Cyber Power and Constraint

Elad D. Gil
The Federmann Cyber Security Center – Cyber Law Program,
Hebrew University, Faculty of Law

Abstract. States operate extensively in cyberspace to advance national security and foreign policy objectives. They carry espionage and surveillance; seek influence over other states; defend against malign activity by states and non-state actors; and engage in offensive cyberattacks. As the volume and significance of hostile cross-border activity in the cyber domain ("cyberwarfare") surges, policymakers are beginning to grapple with the proper legal paradigm through which uses of cyber force should be regulated. One increasingly popular way to deal with the problem is by trying to fit cyberwarfare into existing legal regimes—a body of constitutional, statutory, and administrative law that regulates traditional national security activities such as war, covert action, and intelligence collection. Stretching existing legal frameworks to new settings is common practice in legal reasoning—it provides normative context, helps address novel legal questions, and prevents law-free zones. But in some situations, this practice may fail to capture what is critically new about the new settings and turn out to be counterproductive.

Cyberwarfare belongs to the latter category. The challenges presented by cyberwarfare are conceptually and empirically different from those arising in traditional national security law along four major axes: global regulation, global politics, domestic versus extraterritorial governance, and private sector dominance. Briefly, (1) a wide range of state behavior in cyberspace is not clearly governed by international law. (2) Cyber operations are carried in an international environment that renders strong democracies disadvantaged and vulnerable. (3) Networked technology obscures traditional distinctions between internal and external affairs that are foundational to current law and doctrine. And (4) cyberspace illustrates a problem of overly powerful private actors—the technology companies that control our digital existence and constitute potential victims, aggressors and channels through which attacks can be mounted. The need to hold these companies accountable adds another wrinkle to separation-of-powers concerns that characterize traditional national security law. Each of these features, and especially their cumulative effect, gives rise to 'cyberwarfare exceptionalism'—the idea that cyberwarfare merits different legal and regulatory treatment from ordinary national security activities. This article describes the features of cyberwarfare exceptionalism, elucidates the complex tradeoffs it entails, and set a normative agenda for an overarching legal policy for cybersecurity.

I hope to make three main contributions to the field. First, by considering the phenomenon of cyberwarfare exceptionalism *in toto* and describing its implications, this article will add to the growing empirical evidence on which future work on the domestic regulation of offensive cyber capabilities can draw. Second, as governments worldwide contemplate various models of legislation for regulating cyberwarfare (e.g., general war-like statutory authorizations, government/private sector hack-back laws), the framework suggested in this article will help assess and compare these models, fleshing out their costs and benefits. And third, drawing on a large body of international relations and security studies literature, I hope to connect the legal design discourse to the strategical policy discourse on cybersecurity.