Cyber Power and Constraint

Elad Gil

Governments operate extensively in cyberspace to advance national security and foreign policy objectives. They carry espionage and surveillance; defend against malign activity by states and non-state actors; disrupt foreign disinformation campaigns; conduct counterintelligence; and engage in offensive cyber operations. The increasing volume and aggressiveness of government activity in the cyber domain has attracted considerable academic attention. Scholars have considered the effects of a constant, low-intensity cyber conflict among nations on security, geopolitics, international law, and privacy, amongst others, but one important area has thus far remained unexplored: how government hacking impacts our democracy and our liberty.

This article takes the initial step to fill that gap. One key guarantee to liberty is a commitment to distributed, separated, and checked sovereign power, realized by a system that maintains a balance between power and constraint to promise that no single actor would accrue excessive power over citizens' lives. This Article traces the balance of power and constraint in cyberspace with the goal of examining whether the rise in government hacking presents a danger of unbounded state (and, in particular, executive) power. Rather than examining the traditional constraints on the Executive in the legislature and the judiciary—which play a modest role in this area—the article focuses on four types of external constraint on executive power: international law, international politics, cyberspace architecture, and private sector participation. If our government is adequately constrained in cyberspace, it is mainly thanks to these external constraints. The Article shows that each of these constraints, and especially their cumulative effect, has crosscutting implications. International law fails to clearly regulate a wide range of state activity in cyberspace and, paradoxically, enhances rather than constraints state power; the international political environment, on the other hand, generates significant constraints on strong democracies. Cyberspace architecture imposes some barriers to state power, but governments have found ways to overcome these barriers, even to exploit them to enhance their power. Cyberspace also introduces a new powerful actor to the fray: the private sector, and especially, a handful of multi-billion-dollar technology firms that control many aspects of our digital existence. These private actors constrain the government in some ways but empower it in others.

This complex descriptive account of cyber power and constraint yields important normative insights. First, it shows that fears of a fully autonomous and unaccountable executive, which are common in the areas of foreign affairs and national security, are empirically unfounded in the cyber context, where power is more diffused. Second, it clarifies the limits of the current system and guides where legislative and judicial checks are especially salient. And finally, it provides a prism though which new policies and legislative initiatives can be evaluated.