A ticking time bomb: the importance of moving the international cybersecurity agenda forward

Barbara Weekes

The world today is more interdependent than ever before, globally connected through the Internet via communication networks, computers, and a wide array of mobile devices penetrating the furthest corners of the planet. The benefits of this interconnectedness are widely recognized as having contributed to economic, political and cultural enrichment. However, the security challenges posed by this new cyber world are proving to be very unwieldy and difficult to manage at the international level. We have a global security challenge of the utmost importance, affecting all actors in cyberspace from the individual to the nation state, but the root of this challenge, the "Internet", means different things to different people and nations, cutting to the heart of some of the most politically sensitive issues in the modern world including freedom of expression, human rights, individual empowerment and democracy.

A purely national response is not sufficient to address today's global cybersecurity challenge, but international cooperation and multilateral agreement on key issues remains elusive. The result of this inability to reach agreement is that global citizens and nations remain without the necessary international procedures, agreements and even at a minimum, nomenclature, which could help navigate and potentially resolve future cyber conflicts before they escalate. Organized cyber crime, politically motivated attacks and cyber warfare capability development are also on the rise. We are leaving the doors wide open for cyber criminals and cyber attackers to remain under the radar and slip through the "international cracks" that exist between national legal systems, the applicability of cyber crime legislation and holes in existing national cybersecurity strategies.

These security challenges threaten to undermine the overall stability and trust in the Internet-based global systems upon which we increasingly rely for most of our daily personal, business and political activities. Complicating the situation further are the thorny issues of attribution, third party involvement and the role of non-state actors. International procedures to codify, respond, negotiate and resolve these issues are the only way to ensure a modicum of peace and stability.

Unfortunately, the discussion of international norms of behavior for cybersecurity has become bottlenecked between two camps loosely aligned behind the US and like-minded countries on one side and Russia, China and the Shanghai Cooperation Organization on the other. Other issues where agreement is unlikely include the applicability of international law and, in particular, the Law of Armed Conflict to cyber conflict; an acceptable model of Internet governance; margins of state sovereignty over the Internet, and access to information. With the major cyber powers – the U.S, China and Russia – disagreeing about the extent of national control over the Internet and the free flow of information, any consensus is likely to come at a high price. For those who have expected international agreements to steer national cyber security efforts, the time might be right to reconsider this approach as no major breakthrough is likely anytime soon. Discussions commencing in Dubai about the ITU's role in Internet governance are just one example of the complex issues governments face when trying to reach agreement on cybersecurity.

In an attempt to overcome this lack of progress on the core issues at the international level, the UN and some regional organizations such as the OSCE, have been seeking to negotiate Confidence-Building Measures (CBMs) – voluntary commitments to enhance transparency concerning state-on-state action and avoid escalation of cyber incidents. Rooted in the Cold War arsenal of means and methods of security, CBMs could, for example, define off-limits areas for cyberattacks, share situational awareness and communications systems. Several other multilateral initiatives exist including the UN Group of Governmental Experts, then the so called "London Process" launched at the London Conference last year (continued in Hungary 2012 and Korea in 2013) and within relevant IGOs including the ITU, OECD, APEC and NATO.

Unfortunately, progress in these and other international fora is slow and does not reflect the urgent need to establish systems that would, at a minimum, prevent and mitigate the escalation of cyber conflict. Unless movement is seen, these discussions may remain locked in a process of "catching up" to the reality of a rapidly evolving situation on the ground, allowing nations with the most "cyber power" to set the de facto rules of the game. While this may seem to some cyber superpowers like a politically and militarily advantageous situation, it may well backfire when a copycat, modified Flame or Stuxnet weapon reaches their critical infrastructure installations and government networks. Importantly, there is no recognized or accepted international procedure to manage these kinds of incidents, nor any real assessment mechanism for determining collateral unintended damages to corporations, organizations or individuals once these cyber "weapons" make their way out of the intended target and into the broader online community.

While pushing to have progress on international norms and CBMs at the state level, a realistic and constructive path forward in the interim would be to focus on smaller groups, bilateral discussions, industry-led initiatives, NGOs and stakeholders, with an emphasis on implementing existing national strategies and promoting international industry-wide best practices. Given the huge stake that civil society has in a secure cyberspace, the future may lie in building cybersecurity from the bottom up, focusing on national and international public private partnerships to further the exchange of critical information, provide early warning and explore possible solutions to current and future challenges.

Barbara Weekes, Senior Advisor, ICT4Peace Foundation and CEO, Geneva Security Forum, Switzerland