Roundtable 5: Cyber Neutrality
Co-Authored by: Joseph Roskop and Jackson Colling

The fifth roundtable of the symposium, Cyber Neutrality, featured moderator Davide Giovanelli (CCDCOE), and panelists Hitoshi Nasu (Lieber Institute), Eugenio Benincasa (Center for Security Studies), Kurt Sanger (Integrated Cybersecurity Partners), and Martin Dahinden (Ambassador of Switzerland). The panelists provided an overview of the law of neutrality and paid particular attention to US involvement in Ukraine and the Ukrainian volunteer IT-Army.

Law of Neutrality

Nasu began the panel by providing an overview of the law of neutrality. He outlined the basic principles of neutrality as being (1) abstention, (2) prevention, (3) impartiality, and (4) acquiescence. Further, he elaborated on the basic principle that underpins all of neutrality law, that being neutral is about maintaining peaceful relations with the belligerents. Nasu transferred the law of neutrality to cyber space, emphasizing that neutral states have no obligation to stop non-government actors outside their territory. He was referring to citizens of a neutral state launching cyber operations against a belligerent while outside the neutral state's territory and those citizens routing cyber operation(s) through the neutral state's cyber infrastructure. While there is a duty to prevent cyber operations from being launched on a neutral state's territory when the state has knowledge, there is no issue in failing to stop operations being routed through the state's territory as it is impractical. In the same vein, Nasu stressed that even if a neutral state merely breaches, that does not make it a belligerent to the conflict.

Swiss Perspective and US Involvement in Ukraine

Ambassador Dahinden argued that international law should be apply to states acting in cyber space, to include the law of neutrality. He also explained that neutrality need not be officially declared but may be declared through action. Further, if a state is neutral, it cannot be *militarily* involved with a belligerent. Kurt Sanger provided a perspective on why, despite the US supplying weapons and other forms of support to Ukraine, the US is not running afoul of neutrality law. "Qualified Neutrality" is being used as a rationale for providing material support without breaching neutrality obligations. This concept permits states not party to a conflict to provide lethal support to states that are the victim of an unlawful war of aggression. There is, however, a pervasive concern that this is being done as a political expedient without due attention to the precedent it may be setting.

IT-Army of Ukraine

Eugenio Benincasa gave an overview of the IT-Army of Ukraine, an all-volunteer group who answered Ukraine's call to conduct cyber operations against Russian targets. This group raises the issue of whether civilians are participating in offensive operations. The main answer relies on the definition of "attack," however, additional considerations in answering that question include: 1) the threshold of harm, 2) a belligerent nexus, and 3) potentiality for damage. The protected status of citizens is only implicated if/when citizens are supplying "material support" to warfighting efforts. Current perspectives seem to indicate that because volunteer efforts tend to be limited to temporary and reversible disruptions, such as DDoS attacks and influence operations, they fall short of the type of impact needed to qualify as an "attack," as per a Scale & Effects analysis.