Key Findings
United States-Singapore Cyber & Tech Security Virtual Series
Session #3: Cybersecurity and Big Data in the Time of COVID-19
January 20, 2021 (US) | January 21, 2021 (Singapore)

On January 20, 2021, with the support from the US Embassy Singapore, the Pacific Forum hosted "Cybersecurity and Big Data in the Time of COVID-19," with over 40 participants from governments, private sector, academia, and non-governmental organizations. This was the first of the two closed-door sessions in the United States-Singapore Cyber & Tech Security Virtual Series.

Christina Ayiotis, Cybersecurity and Information Governance Attorney; Shashi Jayakumar, Head of the Center of Excellence for National Security from the S. Rajaratnam School of International Studies; and Aribowo Sasmito, Co-founder and Fact-Check Specialist at MAFINDO, examined the two sides of data. Data can be maximized for the greater good for big data analytics but is also susceptible to weaponization by malicious actors for propaganda or information warfare amid the global health crisis.

Key findings from this meeting are described below.

Managing Big Data and Cybersecurity

As data continues to drive decisions in the post-pandemic environment, questions relating to its ownership and protection will become even more critical. Data will continue to be subject to potential intellectual property theft while the advent of Artificial Intelligence (AI) and Machine Learning (ML) increases its vulnerability to manipulation and cyberattacks. The management of Big Data must abide by the principles of safety, security, and transparency. To assure that data is not manipulated, the ideas of "security" and "ethics by design" should be adopted. In this regard, trust and transparency are paramount to ensure the flow of data across governments and the private sector at the national, regional and global levels.

Data can be maximized for the greater good to drive innovation and change in different sectors, but it is also susceptible to weaponization by malicious actors for propaganda, influence operations, and information warfare. In the United States, the unprecedented impact of COVID-19 brought to light the "human virus of misinformation" spread mainly by paranoia and conspiracy theories. Foreign adversaries have exploited the pandemic to inoculate misinformation on social media, primarily related to the safety, efficacy, and effectiveness of COVID-19 vaccines.

Large tech companies are exploring the growing nexus between Big Data, AI, telehealth, and other innovative digital health solutions, but will likely face evolving regulatory and statutory regimes. Meanwhile, cybersecurity will continue to rely on AI and ML as security tools to combat sophisticated cyberattacks, specifically in flagging anomalies and automating effective countermeasures.

Disinformation: Singapore's Perspective

Throughout the pandemic, Singapore has had to contend with the growing threats of the "weaponization of information." Unlike the United States, which grappled with conspiracy theories and anti-vaccine propaganda, Singapore has faced a different type of disinformation centered on hate-spin, or the incitement of violence through manufactured vilification, and "cancel culture," online shaming or the withdrawal of

public support leading to ostracism. There is a growing polarization on race in social media, exemplified by racial microaggressions.

As Singapore envisions itself to become a "smart city-state," it must recalibrate its approach toward promoting resilience, particularly among the younger population. The physical and the virtual world are gradually becoming integrated, and the latter is being utilized as a sandbox to test threats before they are launched into the former. To build a resilient Smart City, critical thinking comes to the fore. Combatting disinformation or misinformation requires revisiting "heritage skills" embedded in inter- and intra-group contexts to cultivate critical thinking. Greater collaboration between the government and non-governmental organizations is necessary to adopt such a historical approach. Similarly, as Singapore becomes a Smart City, the government is confronted with the daunting task of consolidating its position to ensure the public that its data management is based on the principles of trust and transparency.

Combating the Infodemic/Disinformation

MAFINDO, a not-for-profit fact-checking group in Indonesia, is an example of a bottom-up approach to fighting misinformation and disinformation. As government rules and regulations are often outpaced by technological advancements, collaboration across key sectors from industry, academia, and media organizations in tackling misinformation and disinformation has taken center stage, especially during the pandemic. Aside from its own dedicated team that oversees the crowdsourcing of its fact-checking ecosystem, MAFINDO has established linkages with more than 20 mainstream national media outlets and members of the Indonesian Cyber Media Association and has received support from Google News Initiative.

Amid the global health crisis, MAFINDO has launched a series of online and offline initiatives to combat the spread of the "infodemic." It has established a task force to prioritize and coordinate its hoax-busting activities through its own website and other social media platforms like Facebook and WhatsApp that are widely used in Indonesia. Despite the limitations imposed by the pandemic, MAFINDO has continued its multi-pronged approach—literacy education, rejuvenating journalism, fact-checking, opinion-building, and law enforcement—in fighting disinformation in major cities in Indonesia.

As big tech companies such as Facebook continue to become the battleground in spreading misinformation and disinformation, it becomes imperative to regulate content algorithms—recency, popularity, content type, and relationship—based on transparency, privacy and accountability standards to avoid biased micro-targeting and illicit appropriation of users' personal data without their consent for political advertising. With the rise of data governance frameworks such as the EU General Data Protection Regulation, issues relating to algorithmic fairness and transparency will continue to receive traction.

Future Areas of Cooperation for US and Singapore

Following the revelations of the Facebook-Cambridge Analytica scandal, which shed light on successful influence operations on the outcomes of the 2016 US presidential elections and the Brexit referendum, hostile actors will continue to use information warfare to subvert democratic processes.

As misinformation and disinformation become more integral in the context of hybrid warfare, foreign adversaries will continue to fine-tune their execution to become more sophisticated and intrusive. Proxies in the form of outsourced digital companies, as well as cybercriminals, that operate in the grey zone and conduct information warfare campaigns on behalf of a nation-state will only grow in number.

With the incoming Biden administration, the US and Singapore can continue to build on their cooperation in the realm of cybersecurity, especially in promoting cyber norms and the application of international law. It will be interesting to see how such collaboration progresses to tackle hybrid warfare. As the idea of

techno-nationalism will continue to influence US policy, especially in Southeast Asia, in the short- to medium-term, Singapore needs to recalibrate its approach to find a common ground for dialogue.

This document was prepared by Mark Manantan and Eugenio Benincasa. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Director of Nonproliferation, Technology, and Fellowships at Pacific Forum. These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.