1
Introduction

HERBERT LIN *and* AMY ZEGART

In March 2016 we held a two-day research workshop on the strategic use of offensive cyber operations. The workshop brought together distinguished researchers from academia and think tanks as well as current and former policymakers in the Department of Defense (DoD) and the U.S. intelligence community. All discussions and papers were unclassified.

We organized the workshop for two reasons. First, it was already evident then—and is even more so now—that offensive cyber operations were becoming increasingly prominent in U.S. policy and international security more broadly. Second, despite the rising importance of offensive cyber operations, academics and analysts were paying much greater attention to cyber defense than to cyber offense. Consequently, key issues such as the conceptual underpinnings, doctrine, operational assumptions, intelligence requirements, organizational demands, and escalation dynamics of offensive cyber operations were understudied.

On the increasing prominence of offensive cyber operations for the United States, consider the following:

- The deployment and use of Stuxnet against Iranian centrifuges is widely credited with slowing Iran's progress toward acquiring a nuclear weapon before it was discovered in 2010.[1]

- Presidential Policy Directive 20 (PPD-20), which established U.S. policy for both offensive and defensive cyber operations, was leaked by Edward Snowden in 2013, and much of its content was described in news articles.[2] According to the *Guardian*'s reporting, offensive cyber capabilities can be used broadly to advance "U.S. national objectives around the world."[3]

- The Department of Defense Cyber Strategy, released in April 2015, focuses on "building capabilities for effective cybersecurity and cyber operations to defend DoD networks, systems, and information; defend the nation against cyberattacks of significant consequence; *and support operational and contingency plans*."[4]

- In a speech at Stanford University releasing the April 2015 cyber strategy, Secretary of Defense Ash Carter explicitly noted that one mission of the DoD is "to provide offensive cyber options that, if directed by the President, can augment our other military systems."[5]

- The DoD has publicly acknowledged using cyber weapons in its fight against the Islamic State of Iraq and Syria (ISIS). For example, in February 2016 Secretary of Defense Carter said that U.S. Cyber Command is conducting offensive cyber operations to cause ISIS to "lose confidence in their networks, to overload their networks so that they can't function, and do all of these things that will interrupt their ability to command and control forces."[6] He also noted that Cyber Command "was devised specifically to make the United States proficient and powerful in this tool of war." In April 2016, Deputy Secretary of Defense Robert Work said, regarding ISIS, "We are dropping cyber bombs. We have never done that before," and "Just like we have an air campaign, I want to have a cyber campaign."[7]

- During the 2016 presidential campaign, then-candidate Donald Trump promised to "make certain that our military is the best in the world in both cyber offense and defense."[8] Trump argued in the same speech that "As a deterrent against attacks on our critical resources, the United States must possess the unquestioned capacity to launch crippling cyber counterattacks. . . . America's dominance in this arena must be unquestioned."

On Inauguration Day the White House noted, "We will make it a priority to develop defensive and offensive cyber capabilities at our U.S. Cyber Command."[9]

- In March and April 2017 the *New York Times* published a number of articles describing U.S. efforts regarding certain "left-of-launch" ballistic missile defense methods targeting North Korea's program,[10] in particular cyber methods for compromising a missile before launch. On the basis of what *New York Times* reporters David Sanger and William Broad believed to be an unusually high failure rate of North Korean missile tests, they concluded that the United States had been conducting a cyber campaign against the North Korean missile development program.
- The Trump National Security Strategy of December 2017 states that "the United States will impose swift and costly consequences on foreign governments, criminals, and other actors who undertake significant malicious cyberactivities."[11]

More broadly, the attention paid to cybersecurity issues by policymakers has risen dramatically in the past few years. Cyber threats from China (for example, the 2015 theft of millions of records from the Office of Personnel Management), North Korea (the 2017 WannaCry ransomware attack that affected computers worldwide, including the United Kingdom's National Health Service), Russia (the 2017 NotPetya ransomware attack against Ukrainian institutions, including parts of its critical infrastructure), and Iran (the 2012 attack against Saudi Aramco that destroyed 30,000 computers) have provided strong signals to policymakers that offensive cyber operations are powerful instruments of statecraft for adversaries as well as for the United States. Cyber-enabled information operations, such as the Russian intervention in the U.S. presidential election of November 2016, have further raised the profile of the relationship between cyberspace and national security.

