H-Diplo | ISSF

Roundtable, Volume X, No. 6 (2018)

issforum.org

H-Diplo/ISSF Editors: **Michael C. Horowitz and Diane Labrosse**
H-Diplo/ISSF Roundtable and Web/Production Editor: **George Fujii**

Ben Buchanan. *The Cybersecurity Dilemma: Hacking, Trust, and Fear Between Nations*.
New York: Oxford University Press, 2017. ISBN: 9780190665012 (paperback, $37.95).

Published on **19 January 2018**

Shortlink: tiny.cc/ISSF-Roundtable-10-6
Permalink: http://issforum.org/roundtables/10-6-cybersecurity-dilemma
PDF URL: http://issforum.org/ISSF/PDF/ISSF-Roundtable-10-6.pdf

Contents

Introduction by Joseph S. Nye, Jr., Harvard Kennedy School

Cybersecurity is a relatively new foreign policy problem. A decade ago, it received little attention, but since 2013 the Director of National Intelligence has named cybersecurity risks the biggest threat facing the nation. The non-profit Council on Foreign Relations "Cyber Operations Tracker" contains almost 200 state sponsored attacks by 16 countries. The list includes one attack in 2005 when the data base starts, but over 20 last year.[1] The bad news is that the threat is increasing; but the good academic news is that the problem is now attracting a new generation of bright young scholars–as illustrated by Ben Buchanan's book and its reviewers.

The term cybersecurity covers a wide range of problems. Security was not a major concern among the small community of researchers and programmers who developed the Internet in the 1970s. In 1996, only 36 million people or about 1 per cent of the world population used the Internet. Within two decades, at the beginning of 2017, 3.7 billion people or nearly half the world population used the Internet. As the number of users escalated after the late 1990s, the Internet became a vital substrate for economic, social, and political interactions. Along with rising interdependence, however, comes not just opportunity but also vulnerability and insecurity. In the years to come, with big data, machine learning, and the "Internet of Things," some experts anticipate that the number of Internet connections may grow to nearly a trillion by 2030. The attack surface will expand dramatically.

Many problems of cyber security involve non-state actors, but Buchanan has carefully focused his book on the foreign policy of states and the implications of cyber technology for the classic "security dilemma" of international relations theory and policy. Going back to the pre-Internet theoretical writings of John Herz in the 1950s and Robert Jervis in the 1970s, the concept "security dilemma" refers to defensive efforts by one state that are intended to reduce its insecurity, but which create capabilities that cause fear and insecurity in other states which in turn feel they must respond.[2]

This creates a dangerous escalatory dynamic, particularly in contexts where technology seems to favor the offense over the defense. The cult of the offensive in 1914 is often used as an example. In the cyber age, Buchanan shows how states offensively intrude into other states' networks as a defensive preparation, but the same software that is used for espionage can easily be used for attack. It is often difficult to separate an effort to reconnoiter a possible opponent's capabilities from an effort to prepare the battlefield or to implant a logic bomb. Since the conventional wisdom in the cyber field holds that offense dominates defense, the potential for instability in cyber space appears grave.

Rebecca Slayton challenges that conventional wisdom, and argues that it is more accurate to say that some kinds of offenses have an advantage against some kinds of defenses. There is no technological determinism. Cyberspace is not a uniform thing, and whether defined in terms of relative cost, first mover advantage, or

[1] Council on Foreign Relations, "Cyber Operations Tracker" (website), https://www.cfr.org/interactive/cyber-operations.

[2] John H. Herz, *International Politics in the Atomic Age* (New York: Columbia University Press, 1959); Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30:2 (1978): 167-214.

relative utility, the cyber offense-defense balance must be understood in terms of specific pairs of adversaries, not as a systemic variable.

Jon R. Lindsay questions the strategic implications that Buchanan draws and argues that cyber technology need not exacerbate the political security dilemma between states. On the contrary, cyber may even help moderate the dilemma. Policy makers may be unwilling to use cyber operations early in a crisis because they perceive cyber as too provocative, but they remain unwilling to employ cyber later in the crisis because such operations seem less effective than kinetic military alternatives that they better understand. The real locus of cyber conflict may rest in the gray zones between peace and war that lie below the level of armed conflict such as we saw in Russian information warfare in 2016. States limit escalation because both sides agree de facto to avoid it, and cyberspace provides a venue for them to compete without escalating into kinetic conflict. In Lindsay's words, "awareness of the cybersecurity dilemma may help to disarm it." And as I argued in "Deterrence and Dissuasion in Cyperspace," these gray zones are difficult areas for deterrence to work.[3]

Nina Kollars points out that the security dilemma is inherently a state-centric dynamic, and while Buchanan's focus enhances the contribution of his book to international relations theory, it also narrows it. If states are not alone in cyberspace, how does that crowded space complicate the escalatory logic? Technology does not make all actors in cyberspace equal, but the low cost and low barriers to entry tend to reduce the power gap between state and non-state actors. As Kollars points out, only a state could have produced the Stuxnet attack on Iranian centrifuges, but in October 2016, the non-state Mirai botnet produced the single largest denial of service attack in the history of the Internet. And what is a "state" when the fluidity of agency means actors can move back and forth across a legal category? Some Chinese hackers worked for the People's Liberation Army from 9 to 5 and then for themselves from 5 to 9. How do we determine whether an actor is independent or a state proxy? How is this perceived, and by whom, and how do these perceptions affect security?

All three reviewers praise the importance and originality of Buchanan's book, though they point out that the tightness of his focus on the classic security dilemma leaves open many questions for future research. These include the roles of non-state actors; the nature of agency and proxies; the shaping of perceptions, the effect of changing contexts, the relation of kinetic and cyber options, uncertainties about the nature of escalation, and many others. But that is good news for this rising generation of researchers. Robots will not put them out of work.

Participants:

Ben Buchanan is a Postdoctoral Fellow at Harvard University's Cybersecurity Project at the Belfer Center for Science and International Affairs, where he conducts research on the intersection of cybersecurity and statecraft. His first book, *The Cybersecurity Dilemma*, was published by Oxford University Press in 2017. Previously, he has written on artificial intelligence, attributing cyber attacks, deterrence in cyber operations, cryptography, election cybersecurity, and the spread of malicious code between nations and non-state actors. He received his Ph.D. in War Studies from King's College London, where he was a Marshall Scholar, and earned masters and undergraduate degrees from Georgetown University.

[3] Joseph S. Nye, Jr., "Deterrence and Dissuasion in Cyperspace," *International Security* 41:3 (Winter 2016/17): 44-71; http://www.mitpressjournals.org/doi/pdf/10.1162/ISEC_a_00266.

