# The Turtle Bay Security Roundtable

## Managing the Frontiers of Technology II

## *Understanding Cyber and Cryptocurrency: Managing Threats and Building Opportunities*

An event hosted by the Permanent Mission of Japan in cooperation with the Stimson Center

**Friday, July 6, 2018, 10:00am–2:30pm**
**Japan Society, 333 East 47th Street, New York, NY 10017**

On July 6, 2018, the Permanent Mission of Japan to the United Nations hosted the ninth meeting of the Turtle Bay Security Roundtable series. The event was organized in cooperation with the Stimson Center, an independent think tank dedicated to global security and development. Under the theme "Understanding Cyber and Cryptocurrency: Managing Threats and Building Opportunities", the meeting convened UN Member States, members of the Group of Experts of the 1540 and 1718 Committees and other subsidiary organs of the Security Council, and experts from think tanks, industry, and academia to discuss various tools available to both minimize risks and nefarious uses of these technologies and promote their peaceful use and availability. The event featured a keynote address by Secretary Mr. Geoff Brown (NYC Cyber Command) and panel discussions with Ms. Natasha Cohen (BlueVoyant), Mr. Daniel Kahn Gillmor (ACLU), Mr. Irwin Nack (Deutsche Bank), Mr. Salem Avan (UN), and Ms. Elana Broitman (New America NYC).

### OPENING REMARKS

Ambassador Koro Bessho (Permanent Mission of Japan)

Ambassador Bessho referred to the Secretary-General's Disarmament Agenda "Securing Our Common Future" launched on May 24 and reminded the audience of the importance of tackling frontier issues. He also shared the Secretary-General's concern on armed conflict led by a massive cyber-attack and its serious consequences for peace and security. Ambassador Bessho asserted that although cyber issues are discussed in the UN, the potential impact of cyberattacks remains in need of focus. The examples of recent Wannacry attacks and incidents in Tokyo's Coincheck, a cryptocurrency exchange service where 500 million dollars were stolen, showed that cyberattacks do not respect borders. Furthermore, he said some argue that cybercrimes and cryptocurrencies are now being used as a means to escape from UN sanctions, such as those imposed by the Security Council Resolutions 1718 and 1540. Ambassador Bessho called on the international community to work with governments, academia and private sector to take measures against those threats while ensuring a cyberspace which contributes to the creation of innovative ideas and sustainable development.

## KEYNOTE ADDRESS

### Geoff Brown (Citywide Chief Information Security Officer and Head of NYC Cyber Command)


Geoff Brown began the day's discussion by underlining its importance due to how it brings together digital safety, privacy, and innovation. In order to be successful, participants need to bridge cultures so reach the highest achievements.

Mr. Brown wanted to focus on how various communities can have a more secure cyber space, with a focus on what has been launched since the birth of NYC Cyber Command in July 2017. Specifically, he explored the role of government in cyber security and its ability to provide scalable solutions. He said there is a great deal of room for change. Technology today, like the UN before it, is connecting groups to share knowledge and create partnerships.

However, connectivity is not without its risks. Mr. Brown explained that the excitement to build global technology has in many areas outpaced efforts to secure it. Because security is coming after, it is far harder to protect the technology that has been created, and the people using the technology. This has created fertile ground for threats to public safety that can go beyond local communities across the globe much faster than anyone could have predicted.

Mr. Brown said he finds it "puzzling" that people have not placed expectations on their governments to provide security from these new threats. He goes on to say that he believes there is a lack of leadership by organizations that could take proactive actions. Leadership today is needed to combat cyber security failures that could cripple such services like water, sanitation, and hospitals. Right now, the government only gets involved when the market fails, and Mr. Brown said this is misaligned.

*"Our future peace is imperiled by the threats on and to computers and to the internet, and it's time to commit that we will actually do something about it."*

New York City's proactive tactics fall along this belief that public safety includes cybersecurity. A critical part of this philosophy is that cybersecurity does not need to come at the cost of privacy. Government and industry can each play a role to ensure technology can make this happen.

Mr. Brown said New York's vision started with the idea of creating something that could evolve to meet the unknown and become a permanent part of the city's public safety team, much like the police and fire services. He encouraged other cities around the world to look at NYC Cyber Command and start a conversation around best practices and how to put in place the need infrastructure. Mr. Brown said it is daunting but achievable work.

