Copyright © 2018 by The American Society of International Law

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.

https://doi.org/10.1017/amp.2017.155 Published online by Cambridge University Press

AFRICOM might be able to leverage certain cyber capabilities in support of those ongoing operations, just as it might use any other military capability.

In recent years, there has been quite a bit of thinking about how to incorporate cyber capabilities in a broader tool set for the nation for deterrence, both to deter adversary malicious cyber-actions as well as to use them a tool in the broader deterrence set against other states and nonstate actors. There is a term in vogue these days, particularly among strategists, called the "grey zone." There is some debate about how novel it is along with its utility. Generally, it is used to describe the twilight between war and peace, and the inherent ambiguities in that zone exploited principally by revisionist states. It refers to a level of aggressive behavior below the threshold of warfare, below the threshold of use of force in legal terms, but above the normal peacetime geopolitical competition among states. In this zone, states try to achieve objectives through exploiting political and legal ambiguities in the international environment to achieve strategic objectives. To be sure, this is by no means limited to cyber. As examples of actions in this zone, some will point to China's efforts in the south China Sea, such as the creation of islands and the use of the coast guard in a robust fashion to establish a presence. Some will point to Russia's actions in Ukraine.

Cyber is a fertile area in this regard, and we have definitely seen a lot of activity in this zone. States have embraced cyberspace and cyber capabilities as a means and method of statecraft. Examples include actions attributed to Iran in damaging a multitude of computers belonging to the Saudi Arabian Oil Company (Saudi Aramco) through a cyber operation. Whether it crossed the threshold of a use of force is certainly something that has been debated, but it is on those margins. Here at home, we all are familiar with the U.S. Office of Personnel Management (OPM) breach, the Sony hack attributed to North Korea, as well as the hack of the Democratic National Committee, which has certainly figured prominently in recent days. These are all cyber-enabled operations executed in this zone, which have tended to fall short of warfare, but which are aggressive and concerning from a national security perspective. We are struggling to figure out how we categorize these actions.

A recent quote from the Defense Science Board Task Force on Cyber Deterrence from February of this year is instructive:

> Although progress is being made to reduce the pervasive cyber vulnerabilities of U.S. critical infrastructure, the unfortunate reality is that for at least the next decade, the offensive cyber capabilities of our most capable adversaries are likely to far exceed the United States' ability to defend key critical infrastructures.[1]

Relatedly, in an event at Duke University, John Carlin, the former Assistant Attorney General for the U.S. Department of Justice's National Security Division, recently noted that you cannot build a wall high enough in the cybersecurity world. This fact raises serious questions about what measures you can take, or might need to take, outside of your own networks as a nation-state, to address these threats. Another example sets this problem in context. In 2013, then Chairman of the Joint Chiefs, General Martin Dempsey, was talking about a left of launch air and missile defense program. He highlighted the importance of integrating new, nonkinetic capabilities such as cyber operations into the traditional antiballistic missile tool set to prevent adversaries from effectively employing any of their air and missile weapons against the United States or its allies.[2]

[1] Memorandum from the Co-Chairs, Defense Science Board Task Force to the Chairman, Defense Science Board, Subject: Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence (Feb. 2017), *in* DEP'T OF DEFENSE, DEFENSE SCIENCE BOARD, TASK FORCE ON CYBER DETERRENCE (Feb. 2017).

[2] GENERAL MARTIN E. DEMPSEY, JOINT INTEGRATED AIR AND MISSILE DEFENSE: VISION 2020 (Dec. 5, 2013). *See also* Riki Ellison, Left of Launch, Missile Defense Advocacy Alliance (Mar. 16, 2015), *available at* http://missiledefenseadvocacy.org/alert/3132/ ("The Strategy is based on a preemptive strike with new non kinetic technologies, such as

https://doi.org/10.1017/amp.2017.155 Published online by Cambridge University Press

As these comments illustrate, we are facing the question of how we can manage this new capability in this environment, an area *Tallinn 2.0* took on as its new focal point: the law that governs the space below what is clearly identified as armed conflict. And I would note one salient point to keep in mind when states operate in this space: in order to be prepared to operate in cyberspace, by and large, you have to actually operate. It is somewhat paradoxical. Cyber differs from a lot of other capabilities, such as strategic bombing, for example. In those contexts, you can have assets in home station sitting prepared but dormant. You can fuel them up and have them over targets in relatively short order. That is vital, and it is also an important means of messaging. That approach is much harder in cyberspace. There is a much more sophisticated lead time that is necessary if you are going to be effective, and it requires some degree of activity in the environment outside of your own networks.

The distinctive features of cyber operations therefore raise profound questions, both legal and policy-related, about how you are going to deploy and use these capabilities. With respect to law, from a country dedicated and committed to the rule of law and a rules-based system, we have moved past the foundational question of whether international law applies to state-conducted activities in cyberspace. The answer to that question is clearly yes. But that's where the hard work starts. The facts matter. The question of *how* we apply existing international law and existing regimes to specific factual circumstances is not as easy.

Remarks by Lt. Col. Sean Watts*

doi:10.1017/amp.2017.156

We are still in the early days of the relationship between cyberspace and international law. In many respects, it is a relationship off to an unsteady and uncertain start. But a slow and sporadic trickle of governmental efforts to express or even to shape that relationship has emerged.[1] To date, the most significant multinational clarification from states has been the deceptively modest concession that international law applies fully to cyberspace.[2] States have at least made clear that the novelty and seemingly virtual nature do not exempt cyberspace from existing in international law.

Meanwhile, a flood of private efforts has attempted to lend further clarity. Scholarly articles, books, and dissertations on the international law of cyberspace have proliferated at an astonishing pace. To date, the most comprehensive of these efforts might be the *Tallinn Manual 2.0 on International Law Applicable to Cyber Operations* (*Tallinn 2.0*).[3] As its title suggests, *Tallinn 2.0* is an update to a previous work. Like its predecessor, *Tallinn 2.0* is intended to provide a snapshot of *existing* international law—*lex lata*. Also like its predecessor, its primary audience is

electromagnetic propagation, cyber as well as offensive force to defeat nuclear ballistic missile threats before they are launched, known as 'left of launch.' The strategy is to attach by electronic embedment or through the electronic radar signatures of the threat's command and control systems and the targeting systems of the threatening ballistic missiles.").

* Professor, Creighton University School of Law.

[1] *See, e.g.*, UN Secretary-General, Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/70/174 (July 22, 2015) [hereinafter UN GGE Report 2015]; UN Secretary-General, Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc. A/68/98 (June 24, 2013) [hereinafter UN GGE Report 2013].

[2] *See* UN GGE Report 2015, *supra* note 1.

[3] Tallinn Manual 2.0 on International Law Applicable to Cyber Operations (Michael N. Schmitt ed., 2017) [hereinafter Tallinn 2.0].

https://doi.org/10.1017/amp.2017.155 Published online by Cambridge University Press