Round Table 1: Cyber "Attack" – Toward Greater Precision
Co-Authored by Yeliza Mosquera & Jackson Colling

Under the direction of the moderator, Gary Corn, in the first roundtable discussion on "cyber-attack" and its implications for international law, several prominent experts in the field came together to examine the complex intersection of cyber warfare and legal frameworks. The panelists were: Captain Pete Pascucci, Fleet Cyber Command; Lt. Col. John Schreiner, USMC Cyberspace Officer; Kubo Macak, a senior lecturer in law at the University of Exeter; and Professor Dr. Daphné Richemond-Barak, international law expert at the Lauder School of Government, Diplomacy, and Strategy. The roundtable analyzed the changing nature of warfare in the context of cyber capabilities and operations. The moderator called attention to the importance of adhering to the principles established by international law, particularly the rules governing the use of force and the protection of civilians in combat. The panelists highlighted the challenges posed by new technologies that blur the line between traditional military actions and unconventional cyber activities. In that context, two main issues permeated the discussion.

Definition of "cyber-attack"

In addressing the definition of "cyber-attack," the panelists highlighted the applicability of international law to cyber operations. They identified different national positions to define the notion of attack and thoroughly discussed what constitutes "violence" in the context of Art. 49 of Additional Protocol I's definition of "attack." The panel agreed that the most popular national position is to use an effects-based approach to define "cyber-attack," but the line has yet to be drawn for what constitutes violence. One position discussed was loss of functionality and whether states may consider such loss as an act of violence despite loss of functionality not resulting in physical destruction. The key implication then becomes the importance of the target's lack of functionality to the particular state. Underlying this discussion was the issue of whether IHL applies to cyber as it does to every other method of warfare or whether cyber deserves its own specific set of rules. The panel largely agreed that the tech-neutral approach of applying existing IHL to cyber was the dominant approach. This conversation highlighted the difficulty of classifying cyber operations as traditional attacks under IHL and the ambiguous space in which states operate.

Is Data an object?

The panelists also examined the critical question of whether data is an object in the context of the prohibition of violence against civilian objects. One panelist described three main approaches to the issue: (1) data is non-tangible and non-visible and thus not an object, (2) data is an object because cyber operations against data must comply with IHL targeting rules, and (3) some data is an object, in which not only content is differentiated from operational data, but civilian content data is protected against attack. Another panelist suggested that data is not an object because it is intangible and cannot be physically grasped or destroyed in the traditional sense. He explained that certain categories of data, such as financial information, might warrant enhanced protection. Overall, the panelists found it difficult to classify data as a traditional object under legal analysis.