Roundtable 6: Cyber Spill Over
Co-Authored by: Reganne Hardy, Taylor Gayton, and Jackson Colling

The Cyber Spillover panel was moderated by Eric Jensen from Brigham Young Law School and featured Marguerite Walters, Attorney-Adviser for the Office of the Legal Adviser at the U.S. Department of State, Talita de Sousa Diaz, Senior Research Fellow in the International Law Programme at Chatham House, Matthew Waxman, Liviu Librescu Professor of Law at Columbia Law School, and Duncan Hollis, Professor of Law at Temple Law School. The panel largely focused its conversation on the topics of standards of knowledge, application of international law, and kinetic responses. The panel began by defining "cyber spillover" and assessing the impacts on states. Talita de Sousa Diaz described cyber spillover as the collateral impacts of unlawful acts, whether intentional or foreseeable.

This led to the discussion of standards of knowledge – foreseeability and intent – regarding cyber spillover and how to deal with it. Foreseeability applies specifically in the requisite knowledge requirement for countermeasures to a cyber attack. Marguerite Walters noted how states may impact spillover by their responses. The acting state's state of mind matters in terms of the victim state's countermeasures and response options. Foreseeability alone does not answer questions of legal implications and intent can have a greater bearing, shedding light on the implications of a state's action(s). State intent, however, is often difficult to prove.

Next, the panel wrestled with whether international law applies in cyber space. Duncan Hollis argued that general principles of international law do apply in the cyber domain, noting, however, that some view international law as having a legal gap when it comes to cyber. Talita de Sousa Diaz postulated that applying international law is a choice that considers the unintended impacts of undermining international law. The panelists noted that more states are talking about how international law applies to cyber, lending to the development of norms and capacity building. Some states have made a conscious choice to articulate their views on the applicability of international law to state behavior in cyberspace, while others have made the choice not to articulate their views for strategic ambiguity purposes. The latter permits states to approach issues based on specific facts and unique circumstances without being tied to a hardline rule. States, such as the U.S., may be hesitant to state a position before being put in a position where it must act.

The panel then discussed kinetic responses to cyber-attacks. Talita de Sousa Diaz deconstructed kinetic responses into self-defense, countermeasures, necessity, and proportionality. Necessity requires imminence, peril, or grave danger, whereas self-defense requires justification. Waxman presented another factor to the self-defense calculus to evaluate the fundamental intent of the bad actor to cause harm versus any defenses that minimized impacts. The panelists discussed the evolving U.S. perspective on the issue of countermeasures stating that the early U.S. position held there must be kinetic force. Today, however, the U.S. position is shifting to include non-kinetic effects covering cyber operations or even incoming missiles that are intercepted before having effects on U.S. territory, bases, personnel, etc. The type of non-kinetic cyber action that would provoke a kinetic response, however, such as election interference or economic damage, is not entirely clear. The panelists did stress though that intent is becoming more important to the U.S. perspective.