The Meaning of the Cyber Revolution

Perils to Theory and Statecraft

Lucas Kello

Security policy in the information age faces formidable challenges. Chief among these is to evaluate correctly the impact of cyberweapons on strategy: Does the new technology require a revolution in how scholars and policymakers think about force and conflict?[1] Practitioners confront a predicament in addressing this question: the cyber revolution gives rise to novel threats and opportunities requiring immediate policy responses; yet understanding its nature and its consequences for security is a slow learning process. Interpretation of cyber phenomena involves analysis of a new body of experience that existing theories may be unable to clarify. It presupposes, moreover, a technical understanding of a transforming technology, whose implications require time to master because of its scientific complexity.

The inevitable result has been a delay in the strategic adaptation to cyber realities. If decisionmakers are right—and their views are not equivocal—the contemporary world confronts an enormous cyber threat. The U.S. intelligence community rates this threat higher than global terrorism and warns of the potential for a calamitous cyberattack.[2] Yet as the chief of U.S. Cyber Command, Gen. Keith Alexander, has observed, there is no consensus "on how to characterize the strategic instability" of cyber interactions "or on what to do about it."[3] The range of conceivable cyber conflict is poorly understood by scholars and decisionmakers,[4] and it is unclear how conventional security mechanisms, such as deterrence and collective defense, apply to this phenomenon. In addition, the principles of cyber offense and cyber defense remain rudimentary.

Lucas Kello is a Postdoctoral Research Fellow in the International Security Program and the Project on Technology, Security, and Conflict in the Cyber Age at the Belfer Center for Science and International Affairs at the Harvard Kennedy School.

The preparation of this article was supported by the Belfer Center's Science, Technology, and Public Policy Program and the MIT-Harvard Project on Explorations in Cyber International Relations funded by the Office of Naval Research under award number N000140910597. The author is grateful to Venkatesh Narayanamurti for his insightful comments and advice.

1. The term "cyberweapons" designates the variety of tools that can disrupt or destroy computer network operations.
2. See James R. Clapper to the U.S. Senate Intelligence Committee (Washington, D.C.: U.S. Government Printing Office, March 12, 2013).
3. Keith B. Alexander to the U.S. Senate Committee on Armed Services (Washington, D.C.: U.S. Government Printing Office, April 15, 2010), p. 219.
4. The term "cyber conflict" denotes offensive cyberattack for political or strategic purposes as well as responses to such attack.

International Security, Vol. 38, No. 2 (Fall 2013), pp. 7–40, doi:10.1162/ISEC_a_00138

The growth of cyber arsenals, in short, is outpacing the design of doctrines to limit their risks.

Against this backdrop, there is an evident need for scholars of international relations and security to contribute to the theoretical evaluation of the cyber revolution. Removed from the pressures of having to defeat the cyber threat, yet possessing concepts necessary to analyze it, academics are in a privileged position to resolve its strategic problems. Yet there has been little systematic theoretical or empirical analysis of the cyber issue from the perspective of international security.[5] This article provides such an analysis: it makes a case and establishes guidelines for the scholarly study of cyber conflict.

The article makes three main arguments. First, integrating cyber realities into the international security studies agenda is necessary both for developing effective policies and for enhancing the field's intellectual progress. Second, the scientific intricacies of cyber technology and methodological issues do not prohibit scholarly investigation; a nascent realm of cyber studies has already begun to emerge. Third, because cyberweapons are not overtly violent, their use is unlikely to fit the traditional criterion of interstate war; rather, the new capability is expanding the range of possible harm and outcomes between the concepts of war and peace—with important consequences for national and international security. Although the cyber revolution has not fundamentally altered the nature of war, it nevertheless has consequences for important issues in the field of security studies, including nonmilitary foreign threats and the ability of nontraditional players to inflict economic and social harm. Three factors underscore the cyber danger for international security: the potency of cyberweapons, complications relating to cyber defense, and problems of strategic instability.

