10-20-2015

DOJ's "All-Tools" Approach to Cyber and National Security

Peter Margulies
Roger Williams University School of Law, pmargulies@rwu.edu

LAWFARE

CYBERSECURITY

DOJ's "All-Tools" Approach to Cyber and National Security

By **Peter Margulies** Tuesday, October 20, 2015, 7:07 AM

DayZero: Cybersecurity Law and Policy

Assistant Attorneys General John Carlin (National Security Division) and Leslie Caldwell (Criminal Division) spoke last week at Roger Williams' Cybersecurity conference, outlining an innovative approach to detecting, disrupting, and deterring cyber threats. Caldwell and Carlin cited two recent moves: (1) the U.S.-China agreement to forego theft of intellectual property, and (2) the recent arrest in Malaysia of Ardit Ferizi, a Kosovar who had hacked into U.S. government databases and shared personal identifiable information (PII) about military and other personnel with ISIS (see Ellen Nakashima's story in the *Washington Post* here). For Caldwell and Carlin, these two moves represented deliverables in a comprehensive approach to cybersecurity that involves law enforcement, diplomacy, and (when necessary) the use of force.

Ferizi's arrest signals the government's attention to hacking by ISIS and other terrorist groups. Ferizi, according to the government's criminal complaint in the case, engaged in material support of a foreign terrorist group when he transferred a huge cache of PII regarding U.S. personnel to Junaid Hussain, a U.K. national and ISIS operative. Hussain had been in touch with the Texas gunmen who were killed after they sought to attack attendees at a recent Texas contest eliciting caricatures of the Prophet Muhammad. U.S. authorities will surely question Ferizi to obtain more information about ISIS's cyber plans. The U.S. military has already moved against Hussain, who was killed in August in a drone strike in Syria. Ferizi's case, as Carlin reminded the audience reflects the U.S. comprehensive cyber approach in miniature, utilizing both criminal justice and the use of force.

Carlin also placed the U.S.-China cyber agreement in this comprehensive framework. He noted that this agreement stemmed from two recent moves, one diplomatic and one in the law enforcement arena. President Obama recently issued an executive order that authorized sanctions against malicious cyber actors. The Chinese, who value their global reputation, were concerned that they would be on the receiving end of sanctions pursuant to President Obama's order. That prospect helped bring them to the table.

In addition, the U.S. sent a message with its indictment of Chinese People's Liberation Army (PLA) personnel for theft of intellectual property using cyber means. The indictment signaled that the U.S. could identify bad actors in the cyber arena, despite the challenges of attributing responsibility for cyber attacks. Assistant Attorney General Caldwell of the Criminal Division noted that the indictment, even though it might not result in the prosecution of the named individuals, sent the Chinese a wake-up call: "We know where you live." That display of the United States' capabilities also played a role in bringing China around politically. At the conference last week, U.S. senators Jack Reed and Sheldon Whitehouse and Representative Jim Langevin agreed that the U.S.-China agreement was a significant step.

Carlin and the legislators mentioned above acknowledged that with China and other state actors, the proof is in the pudding. The U.S.-China agreement is only a first step in an arduous path toward compliance (and doubts about Chinese compliance have already arisen). But it is a necessary step that puts China on the record as at least publicly sharing US concerns. With non-state actors such as ISIS, the path is even more challenging, since nonstate actors have no "return address," reducing opportunities for deterrence. In some cases, as with ISIS's Junaid Hussain, the use of force may be the only alternative. The key virtue, Caldwell and Carlin suggested, was openness to using a range of tools to do the job.

Topics: Cybersecurity, Cybersecurity: Crime and Espionage

Tags: Cybersecurity, cyberespionage, counterterrorism, ISIS, China, John Carlin, Leslie Caldwell, Juniad Hussain

Peter Margulies is a professor at Roger Williams University School of Law, where he teaches Immigration Law, National Security Law and Professional Responsibility. He is the author of Law's Detour: Justice Displaced in the Bush Administration (New York: NYU Press, 2010).