New York has sought to empower New Yorkers themselves and have them become active participants in securing both their personal accounts and the city. This includes putting safety measures in public Wi-Fi and giving individuals a free threat protection app that would suggest a course of action if a threat was detected. Much of this is done to educate people about potential risks and how to use technology responsibly.

Mr. Brown said that this will not solve all problems because nothing is future-proof. However, he is optimistic about the course of action. He challenged the audience to take a leap forward by partnering cyber security with public safety. He said it is a myth that communities cannot make a difference and provide protection for the future. Once there is a public dialogue and established cyber security public policy, Mr. Brown suggests that next anything will be possible to unlock human potential for investment in incredible innovations and connectivity.

## FIRST SESSION: Understanding Cyber

### Moderator: Chris Frangione
### Panelists: Natasha Cohen (BlueVoyant), Daniel Kahn Gillmor (ACLU), Irwin Nack (Deutsche Bank)

Moderator Chris Frangione began the first session by asking the panelists on ways cyber can affect people's lives. Daniel Kahn Gillmor spoke from a civil rights perspective and described the ways people, such as dissidents or those involved in domestic conflicts, could have privacy or information security violations that comes from cybersecurity attacks. He stressed that when information security is discussed the needs of those vulnerable people on the margins must be considered. Centralized control is not always the best way to deal with cybersecurity, as a single authority itself would often become abusive.

Irwin Nack explained how currently the threats posed by crypto currencies are not understood by many. Although the recent two attacks on companies that resulted in the loss of crypto currencies worth of about 6 and 17 billion dollars is potentially the largest crime in history, many people are unaware of it. He warned that crypto currency has grown increasingly attractive for criminals because of its nature of easy access, easy use, and relative anonymity.

Natasha Cohen commented on the nation state interest in cybersecurity. First, she highlighted the inherent conflicts within different parts of the governments, notably between the offensive side of the government that needs to develop cyber weapons, and the defensive side that wants to foster a safe eco system. She also highlighted the difference in balance of power when it comes to cybersecurity and relative low investment necessary to have sophisticated cybersecurity capability.

Mr. Frangione pointed out the challenge of balancing between respect of privacy and protection of people. He asked the panelists how nations, federal and local governments, or companies balance privacy and civil liberty. Mr. Gillmor argued the most important thing in cybersecurity is information control. Some law enforce-

ment and national security agencies may think they should have access to all information and that encryption makes part of their jobs harder. However, on balance, the stronger cryptography and defensive infrastructure, the better public safety, cybersecurity, and privacy.

Mr. Nack noted the challenges that banks face in complying with obligations that are not specifically spelled out in regulations. For example, banks have been complying with Know Your Customer (KYC) for years where they identify whether their customers' activities are consistent or suspicious and unusual, but until this year, there had never been a written KYC regulation. In respect to compliance, Mr. Gillmor also pointed out that it is entirely possible to have a set of unfulfillable regulation. A company wanting to do business in two states with contradicting regulations, for example, might have to break one of their laws. He suggested more coordination in this realm.

Lastly, Mr. Frangione invited the panelists to talk about conflicts within governments on cybersecurity. Ms. Cohen gave an example of the case in which the US government found vulnerabilities in technology that affected the government system and the entire eco system. While one side wanted to use it for exploitation of tech operations, the defensive side argued that it would affect the economy, citizens, and corporation. She said there are number of different qualifications that the US government need to go through to keep new technologies.

Mr. Nack spoke about conflicts between law enforcements and regulators. Banks conduct tremendous amount of reporting, as they are inspected by regulators. There has been conversations going on whether this reporting has been too burdensome, but from the law enforcement perspective, this means more information, which is what they focus on.
Mr. Gillmor described a situation where the law enforcement struggle with data "going dark" or encrypted so that they are unable to enforce the law. On the contrary, the amount of information that is available is astronomical that they are also looking for efficient computing mechanism.

## SECOND SESSION: Regulating Innovation: Managing Threats and Building Opportunities

Moderator: Brian Finlay
Panelists: Salem Avan (UN), Elana Broitman (New America NYC)

The discussion next took a closer look at the opportunities new technologies could present to international actors and communities. Moderator Brian Finlay asked the panelists to identify how these technologies could be used to improve the human condition and how the international community should exploit the technology while also putting up safeguards.

