime Centre. Regional centers would allow countries with limited budgets and capabilities to share resources and technology and exchange information. The centers and their staff could promote best practices and due diligence in cybersecurity among millions of new internet users each year.

Secondly, a campaign led by the new UN Envoy on Technology that promotes “cyber hygiene” could help new users around the world protect themselves, their data, and their assets from

cybercrime. Such a campaign promises significant benefits in terms of prevention, seeing the staggering global cost of cybercrime, easily outweighing the limited costs of such a campaign.

Strategy for Reform on the Road to 2020 (UN75):

If the goal is to “usher in order to the Wild West of cyberspace,”¹¹ the abovementioned innovation proposals are essential for ensuring that existing and emerging capacities are being used efficiently, frameworks of cooperation become effective, and cybercrime can be prevented as much as possible. In this quintessentially transnational domain, weak links among both state and non-state actors contribute to insecurity on a global scale. Therefore, also countries that already have stringent cybercrime regulations and state-of-the-art enforcement capacities have an interest in sharing their expertise with others that do not. Such sharing is not only a form of development cooperation but an essential contribution to the human security.

The UN75 Declaration gives priority to realizing of “the full potential for beneficial technology usage, and addressing digital trust and security.”¹² Such trust and security can only be achieved if expertise and capacities are used efficiently and a global awareness of the risks of cyberspace is created.

ENDNOTES

- Lewis, James. *Economic Impact of Cybercrime—No Slowing Down*. Washington, D.C. and Santa Clara, CA: Center for Strategic and International Studies and McAfee, February 21, 2018, 4.
- Ibid, 4.
- UN General Assembly. *Roadmap for digital cooperation: implementation of the recommendations of the High-level Panel on Digital Cooperation*. Report of the Secretary-General. A/74/821. May 29, 2020.
- United Nations. Office of Disarmament Affairs. “Open-ended Working Group.” Accessed May 28, 2020. <https://www.un.org/disarmament/open-ended-working-group/>
- Global Forum on Cyber Expertise. “Our Members.” Accessed May 23, 2020. <https://thegfce.org/member-overview/>
- Global Commission on the Stability of Cyberspace. *Advancing Cyberstability*. Final Report. November 2019. Accessed May 23, 2020. <https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf>
- International Telecommunications Union. *Global Cybersecurity Index 2018*. Geneva: International Telecommunication Union, 2018, 6.
- United Nations. Secretary-General’s High-level Panel on Digital Cooperation. *The age of digital interdependence*. June 2019, 7.
- United Nations. General Assembly. *Advancing responsible State behaviour in cyberspace in the context of international security*. A/RES/74/28. December 18, 2020, preamble.
- Commission on Global Security, Justice & Governance (Albright-Gambari Commission). *Confronting the Crisis of Global Governance*. The Hague and Washington, D.C.: The Hague Institute for Global Justice and Stimson Center, 2015, 71.
- UN Secretary-General António Guterres. “Remarks to the General Assembly on the Secretary-General’s priorities for 2020.” January 22, 2020. Accessed April 16, 2020. <https://www.un.org/sg/en/content/sg/speeches/2020-01-22/remarks-general-assembly-priorities-for-2020>
- United Nations. *Declaration of the Commemoration of the Seventy-Fifth Anniversary of the United Nations*. Draft, July 3, 2020, 3. Accessed July 3, 2020. <https://www.un.org/pga/74/wp-content/uploads/sites/99/2020/07/UN75-FINAL-DRAFT-DECLARATION.pdf>