Joseph S. Nye, Jr., is University Distinguished Service Professor and former Dean of the Kennedy School of Government at Harvard University. He received his bachelor's degree summa cum laude from Princeton University, studied at Oxford University on a Rhodes Scholarship, and earned a Ph.D. in political science from Harvard where he joined the faculty in 1964. From 1977-79, Nye was a deputy Undersecretary of State and chaired the National Security Council Group on Nonproliferation of Nuclear Weapons. In 1993-94 he chaired the National Intelligence Council, and in 1994-95 served as Assistant Secretary of Defense for International Security Affairs. He won Distinguished Service medals from all three agencies. Nye has published fourteen academic books, a novel, and more than 150 articles in professional and policy journals. Recent books include *Soft Power*, *The Powers to Lead*, *The Future of Power,* and *Is the American Century Over?* He is a fellow of the American Academy of Arts and Sciences, the British Academy, the American Academy of Diplomacy, and an honorary fellow of Exeter College, Oxford. He is the recipient of Princeton University's Woodrow Wilson Award, the Charles Merriam Award from the American Political Science Association, France's *L'ordre des Palmes académiques,* Japan's Order of the Rising Sun, and numerous honorary degrees.

Nina Kollars is an Assistant Professor of Government at Franklin & Marshall College and a scholar of military technological change. Her work emphasizes the role of individual and group adaptations to existing practices in war and conflict. She is author of several articles on technology and war, including "War's Horizon: Soldier-led Adaptation in Iraq and Vietnam," *Journal of Strategic Studies* 38.4 (2015): 529-553; "Military Innovation's Dialectic: Gun Trucks and Rapid Acquisition," *Security Studies* 23.4 (2014): 787-813; and "The Rise of Smart Machines: The Unique Peril of Intelligent Software Agents in Defense and Intelligence" in Michael Goodman, Huw Dylan, and Robert Dover, eds., *Palgrave Handbook of Intelligence and Security* (Palgrave Macmillan, 2017).

Jon R. Lindsay is the Director of the Trudeau Centre for Peace, Conflict, and Justice and Assistant Professor of Digital Media and Global Affairs at the Munk School of Global Affairs at the University of Toronto.

Rebecca Slayton is an Associate Professor jointly appointed in the Department of Science & Technology Studies and the Judith Reppy Institute for Peace and Conflict Studies, both at Cornell University. She is author of *Arguments that Count: Physics, Computing, and Missile Defense, 1949-2012* (MIT Press, 2013), and is currently working on a second book project, *Shadowing Cybersecurity*, which examines the historical emergence of cybersecurity expertise through the interplay of innovation and repair.

Review by Nina A. Kollars, Franklin & Marshall College

It is both necessary and regrettable that in the face of new phenomena, scholarship must first look back before moving forward. What else could explain the nearly decade long tradition of attaching the adjective 'cyber' to every possible concept in international relations? 'Cyber' wars will be launched, particularly those leading to 'cyber' Pearl Harbors, only to be outdone by the rise of 'cyber' terror-ism-ists, and the mother of all debates—the feasibility of 'cyber' deterrence. To be sure, these works must be written. It is the testing of all the tried and true organizing concepts of the past in order to leverage—however achingly slowly—our thinking forward. And so, in this vein, Ben Buchanan has done this service for international relations theory by resurrecting the security dilemma's logics and asking whether they also holds for cybersecurity.

Buchanan argues in the affirmative. States, he finds, are driven to offensively intrude into other states' networks as a means of defensive preparation. In doing so, the incentives for aggression in the name of defense emerge. And, as one might anticipate, concomitantly all of the associated concepts elucidated by Robert Jervis' expansion of John Herz and Herbert Butterfield's insights including: offense-defense balance, distinguishability, and arms racing.[1] As a piece of scholarship in an often murky hyper-technical new literature, Buchanan's book deftly weaves together foundational security dilemma concepts with clear technical prose that helps to illuminate the processes of computing systems exploitation. For these reasons alone, the book is an accomplishment, and a likely core addition to the canon of works in cybersecurity, (not to mention graduate-level courses in security studies, and cyber security policy).

The security dilemma is, at its core, a state-centric dynamic. It is a story about great powers interacting with other great powers and the potential escalatory effects of uncertainty mixed with weaponized technology. Working in lockstep with the concept's core assumptions, Buchanan also narrows the relevant units of analysis to states (though not necessarily great powers). He provides a double logic for the move. First, he selects states in order to situate his work 'within a long tradition of international relations scholarship.' Then he follows his disciplinary justification with an empirical one: "although non-state actors are quite important in cybersecurity and quite active in performing network intrusions, for the most part the most sophisticated capabilities still belong to states or those actors, such as contractors, serving in the interests of a state." (11)

Buchanan's disciplinary excuse for the state-centered hand wave is justified after a footnote clarifies that he is writing via the disciplinary tradition of realism. Quibbles among realists notwithstanding, there are obviously additional units of analysis and schools of thought (and their associated graduate school debates) in the spectrum of international relations literature. It is the second claim, that states are the most important actors in an era of digital hyper-connectivity that perhaps deserves additional consideration. Again, if the most important security question is whether the cybersecurity dilemma reveals similar dynamics in a world where states are the only relevant actors, the answer as amply demonstrated by Buchanan is yes. The uncertainty over state intent plus the characteristics of digital exploitation of computer systems logically creates an escalatory dynamic between states in terms of cyber conflict, and potentially spilling over into physical conflict.

[1] Robert Jervis, "Cooperation under the security dilemma." *World Politics* 30:2 (1978): 167-214.

But what if states are not alone in cyberspace? This, I worry, is the keystone that may interrupt or complicate the escalatory effects of the logic. On the heels of the 25th DefCon hacking convention held just after Black Hat and B-Sides (three of the most well-known cybersecurity industry conferences) in Las Vegas every year, I must admit, from the trenches it is nigh well impossible to imagine the dynamics of the international cybersecurity dilemma as constrained only to states.[2] In a mob of over 25,000 security researchers from around the world, more than 150 official speakers, and more than fourteen independent 'villages' where additional talks and hacks (vulnerabilities) are being shared, it is anyone's guess who is a state agent, independent agent, representative of an organization, or all three. What unifies them is that the elite security researchers in this community, the ones with the technical skill to conduct attacks or infiltrate state systems, do not aggregate well into the state.