This study has two important caveats: first, its scope is limited because many aspects of national and international security lie beyond the reach of cyberspace though increasingly less so; second, its conclusions are provisional because the observed phenomena are still incipient and could evolve in ways

5. The number of articles in academic international relations journals that focus on security aspects of the cyber revolution is small. They include Ronald J. Deibert, "Black Code: Censorship, Surveillance, and Militarization of Cyberspace," *Millennium*, Vol. 32, No. 2 (December 2003), pp. 501–530; Johan Eriksson and Giampiero Giacomello, "The Information Revolution, Security, and International Relations: The (IR)relevant Theory?" *International Political Science Review*, Vol. 27, No. 3 (July 2006), pp. 221–244; Lene Hansen and Helen Nissenbaum, "Digital Disaster, Cyber Security, and the Copenhagen School," *International Studies Quarterly*, Vol. 53, No. 4 (December 2009), pp. 1155–1175; and Mary M. Manjikian, "From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik," *International Studies Quarterly*, Vol. 54, No. 2 (June 2010), pp. 381–401.

difficult to predict. Thus, although the nature of the cyber threat is open to debate, the danger cannot be ignored. If scholars accept the existence of a cyber peril, then they must begin to develop a theoretical framework for understanding both the threat and its consequences for security. Conversely, if the danger appears inflated or has been misinterpreted, then they are obliged to articulate theoretical and empirical challenges to the conventional policy wisdom.

The article has three sections. First, it reviews the sources and costs of scholarly inattention toward the cyber issue and argues why this must change. Second, it presents a selection of common technical concepts to frame the issue from the perspective of security scholars. Third, it assesses the potential consequences of cyberweapons for international security. The article concludes by outlining a research agenda for future cyber studies.

Why Study the Cyber Issue?

It is superfluous to state that the field of international security studies is skeptical of the existence of a cyber danger: it has barely acknowledged the issue, as reflected in the scant relevant literature. Thus the prevailing skepticism seems more visceral than analytical; nevertheless, its sources and degrees can be detected in the notable commentaries that do exist. This section examines the roots of scholarly inattention to the cyber threat and its costs for the intellectual development and policy relevance of the field.

DEGREES OF SKEPTICISM

Some scholars have expressed skepticism about the importance—or even the feasibility—of cyber studies. Those who are deeply skeptical emphasize two major obstacles. The first concerns the paucity of cases available to propose, test, and refine theoretical claims on cyber phenomena. As Jack Goldsmith states, "There is a worry [among political scientists] that writings in this area will have a dearth of relevant data and will not be valued."[6] Paradoxically, this problem reflects a combination of too much and too little data. Reports of hostile cyber events are profuse, with governments and private industry registering incidents on an ongoing basis.[7] Yet it is often difficult to ascertain the relevance of such cases to security studies, given either poor techniques of data

6. Author interview with Jack Goldsmith, Cambridge, Massachusetts, September 13, 2012.
7. For instance, the Department of Homeland Security reported 50,000 intrusions of or attempts to intrude American computer systems between October 2011 and February 2012. See Michael S. Schmidt, "New Interest in Hacking as Threat to Security," *New York Times*, March 13, 2012.

collection or the lack of suitable metrics to codify the events. At the same time, the tendency of governments to overclassify information has led to a significant data gap. The most important tactical maneuvers in cyberspace remain shrouded in secrecy,[8] complicating scholarly investigation of the motives and aims of cyberattack as an instrument of foreign and defense policy. Other factors magnify the problem. For example, the private firms that operate the majority of critical computer systems are often reluctant to report damaging cyber incidents because of their potential to create reputational and other costs.

Skeptics also cite a more fundamental problem with cyber studies: they claim that rather than being merely unknown, the properties of cyber phenomena are unknowable. According to Stephen Walt, "[T]he whole issue is highly esoteric—you really need to know a great deal about computer networks, software, encryption, etc. to know how serious the danger might be."[9] It is possible, in other words, that the barriers to scholarship are intrinsic to the new technology, which is so specialized as to bar entry to laypersons.