If recent history is any guide, the interest in using offensive cyber operations is likely to grow. Already, there is robust discussion about whether the current requirement articulated in PPD-20 for "specific presidential approval" of offensive cyber operations with significant consequences should be relaxed to allow greater delegation to theater combatant commanders. Strategically, greater receptivity to the use of offensive cyber operations may suggest that such operations could be the instrument of first military use if nonmilitary measures (diplomatic, economic, or legal measures) fail.

A logical consequence would also be continuing or expanded efforts to establish a ubiquitous presence on possible cyber targets, an outcome discussed at greater length by Chris Inglis (chapter 2 in this volume).

Other significant changes may also be in the offing. For example, greater receptivity to the use of offensive cyber operations may lead to a greater willingness to employ destructive or disruptive active defense measures, or to allow their use by the private sector in extremis. The U.S. government's Vulnerabilities Equities Process, which determines whether software vulnerabilities discovered by intelligence agencies should be disclosed to private sector vendors so that they can be patched, may also shift. Under the Obama administration, this process reportedly tilted toward disclosing vulnerabilities to companies. The rising use of offensive cyber operations may shift the calculus toward stockpiling vulnerabilities instead so that they can be used by the U.S. government in subsequent offensive operations. In addition, more open and vigorous support may be offered to efforts that promote exceptional access to encrypted files and communications for law enforcement and intelligence agencies.

Last, the elevation of U.S. Cyber Command from unified subcommand under U.S. Strategic Command to a full unified combatant command—mandated by Section 923 of the National Defense Authorization Act for FY 2017[12]—occurred on May 4, 2018.[13] The full operational implications of this organizational change will unfold over time, but it is possible that as a full unified combatant command, Cyber Command will have greater independent authority to conduct operations, both offensive and defensive, in cyberspace.

The increasing prominence of offensive cyber operations as instruments of national policy alone would warrant serious research conducted by independent scholars at universities and think tanks in the same way that a great deal of research has been conducted on defense-related topics such as missile defense, nuclear strategy, and naval operations. Because these topics are important to national defense and international security, they are appropriate for independent scholars to study, if only because independent perspectives contribute to the overall body of useful knowledge on which policymakers can draw.

To date, academics and analysts have paid much more attention to cyber defense than to cyber offense. One important reason underlying this imbalance is a high degree of classification about nearly every aspect of U.S. offensive cyber capabilities. Indeed, Michael Hayden, former director of both

the National Security Agency and the Central Intelligence Agency, has noted that, as recently as the early 2000s, even the phrase "offensive cyber operations" was classified. Not what it might mean, or what the targets would be, or what technologies would be involved—merely the phrase itself.

High levels of classification and excessive secrecy are especially problematic when policymakers try to understand a new domain of conflict because secrecy inhibits learning across traditional boundaries, and new types of conflict necessarily require learning across traditional boundaries. Again, quoting Hayden:

> Developing policy for cyberops is hampered by excessive secrecy (even for an intelligence veteran). I can think of no other family of weapons so anchored in the espionage services for their development (except perhaps armed drones). And the habitual secrecy of the intelligence services bled over into cyberops in a way that has retarded the development—or at least the policy integration—of digital combat power. It is difficult to develop consensus views on things that are largely unknown or only rarely discussed by a select few.[14]

Thus we convened the 2016 workshop in large part to promote and demonstrate the realistic possibility of collaboration between government policymakers and independent nongovernment researchers working on strategic dimensions of offensive cyber operations on an unclassified basis. Although over the years a few scholars have ventured into the realm of strategy and doctrine around offensive cyber operations without access to classified materials, the vast majority have found it easier to stay away from the subject matter entirely. The result has been a deep loss for strategic thought and a stark contrast from the roles that key nongovernment researchers played in developing nuclear strategy during the Cold War.[15]

For example, Bernard Brodie developed the fundamentals of deterrence by threat of retaliation as an essential underpinning for nuclear strategy and also the importance of a secure second-strike capability (that is, deliverable nuclear weapons that could survive a first strike by an adversary) for strategic stability.[16] Herman Kahn introduced the key strategic notion of an escalation ladder as it might apply across the entire range of quite limited conventional conflict to all-out nuclear conflict.[17] Thomas Schelling and Morton Halperin developed influential theories for promoting arms control involving strategic nuclear weapons.[18]

The workshop focused on strategic dimensions of offensive cyber operations, which can be used across a wide range of scenarios and for a wide range of purposes. Tactical uses of a weapon (cyber or otherwise) focus on short-term, narrow goals—how to defeat the adversary in the next village tomorrow. Strategic uses of weapons, by contrast, focus on longer-term, more overarching goals and are designed to affect the broader dynamics between potential adversaries both on and off the hot battlefield.