Take, for instance, the fact that within that mob of security researchers was MalwareTech (aka Marcus Hutchins), the British security researcher who identified the kill switch for the WannaCry global ransomware attack on hospital systems. As I write this, MalwareTech remains in the United States awaiting trial. He was arrested by the FBI as he attempted to fly home to Devon from DefCon on six counts of creating the malicious code that resulted in the Kronos banking trojan--an allegation that Hutchins denies. MalwareTech is not working under the aegis of the state, and can only sometimes be understood as part of an organization. He is attacker, defender, and independent agent all at once. What he is not, in any part of this, is the state. When it comes to cybersecurity and the potential for escalatory conflict, it might well be that this particularly technically savvy set of individuals matters. They can be employed by states, private security firms, or simply operate out of their own homes. These are the non-state actors that Buchanan refers to.

The problem with constraining analysis of the escalation potential between two states strictly to states is that technically talented individuals can move fluidly into and out of the state's unitary grasp. The motivations of an expert in systems intrusion could varyingly be loyalty to country, economic pragmatism, revenge, activism, or the 'lulz' (fun). This fluidity of agency creates uncertainty regarding the attacking agent. That is, in cyber attacks, it is often unclear whether an attack has been orchestrated by a state, encouraged by a state, or that the state is simply a beneficiary of the attack. The WannaCry ransomware attack is purported to be traceable to Lazarus Group--a North Korean affiliated hacking group, but to what degree can the state be understood to have directed the criminal money-making attack? It is this kind of uncertainty that cyber attacks may create new uncertainties not yet clearly laid out in the security dilemma.

Under traditional security dilemmas, the two key areas of uncertainty are that of state intent and technological performance. What remains under-theorized here is uncertainty over the agent's degree of separation from the state. And, if there is uncertainty regarding the agent and their degree of separation this could change states' calculations regarding escalation. Ostensibly, states experiencing the effects of offensive moves for defensive purposes may well choose not to escalate violence because they cannot be sure that individuals and organizations may be the primary culprit, and the state simply the beneficiary.

A revisionist state may direct such attacks and attempt to plausibly deny having done so, particularly because attacks like WannaCry appear primarily financial, even though the disruption to hospital systems was clearly the secondary effect. Likewise two status-quo states may find themselves stuck in an ever-increasing frequency

[2] Information regarding these conferences can respectively be found at: Defcon.org, bsideslv.org, and blackhat.com.

of intrusions by all agents, but because of all the newly generated noise reveals an overall reluctance to treat intrusions as necessitating a physical response. It is these lines of thinking that are left by the wayside when Buchanan selects purely on states. There are likely more easily justifiable reasons to select states. Personally, I would start with the fact that the security dilemma is essentially a state-centered logic and therefore the responsible first step in analysis is to import those assumptions. In any case, Buchanan's conceptual justification feels largely like a rhetorical tool that permits him to bracket his observations and provide analysis.

In this sense, these comments are an invitation for scholars who follow Buchanan to build into these spaces. At a minimum, moving beyond state-only analyses might help explain the disjunction between the predictions of cyber warfare between great powers and its absence to date.

More importantly, it remains to be said that individuals matter in cybersecurity. They matter differently than individuals in international organizations, advocacy networks, or in any 'great man theory' of canonical international relations debates. Individuals matter in cybersecurity because while those prior individuals must rely on shaping opinions and setting norms, this set of technically savvy individuals can rewire bits of the architecture itself. And they do so, daily. One tinkerer needs only to find one vulnerability within a vast and simultaneously interconnected ecosystem. One tinkerer can be motivated by lust, lulz, or loyalty. And this all plays out on the overlapping digital playing fields of the world. Cyber attack and defense is not constrained to closed state-owned systems. Most of the attacks are happening outside the military and intelligence domains of control. This is why much of the panic in cybersecurity defense focuses on critical water and energy infrastructures.

The problem with lingering too long in rehashed logics like the security dilemma is that state centrality is embedded as a central component of the framework. From my vantage point, state-on-state cybersecurity dilemmas are not the central political problem underlying digital hyper-connectivity. Buchanan indicates that states have the upper hand on sophistication when it comes to cyber weaponry, but we should question whether sophistication would be the metric to grant states the crown in analytical priority. Sophistication made Stuxnet, the surgical weapon that disrupted Iranian centrifuges. Or perhaps there are other metrics. In October of 2016, the single largest distributed denial-of-service (DDoS) attack in the history of the internet was unleashed. The Mirai denial of service attack on Dyn (a Northeast internet traffic routing corporation) disrupted service for thousands of companies across Europe and the United States for days on end. The code for the Mirai botnet redirected the energies of tens of thousands of Internet enabled consumer devices like DVD players and digital cameras. Security journalist Brian Krebs traces the source of Mirai back to a turf war over customers who play Minecraft.[3] Yes, Minecraft, the online game. Krebs suggests that a Rutgers University student named Paras Jha, who runs a company called ProTraf that protects sites that profit from Minecraft players, may have written the program. The Mirai botnet was no sophisticated hack. It simply marshalled the security vulnerabilities known to exist in the internet of things ecosystem. While we continue to give analytical priority to states in all things 'cyber,' deep down in the weeds of information and computer security lurk the architects and tinkerers of the system. It may be time to bring them into the story.

[3] For more on Krebs' work see: Brian Krebs, "Who is Anna-Senpai, the Mirai Worm Author." *Krebs on Security* (2017), https://krebsonsecurity.com/2017/01/who-is-anna-senpai-the-mirai-worm-author/.

Review by Jon R. Lindsay, University of Toronto

The small but growing international relations (IR) literature on cybersecurity has developed as a stylistic debate between technologists and skeptics. The former argue that traditional IR theory cannot accommodate the technological novelty of cyberspace,[1] while the latter argue that cyberwar is little more than a new variation on age-old themes of espionage and covert action.[2]Yet the skeptical line of argument only shifts the question to whether and how intelligence activities matter for important IR outcomes such as the onset of war and the dynamics of escalation. The strategic import of intelligence (as distinguished from the politics of intelligence organizations or narratives of particular historical operations which comprise the current field of intelligence studies) is an understudied topic in the theory of IR, even as the use of secret ways and means for the ends of statecraft is an important part of the practice of IR. Intelligence is especially important in the twenty-first century because ubiquitous, globally interconnected technologies in every societal and governmental sector expand both the supply and demand for covert collection and influence. Providentially, the secret dimension of statecraft has recently begun to receive more attention from IR scholars, notably Austin Carson, Dov Levin, Michael Poznansky, Joshua Rovner, and Keren Yarhi-Milo.[3] With *The Cybersecurity Dilemma*, Ben Buchanan contributes to this emerging body of work by grounding cybersecurity in intelligence as a starting point for his analysis rather than dismissing it as a conclusion.