A less fundamental but still powerful form of skepticism focuses on substantive aspects of the cyber issue. Some scholars intimate that the cyber threat is merely a phantasm: it haunts policymakers but has little grounding in reality. These skeptics invoke the logic of Carl von Clausewitz to argue that the cyber danger is overstated because the related technology does not alter the character or means of war. They claim that cyberattacks are not violent and do not create collateral damage; therefore, the new phenomena do not qualify as acts of war.[10] Moreover, skeptics argue that, insofar as cyberattacks can be destructive, they nevertheless will be rare owing to their high costs.[11] Finally, some analysts challenge the common wisdom that cyberweapons confer asymmetric power on weak states, contending that, instead, the United States and other large states are "well ahead of the curve" when it comes to "military-grade

8. See David E. Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown, 2012), p. 291. Google e-book.
9. Stephen M. Walt, "Is the Cyber Threat Overblown?" *Stephen M. Walt* blog, *Foreign Policy*, March 30, 2010, http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown. Elsewhere, Walt calls for systematic study of the cyber issue by a "panel of experts." See Stephen M. Walt, "What Does Stuxnet Tell Us about the Future of Cyber-Warfare?" *Stephen M. Walt* blog, *Foreign Policy*, October 7, 2010, http://walt.foreignpolicy.com/posts/2010/10/07/what_does_stuxnet_tell_us_about_the_future_of_cyber_warfare.
10. See Thomas G. Mahnken, "Cyber War and Cyber Warfare," in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (Washington, D.C.: Center for a New American Security, 2011); and Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5–32.
11. See Thomas Rid, "Think Again: Cyberwar," *Foreign Policy*, Vol. 192 (March/April 2012), pp. 80–84.

offensive [cyber] attacks."[12] The consoling and predictive title of an article by Thomas Rid sums up skeptics' perception of threat inflation: "Cyber War Will Not Take Place."[13]

The two forms of skepticism described above—deep and substantive—have resulted in considerable neglect of the cyber issue. First, the presumption of the inscrutability of cyber technologies has created a sense of resignation, suggesting that the cyber danger—if real—lies beyond the ability of scholars in our field to understand it. Among some observers, there is a sense that the cyber issue is fraught with danger; anyone who attempts to master it will be overwhelmed by its intricacy. Second, the claim of threat inflation makes a direct appeal to the preconceptions of security scholars, arguing that threats that appear to lack an overtly physical character or that do not rise to the level of interstate violence are intellectually uninteresting.[14] To the question: Does the cyber issue merit investigation? it is tempting to answer: Perhaps not, because its hazards are not of a magnitude considered relevant to theory. This view contains an element of intellectual conceit: its adherents claim to perceive a truth that somehow eludes practitioners who possess experiential insight and privileged facts on the cyber issue. A paradoxical effect, moreover, is that this perspective supplies substance for debate while possibly reinforcing the very skepticism that inhibits it.

Crucially, these two viewpoints cannot logically coexist. The thesis of threat inflation presupposes that the scale of danger can be accurately assessed, thus defeating the notion that the cyber issue is incomprehensible. Yet, the absence of any systematic account of why this issue is beyond grasp suggests that the two views coexist in the minds of some observers. This posture is untenable: either both positions are wrong—as this study argues—or only one, the notion of threat inflation, is accurate.[15] The remainder of this section assesses the price paid for the scholarly void that is a consequence of the prevailing skepticism.

COSTS OF THE SCHOLARSHIP GAP FOR THEORY AND PRACTICE

States and other actors will continue to employ code as a weapon regardless of the reluctance of theorists to merge it into their thinking. Therefore, the with-

12. Ibid., p. 84. Rid does not explain why sophisticated cyberattack should not therefore concern lesser powers.
13. Ibid.
14. See Barry Buzan and Lene Hansen, *The Evolution of International Security Studies* (Cambridge: Cambridge University Press, 2009), p. 12.
15. As a matter of principle, both viewpoints could be correct, but in the presence of the first, the second cannot be validated.

drawal of scholars from the study of cyber realities—whether the result of perplexity or indifference—risks eroding the crucial relationship of theory to science—that is, the relevance of our theoretical concepts to ongoing technological transformations. Unless the cyber issue is subjected to serious scholarly appraisal, the gap between contemporary affairs and the craft of international security studies will grow. The consequences for both theory and the capacity for policy guidance are potentially profound.

