FRS – Japan Program

CYBER SECURITY GROWING CHALLENGES AND SOLUTIONS : A VIEW FROM JAPAN

Mihoko Matsubara

Mihoko Matsubara is Chief Cybersecurity Strategist, NTT Corporation, Tokyo, being responsible for cybersecurity thought leadership. She worked at the Japanese Ministry of Defense before her MA at the Johns Hopkins School of Advanced International Studies on Fulbright. She is Adjunct Fellow at the Pacific Forum, Honolulu, and Associate Fellow at the Henry Jackson Society, London. She published a book on cybersecurity, attackers, defenders, and cyber threat intelligence in Japanese from the Shinchosha Publishing Co., Ltd. in 2019.

Question 1: Beyond the Internet, what does "cyber" mean for the industry and our societies?

In 2919, NTT Corporation revealed a new concept with concrete applications called IOWN (Innovative Optical & Wireless Network) to bring an answer to the many challenges the internet is facing such as growing data traffic. As the world is becoming smarter with more connected cities, healthcare, manufacturing, etc., it is crucial to overcome digital divide and achieve sustainable development based on low latency and power consumption and high capacity and quality.

Thus, further evolution of technology requires a major change in the way we think: information should be treated as it is without being filtered by human values. In that sense, "natural technology" is key to bridge the digital divide, eliminate stress to juggle between different applications and devices, and open a new horizon for humans to be freely creative. The focus will be on eleven technologies to achieve such a "smart world": artificial intelligence, cybersecurity, additive manufacturing, advanced materials, augmented and virtual reality, biotechnology and medical care, energy, human machine interface, information processing infrastructure, network and quantum computing.

IOWN aims to achieve sustainable and environmentally friendly economic growth. It should help people perceive information in a natural way. IOWN also emphasizes the importance of ultimate safety, security, and trust, and seeks to optimize a better balance between individuals and cohesion to embrace diversity.

Since this effort requires industry-wide collaboration, NTT, Intel, and Sony announced in October 2019 the launch of a new industry forum to look beyond current internet technologies to build the future communication frontier. The IOWN Global Forum aspires to accelerate innovation and the adoption of a new communication infrastructure to meet our future data and computing requirements. This objective could be achieved through the development of new technologies, new frameworks, specifications and reference designs in areas such as next-generation photonics-based technologies.

Question 2: After the G20 Osaka Summit in 2019 agreed to promote integrity and transparency in infrastructure development and support sustainable growth, how does the international community help countries to develop IT infrastructures in an open and sustainable manner?

One way to answer this question was to launch the Blue Dot Network, a financially sustainable infrastructure. In November 2019, the United States' Overseas Private Investment Corporation (OPIC), Australia's Department of Foreign Affairs and Trade (DFAT), and Japan's Japan Bank for International Cooperation (JBIC) unveiled the Blue Dot Network project. This is a multi-stakeholder initiative that brings together governments, the private sector, and civil society "to promote high-quality, trusted standards for global infrastructure development in an open and inclusive framework", according to the OPIC website.

The Blue Dot Network will evaluate and certify designated infrastructure projects based upon the global principles such as the G20 Principles for Quality Infrastructure Investment, the G7 Charlevoix Commitment on Innovative Financing for Development and the Equator Principles. These initiatives will promote market-driven, transparent, and financially sustainable infrastructure development in the Indo-Pacific region and around the world.

JBIC governor Tadashi Maeda, acknowledges the important role that the Blue Dot Network will play in the world. "Blue Dot Network is an initiative that leads to the promotion of quality infrastructure investments committed by G20 countries" said Maeda. "As JBIC has a long history of infrastructure financing all over the world, JBIC will be pleased to share such experience and contribute to further development of Blue Dot Network."

Question 3: What can global companies do to address growing cyber threats?

Since industry leads innovation and owns a large amount of IT assets, it is crucial for them to drive global cybersecurity collaboration to share cyber threat intelligence and best practices. Unfortunately, damages by cyberattacks have been growing. Cybersecurity Ventures estimated in 2017 that cybercrime damages will cost the world $6 trillion annually by 2021, which doubled their estimated figure in 2015. In spite of these rising threats and potential costs, NTT found that only 52 % of companies have put in place an incident response plan, and 57 % of them are fully aware at all levels of the content of this plan. This lack of planning and awareness can be qualified as a cybersecurity crisis that can affect not only companies but also countries. Global security collaboration among companies is indispensable to protect the society and enhance resiliency. There are several initiatives launched by industry. First, the Council to Secure the Digital Economy (CSDE) was launched to promote secure digital economy together with multinational companies in IT and communication industries in2018.

"Cybersecurity Ventures estimated in 2017 that cybercrime damages will cost the world $6 trillion annually by 2021"

CSDE brings together leading global enterprises from across the information technology, communications, and cybersecurity sectors to combat cyber threats through collaborative actions.

The founding partners of the CSDE initiative include Akamai, AT&T, CenturyLink, Cisco, Ericsson, IBM, Intel, NTT, Oracle, Samsung, SAP, Telefonica, and Verizon. The CSDE shares best practices and solutions. For instance, in 2018, they published the *2018 International Anti-Botnet Guide* to share a comprehensive set of practices aimed at protecting the global digital ecosystem from the threat of botnets and other automated distributed attacks.

Second, the Charter of Trust was founded at the Munich Security Conference in 2018 to "protect our democratic and economic values against cyber and hybrid threats" initiated by Siemens and inviting global companies such as Airbus, Allianz, Cisco, Dell Technologies, IBM and TÜV SÜD. The membership currently includes Japan-based global companies, Mitsubishi heavy industries and NTT.

The Charter of Trust works closely with governments and pursues to "make every effort to protect the data and assets of both individuals and businesses, prevent damage to people, businesses and infrastructures and build a reliable basis for trust in a connected and digital world". That is why the consortium implements its ten principles including "responsibility throughout the digital supply chain" and "security by default" to make the digital world more secure.

These industry-driven initiatives showcase growing interests among global companies to contribute to make the society more resilient and secure. Such public-private partnerships such as CSDE and the Charter of Trust are growing internationally to tackle with cyber threats.

March 2020