Academics and practitioners will find much to like about this book—and much to debate. Buchanan charts a promising middle path between the technological Cassandras and the political skeptics by leveraging a foundational IR concept to make sense of the unique challenges of global information systems. His text is grounded in technological detail without being technologically determinist, making good use of open source threat reporting and the rich trove of classified data leaked by Edward Snowden and others. Buchanan also insists on the importance of political context, for example by highlighting the non-technical aspects of attributing responsibility for an intrusion such as the assessment of political motivations and corroborating evidence from non-cyber sources, without minimizing the significance of pervasive digital infrastructure in contemporary global politics. The highlight of the book is Buchanan's elegant and accessible account of the operational characteristics of covert cyber campaigns. However, I question some of the strategic implications

[1] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012); Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38:2 (2013): 7-40.

[2] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35, no. 5 (2012): 5-32; Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38:2 (2013): 41-73; Brandon Valeriano and Ryan C. Maness, *Cyber War versus Cyber Realities: Cyber Conflict in the International System* (New York: Oxford University Press, 2015).

[3] Austin Carson, "Facing Off and Saving Face: Covert Intervention and Escalation Management in the Korean War," *International Organization* 70:1 (2016): 103-131; Dov H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* 60:2 (2016): 189-202; Michael Poznansky, "Stasis or Decay? Reconciling Covert War and the Democratic Peace," *International Studies Quarterly* 59:4 (2015): 815-826; Joshua Rovner, *Fixing the Facts: National Security and the Politics of Intelligence* (Ithaca: Cornell University Press, 2011); Keren Yarhi-Milo, *Knowing the Adversary: Leaders, Intelligence, and Assessment of Intentions in International Relations* (Princeton: Princeton University Press, 2014).

he draws about their escalatory potential. The cybersecurity dilemma, as Buchanan describes it, need not necessarily exacerbate a political security dilemma between states, and may even help to moderate it.

The security dilemma arises in anarchy when one state's defensively-motivated acquisition of military capability ends up posing offensive threats to other states, thereby heightening the risk of conflict spirals. In short, more power leads to less security. The idea is attractive for explaining, as Buchanan writes, "how misinterpretation can lead to outcomes that no state wants" (194). As one of the most venerable conceptual tools in the IR theory kit, it has been applied to problems as varied as arms racing, alliance relations, the onset of World War I and the Cold War, and ethnic civil war, although not always consistently.[4] The most influential modern articulation by Robert Jervis, moreover, lends itself naturally to the study of intelligence, which can be expected to have some effect on perception and misperception in international politics. Jervis explicitly includes technology in his seminal article on the security dilemma, arguing that when offensive capabilities have a relative advantage over defensive measures and offense cannot be distinguished from defense the security dilemma becomes "doubly dangerous."[5] Buchanan argues analogously that the tactical advantages enjoyed (or perceived to be enjoyed) by the attacker in cyberspace, together with the fungibility of methods used for intelligence collection and infrastructure disruption, gives rise to a "cybersecurity dilemma" whereby defensive intrusions by one state undermine the cybersecurity of the target state, potentially undermining strategic stability.

The extension of classic security-dilemma logic to the intelligence arena, and in particular to cyber sources and methods, requires Buchanan to take some extra steps to link intelligence mechanisms to the diplomatic mechanisms at the heart of the security dilemma. Intelligence (and counterintelligence efforts to block or redirect it) takes place in peacetime as well as war and may be quite active even in the absence of overt military moves. Intelligence has the potential to enhance the potency of the state's military capabilities (e.g., by improving battlefield surveillance, targeting, and combat assessment), and it can provide information about vulnerabilities in the military capabilities of target states. As such, intelligence may be an intervening variable in the development of offensive potential that activates security-dilemma logic. Yet Buchanan goes further to highlight the ways in which some intelligence activity more directly complicates the target assessment of intentions. Buchanan argues that "close access" collection programs (e.g., human agents in foreign societies, air or submarine penetration of territorial airspace or waters, and computer network intrusions) "can also pose a direct threat" because they "violate the sovereignty of another state, come alarmingly close to doing so, or are otherwise deeply intrusive," which in turn prompts the target to "worry that intruders might be attackers, rather than collectors" (25). Buchanan thus extends the classic problem of offense-defense indistinguishability to the related but distinct intelligence problem of collection-disruption indistinguishability. This is not a cyber problem per se, as a human agent can work as a spy one day and a saboteur the next, but the problem is particularly acute in the cyber domain.

Buchanan makes the case for the exceptional nature of cyber operations in this respect in three steps (which he describes as "pillars of the cybersecurity dilemma"). First, he argues that intrusions into complex, arbitrary, remote, sensitive target networks require considerable advanced preparation, organizational skill, and may maintain persistence for years. This important point runs counter to the conventional wisdom on cyberwar

[4] Shiping Tang, "The Security Dilemma: A Conceptual Analysis," *Security Studies* 18:3 (2009): 587-623.

[5] Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30:2 (1978): 167-214.

that it is a low cost, high speed form of operations. Disruptive moves in cyberspace that aim to create targeted and thus politically useful destruction require a lot of supporting intelligence and planning, and in many cases leverage the same methods to penetrate the target, thus advance collection becomes a latent operational threat. Second, Buchanan argues that defensive cyber operations must also engage in offensive intrusions to identify intrusions aimed against them, learn about adversary capability, and, potentially, engage in active counterintelligence efforts to subvert or redirect the adversary's cyber operations. Defense cannot be purely local or passive, in other words. Chapters 2 and 3 (which make the offensive and defensive arguments, respectively) are the highlight of the book and deserve a place on syllabi for IR courses on cybersecurity. They provide a fresh, nuanced, and richly illustrated overview of how modern cyber operations work, grounded in extensions of intelligence tradecraft rather than the inappropriate military metaphors found in so much popular cyber discourse.

Buchanan's third "pillar" is an argument that intrusions have an inherent escalatory potential because they can be leveraged to stage disruptive strategic attacks on critical infrastructure, promote more potent operations in other domains, and drain counterintelligence resources. This argument is less convincing. Research by Jaqueline Schneider involving a series of wargames conducted by U.S. civilian policymakers and military personnel finds that players were unwilling to employ cyber operations early in a crisis, because they were perceived as too provocative, but were unwilling to employ them later in lieu of kinetic military options, because they seemed less effective in pursuing their strategic goals.[6] How can hacking be both provocative and ineffective? One possible answer is that real offensive cyber operations are most attractive precisely in situations where actors would like to avoid escalation and thus make a strategic choice to act below the target's threshold of retaliation, i.e., in the so-called gray zone between peace and war. It is notable that states hit by disruptive attacks and concerted espionage campaigns have either done nothing, responded with less provocative measures like economic sanctions, engaged in restrained covert responses, or otherwise pulled their punches. Escalation is avoided, in part, because both sides agree to avoid it, and cyberspace provides a venue for them to compete without escalating into kinetic conflict. Awareness of cybersecurity dilemma may help to disarm it.

