Today’s Revolution: Cybersecurity and the International Order

KRISTEN EICHENSEHR

Review of Lucas Kello, The Virtual Weapon and International Order (Yale, 2017)

With nearly every cybersecurity incident come assertions that the latest one is “the big one,” the incident that is truly gamechanging, disastrous, or sure to trigger the U.S. Congress to address cybersecurity. Such assertions are usually overblown as to any single event, but in his new book “The Virtual Weapon and International Order,” Lucas Kello takes on the more fundamental challenge of gauging the significance of cyber weapons, in the aggregate, to international order. This work of political science argues that they are revolutionary in not one, but three different ways. And Kello issues a clarion call to international relations and security studies specialists to address this new reality, lest they be left behind by “prioritize[ing] the physical over the virtual world, interstate violence over sub-threshold conflict, the interests and capabilities of states over unconventional actors” (3).

While early chapters focus on international relations theory, this important book has much to offer to a broader audience. Some of its discussion will be familiar to legal audiences, who Kello notes have been bolder than international relations scholars both in addressing cybersecurity challenges and in adapting existing concepts to new technological realities. Kello combines his theory of three ways technology can be revolutionary with lucid explanations of just how cyber weapons have changed the international order, drawing on examples like Stuxnet and Russian interference in the 2016 U.S. election. He also contributes to debates over familiar topics like deterrence in the cyber realm and private sector hacking back. Kello argues that “[t]he growth of technological ability is rapidly outpacing the design of concepts to interpret it” (7) and situates his book as a step toward conceptual catching up. Though his critique focuses on international relations and cybersecurity, the challenge Kello identifies is more broadly applicable, both to other fields, like law, and to other technologies, like artificial intelligence.

Kello identifies three ways that technology
can cause revolutions in the international order and argues that “[t]he cyber revolution expresses all three orders of technological revolution in different degrees” (14). The least significant type of revolution is “third-order revolution, or systemic disruption, which involves the appearance of a new technology that disturbs the regularized interactions of rational state contenders (because, for example, it alters the balance of offensive and defensive forces)” (13). Kello argues that cyberspace and cyberweapons cause systemic disruption by breeding instability. Uncertainties about how cyber weapons will behave, difficulties in attribution, and the dominance of offense over defense all increase the risk of conflict and conflict escalation, even among rational states.

Kello’s second-order revolution or “systemic revision” occurs when technology enables “the ascent of a state or a group of states that repudiates the shared basic purposes of [the international order] and rejects the accepted methods of achieving them, in particular restraints on the objectives and means of war” (90). Outside the cyberspace context, Kello’s examples of second-order revolution include the Soviet Union’s “pursuance of ‘world revolution’” and “the contemporary project of European union” (91). In the cyber realm, Kello cites North Korea’s cyber activities as emblematic of systemic revision (145-59).

The final and most fundamental type of revolution is first-order revolution, or what Kello terms “systems change” (13). This phenomenon “concerns not the balance of power but the balance of players” (251), and it occurs when “new players (hacktivists and technology firms, for instance) challenge the traditional supremacy of states, thus altering the system’s very building blocks” (13).

This most fundamental type of revolution is also the most interesting. Kello is clear-eyed in his portrayal of the changes wrought by cyberweapons. He does not argue that they are causing the disappearance of states; rather he argues that although states maintain their primacy in the international order, the rise of non-state actors is diluting states’ role. Kello identifies three manifestations of what he calls “the Sovereignty Gap” (190). The first is the rise of non-state actors as threats to state security. The second is the rise of non-state actors as providers of national security, including in ways that “in previous eras governments would have deemed an unacceptable renunciation of national security to actors other than themselves” (190). And finally, states can no longer expect to control even interstate conflicts because of the “dangers that private culprits will intervene in ways that accelerate the crisis or that move it in a direction that the system’s old stewards do not want to go” (191).

Whether termed a revolution or not, the rising importance of private parties has become a frequent theme in academic and popular work on cybersecurity. Kello’s aim in “The Virtual Weapon” is largely diagnostic, as he puts it to “provide[] international relations specialists with a conceptual apparatus on which to build a new field of cyber studies” (10). But for those convinced by his diagnosis of how cyberweapons are causing systems change, there is a need to move beyond diagnosis to prescription. What are states, private parties, academics, and individuals to do about the rise of private parties and diminishment of state primacy?

In answering that question, the legal community has made some progress. For example, I have argued that where private parties are playing public functions in cybersecurity—like engaging in transnational crime control and national defense—they should be held to public law values, such as accountability and transparency, that apply to governments. More doctrinally, the drafters of the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations have attempted to set out in detail how existing international law on issues like state responsibility and the principle of non-
intervention apply to new fact patterns where non-state actors are playing significant roles.

As part of his critique of international relations and security studies scholars, Kello highlights their failure to participate in an imagined “Congress of Disciplines” (29). He recognizes that “[t]he dislocations of the cyber age are so complex that the interaction of many communities of knowledge is necessary for a full appraisal of its problems” (247) (and, I would argue, also of its eventual solutions).

The need for interdisciplinary discussion holds true for Kello’s own proposals, some of which could benefit from greater interactions with legal standards. For example, in discussing the Russian government’s complicity in distributed denial-of-service attacks on Estonia in 2007 and Georgia in 2008, Kello proposes a four-part “spectrum of proximity between private actors and the state,” ranging from “coordinated action” between governmental and private actors to “forbearance” where the state doesn’t support private actors but knows their identity and “decides not to penalize them” (176). Instead of creating a new typology, Kello’s analysis of state complicity could have drawn on the existing international law of state responsibility, which provides standards for when states are and are not responsible for the actions of non-state actors. As set out in the International Law Commission’s Articles on the Responsibility of States for Internationally Wrongful Acts, the legal inquiry turns on whether the non-state actor is “acting on the instructions of, or under the direction or control of, [the] State in carrying out the conduct” (Art. 8).

Beyond providing a clarifying point of reference, international law may also cabin certain of Kello’s proposals. To take one example, he suggests a strategy of “punctuated deterrence”: responsive actions that “address[] not single actions and particular effects, but series of actions and cumulative effects” (197). As a policy matter, the approach has much to recommend it, including, as Kello argues, strengthening deterrence by making response by victims more likely and more substantial and giving victims more control over when to respond, rather than requiring a response shortly after any particular cyberattack. But at the same time, these alleged benefits may create legal problems. Temporal distance between a cyberattack and the victim’s response may run afoul of legal prohibitions on purely punitive actions. If the responsive action takes the form of countermeasures—actions that would violate international law but for the prior internationally wrongful act—delay may make it more difficult for the responding state to meet the requirement that countermeasures be taken to induce the offending state to comply with international law.

The questions that Kello’s proposals raise simply prove his point about the need for interdisciplinary discussions to tackle the multifaceted challenges that cybersecurity poses. The book’s three-part typology of technological revolution will be particularly helpful in framing future discussions of cybersecurity both within and outside of international relations. And it can also be deployed to assess future technological developments. As Kello notes, “the distinguishing feature of security affairs in the current epoch is not the existence of a revolution condition but the prospect that it may never end” (257). Cyberweapons are today’s revolution, but tomorrow will surely bring another.

Kristen Eichensehr is an assistant professor at the University of California at Los Angeles School of Law.