The Security Dilemma of Cyberspace: Ancient Logic, New Problems

LUCAS KELLO


Students of international relations are trained to read history—even ancient history—as a prelude to the future. Among the eternal notions that theorists commonly invoke, one enjoys special appeal: the security dilemma. It originates in Thucydides’s famous claim that “increasing Athenian greatness and the resulting fear among the Spartans made [their] going to war inevitable.” A similar fear had fueled Athens’s grab at empire. Therein lies the dilemma: in the anarchic international system, the growing security of one state ensures the growing insecurity of others. This perverse logic produces occasional outbreaks of war, even when the contenders wish to avoid it, as in 431 B.C.

In The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations, Ben Buchanan argues that this ancient logic explains much of the incessant hostility that mars interstate dealings in cyberspace. The argument has three “pillars.” They can be summed up as follows: the development of offensive weapons requires advance intrusion into other states’ networks; maximizing defense also necessitates intrusion; therefore, states penetrate foreign networks whenever they can—even while interpreting intrusions against them as threatening. The cycle repeats incessantly. Let us first take the offensive incentives. They are familiar to security analysts. States penetrate other networks to develop weapons well in advance of needing them. This is because the design of sophisticated malware requires time, skilled operators, and intimate knowledge of the target system’s technical specifications. Without such knowledge the offensive craft is untenable. An attacker who does not burrow himself deeply into opponents’ cyberspace risks having an empty arsenal when a conflict occurs.

Operation “Nitro Zeus” illustrates this thinking. As Buchanan explains, in the early stages of the Obama Administration, U.S. hackers went on an expansive hunt for “zero-day” vulnerabilities in Iran’s strategic infrastructures. The raid targeted the Fordo nuclear facility that Washington suspected was purifying uranium to weapons grade. But that was not all. The United States also penetrated Iran’s financial, transportation, and air defense systems. The invaders acted in anticipation of the possible failure of diplomatic efforts to curtail Iranian enrichment activity peacefully. They
crafted weapons of war even as they strived to avert it.

The second pillar of the “cybersecurity dilemma” also involves a compulsion to hack, but for opposite reasons. Buchanan is no skeptic when it comes to the question of the offense-defense balance in cyberspace, which is a growing topic of debate within the security studies community. Like most policymakers, he accepts that the offense holds a notable advantage over the defense. The defender can reduce the yawning gap between the two sides if he complements passive measures (such as honeypots) with active defenses, or what I have described elsewhere as actions to neutralize threats within an adversary’s or a neutral party’s computer terrain. Buchanan’s use of the term “active defense” is consistent with that of information security specialists: that is, proactive measures that the defender takes within his own network. But, in fact, his main concern is external intrusions. These allow the defender to observe the adversary “in action” and obtain information about his future targets and weapons, as well as develop and deploy “tailored countermeasures” to neutralize them. Here emerges a twisted irony which fuels the security dilemma of cyberspace: intrusion in other states’ networks helps to identify and curtail intrusion in one’s own terrain.

Operational needs, therefore, drive states’ compulsion to penetrate—whether offensively or defensively. Thucydides explained the expansionist avarice of Athens on the basis of timeless verities of human nature. Buchanan’s study need not invoke them. He can explain computer intrusions in simple terms of rational and operational necessity. An important point about technological determinism flows from this observation: the technology itself aggravates the security dilemma. In conventional domains of conflict, defensive intelligence gathering is possible largely by means of remote observation: for example, the use of spy satellites to assess the enemy’s troop movements. But in cyberspace, the assessment of capabilities is far more difficult. It is possible only through deep and persistent insertion into the adversary’s computer terrain.

The third pillar unifies the first and second pillars to paint a dire scenario of fear and distrust. Because offensive action requires prior intrusion, because even defensive intrusion yields information that is valuable to the offense, states interpret all invasions of their vital infrastructures as inherent threats. This situation reflects an old bane of anarchic international politics: the unreliability of other states’ intentions as a measure of one’s own security. In the international jungle, even if an opponent assumes a seemingly non-offensive stance, by the time his aims are confirmed it could be too late to affect them. Capabilities, therefore, are the chief criterion by which states must assess foreign security threats. They determine the ability of adversaries to realize not only probable but also the worst-possible aims. When evaluating security threats, the politics of anarchy prioritizes relative power over intent.