The danger of the cybersecurity dilemma in Buchanan's account relies on the assumption that "escalation makes sense" when "higher stakes lead to greater urgency and fear" (99). Sometimes, however, high stakes can make de-escalation attractive. If the discovery of systematic intrusions reveals either that the intruder will have a decisive military advantage in war or is more resolved the fight for the issue at stake, then the target has an incentive to make concessions rather than fight a war that it has learned through the discovery will leave it worse off. Buchanan holds that "the core of the cybersecurity dilemma is about fear and escalation" (193), but this is based more on speculation about crisis misinterpretation rather than a theory of escalation that couples the cybersecurity dilemma to the political security dilemma. Chapter 1 opens with an anecdote about an American U-2 spy plane that strayed into Soviet airspace at the height of the Cuban Missile Crisis. It might have started World War III, perhaps, but in fact it did not. Cyber operations might similarly cause inadvertent escalation, but so far they have not. Cybersecurity research in general has struggled to move from technological possibility to political probability grounded in a causal and conditional mechanisms.

[6] Jacquelyn Schneider, "The Information Revolution and International Stability: A Multi-Article Exploration of Computing, Cyber, and Incentives for Conflict" (Ph.D. Dissertation, George Washington University, 2017).

Throughout the Cold War both the United States and the Soviet Union engaged in aggressive intelligence collection against the other. Because intelligence had the potential to confer military advantage and subvert friendly institutions, each side had an imperative to counter these efforts, and thus to detect and avoid these very countermeasures. The intelligence-counterintelligence contest was costly but also informative. Both sides learned what the other side cared about, and also about how and where aggressive moves might be challenged. Both sides adapted their tradecraft continually and sought new intelligence and covert advantages, but by doing so managed to avoid more costly contests. As Brendan Green and Austin Long demonstrate, the U.S. military aggressively pursued counterforce options against Soviet strategic forces that relied on intrusive clandestine intelligence collection, and as the Soviets detected these efforts they became better informed about their strategic disadvantages.[7] The notion of the stability-instability paradox—the idea that nuclear deterrence credibly prevents nuclear war over vital interests but cannot credibly prevent and thus encourages conventional and subconventional challenges in peripheral theaters—is often represented as a tragedy because it generates excess conflict; an unappreciated upside, however, is that conflict at low levels (i.e., in the gray zone) may be the price of stability at more dangerous levels. An active intelligence-counterintelligence contest may be important precisely for avoiding escalation. In the twenty-first century, this could translate into a high degree of instability within the cyber domain, but not necessarily strategic instability across other military domains.

Buchanan is persuasive in demonstrating the incentives for both sides to actively and continuously engage in intrusive operations, both to prepare future offensive contingencies and to identify and defeat them; however, it is a logical leap to couple this intelligence-counterintelligence contest to a downward spiral in strategic stability. If offensive intrusions require careful planning, as Buchanan convincingly demonstrates, and if those intrusions become even more difficult in the face of defensive intrusions, as Buchanan also demonstrates, then a skilled attacker will be reasonably concerned about the efficacy of its own disruptive attacks. If collection and disruption depend on the same methods, and a failed disruption attempt reveals offensive exploits, then the failure ends future collection opportunities that use the same methods. Opting to preserve collection and forego disruption, on the other hand, remains quite attractive because while success might mean political or military intelligence advantage, failure means only the loss of sources and methods that, albeit with some effort, might be reconstituted without necessarily conveying hostile intent. To put it another way, cyber operations are *so* good for collection that the collection-disruption indistinguishability at the heart of the cybersecurity dilemma may not be as dangerous as Buchanan suggests.

The Cybersecurity Dilemma takes an important step toward grounding cybersecurity in intelligence affairs, and it deserves a wide readership. Yet in skillfully navigating many contemporary strategic conundrums, Buchanan stops short of explaining the political utility of covert means, in particular the decision to resort to particular cyber tools at a particular level of severity in a given international situation. This is in part an issue of scope, as Buchanan himself recognizes. He notes that the most dangerous cybersecurity dynamics may be activated only when the most vital systems are involved and only in the most unstable crisis situations. Yet the vast majority of cyber insecurity we observe, the empirical examples Buchanan uses to illustrate his points, and the threats about which policymakers are rightfully concerned, seem to fall outside this scope. Headlines are full of major

[7] Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38:1-2 (2014): 38-73; Brendan R. Green and Austin Long, "The MAD Who Wasn't There: Soviet Reactions to the Late Cold War Nuclear Balance," *Security Studies* 26:4 (October 2017): 606-641.

breaches of leading firms, government agencies, and civil society organizations, interference in foreign elections, and sophisticated elaborations of covert action that are frustrating because they elude traditional means of mitigating threats, and that is precisely why strategic actors choose them. Something like a cybersecurity dilemma is probably at work driving innovation and proliferation in these pervasive intelligence-counterintelligence contests, but more work remains to be done in disentangling the logic of the security dilemma, conflict spirals, escalation, covert action, and restrained or gray-zone conflict. The instrumental use of deception in all of its forms is a lacuna in the traditional canon of IR theory; fortunately, this is beginning to change through the efforts of scholars like Buchanan. Meanwhile, the practical opportunities for deception are increasing, ironically enough, precisely because of the greater willingness of actors of all kinds to trust their affairs to digital systems. An underlying paradox that Buchanan approaches but does not engage is the fact that the security dilemma is grounded in anarchy, and yet cyber insecurity is founded on global sociotechnical institutions, nearly the opposite of anarchy. Cyber conflict persists within and shapes the cooperative buildout of the shared infrastructure that enables it.

Review by Rebecca Slayton, Cornell University

The security dilemma is a well-established problem in international relations: in order to assure their own security, states build up military strength and take other measures that appear threatening to other states, which respond in kind in order to assure their own security, leading to continued escalation and heightened risks of conflict. In this well-researched and clearly-written book, Ben Buchanan applies this concept to contemporary cyber conflict. An introductory chapter defines the "cybersecurity dilemma:"

> To assure their own cybersecurity, states will sometimes intrude into the strategically important networks of other states and will threaten—often unintentionally—the security of those other states, risking escalation and undermining stability (3).