Generally speaking, offensive cyber activities compromise the confidentiality, integrity, or availability of information. An activity that affects the confidentiality of information is considered a "cyber exploitation," while an activity that degrades the integrity or availability of information is considered a "cyberattack." In this volume we define offensive cyber operations more specifically as: the use of cyber capabilities for national security purposes intended to compromise the confidentiality, integrity, or availability of an adversary's information technology systems or networks; devices controlled by these systems or networks; or information resident in or passing through these systems or networks.

A good place to start thinking about offensive cyber operations in a strategic context is to consider some of the unique characteristics of cyber weapons and their operation in cyberspace.

- In cyberspace, instruments used to gather intelligence and inflict damage are difficult to distinguish. Because the same techniques are usually used to gain access to an adversary's systems and networks for intelligence gathering and for causing harm, an adversary that detects a penetration cannot be certain of the penetrator's intent and therefore may misperceive an attempted intelligence operation as an attack.

- Offensive cyber operations act most directly on intangibles—information, knowledge, and confidence. To be sure, cyber operations can cause tangible effects, as when the information in question is integral to the operation of devices or equipment that affect the physical world. But offensive cyber operations are fundamentally deceptive in nature—at a tactical level, no cyberattack tells the user of a computer "click on this link and your computer will be compromised by a malicious adversary." Human cognition is of course based on the availability of information—and if the humans involved doubt the provenance of the information available to them, their concerns may well prompt them to assume the worst.

- The effectiveness of a cyber weapon is a very strong function of the target's characteristics. In cyberspace, a small change in configuration of the target machine, system, or network can often negate the effectiveness of a cyber weapon against it. This is not true with weapons in other physical domains. Any ship hit by a torpedo with a sufficiently large warhead will be damaged, whether the ship is made of wood or steel. Anything within the crater of a nuclear weapon will be destroyed, regardless of how it was built. The nature of target-weapon interaction with kinetic weapons can usually be estimated on the basis of physics experimentation and calculation. Not so with cyber weapons. For offensive cyber operations, this extreme "target dependence" means that intelligence information on target characteristics must be precise, high-volume, high-quality, current, and available at the time of the weapon's use.
- Interaction with the target in advance of an actual cyberattack on it is often a prerequisite for an attack's success. That is, the attacker may have to prepare a cyber target well before the actual attack—for example, by surreptitiously installing a "back door" that will grant the attacker access at a later time for downloading a customized attack payload that takes into account new intelligence information that may then become available.
- Military planning often involves drawing up lists of targets that are well known and understood—military bases, headquarters buildings, ammunition and fuel storage facilities, telecommunications facilities, and so on. By contrast, many targets in cyberspace can appear and disappear from the internet with the flick of a switch.

These characteristics appear in the four interrelated themes explored by the chapters in this volume: (1) cyber strategy and doctrine for offensive use of cyber weapons, (2) operational considerations in using cyber weapons, (3) escalation dynamics and deterrence, and (4) the role and relationship of the private sector to offensive cyber operations. We selected these four themes because of their obvious importance to policymakers, because of their clear relevance to offensive operations in other domains, and because they will advance our understanding about what is and is not different when it comes to the strategic effects and impacts of offensive cyber operations, both now and in the future. In the chapters that follow, contributors go both deep and broad. Some offer specific expertise about individual country challenges (such

as Adam Segal's examination of China in chapter 13). Others take a broader view of a conceptual challenge (such as Henry Farrell and Charles Glaser in chapter 3). Still other chapters focus on technical dimensions of cyber capabilities and how they might be utilized for precise targeting (Steven Bellovin, Susan Landau, and Herbert Lin in chapter 11) or sabotaging a missile development program (Lin in chapter 7). Together, the chapters offer what we hope is a compelling and comprehensive view of many of the key technical, political, historical, and legal dimensions of offensive cyber operations.