Salem Avan spoke about the unpredictability of the technology, noting that many of the developments of the past two decades could not have been predicted, something he urged the audience to remember as the international community tried to plan for the future. Any movement forward must be done in a mindful way to enhance inclusion from the whole world. Elana Broitman echoed Mr. Avan that technology is an opportunity but it must be used carefully. She urged the development of infrastructure to enhance countries' ability to use technology and praised efforts by the UN to deliver such programs. That led to a discussion about the UN's sustainable development goals and the role of technology there.

Ms. Broitman said that much of development remains "old school." However technology does enhance the ability to be efficient and democratize efforts.

Turning back to challenges, Mr. Avan said that the UN at its core is a post-WWII institution designed to hamper the threat of war. He wondered if the UN has adjusted adequately current events, where any confrontation may be preceded by a cyber-attack. Conventional warfare is no longer the only threat to consider. Mr. Avan also touched on an individual impact of the technologies: pronounced isolation while being surrounded by much more stimulation, information, and "noise." He worried that it could become unmanageable and even a health threat.

Mr. Finlay tried to move the conversation to ways outside the formal processes of the UN that could be used to set up norms for cyber, but Ms. Broitman said that any efforts should be complementary to the UN because it has the biggest podium from which to speak. Still, she praised the concrete work done in the Asia-Pacific region by its technologists and suggested it could be a model for other regions. Instead of focusing on attribution, these experts are focused on improving the overall situation through incremental and practical efforts.

Finally, Mr. Finlay brought the conversation to access. He asked how the technologies can be scaled more broadly to more people can access and benefit from the opportunities they present. Mr. Avan said that this is difficult because all member states are different with different challenges. He agrees it is important to not increase the digital divide, especially by gender, and so the UN has been acting to integrate different areas. For example, it is working with many different countries to establish innovation labs. What is important is to work with members of all areas, such as academia and the private sector, to come up with an efficient approach to disseminate technology.

## CLOSING REMARKS

Ambassador Koro Bessho (Permanent Mission of Japan)

In closing, Ambassador Bessho expressed his gratitude to all the participants for taking part in rich and informative discussions. This roundtable provides a unique opportunity to listen to many different perspectives, which is important in balancing innovation and security in cyberspace, he said. Finally, Ambassador Bessho encouraged the participants to continue their dialogue and looked forward to holding another roundtable soon.

## ABOUT THE TURTLE BAY SECURITY ROUNDTABLE SERIES

The Permanent Mission of Japan has been hosting a series of events that focus on various security challenges posed in today's world. The seminar is organized in cooperation with the Stimson Center—an internationally renowned think tank based in Washington DC—and enjoys strong support from the United Nations. Its inaugural conference held in May 2011 was blessed with the presence of Secretary-General Ban Ki-moon, who emphasized in his keynote speech the significance of international efforts in the area of non-proliferation, disarmament and the important role relevant UN Security Council resolutions play in non-proliferation efforts.

These events have invited not only UN diplomats and leading experts in the area of disarmament and non-proliferation but also corporate executives and scholars in order to promote candid, in-depth and thought–provoking discussions. The organizers have also tried to facilitate cross-cutting analysis of wide-ranging issues by welcoming the participation of experts in the area of development and peace-building, which are two key components of promoting international peace and stability. Below are links to previous sessions:

## TURTLE BAY SECURITY ROUNDTABLE EVENTS

| | |
|---|---|
| First event (May 31, 2011): | http://www.un.emb-japan.go.jp/events/060211-2.html |
| Second event (December 5, 2011): | http://www.un.emb-japan.go.jp/events/120711_2.html |
| Third event (May 21, 2012): | http://www.un.emb-japan.go.jp/events/051212.html |
| Fourth event (January 18, 2013): | http://www.un.emb-japan.go.jp/events/011813_2.html |
| Fifth event (June 10, 2013): | http://www.un.emb-japan.go.jp/events/2013/061013.html |
| Sixth event (March 26, 2014): | http://www.un.emb-japan.go.jp/events/2014/032614.html |
| Seventh event (March 27, 2015): | http://www.un.emb-japan.go.jp/events/2015/032715.html |
| Eighth event (March 23, 2018): | http://www.un.emb-japan.go.jp/itpr_en/events_032318.html |
| Ninth event (July 6, 2018): | リンク |

STIMSON