Buchanan draws on a number of new sources to make this argument, including material leaked by Edward Snowden. The result is an accessible and informative analysis of international cyber conflict which will be widely read and cited. The great strength of the book is its applying an established framework to the highly specialized and secretive worlds of military and intelligence cyber operations. However, these are relatively narrow terms of reference which lead to some limitations, such as an occasional over-emphasis on the novelty of cyber conflict and a tendency to lose sight of broader context. In this review I will briefly outline the chapter-by-chapter arguments of the book with comments on some minor areas of potential disagreement, before discussing three broader limitations.

The first chapter briefly outlines scholarship on the security dilemma, a notion first proposed in the 1950s. Buchanan notes that some scholars believe that the security dilemma is unavoidable, others argue that its risks can be mitigated, and still others believe it can be transcended; he places himself in the "mitigator" (22) camp.

Chapter two models the process of network intrusions and argues that "the dangerous incentive structure of the cybersecurity dilemma derives directly from this operational reality" (33). Here Buchanan describes the slow and meticulous process of cyber intrusions, which is a refreshing departure from slogans about such operations occurring at the 'speed of light.' Nonetheless, this chapter may over-emphasize differences between cyber and conventional operations. For example, it claims that unlike conventional operations, cyber operations don't gain momentum in their final stages because intruders can maintain persistence—communication with their malicious software—with an indefinite period of time in which to activate their payload. In practice, cyber intrusions may gain momentum for at least three reasons: persistence can be particularly difficult to obtain and maintain in systems not connected to the internet; the longer an intruder waits, the more likely it is to be discovered; and the target could at any moment change its computer system in ways that either deliberately or accidentally render an exploit obsolete.[1]

[1] On the difficulty of maintaining persistence, see Dale Peterson, "Offensive Cyber Weapons: Construction, Development, and Employment," *Journal of Strategic Studies* 36:1 (2013). The timing issues are discussed in more detail in Drew Herrick and Trey Herr, "Combating Complexity: Offensive Cyber Capabilities and Integrated War Fighting," (2016) https://ssrn.com/abstract=2845709.

The overall argument of chapter two is that "since states are able to do more kinds of preparation" for cyber operations than for other kinds of operations, they have "good reason to do more than plan and build—they have incentives to intrude and gain access" (48). Although the chapter focuses on the unique process of preparing for cyber operations, the issue is a more general one; cyber intrusions provide expanded means of preparing for *many* kinds of operations, as suggested in Chapter four.

The third chapter models the process of cyber defense, and uses this to argue that "fully maximizing network security necessitates intrusion into the networks of other actors" (52). In simplest terms, states use cyber espionage to maximize their cybersecurity. This is an important observation, but again, it is not unique to cybersecurity—cyber intelligence is used to maximize all kinds of security.

A fourth chapter explores several types of threats posed by network intrusions: they can enable cyberattacks or establish a beachhead from which to launch additional operations, including operations with kinetic effects; they can change the conditions of future conflict or operations; and they can be used for counterintelligence, i.e. discovering and thwarting an adversary's intelligence operations. Here the uniqueness of cyber operations appears more persuasive. Cyber operations provide a new set of methods for accomplishing military, economic, and political objectives, and they blur the lines between espionage and use of force. The difference between an offensive and defensive intrusion is largely in the intention of the intruder, and thus even defensive intrusions create considerable anxiety for their target.

Chapter five explores four "variables" that have been proposed to mitigate the security dilemma, arguing that each fails in the arena of cybersecurity. First, if geography and technology favors the defense, states will not feel the need to prepare for offenses; Buchanan argues that cyberspace favors the offense. As I suggest below, this is overly simplistic. Second, if offensive and defensive technologies are distinguishable, then states can agree to pursue defensive technologies and thereby alleviate anxieties; the offensive or defensive nature of many cyber operations, however, often lies only in the intention of the operator. Third, states can use policy measures such as arms control agreements, defensive doctrines, or unilateral restraint to signal non-threatening intentions; Buchanan argues that these measures fail (though a concluding chapter proposes policies that would signal non-threatening intentions). Fourth, democratic peace theory proposes that democracies are more transparent and less likely to go to war, features that ought to mitigate the security dilemma; here Buchanan objects that states' misplaced confidence in the correctness of their internal political systems could amplify the security dilemma.

In Chapter 6 Buchanan proposes two additional variables which he claims are implicit in the security dilemma, but become particularly visible in the cybersecurity dilemma. The first concerns the credibility and timeliness of information about capabilities relative to the speed with which capabilities are developed and deployed. Buchanan argues that the most dangerous situation is one in which states have some information about others' capabilities as they are developed and deployed, but nonetheless have substantial uncertainties, and that this is where cybersecurity is positioned. Second, Buchanan claims that the security dilemma usually presumes a status quo from which actions of states begin to appear threatening. While status quo understandings of the significance of technologies like nuclear weapons and anti-ballistic missiles were eventually reached, very little agreement has been reached about cyber weapons.

Chapter 7 anticipates and responds to three objections to the book's argument; for the sake of brevity, I will not recapitulate these here. Chapter 8 recommends three mitigations to the cybersecurity dilemma: developing baseline defenses that make successful offenses more difficult; advancing bilateral trust among the

most powerful and capable states; and contributing to system-wide security through costly signaling measures, such as enabling stronger encryption and releasing zero-days. A concluding chapter reiterates the dangers of the cybersecurity dilemma.

The book is written for a broad audience, including policymakers who may be unfamiliar with international relations theory. This may be why it simplifies or ignores some substantial disputes within the scholarly field of international relations. For the most part it applies a particular interpretation of the security dilemma (defensive realist) to a particular set of ideas about cyberspace (offense dominates, persistence is straightforward, etc.) Unfortunately, this somewhat narrow framing limits the validity of some of the conclusions. Here I outline three limitations.

The first is implicit in the very definition of the cybersecurity dilemma. States intrude into others' networks not to "assure their own cybersecurity," but to assure their own security more broadly, as well as to gain strategic economic, political, and military advantages. The United States and Israel intruded on the networks of Iran's nuclear enrichment facilities, not to protect their own cybersecurity, but rather to protect Israel from the prospect of an Iranian nuclear weapon, and as an alternative to Israeli calls for an overt bombing attack. Chinese industrial espionage is not an effort to protect China's cybersecurity, but to gain economically and sometimes militarily. The book certainly does recognize these broader implications, particularly in Chapter 4. But it does not analyze the detailed interaction between cyber operations and other kinds of operations; the book's careful models of network intrusions and network defenses are largely separated from broader strategic context. This is unfortunate, because the interactions between cyber operations and military operations have important implications for the book's argument. For example, Erik Gartzke has persuasively argued that if military offenses rely more heavily on command and control than military defenses, as is generally assumed, then the presumed offense-dominance of cyberspace would actually favor military defenses.[2] Cyber operations would then mitigate the security dilemma, contrary to the implication of the book.