Cyber Strategy and Doctrine

Strategy and doctrine are foundational to achieving strategic effects of offensive cyber operations. In chapter 2, Chris Inglis sets the stage by examining the intelligence, surveillance, and reconnaissance (ISR) infrastructure needed to support an effective U.S. cyber strategy. He argues that ISR capabilities for cyberspace must be ubiquitous, real-time, and persistent. Capabilities must be ubiquitous because cyberspace is global, and the cyber targets that operational plans call for attacking are potentially located anywhere. They must be real-time because up-to-the-minute information on target characteristics is almost certainly necessary for an offensive cyber operation to be successful. And they must be persistent because operational preparation of the cyber battlefield is time-consuming and it is not known in advance when a given offensive cyber operation may need to be executed. The aspirational goal for ISR to support cyber operations is that it enables offensive cyber operations to sprint from a standing start at any given moment.

How should the United States choose between cyber and kinetic (or physical) responses to cyberattacks? Since the early 2000s, the United States has made a variety of statements addressing some aspects of this question. The 2004 National Military Strategy said explicitly that U.S. nuclear capabilities played an important role in deterring the use of weapons of mass destruction or effect, including "cyberattacks on U.S. commercial information systems or attacks against transportation networks"[19] that have a "greater economic or psychological effect than a relatively small release of a lethal agent."[20] The DoD's 2015 Cyber Strategy specifically states that the United States will respond to cyberattacks against its interests "at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law."[21] The 2018 Command

Vision for U.S. Cyber Command argues for a strategy of persistent engagement in cyberspace below the threshold of armed conflict.

In chapter 3, Henry Farrell and Charles Glaser take a step back from these pronouncements. Their starting premise is that decisions about deterrence and warfighting should be based on the effect a given U.S. attack will have, not the means by which that effect is produced. But, they note, perceptions matter as well: adversaries may perceive different forms of retaliation that do equal damage as differently punishing and differently escalatory. In particular, kinetic damage may be perceived as "more serious" than comparable damage caused by a cyberattack, thus reducing the likelihood and value of kinetic retaliation for deterring and responding to cyberattacks.

In chapter 4, Max Smeets and Herbert Lin review the March 2018 Command Vision for U.S. Cyber Command. Superseding the Command Vision released in June 2015, the new document demonstrates a marked change in Cyber Command's thinking and approach to engaging adversaries in cyberspace. Perhaps the most significant change is the acknowledgment that adversary cyber operations below the threshold of armed attack or the use of force (both terms recognized by the United Nations Charter) can still have strategic significance—small actions can create large consequences. In large part, the new Command Vision is the result of the observation that previous U.S. practices of restraint in cyberspace have not been sufficient to deter adversaries from below-threshold operations. The 2018 Command Vision articulates a new approach that is based on persistent engagement—that the United States must be willing to engage actively and affirmatively below the threshold if it is to compete successfully in cyberspace, and thus implicitly downplays the escalation risks inherent in a more active stance. Even the title of the 2018 Command Vision—"Achieve and Maintain Cyberspace Superiority"—sets up Cyber Command's aspirational vision in cyberspace.

Operational and Tactical Considerations

Operational considerations are implicated in the strategic use of weapons in that they speak directly to how military forces are employed to gain military advantages over an adversary and thereby attain strategic goals. Such considerations focus on the design, organization, and conduct of major operations and in-theater campaigns. Of course, the borderless nature of cyberspace makes the definition of "in-theater" problematic, a point suggesting

that offensive cyber operations are themselves likely to be conducted without regard for national borders.

An operation plan is a complete and detailed plan for military operations that would be executed upon receipt of appropriate orders for particular military contingencies. In 2013 the *Guardian* reported that PPD-20 called for the identification of "potential targets of national importance" where offensive cyber capabilities "can offer a favorable balance of effectiveness and risk as compared with other instruments of national power."[22] Identification of such targets is analogous to the development of a target list for the Single Integrated Operating Plan for using strategic nuclear weapons, today known as OPLAN 8010, "Strategic Deterrence and Global Strike."

With the backdrop offered by PPD-20, Austin Long (chapter 5) uses the frame of nuclear planning processes to understand how strategic targeting using cyber weapons might occur, considering how the organizational processes used to plan for the use of nuclear weapons and to execute such plans could in fact be applied to cyber weapons as well. Long considers how and to what extent strategic influence emanating from an adversary complicates planning for strategic responses, in particular asking under what circumstances strategic influence could be regarded as a strategic cyberattack. He also discusses whether the oft-mentioned clandestine nature of offensive cyber operations has an impact on deterrence, drawing an analogy to Cold War strategic electronic warfare as precedents for that possibility.

In chapter 6, Martin Libicki considers the connection between tactics and the conduct of an extended cyber campaign that could have strategic impact. He notes that adversaries are likely to adapt as we conduct offensive cyber operations against them. Such adaptations could occur relatively quickly and may reduce the effectiveness of subsequent operations unless the initial operations are crafted carefully to minimize adversary opportunities to adapt.

In chapter 7, Herbert Lin looks at some of the technical issues that a program of cyber-enabled sabotage might entail if it were conducted against a nation's missile development program and considers its relevance to an operational ballistic missile defense. Although Lin's piece is not based on any specific knowledge regarding any particular nation's program, it is noteworthy that press reports in 2017 described a U.S. program using various cyber means to disrupt and delay the North Korean missile development program.

Escalation Dynamics

Escalation dynamics and deterrence refer to processes by which conflict can start, how smaller conflicts can grow into bigger ones, and how these processes can be interrupted to make the outbreak or escalation of conflict less likely.

As one important example, intelligence collection—one of the primary functions of certain types of offensive cyber operations—can easily lead to misperceptions with escalatory implications. Consider, for example, the sensitivity of nations to the security of their nuclear capabilities, which are regarded as the ultimate guarantor of their security against hostilities from other nations. Gathering intelligence that could shed light on an adversary's intentions is often regarded as enhancing stability, since it can provide reassurance about the putative intent of an adversary. But because it is often unclear in the initial stages of an offensive cyber operation whether such an operation is intended to gather intelligence or to prepare the cyber battlefield (and because offensive cyber operations are likely to be used early in a conflict),[23] cyber-enabled intelligence collection directed against nuclear command and control facilities—especially if noticed by an adversary during a crisis—may be misinterpreted as a sign that a preemptive attack on its nuclear capabilities is imminent, and thus undermine nuclear stability.

A second escalatory path may be the comingling of assets for command and control of nuclear and conventional forces. An adversary's command and control assets are explicitly called out as a target for U.S. offensive cyber operations in the DoD Cyber Strategy;[24] if the early phases of a conflict involve conventional forces (and hence the United States launches cyberattacks on the command and control assets for these forces), the adversary may well see such attacks as attempts to compromise the command and control of its nuclear forces—a perception that might lead to escalation of the conflict.

A third factor in unintended escalation is an inappropriate scope and nature of the rules of engagement for the use of cyber weapons. One basic rule of engagement for offensive cyber operations appears to be articulated in PPD-20. According to public news reports, PPD-20 directs that cyber operations "reasonably likely to result in significant consequences require *specific presidential approval*" (emphasis added) where "significant consequences" are known to include loss of life, serious levels of retaliation, damage to property, adverse foreign policy consequences, or economic impact on the country.[25]

A fourth factor that may drive escalation is public opinion and pressure on decision makers. Public opinion has certainly influenced decision makers to go to war—a fact known since the outbreak of the Spanish-American War in 1898.[26] Even if such pressures themselves are insufficient by themselves to cause war, they can create climates conducive to conflict escalation in which the perceived significance of small incidents grows out of all proportion to its actual significance—and there is no reason to suppose that conflict in cyberspace would be an exception.

Last, the use of a weapon that caused more damage than was intended by the attacker might cause unintended escalation of a conflict. Both PPD-20 and the DoD Cyber Strategy note that offensive cyber operations must be conducted in accordance with the laws of armed conflict (LOAC), just as all other U.S. military operations are conducted. To address issues of collateral damage, the DoD has established a "No-Strike and the Collateral Damage Estimation Methodology"[27] that requires commanders to compile a list of "no-strike entities" upon which kinetic or nonkinetic attacks would violate LOAC. Public reports also indicate that PPD-20 directs officials to weigh "the potential threat from adversary reactions" and "the risk of retaliation," both considerations in managing risks of escalation. Such considerations would help to shape the establishment of a restricted target list comprising valid military targets that for non-LOAC considerations, such as escalation, should not be attacked in certain specified ways. Mission-specific rules of engagement (also known as supplementary rules of engagement) account for no-strike entities and restricted targets.

