Army War College, Penn State Dickinson Law School partner for Cyber education

By Gregory D. Hillebrand, Space and Cyber Analyst, USAWC Center for Strategic Leadership 21 April 2021

The CyberLaw Exercise partners Army War College students with Penn State Dickinson Law School students to understand, analyze, and develop responses within international law for cyber events related to crime, espionage, and use of force.

The United States is under cyber siege. The Army War College seeks to develop its students' ability to make informed decisions in this complex and evolving environment of cyberspace, international cyber law, and policy implications. The use of cyberspace is integrated into the American way of life and way of war. Bad actors around the globe know this and stop at nothing to work asymmetrically through cyberspace to take away the American advantage in industry, commerce, and war. According to PurpleSec, a cyber security firm, the United States is the number one global target, with 37% of all cyber-attacks aimed at the U.S. For 2018, that added up to 80,000 cyber-attacks per day, 30 million attacks per year.

The U.S. Army War College's core curriculum introduces students to cyberspace operations, as well as operations in the domains of Space, Air, Sea, and Land. For those who want to learn more, *Cyberspace Issues:*

Fundamentals and Strategy is a non-technical course examining the global nature, legal and ethical issues, and the physical and non-physical attributes of cyberspace. The elective faculty partner with Dickinson Law School faculty and students for an experiential learning exercise to facilitate a deeper understanding and analytical skills relevant to cyber challenges.

Cyber exercise examines cyber acts of crime, espionage, use of force

The cyber exercise develops foundational understanding of international cyber law as it applies across the cooperation-competition-conflict spectrum. While arguably the bulk of cyberspace activity is the legitimate flow of information and commerce, this exercise looks at the domain from military, political, and commercial perspectives, examining cyber acts committed between nations.

The faculty team carefully selects these cyber acts, focusing on the often related and overlapping operations of crime, espionage, and use of force. Each of these categories fall under different international legal regimes: a nation's response to a cybercrime, viewed through international law, should be different from that nation's response to destruction of property (use of force) through cyberspace. Determining the relevant category of a cyber event – crime, espionage, or use of force – influences in large part a nation's response per international law. All nations may not interpret a cyberspace event the same way as they each interpret the event through the lens of how they view cyberspace.

Ambiguity is the basis of the exercise.

Refined over the last four years, the Spring 2021 cyber exercise simulates United Nations discussion and debate. Teams including both USAWC and Dickinson Law students represent varied countries and organizations, addressing a series of cyber incidents that are modeled after real world events. The student teams analyze these incidents through the lens of national/ organizational policy and international law, and present their positions to a UN panel.

The exercise drives the students to examine these cyberspace incidents through the crime –espionage -- use of force spectrum. In their presentations to the panel of legal and cyberspace experts, the teams advocate for their characterization of the incidents, and make recommendations on what may be a legal state response under international law.

Army War College, Dickinson Law School leverage each other's

strengths

Learning from each other, students from both institutions are teamed together; they explore and develop skills beyond cyberspace, working with students of very different perspectives whose experiences lead to different approaches to address challenges. USAWC students are typically military professionals with more than 20 years of experience, while the Law students are often 20 years younger, just starting their professional careers. Representing diverse backgrounds, Law students contribute a depth of recent and specific knowledge in law. In many ways the Law students represent the experience and background of U.S. government agency personnel with whom USAWC students will work, post-graduation. Working through these cyberspace legal issues, bringing together diverse perspectives, and building consensus on complex issues, USAWC students practice the skills they will need to address real world strategic problems.

Prior to the exercise, USAWC faculty teach the Law students a foundational understanding of cyberspace as a domain of both information flow and conflict; Dickinson Law faculty teach USAWC students the fundamentals of international law relating to cyberspace. This stage-setting learning event complements the material taught in the cyberspace electives at each institution and allows the students to meet each other prior to the actual exercise.

Two-part exercise: analysis and application

The exercise has two primary learning objectives: analyzing international cyberspace laws, policies and norms and understanding how these elements impact international relations. To analyze national, corporate, and international organization's perspectives on international cyberspace norms, the teams examine a series of cyber events – impacting finance; affecting internet censorship firewalls; and causing physical damage to a refinery – interpreting how international law would categorize these events. The teams categorize each event as crime, espionage, or use of force, each a different category under international law. Mid-way through the exercise, the teams present their analysis, agnostic of their specific country or organization perspective. This initial analysis provides the teams a foundational understanding, based on international law, national policy, and cyberspace norms.

For the second part of the exercise, the teams develop a country or organization specific evaluation of the series of cyber events; this becomes their presentation to the UN panel. Using a broad range of research, the

students examine what their nation or organization has said, written, and done with respect to cyberspace. The goal of this second part is to build an understanding of the cyberspace equities of nation-state and non-state actors and the impact on international relations. This challenges the students to see beyond bias and to understand how other nations interpret activities in cyberspace. In this exercise, the students are generally biased toward seeing cyberspace the way the average American sees it: free and open. This is not necessarily the perspective held by China or Iran, which may view government control of the internet and information flow as a sovereign right.

Addressing critical need

Given the extent to which cyber is integrated into the way we live, exist as a nation, and fight, it becomes increasingly critical for senior leaders to develop a working knowledge of this evolving domain. The same cyberspace that provides global information flow and commerce is also a place of crime and violence. Senior leaders need to understand the range of cyberspace operations (crime, espionage, and use of force), how they present themselves across the cooperation-competition-conflict spectrum, and their international legal implications. The cyberspace experiential learning exercise, part of the *Cyberspace Issues: Fundamentals and Strategy* elective, leverages the strengths of both the USAWC and Dickinson Law to build in the students an understanding of these elements of the cyberspace.