A second and related limitation is the book's acceptance of both offense-defense theory and the common assumption that cyberspace favors the offense. The book does not define offense-defense balance, stating simply that it is determined by geography and technology. Yet this is not an uncontroversial claim. Much ink has been spilled about how to define offense-defense balance, and whether it is even a meaningful concept.[3] Some of the relevant texts appear in a footnote about a literature that is described as having "spun off from the original discussion" by addressing the "general challenges" of categorizing technologies as offensive or defensive (226). However, this mischaracterizes what has been a more fundamental debate about the very concept of offense-defense balance.

[2] Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security* 38:2 (2013).

[3] Much of this debate is represented in Michael E. Brown et al., eds., *Offense, Defense, and War* (Cambridge: MIT Press, 2004). See also Jack S. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28:2 (1984); Sean Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4:4 (1995). Whereas most offense-defense theories focus on the role of technology, Stephen Biddle has persuasively argued that operational skills are much more significant in determining who prevails in war and under what circumstances. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton: Princeton University Press, 2004).

The book's acceptance of cyber offense-dominance is somewhat surprising, since it details many challenges for the offense. In fact, one of the recommended mitigations for the cybersecurity dilemma is to invest in "baseline defenses" (158)—something that would seem to be a losing battle if cyberspace inevitably favors the offense. It even claims that zero days are "rare" (a characterization some would dispute) and notes that the majority of successful intrusions utilize known vulnerabilities that could in principle be patched (108). Buchanan nonetheless argues that offenses are dominant because geography, a principle source of defensive advantage in territorial conflict, is "minimally present in cyber operations" (106), and because vulnerabilities are difficult to fix in older computer systems that are no longer supported by the manufacturer.

It is undoubtedly true that some computer systems—particularly older systems and industrial control systems running physical machinery—are difficult to patch. However, this also suggests that defensive disadvantage is not universal. It would be more accurate to say that some kinds of offenses have an advantage against some kinds of defenses. It is much easier to gain access to and persistence within an internet-connected network than it is to gain access and persistence in a physically isolated and air-gapped network in a hostile nation (in some cases, geography is very present). Evidence suggests that mature organizations can reduce the costs of defense through better management capabilities; likely the same could be said about the costs of offense. Given the vast variation in computer systems and organizational capabilities for maintaining those systems, it simply does not make sense to speak of cyberspace favoring the offense or defense, as if cyberspace were a uniform thing. However it is defined—in terms of relative cost of offense or defense, first-mover advantages, or relative utility—the offense-defense balance of cyber operations must be understood in terms of specific dyads of adversaries and not as a systemic variable.[4]

The book notes that several prominent defense officials emphasize offensive advantage. While these perceptions are ultimately what create the cybersecurity dilemma, they should not be taken at face value. This is related to a third limitation: the book tends to overlook domestic political and economic interests that contribute in substantial ways to international anxieties about cyber-intrusions. Claims about the offense-dominance of cyberspace have a bureaucratic political context: they are often implicit or explicit requests for greater authority and resources for offensive cyber-operations. Judging from the rapid expansion of Cyber Command, these claims have been somewhat successful. This doesn't mean that the claims are disingenuous, but sincere beliefs can nonetheless be misguided—indeed, this is the basis for arguments about the "cult of the offensive."[5]

Similarly, cybersecurity is a growing industry that capitalizes on and often encourages anxieties about cyber-intrusions. Buchanan acknowledges industry interests in passing. He draws much of his technical evidence from "professional reports on noteworthy intrusions by computer forensic analysts," and notes: "Splashy report covers, sometimes replete with custom logos, demonstrate that marketing is an ancillary purpose for some of these files" (10). I have no qualms about Buchanan's use of technical information from these reports. However, these reports are not merely sources of technical information; they also help to shape the

[4] For a more thorough discussion of different conceptions of cyber offense-defense balance, with an empirical analysis showing that Stuxnet likely favored the defense, see Rebecca Slayton, "What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment," *International Security* 41:3 (2017).

[5] For similar arguments in the context of cyberspace, see Peter Singer and Allan Friedman, "Cult of the Cyber Offensive," *Foreign Policy*, 15 January 2014, http://foreignpolicy.com/2014/01/15/cult-of-the-cyber-offensive/.

perceptions of threat that are the focus of the book. Anxieties about cyber operations and the tendency to build up offensive capabilities are not simply a result of interactions between nation-states, i.e. the "cybersecurity dilemma"; they are also a result of domestic political and economic processes.

Despite these limitations, there is much to like about this book. It highlights a serious problem—growing international tensions and anxieties about cyber-intrusions, and associated risks of conflict escalation and instability. It provides accessible models of how cyber-intrusions and cyber-defenses proceed, and thereby highlights the challenges of both offense and defense. It also provides several practical recommendations for actions that could help to ease international tensions. For all of these reasons, it should be widely read.

Author's Response by Ben Buchanan, Harvard University

One of the curiosities of the book publishing process is the temporal gap between watching a manuscript at last go off to the presses and hearing feedback on how it fared. This wait is one of anticipation but also one of apprehension. What if the book, the product of years of work, is misunderstood? What if it is not appreciated? What if it is not read at all?

For me, the anticipation and apprehension began to resolve partially with a series of reviews of *The Cybersecurity Dilemma* after its publication. But few venues can go into as much depth as an H-Diplo/ISSF Roundtable does, and so reading the thoughts of Joseph Nye, Nina Kollars, Jon Lindsay, and Rebecca Slayton has been an additional delight. I am grateful to all of them for taking the time to consider my book and write thoughtful analyses. Each reviewer shows that he or she understood the aims of my work. I am gratified to hear that they for the most part seem to think I have achieved those goals and recommend the final product.

In particular, I am heartened to hear that each reviewer praised the book's discussion of the mechanics of cyber operations as interesting and useful. *The Cybersecurity Dilemma* is unabashedly a work of political science, but it by necessity draws on technical sources and seeks to explain these in an accessible fashion to the reader. Too often, in international relations the frame is solely strategic, with less appreciation for the operational reality that informs, or ought to inform, the strategy. My goal was to focus first on this operational reality—the laws of physics that govern international hacking—and then use those insights to craft and analyze strategy. I acknowledge that, because of the technical nature of the topic, doing so was risky. I am grateful to hear that the decision paid off, at least in the minds of these three reviewers.