DANGERS OF THEORETICAL STAGNATION

The costs of scholarly neglect of the cyber issue to the advancement of theory are apparent: when the range of empirical topics that theory is able to elucidate narrows, the academic enterprise inevitably enters a process of internal corrosion, which reveals itself in one or both of two ways—a loss of conceptual fertility or a reduced capacity for explanatory analysis, each of which inhibits intellectual progress in the study of international relations.[16]

As a starting point of theory, the analysis of international security relies on concepts that reduce complex empirical facts to a manageable degree of simplicity.[17] Foundational concepts such as "anarchy," "order," and "system" guide the formulation of ordered research questions as well as the selection of dependent and independent variables when answering those questions. These guiding concepts are especially important when thinking about rapid technological change in weapons systems, because they mediate the relationships among the new technology, its effects on international relations, and scholars' explanatory theories. At the same time, conceptual frameworks can be altered by the very technology that scholars seek to interpret, possibly leading to theoretical breakthroughs. Accordingly, past generations of thinkers have tended to respond to technological revolutions by at least testing their concepts against them. One example is Kalevi Holsti's analysis of the implications of nuclear weapons for the notion of power in international relations.[18]

All of the central trends in security studies, in contrast, seem arrayed against the technological currents of the present cyber revolution. One of the few serious efforts to merge new realities into core theoretical concepts is the work of

16. See Stephen M. Walt, "The Enduring Relevance of the Realist Tradition," in Ira Katznelson and Helen V. Milner, eds., *Political Science: State of the Discipline* (New York: W.W. Norton, 2002), p. 220.
17. See Stanley Hoffmann, *The State of War: Essays on the Theory and Practice of International Politics* (New York: Praeger, 1965), pp. 7–8.
18. See Kalevi J. Holsti, "The Concept of Power in the Study of International Relations," *Background*, Vol. 7, No. 4 (February 1964), pp. 179–194.

Joseph Nye on "cyberpower,"[19] but the analysis of other foundational notions remains primitive. The implications of cyber activity for international anarchy and order, for example, have not been explored—even though practitioners repeatedly warn of global chaos. The conceptual apparatus of international security, in brief, is behind the times.

Second, we are witnessing an explosion of rivalrous cyber phenomena in the absence of theories to give them coherence. Security studies scholars have barely begun to apply their theoretical toolkits to explain, model, or predict competition in the cyber arena; in a realm of study that should be theirs, they have provided no school. The scholarship gap has two dimensions. First, it is fundamental inasmuch as the void reflects the partial irrelevance of existing theory. For example, if the dispersion of cyberpower away from states distorts the Westphalian mold in which our dominant theories are cast, then the mismatch between theory and cyber realities only worsens the problem of "change" in international relations: it confirms the charge that the discipline has a recursive, but no transforming, logic.[20] Second, intellectual stagnation can take an applied form. Here, a novel phenomenon that is in principle explainable remains unexplained; intellectual progress is thus inhibited even where extant theory applies. Whatever its form, the dilatoriness of scholars devalues the stock-in-trade of the field, which, as an eminently empirical science, is to elucidate major trends in contemporary security relationships.

DANGERS OF POLICY IRRELEVANCE

Scholarly neglect of the cyber danger degrades the policy relevance of the security studies field. This is a perfect situation—if it be the object of security studies to allow policy to practice itself. Many thinkers, however, regard the notion of the irrelevance of theory to policy as repugnant. Stephen Walt expresses this general view: "There is no reason why policy relevance cannot be elevated in our collective estimation."[21] This exhortation applies to the cyber issue even—and perhaps especially—if its associated dangers appear to be a mirage. The possibility that practitioners could be wrong in their estimation of a particular danger does not make scholars' withdrawal into the cloistered

19. See Joseph S. Nye, *The Future of Power* (New York: PublicAffairs, 2011), chap. 5.
20. See, for instance, Friedrich Kratochwil, "The Embarrassment of Change: Neo-Realism as the Science of Realpolitik without Politics," *Review of International Studies*, Vol. 19, No. 1 (January 1993), pp. 63–80.
21. Stephen M. Walt, "The Relationship between Theory and Policy in International Relations," *Annual Review of Political Science*, Vol. 8 (2005), pp. 41–42.

halls of academic life acceptable; on the contrary, it increases the need to challenge governing misconceptions as an essential step toward developing sensible security policy.

