Improving cybersecurity means understanding how cyberattacks affect both governments and civilians

July 20 2021, by Debora Irene Christine

Credit: AI-generated image (disclaimer)

For nearly two years, 68 United Nations member states—along with private enterprises, non-governmental organizations, technical communities and academics—participated in an open-ended working group on developments in information and telecommunications in

international security (Cyber OEWG). The working group deliberated on responsible state behavior in cyberspace.

In March 2021, the working group produced a final report. The report comes at a critical time in light of the high-profile cyberattacks on SolarWinds and Microsoft Exchange Server, as well as ransomware attacks on critical civilian infrastructures and essential public services.

Multi-stakeholder inclusion

The Cyber OEWG was established in 2018. It was tasked to continue cybersecurity negotiations in a more democratic, inclusive and transparent way. The process is open to all interested member states.

The Cyber OEWG publicly consults with non-state organizations over concerns about new threats posed by communications technologies. These include online interference in electoral processes, cyberattacks on supply chains and infrastructure and ransom attacks on medical facilities.

Civil society organizations have raised concerns with Cyber OEWG about the potential humanitarian consequences of malicious activities related to information and communications technologies (ICT). They demand considering the societal impacts of cyber threats in favor of merely focusing on the economic and political impacts.

Impacts of malicious cyber activities

Increasingly, rampant cyberattacks target critical civilian infrastructures, including health facilities, pipelines, water plants and food supply chains. Attacks on technology firms have also become commonplace.

These cyber incidents have impacted organizations of all sizes, including those with less awareness and capacity to defend themselves, such as civil society organizations and small businesses. Civilians may also be affected through ensuing personal data breaches and disrupted public services.

Harm to individuals resulting from a data breach can be physical, financial, emotional or reputational. Disrupted public services have also resulted in death by delaying treatment.

Centering civilian security

People experience cyber threats, incidents and harms differently depending on their gender identity, ethnicity, race and other social and cultural hierarchies. Those who are in vulnerable and marginalized positions may be disproportionately harmed by cyberattacks.

Organizations such as the UN Institute for Disarmament Research and the Association for Progressive Communications examine these uneven aspects of cybersecurity. Addressing these inequalities in cybersecurity requires human-centric and inclusive approaches to cybersecurity.

A human-centric approach to cyber-security prioritizes people when assessing cybersecurity threats, incidents, technologies and practices. It recognizes that people's intersecting identities shape their cybersecurity needs and experience of cyber incidents. Consequently, cybersecurity measures and instruments should be designed to address structural inequalities which lead to insecurity.

Disaggregated data by socio-economic factors on people's participation in cybersecurity fields and on victims of cyber incidents need to be collected. Efforts to increase underrepresented and minority groups' participation in cybersecurity workforce should go beyond providing

access to education and skills development. Further, cybersecurity skills-building should be tailored to the specific needs and capabilities of targeted population groups, including people with disabilities, the elderly and children.

Building a cyber-resilient society

The exploitation of vulnerabilities in ICT systems and their weakening of encryption standards can undermine trust and confidence in cyberspace overall. When any one sector or state is more secure, we all reap the benefits. On the other hand, enabling insecurity by design and malicious ICT acts degrade the entire security of the cyber ecosystem.

Threats to cybersecurity can emanate from any sector within society, due to human error, natural disaster, technical issues or cyberattacks. The effect can cascade across sectors and levels in unanticipated ways—as demonstrated in the cyberattacks targeted at giant tech firms.

To address the origins and systemic effect of cybersecurity threats, we need to build societal cyber resilience. This would require equal distribution of the resources needed to build cyber capacity and the broad, participation of all affected stakeholders—governmental, private sector and civil society—to shape cybersecurity research, policy and practice.

While facing the same persistent cyber threats experienced by states and private entities, civil society organizations are equipped with far fewer resources to defend themselves. Addressing such cross-sectoral cybersecurity resource inequalities could be done through establishing cyber-incident response teams that cater to the need of all affected stakeholders, not just firms operating critical infrastructures.

Cybersecurity funding for financially constrained sectors, such as civil

society organizations and small businesses, is also needed. It is crucial to provide cyber skills building programs for employees in these organizations, including awareness of cyber threats, the importance of cyber hygiene habits and how to respond to cyber incidents.

Good practices at the national level include formalizing civil society organizations' participation in shaping cybersecurity-related legislation and policies. This would include developing measures to deter cyberattacks, designing cyber capacity building programs and sharing information about cyber threats.

States have started to embrace this inclusive approach to cybersecurity. Several Asia-Pacific countries, including Australia, the Philippines and Sri Lanka, have established national cyber incident response teams that accept reporting from civilians.

Recently, Canada, Australia, New Zealand, the United Kingdom and the United States—an intelligence alliance knows as the Five Eyes—committed to develop a collective response against the threat of ransomware.

The UN is making incremental progress towards multi-stakeholder inclusion and prioritizing civilian security in cybersecurity negotiations. However, much work still needs to be done to follow up on the Cyber OEWG's proposed actions. Future cybersecurity discussions must establish an accountability mechanism for states' cyber operations and resolve how international law applies to cyberspace.

Provided by The Conversation