These examples of possible escalatory pressures ground the discussion of the book's third theme—escalation dynamics in cyberspace—to which six chapters are devoted.

First, Jason Healey (chapter 8) examines historical case studies and finds that cyber conflict is more often escalatory than not. According to his analysis, U.S. cyber actions often lead to misinterpretations and overreactions by adversaries, resulting in those states increasing their own cyber capabilities as a result of fear in what might be called strategic escalation or the cyber manifestation of the security dilemma.[28] Thus, he argues, an open display of offensive cyber capabilities—advocated by many as a measure supporting deterrence—is likely to inflame relationships between states as a result of "worst-case" judgments on both sides.

Erik Gartzke and Jon Lindsay (chapter 9) raise another important question regarding escalation dynamics. Motivated by press reports regarding

U.S. attempts to compromise the North Korean missile development program and noting that cyber capabilities depend on concealing information about cyber vulnerabilities from the other side, they argue that if the latter has nuclear capabilities its confidence in its ability to use those capabilities may be excessively high, and that it will be less likely to back down in a crisis—thus increasing the likelihood that nuclear war will break out. They further distinguish between offensive cyber operations used for preventative counterproliferation and for preemptive counterforce, the former extending over a longer period of time than the latter. The persistence of such operations over longer times increases the likelihood that those operations will themselves be compromised, an outcome that would tend to undermine the further effectiveness of a preventive operation and increase the possibility that those operations could be used for preemption.

Michael Gross, Daphna Canetti, and Dana Vashdi (chapter 10) focus on the psychological harm and consequential impact of offensive cyber operations on public confidence in important national institutions, noting especially how the mystique and omniscience associated with cyber operations affect the risk perception of civilians and how access to the internet has become a prima facie requirement for realizing certain basic human rights, both of which open new avenues for cyber terrorism. They observe in experiments that in the face of hostile cyber activity, many citizens reevaluate their confidence in public institutions and increase their support for harsh military responses, tendencies that may well increase public pressures for cyber or even kinetic escalation.

Steven Bellovin, Susan Landau, and Herbert Lin (chapter 11) point out that with appropriate intelligence in hand, cyberattacks can be designed and conducted in a way that limits damage to the intended targets: discriminating cyber weapons are technically possible. The chapter also addresses technical means for limiting the proliferation of cyber weapons that could otherwise occur, a factor that can mitigate the security dilemma in cyberspace.

C. Robert Kehler, Herbert Lin, and Michael Sulmeyer (chapter 12) provide an overview of how the DoD normally conceptualizes such rules of engagement, but without reference to PPD-20. They note that the U.S. military seeks as much as possible to integrate cyber weapons into its operational toolkit within a common framework of principles that apply to all weapons, and that, from the DoD perspective, principles that inform rules of engagement for traditional kinetic weapons can and do inform rules

of engagement that govern cyberspace operations as well. Nevertheless, several characteristics of operations in cyberspace and the use of cyber capabilities complicate the formulation of cyber-specific rules of engagement, including the borderless geography and range of effects possible on the internet, ambiguity of adversary intent arising from the difficulty of distinguishing between intelligence gathering for reconnaissance and preparation for attack, and difficulties of attribution in cyberspace. A paucity of historical experience with cyber operations in a military context will hamper the formulation of rules of engagement for cyber weapons; consequently, special efforts should be made to impart experience (such as might be developed through war gaming and tabletop exercises) to the appropriate leaders and commanders.

Finally, Adam Segal (chapter 13) offers a possible case study addressing the escalation potential of U.S. offensive cyber operations in a China-U.S. military confrontation. Segal notes that while China is increasingly a target-rich environment from both tactical and strategic perspectives, the use of offensive cyber operations against these targets is likely to be highly escalatory. Complications will arise from differing conceptions of deterrence and crisis management, a lack of transparency into the political control of cyber forces, and an expansive view of competition in cyberspace. Yet neither the United States nor China will eschew the use of offensive cyber operations, a point suggesting the importance of both sides considering measures that reduce the likelihood of escalation from tactical to strategic attacks undertaken through cyber means.

The Role of the Private Sector in Offensive Cyber Operations

The private sector is an important part of cyberspace. Unlike other physical domains, private actors in cyberspace can significantly influence the nature, execution, and prospects for success of offensive operations. It is uncontestable that cyber weapons are available to private actors, but the policy implications of such availability are controversial and widely debated. Each of the three chapters in this section tackles a different dimension of the private sector's role in cyberspace.

David Aucsmith (chapter 14) argues that because governments are incapable of defending cyberspace for all denizens, private parties must have the capability to defend themselves—a capability that necessarily includes the ability to inflict harm on attackers. However, the existing legal regime lim-

its the actions private organizations can pursue in cyber defense. A variety of changes to the existing legal regime would allow private companies to take actions consistent with the self-defense constraints of necessity, proportionality, and immediacy, and improve an organization's ability to both defend itself and attribute actions to the aggressors. Lucas Kello (chapter 15) comes to the opposite conclusion in his chapter. Kello grants that the potential defensive and other benefits of cyber weapons in this role are significant, yet he finds that the risks to defenders, innocent third parties, and international conflict stability are greater.

Finally, in chapter 16, Irv Lachow and Taylor Grossman explore the critical roles that companies play in supporting offensive cyber operations, including intelligence/reconnaissance and planning and mission support for such operations. Cyber contractors provide U.S. and other militaries access to rapidly evolving technologies and necessary human talent. At the same time, the use of such contractors has international ramifications. For example, the availability of cyber contractors may affect the balance of power of states, as effective offensive cyber capabilities become available to nations willing to simply buy them. Cyber contractors involved in offensive cyber operations may face some uncertainties about their international legal status. And because their services are in principle available to any party willing to pay for them, a contracting company may find itself on both sides of a cyber operation.

Conclusion

It is only within the last few years that the Department of Defense has designated cyberspace a domain of conflict, and many policymakers are struggling with how best to integrate offensive cyber capabilities with other instruments of military and national power. Taken as a whole, the chapters in this volume suggest that thinking about offensive cyber operations as instruments of national policy need not require de novo construction. Indeed, many of the questions and issues that attend to the strategic dimensions of offensive cyber operations arise in other kinds of military operations. However, because the cyber domain is unlike other domains of conflict in important ways, it is not surprising that some of the answers and responses to these questions and issues in the cyber domain are different. More clearly delineating what's new and what isn't in offensive cyber operations is an important step forward.

Notes

1. See, for example, William J. Broad, John Markoff, and David E. Sanger, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay," *New York Times*, January 15, 2011; and "Iran's Natanz Nuclear Facility Recovered Quickly from Stuxnet Cyber Attack," *Washington Post Foreign Service*, February 16, 2011. However, estimates vary about the extent of delay in the Iranian nuclear program that Stuxnet caused.

2. The leaked PPD-20 can be read in full at https://fas.org/irp/offdocs/ppd/ppd-20.pdf. As noted in the main text of this chapter, PPD-20 has also been the subject of news articles and editorials, including Glenn Greenwald and Ewen McAskill, "Obama Orders U.S. to Draw Up Overseas Target List for Cyber-Attacks," *Guardian*, June 7, 2013; "Cyberwar: The White House Is Thinking Ahead," Editorial, *Washington Post*, June 16, 2013; Bill Gertz, "Cyber War Details Revealed," *Washington Free Beacon*, June 11, 2013 (http://freebeacon.com/national-security/cyber-war-details-revealed/); and Mark Clayton, "Presidential Cyberwar Directive Gives Pentagon Long-Awaited Marching Orders," *Christian Science Monitor*, June 10, 2013. Because those with clearances are allowed to read press stories reporting on leaked classified documents but not to read these documents themselves outside of cleared facilities, references to PPD-20 in this introduction should be understood as being derived from these articles and not from the original document. In addition, papers in this collection written by individuals who have had proper access to classified cyber-related documents have passed through DoD security review; these papers contain no references to PPD-20, and no individuals with security clearances had any input into this introduction.

3. In May 2018 it was reported that the Trump administration is considering rescinding PPD-20 to streamline decision making and facilitate the faster approval of offensive cyber actions. Chris Bing, "Trump Administration May Throw Out the Approval Process for Cyber Warfare," *Cyberscoop*, May 2, 2018 (www.cyberscoop.com/ppd-20-white-house-national-security-council-cyber-warfare-tactics/).