The need to establish a field of cyber studies rests on the premise that policy succeeds or fails based on the correctness of the theory it presupposes. A policy based on flawed assumptions is foredoomed to fail unless rescued by good fortune; one drawing on sound theory can be defeated only in its execution. The theory-policy nexus is especially close in a period of rapid technological change, in which threats and opportunities arising from a new class of weapon produce pressures to act before the laborious process of strategic adaptation is concluded. Consequently, axioms are applied that may have outlived their validity. Historically, bad theories of new technology have been behind many a strategic blunder. In 1914, British commanders failed to grasp that the torpedo boat had rendered their magnificent surface fleet obsolescent. In 1940, French strategic doctrine misinterpreted the lessons of mechanized warfare and prescribed no response to the Nazi tank assault.

The cyber revolution is no exception to this problem of lag in strategic adaptation. Nye observes that, in comparison with the early nuclear era, "strategic studies of the cyber domain are chronologically equivalent to 1960 but conceptually more equivalent to the 1950s."[22] Circumstances in the lead-up to the U.S. offensive cyber operation known as "Olympic Games," which destroyed enrichment centrifuges in Iran, vividly demonstrate the problem. The custodians of the worm (named Stuxnet by its discoverers) grappled with three sets of doctrinal quandaries: (1) ambiguities regarding the tactical viability of cyberattack to destroy physical assets; (2) concerns that the advanced code would proliferate to weaker opponents who could reengineer it to hit facilities back home; and (3) anxieties over the dangerous precedent that the operation would set—would it embolden adversaries to unleash their own virtual stockpiles?[23] These quandaries were real enough to Stuxnet's handlers. President Barack Obama and his team of advisers are the kind of decisionmakers who, recognizing that a new genus of conflict is in the offing, are inordinately obstinate in searching for satisfactory answers to the hazards it portends. Nevertheless, in the race against Iran's development of a nuclear bomb, they decided to

22. Joseph S. Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly*, Vol. 5, No. 4 (Winter 2011), p. 19.
23. For an excellent account of the Olympic Games deliberations, see Sanger, *Confront and Conceal*, chap. 8.

act; it still remains for scholars to develop a theoretical scheme to address the quandaries of cyber conflict for the future.

The torments of decisionmaking faced by practitioners are an opportunity for scholars. Whatever aspect of the cyber issue one considers—its strategic, tactical, or moral problems—there is in it a chance to demonstrate the merits of academic insight in the resolution of pressing policy challenges. So long as the impression of a cyber danger persists at the highest strata of government, the reluctance to assess its consequences risks nourishing the preconception that international security studies is, as one diplomat put it, "irrelevant" and "locked within the circle of esoteric scholarly discussion."[24]

Conceptual and Technical Rudiments for Cyber Studies

So, is it possible for a field of cyber studies to flourish? Some skeptics presume that basic methodological obstacles—the scarcity of cases to analyze and the sheer scientific complexity of the related technology—inhibit orderly investigation of the cyber issue. These barriers to scholarship are smaller than they have been made out to be.

FILLING THE DATA GAP

Cyber studies is not confined to ahistorical abstraction: there are comparatively more cases to examine than in other technological domains, such as the nuclear and biological fields, in which a paucity of events has not prevented a field of study from thriving.[25] At most, the data gap will reduce the degree of certainty of hypotheses; theorists should seek to maximize the leverage of their claims by avoiding single-case inferences and, where possible, drawing on the variety of known cases.

While the shroud of government secrecy shrinks the pool of observable cyber events and reduces available details about them, this is true of all national security activity. Moreover, the cyber research community has the unique advantage that the very technology that governments are eager to conceal is itself capable of piercing the veil of secrecy. The diffusion of the internet means that, once released, many malware agents will eventually replicate to third parties, thereby raising the chances of eventual detection. As Olympic

24. David Newsom, "Foreign Policy and Academia," *Foreign Policy*, Vol. 101 (Winter 1995), p. 66.
25. See Nye, "Nuclear Lessons for Cyber Security?" *Strategic Studies Quarterly,* Vol. 5 (Winter 2011), p. 26.

