RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

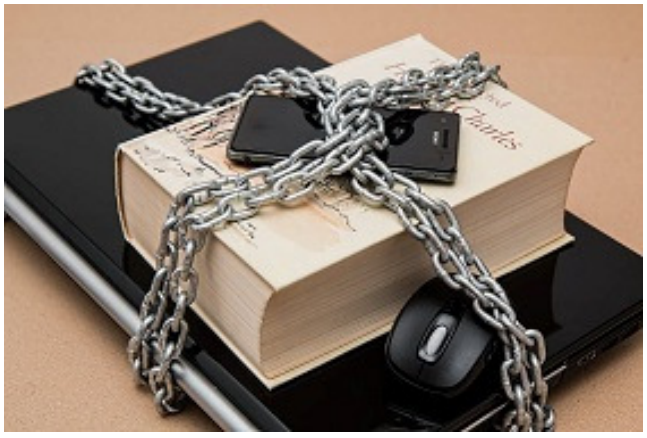
www.rsis.edu.sg No. 138 – 6 July 2020

Leadership in Cyber Security: Who Takes Responsibility?

By Kogila Balakrishnan

SYNOPSIS

COVID-19 has revealed vulnerabilities in many different sectors and amplified the risk of cyber security attacks. As humanity turns to digital platforms and connectivity, the cyber domain becomes increasingly critical but challenging. Who takes responsibility for providing leadership in cyber security?



Source: Pixabay: Pexels.com

COMMENTARY

COVID-19 HAS opened up new possibilities and transitioned the world rapidly into

digital working. Many organisations and corporate leaders now appreciate that one can work from anywhere around the world, provided one has access to the right tools and infrastructure.

Yet the digital revolution and alarming rate of usage of online platforms and digital technology for work has also opened Pandora's Box. We are now faced with increasing rates of cyber vulnerabilities and susceptibility to cybercrime.

Leadership in a Vulnerable Cyber World

Cyber threats are diverse and complex. Industrial supply chains, logistics companies and banking systems have been hacked to disrupt, steal and monetise commercial information.

The recent London CogX 2020 festival of Artificial Intelligence and emerging technology addressed the issue of cybercrime and what we can do to create a safer and secure cyber environment. However, the question remains: who assumes leadership for tackling the cyber security challenges?

The common challenges that keep emerging in the cyber world centre on the lack of a common language and a lack of collaboration among states and industries to adhere to cyber law. There is also the question of a lack of transparency and ethics in how to operate in a cyber environment.

A United Nations for Cyber Security?

It should be highlighted that the Budapest Convention on Cyber Security was drawn up by the Council of Europe in Strasbourg in 2004. The convention called for a harmonisation of national laws and improved investigative techniques and greater cooperation. As of 2019, 64 countries have ratified the convention.

The panel at the CogX conference looked at cyber security as a global problem and called for stronger global collaboration, even suggesting a 'United Nations for Cyber Security'. This spontaneous proposal came about as most speakers on the panel were sceptical of the existing role of the United Nations and its capacity to combat cybercrime.

A few existing international groups that address cyber issues include the European Union Agency for Cyber Security (ENISA), Asia Pacific Computer Systems Response Team (APCERT), and the International Corporation for Assigned Names and Numbers (ICANN).

But collaborative initiatives have also been challenging, as governments either do not want to collaborate due to mistrust, or industries are too conscious of commercial sensitivities.

In 2004, the UN Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was established.

Its mission is to develop a common approach on how governments should behave in cyberspace. Its 2015 report provided the foundation for an internationally-recognised governmental cyber code of conduct.

The report highlights the urgent need to improve communication and consensus mechanisms between states in regard to cyber security. Finding a working solution to this will be a challenge as states seek to project sovereignty in the cyber domain.

Future Trend

The number of people adopting and migrating to digital platforms will surge in the coming years. This is witnessed by the number of people who were reliant on online platforms for grocery shopping, retail and food at the height of the pandemic.

However, this also mean we are going to become more vulnerable to cyber crime and hacking. Hence, what should we do to increase vigilance in cyber security.

There is increasing effort to address risks and weaknesses in tackling cyber crime. Usage of specific technologies such as distributed ledgers and artificial intelligence may increase transparency in the digital world. Further, there could be greater initiatives to integrate AI, Internet of Things (IOT) and 5G to enhance digital platforms.

Nevertheless, the emergence of new technologies, such as cloud computing and autonomous vehicles or drones, comes with its own challenges and the question of how to create an end-to-end secure system. Further, governments need to seriously consider investing in cyber security infrastructure and tools that protect SME-scale companies from hackers.

Challenges of Leadership in Cyber Security

Finally, industries such as the banking sector, telecommunication, logistics and online retail traders must also do their part in securing their platforms from identity theft and monetary or business losses.

We require an independent body at the international level that ratifies states adherence to any new cyber treaties. More effort should be channelled towards building cyber capacity. All levels of society - in policy, management, business, technology and technical sectors - should be exposed to cyber education and training.

Underlying all of these efforts, relevant stakeholders need help to mitigate cyber risks. Overall, state or non-state actors operating in the cyber domain need to work towards a common set of agreed values.

At least three possible directions may evolve:

First, increased power and support for Interpol as an approach to cyber policing. This will improve the deterrence factor, by increasing the chance of malicious actors being caught. This has the advantage of posing a low political threat to states.

Second, increased power to an existing or new UN body with authority over the cyber domain. It is also unlikely that this will be perceived as a threat to the cyber autonomy of states.

Three, improved cooperation between the major ISP providers and legal/police authorities. If this occurs one area that will require improvement is the issue of jurisdiction and disjointed legal positions across nation states on cyber legislation.

Ultimately, leadership in cyber space is a cultural and education issue, not one of political/authority leadership. Hence, this is not about a top down imposition, but a collective bottom- up agreement on norms and values.

But who should take responsibility for leadership in cyber security? Perhaps, a country like Singapore that has invested heavily in cyber research and capacity development, should take the helm. In fact, Singapore features as the top-ranking country in the UN Global Security Index for commitment in cyber. Hence, at a time like this when the major powers are embroiled in turmoil, Singapore could step in to collaborate with ASEAN members and at the same time build global partnership in building a cyber-resilient eco-system.

Kogila Balakrishnan is Director for Client and Business Development (East Asia) at WMG, University of Warwick. She is also a policy advisor and formerly Under Secretary for Defence Industry Department at the Malaysian Ministry of Defence. An occasional participant of RSIS events, she contributed this to RSIS Commentary.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg