INTERNATIONAL LAW AND CYBERSPACE: CHALLENGES FOR AND BY NON-STATE ACTORS

This panel was convened at 9:00 a.m., Thursday, April 13, 2017, by its moderator, Laura Dickinson of George Washington University, who introduced the panelists: Col. Gary Corn of U.S. Cyber Command; Lt. Col. Sean Watts of Creighton University School of Law; and Jeannie Rhee of Wilmer Hale.

Introductory Remarks by Laura Dickinson*

doi:10.1017/amp.2017.154

The growing use of cyberspace by state and nonstate actors is testing the limits of our international legal rules. And the recent issuance of the *Tallinn Manual*, both in its first iteration and now in its second version as *Tallinn 2.0*, attempts to identify the emerging law in this area. But many of the principles it asserts are controversial. This panel grapples with some of the key contested issues in this emerging domain.

Remarks by Col. Gary Corn†

doi:10.1017/amp.2017.155

First, I should note that I am speaking today in my personal capacity only, and my views do not represent those of the U.S. government, the Department of Defense, or U.S. Cyber Command. At the outset, let me provide a brief overview of U.S. Cyber Command. It is a relatively new command within the Department of Defense. Established about seven years ago as a subunified command, it is an operational headquarters at the strategic level but at the moment subordinate to U.S. Strategic Command, one of the combatant commands within the Department of Defense. The 2017 National Defense Authorization Act included a provision stating that there shall be established a combatant command known as U.S. Cyber Command. As a result, there is now a lot of movement afoot to see how we will meet that legislative intent. In all likelihood, U.S. Cyber Command will elevate at some time in the future as a full combatant command.

U.S. Cyber Command is missioned and responsible for three primary things. First, we secure, operate, and defend the information networks of the Department of Defense. The Department runs and utilizes a massive set of information technology networks on a day-to-day basis as well as in support of war-fighting functions. That is one of our primary functions on the cyber security defensive side. Second, we are missioned to be prepared to defend the United States broadly and also specifically from cyberattacks of significant consequence to the nation. Third, when directed, we use cyber capabilities in support of the geographic combatant commanders in their war-fighting functions. Thus, if U.S. Africa Command (AFRICOM) were to direct an operation in Libya,

* Oswald Symister Colclough Research Professor and Professor of Law, George Washington University.

† Staff Judge Advocate, U.S. Cyber Command.