4. *Department of Defense Cyber Strategy* (April 2015) (www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DOD_CYBER_STRATEGY_for_web.pdf); emphasis added.

5. Ash Carter, "Remarks by Secretary Carter" (Drell Lecture, Stanford Graduate School of Business, Stanford, California, April 23, 2015) (www.defense.gov/News/News-Transcripts/Transcript-View/Article/607043).

6. Sean Lyngaas, "The Business of Federal Technology," *FCW,* February 29, 2016 (https://fcw.com/articles/2016/02/29/carter-isis-networks.aspx).

7. Ryan Browne and Barbara Starr, "Top Pentagon Official: 'Right Now It Sucks' to Be ISIS," CNN, April 14, 2016 (www.cnn.com/2016/04/13/politics/robert-work-cyber-bombs-isis-sucks/).

8. Daniel White, "Read Donald Trump's Remarks to a Veterans Group," *Time*, October 2, 2016 (http://time.com/4517279/trump-veterans-ptsd-transcript/).

9. The White House, "Making Our Military Strong Again," January 20, 2017.

10. William J. Broad and David E. Sanger, "U.S. Strategy to Hobble North Korea Was Hidden in Plain Sight," *New York Times*, March 4, 2017; David E. Sanger and William J. Broad, "Trump Inherits a Secret Cyberwar against North Korean Missiles," *New York Times*, March 4, 2017; David E. Sanger and William J. Broad, "Hand of U.S. Leaves North Korea's Missile Program Shaken," *New York Times*, April 18, 2017.

11. White House, *National Security Strategy of the United States of America*, December 2017 (www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf).

12. U.S. Congress, *National Defense Authorization Act for Fiscal Year 2017*, January 4, 2016 (www.congress.gov/114/bills/s2943/BILLS-114s2943enr.pdf).

13. Katie Lange, "Cybercom Becomes DoD's 10th Unified Combatant Command," May 3, 2018 (www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/).

14. Michael V. Hayden, "The Making of America's Cyberweapons," *Christian Science Monitor*, February 24, 2016.

15. The points made in this paragraph and additional discussion of the deleterious effects of overclassification regarding offensive cyber operations can be found in Herbert Lin and Taylor Grossman, "The Practical Impact of Classification Regarding Offensive Cyber Operations," in *Cyber Insecurity: Navigating the Perils of the Next Information Age*, edited by Richard M. Harrison and Trey Herr (New York: Rowman & Littlefield, 2016), pp. 313–27.

16. Bernard Brodie, *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, 1946); and Bernard Brodie, *Strategy in the Missile Age* (Princeton University Press, 1959) (www.rand.org/pubs/commercial_books/CB137-1.html).

17. Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).

18. Thomas Schelling and Morton Halperin, *Strategy and Arms Control* (New York: Twentieth Century Fund, 1961).

19. Joint Chiefs of Staff, *The National Military Strategy*, 2004 (http://ssi.armywarcollege.edu/pdffiles/nms2004.pdf), p. 12.

20. Joint Chiefs of Staff, *The National Military Strategy of the United States of America*, 2004 (http://ssi.armywarcollege.edu/pdffiles/nms2004.pdf), p. 1.

21. *Department of Defense Cyber Strategy*, p. 11.

22. Greenwald and McAskill, "Obama Orders U.S. to Draw Up Overseas Target List."

23. Herbert Lin, "Reflections on the New DOD Cyber Strategy: What It Says, What It Doesn't Say," *Georgetown Journal of International Affairs* 17, no. 3 (2017), pp. 5–13.

24. *Department of Defense Cyber Strategy*, p. 14.

25. See, for example, "Cyberwar: The White House Is Thinking Ahead"; and Greenwald and McAskill, "Obama Orders U.S. to Draw Up Overseas Target List." All references to PPD-20 in this chapter are based on these public news reports and not on any classified document that may have been leaked into the public domain.

26. Office of the Historian, U.S. Department of State, "U.S. Diplomacy and Yellow Journalism, 1985–1898" (https://history.state.gov/milestones/1866-1898/yellow-journalism).

27. Chairman of the Joint Chiefs of Staff, Instruction, *No-Strike and the Collateral Damage Estimation Methodology*, October 12, 2012 (https://info.publicintelligence.net/CJCS-CollateralDamage.pdf).

28. See, for example, Ben Buchanan, *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations* (Oxford University Press, 2017).