With the remaining space I have, I would like to focus on the areas where the reviewers and I might differ and on where the academic research could go from here. In considering Rebecca Slayton's analysis, the area of her discussion that deserves the most attention is that of offense-defense balance. Here, she suggests that "The book's acceptance of cyber offense-dominance is somewhat surprising, since it details many challenges for the offense." I do not agree with this characterization; I do not think, nor did I try to suggest, that the offense has a systemic advantage. In fact, I agree with Slayton that it is not particularly sensible to think of the offense-defense balance as a global variable, and it is more tenable to treat it as a dyadic one. Even if one does think of it as systemic, Slayton is right to point out that I spend an enormous amount of space on the significant challenges in offensive operations, with an entire chapter devoted to that point.

What I do suggest, however, is that it does not particularly matter what I or any academic thinks on the matter of offense-defense balance in cybersecurity. Instead, I write, "With offense-defense balance it is perception, not reality, which is most important." As I outline with the exemplar of World War I, it is the conception of policymakers that matters for security dilemmas, not ground truth nor scholars' attempts to discern it. The cybersecurity dilemma does not require offense to have a global advantage in cyberspace; it merely requires that policymakers think this to be the case. As I show with a range of examples, up to and including President Barack Obama, senior military and intelligence leaders, and analysis of Chinese doctrine, this perception of offense-dominance is widely held. For her part, Slayton notes that, "While these perceptions are ultimately what create the cybersecurity dilemma, they should not be taken at face value." I do not take these perceptions as a substitute for facts—and I know that Slayton has made her own admirable

attempts to think critically about what the facts of offense and defense in cyberspace are[1]—but there is no real dispute that it is policymaker perceptions and misperceptions that create security dilemmas of any type.

Nina Kollars is more interested in the role of non-state actors in all of this. She accepts my initial move to focus on the activities on states in my analysis, rightly noting that the security dilemma discussion has long been state-centric. She does wonder, though, whether future analyses could build on my work and focus on non-state actors, too. I certainly encourage this line of further inquiry and think that the consideration of non-state actors in the cybersecurity dilemma is a natural next step.

Though Kollars and I agree on the direction of future research, I am slightly more skeptical than she about the power of non-state actors. She cites the DEF CON hacking conference, with its many participants, as a sign of the prowess of individuals. As a fan and attendee of DEF CON and hacking conferences, I certainly accept this. However, I do think there are reasons to believe that states have enormous capabilities that no individual could attain. I outline in the book, for example, how secret relationships between telecommunications companies and the United States intelligence community, as well as the American compromise of overseas telecom networks, provide the United States with an asymmetrical advantage in gathering secrets and in delivering malicious code in a stealthy fashion. For their part, the Chinese deftly turned their Great Firewall—a tool only a state, and indeed only that state, could build—into a Great Cannon in 2015 when they attacked GitHub. States have power that individuals simply do not, and, as I have explored in other work, often the flow of new large-scale hacking tools and techniques is from the state to the individual, not the other way around.[2]

For those focusing on non-state actors, what is potentially more interesting than non-state actors' power to disrupt and destroy is the power to expose and explain. As I outline in my discussion on sourcing, cybersecurity researchers exposed many of the cyber operations that I discuss, including some that likely cost tens of millions of dollars. Operations that were likely classified at some of the highest levels of government make their way into public view due to the power of investigating individuals. This is remarkable, and without much precedent; during the Cold War, for example, there did not exist an entire industry and schools of academic thought dedicated to finding and disclosing the human intelligence sources of the United States and Soviet Union. The work and effects of cybersecurity researchers should both inform academic study as well as be the subject of it. As an aside, Slayton notes that academics might be misled by the profit motive of some of these companies; this is a fair concern, and I note in the book how I took care on this point (10), but it is important to acknowledge that the analyses of competing companies often agree, and that many of the researchers, such as academics or those at civil society groups like Citizen Lab, do not have a profit motive.

This brings us to Jon Lindsay's review. He deftly grasps the way in which computer hacking is an outgrowth of an intelligence, not a military, capability. He and I agree about the need to focus on practical cyber capabilities rather than old metaphors or abstract ideas. Where we differ, at least slightly, is on how provocative cyber capabilities are perceived to be. Lindsay suggests that policymakers will be able to manage

[1] Rebecca Slayton, "What Is the Cyber Offense-Defense Balance?" *International Security* 41:3 (2017): 72-109.

[2] Ben Buchanan, "The Life Cycles of Cyber Threats." *Survival* 58:1 (2016).

the fear associated with suffering a critical network intrusion, choosing not to escalate and forestalling the cybersecurity dilemma.

The evidence on this point is mixed. Lindsay is right in that no kinetic strike has ever been launched in response to a cyber attack. He is right as well that the vast majority of cyber operations take place in the gray zone. I would go so far as to suggest that these hacking activities in the gray zone represent one of the most understudied parts of international affairs. On the other hand, states that suffer hacking, even when the operations are not disruptive, often conceptualize the threat using military concepts, not intelligence ones. The then-deputy Secretary of Defense Paul Hamre warned Congress that "Moonlight Maze," a massive Russian espionage into unclassified American networks in the late 1990s, meant that the United States was "in the middle of a cyber war."[3]

Similarly, during "Solar Sunrise," an espionage effort in 1998 against the American military, top government officials feared it was a harbinger to a crippling blow by Saddam Hussein's hackers. Instead, it was a hack carried out for fun by three teenagers and a twenty-year-old. In short, the record indicates that misinterpretation does sometimes happen, and minor incidents are mistaken for serious ones. I, like Lindsay, am grateful that this has not yet escalated into conflict, but I am less reassured that it will never do so, especially as cyber capabilities continue to develop in potency. My fear is that this will happen during an already-existing crisis, when policymakers will not be as staid and restrained as we might like.

Most significantly, Lindsay acknowledges that it is perception that once again governs. These perceptions can change, both over time and with shifts in leadership. For example, future historians will likely conclude that the Obama Administration, which was perhaps too cautious on Russia's cyber activities against the American election in 2016, was more reserved than the Trump White House. One role for policy-relevant research is to lay out the facts and provide explanations, thus shaping the perceptions that matter most. Lindsay notes that "Awareness of cybersecurity dilemma may help to disarm it." Indeed, I could not agree more; that was my enduring motivation for writing this book.

[3] For more on this case and Solar Sunrise, see Thomas Rid, *Rise of the Machines* (New York: W.W. Norton, 2016).