Roundtable 7: Regional Perspectives
Co-Authored by: Kristin Rheins and Jackson Colling

The "Regional Perspectives" panel was moderated by Danielle Yeow from the Centre for International Law at the National University of Singapore, and included: Yang Fan, Assistant Professor of International Law at Xiamen University; Masahiro Kurosaki, Professor of International Law and Director of Study of Law, Security and Military Operations at the National Defence Academy of Japan; Paul Lie, the head of International Law and Legal Services at the Singapore Ministry of Defense, Arun Sakumar, a Postdoctoral Researcher at Leiden University, and Isaac Morales Tenerio, Senior Director for Cybersecurity and Data Privacy Communications at FTI Consulting.

Yeow first directed questions at Fan**,** asking about the prominence of cybersecurity and its various dimensions in the Chinese government. Fan claimed that China has released national documents that endorse internationally agreed-upon ethical principles that avoid turning cyberspace into a new battlefield. Fan also offered his definition of "cyber operation" as state conducted or sponsored operations in or through cyberspace for data intelligence purposes or to cause physical or non-physical effects in a state's territory. Fan maintained that such an operation is different than an information operation.

Kurosaki spoke on the impact of the Russia-Ukraine war on Japan's public and private sectors. He noted the growing number of malware attacks that have drastically increased since Russia's invasion and explained how Japan is committed primarily to defensive operations with the Japan Self-Defense Forces. Kurosaki also noted that while Japanese hackers are active in the Russia-Ukraine war, the location of the hackers' effects keeps them from being targeted by Japanese law enforcement as such acts are seen as extraterritorial crimes.

Lie discussed self-defense and Singapore's position on the application of IHL to the cyber domain. Lie stated that Singapore acknowledges that IHL is applicable to cyber in armed conflict and emphasizes distinction and proportionality. Lie also noted the central role of cyber and tech in Singapore's governance and Singaporeans' daily lives and the constant threat Singapore faces from malign cyber action. This is a primary reason why Singapore regards some cyber-attacks as armed attacks and reserves the right to use force against perpetrators.

Sakumar elaborated on India's strategic neutrality in the war in Ukraine. He claimed that current geopolitical tension makes it difficult for the Indian government to support of any one party and that legal and political reasons make India cautious to foreclose any possibilities or alliances (formal or informal). Sakumar also explained India's lack of position on the application of IHL to cyber space and offered that India does not wish to constrain itself in the cyber realm given its regional neighborhood.

Finally, Tenerio, spoke on the nature and scope of cyber in Latin America. He explained that there is no unified view or understanding of cyber conflict nor of cyber space as a domain for cyber operations. He pointed out both Costa Rica's and Brazil's statements, but noted that these are outliers. Tenerio concluded that more Latin American engagement in cyber conflicts have to do with the recent ransomware attacks in the region.