Games reveals, this can occur even in connection with covert operations involving "air-gapped" computer systems (i.e., those not joined to the internet).[26] Olympic Games also shows that the consequences of a successful cyberattack can be difficult to hide, particularly if they contain a destructive element. In addition, legislative efforts are under way in a number of countries to give private industry incentives to report network breaches that escape public detection because of their subtle impact. Finally, the common reluctance of officials to discuss offensive cyber policy may ease—at least off-the-record—as the need for public debate on its strategic quandaries intensifies.

THE NEED FOR A CONGRESS OF DISCIPLINES

The cyber issue is scientifically esoteric: no one familiar with the workings of computer code would deny it. Cyber studies, however, does not require a miracle of learning; only the minimum degree of technical acuity is needed, which reveals the scope of maneuver in the cyber domain. Cyber studies requires a congress of disciplines that includes not only the engineering sciences but also the political and social sciences. Certain aspects of the cyber issue, such as the analysis of code, belong to the computer specialist; others require the expertise of researchers versed in the contests of international anarchy.

So far, however, the analysis of cybersecurity has effectively been ceded to the technologists. Consequently, public perceptions of the cyber issue display the following tendencies:[27] (1) a propensity to think of "cyber threats" as pernicious lines of code—instead of focusing on the human agents who utilize them, and their motives for doing so; (2) an inclination to conceive of "security" as the safety of a computer system or network—without paying sufficient attention to the safety of critical activity (e.g., nuclear enrichment) that is beyond cyberspace but reliant on computer functionality; and (3) the habit of labeling any hostile cyber action—from the theft of personal data to the destruction of nuclear turbines—as an "attack," ignoring the potentially serious connotations of that term in an international context. All of these tendencies involve aspects of international security that technologists are unequipped to address, for technical virtuosity is not identical to strategic insight: it can illuminate the properties of a new class of weapon yet contribute little to explaining the reasons that inspire its use.

---

26. Although Stuxnet's custodians sought to contain the worm within the Natanz facility, thousands of external machines were infected (more than 40 percent of these outside Iran).
27. This trend is reflected in the overtly technical tone of important works of military tactics, such as Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University Press, 2007).

COMMON TECHNICAL CONCEPTS

The field of international security studies requires commonly accepted technical concepts that lay out the various dimensions of the cyber issue. Such a schematization can perform three important functions. The first is to frame the complex scientific properties of the cyber issue in a manageable way. The second is to identify the features of the technology and its related phenomena that are most relevant to the field while eliminating activity that does not rise to the level of national or international security. The third function of the framework is to orient theory development, allowing scholars to organize and codify data collected after a cyber event becomes known, search for causal chains linking determining factors to the event, and establish conceptual benchmarks for evaluating competing explanations of it. The schematization below fills the conceptual void. It contains the following six elements: cyberspace, cybersecurity, malware, cyber crime, cyberattack, and cyber exploitation.[28]

CYBERSPACE. Cyberspace is the most elemental concept in the cyber field: it establishes the technical markers within which the virtual weapon can operate. One common definition construes cyberspace as all computer systems and networks in existence, including air-gapped systems.[29] Another excludes isolated nodes.[30] For the purposes of this study, the first definition is appropriate. Total isolation of computer systems is rarely feasible today. The ubiquity of computing devices, ranging from removable drives to personal laptops—each a potential carrier of malware—has multiplied the access vectors through which an attacker can bridge an air gap. Moreover, the computer systems likeliest to be shielded by air (e.g., nuclear facilities) are ordinarily of high significance to national security and therefore should not be excluded from the plane of action. Cyberspace can thus be conceived as comprising three partially overlapping terrains: (1) the internet, encompassing all interconnected computers, including (2) the world wide web, consisting only of nodes accessible via a URL interface; and (3) a cyber "archipelago" comprising all other computer systems that exist in theoretical seclusion (i.e., not connected to the internet or the web). This conceptualization reflects an important consideration in security planning: not all threats propagated through the web can transmit via the internet, and those

28. The proposed framework draws from, but also adapts, concepts introduced in William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009).
29. See Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), p. 69.
30. See German Federal Ministry of the Interior, *Cyber Security Strategy for Germany* (Berlin: German Federal Ministry of the Interior, February 2011), p. 14.

that are transmissible cannot use the internet to breach the cyber archipelago. On these terms, there are two basic kinds of targets: (1) remote-access and (2) closed-access. Each is susceptible to different methods of approach in a cyberattack.