But in the cyber domain, Buchanan explains, players often lack knowledge of both. This situation distinguishes the security dilemma of cyberspace from the classical security dilemma. Traditionally, contenders had access to reliable information about each other’s capabilities even if they doubted each other’s intentions. In the current context, however, they also lack credible or complete information about capabilities. Here is another splendid irony: states have both too much and too little knowledge—too much because they know about the existence of offensive arsenals (some nations such as Britain have openly admitted to their deployment) and not enough because the players do not know the weapons’ full potency or intended targets. Intelligence gathering by intrusion is the only viable way to gain such information. Thus knowledge and ignorance combine to intensify the fear
that lies at the heart of the security dilemma of international politics.

Buchanan’s account is not all gloom. It identifies possible “mitigator” pathways that could lessen the severity of the security dilemma. These include arms control measures, signaling techniques, and unit-level factors. The obstacles and poor record of each, however, steer the author away—faithful student of Thucydides that he is—from the Kantian hopes that animate the “transcender” camp of optimists. Take arms control. Despite a genuine desire among some nations to curtail the expansion of offensive weapons, the nearly massless properties of code complicate the task of arms verification, which is the essential prerequisite of successful arms control. Despite Buchanan’s alarm about the gravity of cyber threats, a careful reader will not confuse him for a fatalist. But he is no Kantian idealist either. He does not champion the false cause of “cyber peace”. One cannot dismiss the limited potential of the mitigator variables, he argues. Yet nor can one stake national security on the assumption that they will succeed.

Despite its many strengths, the work is not without limitations. One stands out: the priority it gives to state actors above all others. The book recognizes the potential of nonstate actors to cause problems. Their actions can interfere with interstate signaling during a crisis. They complicate attribution after an attack has occurred. Their number and offensive ability hinder the task of international arms verification. A powerful example of this problem was the intrusion by three teenage hackers (one of them foreign) into the U.S. military’s logistics systems in 1998, a move that Pentagon officials initially misattributed to Iraqi operators. Then there are the cyberattacks against Estonia and Georgia, both of which prominently featured private culprits. On Buchanan’s own terms, then, the book’s almost exclusive focus on state actors seems misplaced. All the more so because the destabilizing influence of players alien to the international system represents a major departure from the classical statist logic of the security dilemma. Greater attention to them would have strengthened the book’s central thesis, which is that the current security dilemma is similar but also worse than before. In seeking to apply Thucydides’ message, the author has read the old master all too closely.

Overall, what emerges from these lucidly written pages is an important service to the scholarship of both cyber issues and international relations. This combination of gains is rare. Some observers claim that the field of cyber studies in international relations is flourishing. It is not. For the existing literature betrays an important gap: it rarely engages directly with the theory and concepts of international relations. The notion of the security dilemma is a prized coin in the intellectual currency of the discipline. Buchanan’s conceptual analysis deals in gold.

Thucydides wished his epitaph to be, “I wrote for all the ages.” He would want to know how his teachings fared. The Cybersecurity Dilemma gives them new substance and credence. Drawing on contemporary theory of international relations, it adapts and applies the historian-prophet’s core insights to a new realm of conflict. Today many of his successors do not dare enter this unfamiliar field of study. They struggle to find points of relevance, or else they are daunted by technical arcana. This book shows that cyber studies within political science is both possible and promising. Theorists can apply classical concepts to elucidate new phenomena and to enrich the theory of their discipline. About the security dilemma of cyberspace the final sentence of the work states: “There is no easy way out.” Through careful theorization and detailed empirical work, Buchanan shows that for international relations specialists seeking to study this and other security problems, there is at least an easy way in.