CYBERSECURITY. Cybersecurity consists of measures to protect the operations of a computer system or the integrity of its data from hostile action. Cybersecurity can also be conceived of as a state of affairs: the absence of unauthorized intrusion into computer systems and their proper functioning. Crucially, the concept encompasses the safety and survivability of functions operating beyond cyberspace but still reliant on a computer host, to which they are linked at the logical or information layer.[31] Insofar as measures of security are the purview of the military or impinge on military capabilities, they constitute cyber defense. An alternative conception of cybersecurity, often labeled "information security," involves government protection of channels of information flow in domestic society (e.g., internet censorship). Such differences of interpretation of the meaning of cybersecurity have hindered efforts to establish international regimes of rules and norms of cyber conduct.

MALWARE. Malware involves software designed to interfere with computer functionality or to degrade the integrity of data. It encompasses the gamut of mischievous computer code—viruses, worms, Trojans, spyware, adware, and so on. Malware can be designed to open an avenue of access to an adversary's computer system, or to attack it, or both. Thus, the use of malware is an instrument of cyber hostility and not, as is sometimes implied, a separate category of action.[32] Almost all cyber hostilities involve the use of malware.[33]

CYBER CRIME. Cyber crime entails the use of a computer for an illicit purpose under the existing penal code of a nation. It includes credit card fraud and transmission of prohibited data such as child pornography. Because domestic criminal law is unenforceable against states, cyber crime prevention focuses on private agents prosecutable in national jurisdictions. For this reason,

31. The logical layer comprises the service platforms on which computer systems and networks function (e.g., software applications). The information layer includes the data that flow between interconnected nodes. The physical layer comprises physical machines. On the "layers" model, see Nazli Choucri and David Clark, "Cyberspace and International Relations: Towards an Integrated System," paper presented at Massachusetts Institute of Technology, Cambridge, Massachusetts, August 2011.

32. An example of such misconstrual is Myriam Dunn Cavelty, "The Militarization of Cyber Security as a Source of Global Tension," *Strategic Trends 2012: Key Developments in Global Affairs* (Zurich: Center for Strategic Studies, 2012), p. 108.

33. One possible exception involves distributed-denial-of-service (DDoS) attacks. Although most DDoS operations employ malware to recruit zombie machines, participants can also be mobilized to download attack tools onto personal machines voluntarily.

it is the least contentious aspect of the cyber issue at the intergovernmental level. It is also the only dimension expressly regulated by treaty (the 2008 Council of Europe Convention on Cyber Crime). In the usage proposed here, cyber crime lacks political or strategic intent; therefore, it rarely has an impact on national or international security.

CYBERATTACK. Cyberattack refers to the use of code to interfere with the functionality of a computer system for a political or strategic purpose. The first significant cyberattack reportedly occurred in 1982, when a so-called logic bomb caused a Soviet oil pipeline to explode.[34] Cyberattacks are characterized by the attackers' desire and capability to disrupt computer operations or to destroy physical assets via cyberspace; thus, if the defender unnecessarily ceases computer operations as a consequence of misinformation or misinterpretation, the incident does not constitute cyberattack. Neither the goal nor the effects of a cyberattack need be contained in cyberspace. That is, the final object may be to incapacitate the computer system itself or to degrade social, economic, or government functions dependent on its proper operation. Accordingly, two main types of cyberattack "effects" can be identified: (1) direct effects, which unfold within the logical environment of the target machine complex (e.g., destruction of nuclear centrifuges by manipulating their industrial controller);[35] and (2) indirect effects, which hinder activity or functions that lie beyond the logical habitat of the compromised computer system but which rely on that system (e.g., interruption of the chemical process of uranium isotope separation necessary for the material's weaponization).

This description of the effects of a cyberattack departs from common understanding, which situates the effects boundary at the physical frontier of logically tied machines.[36] Take, for example, Olympic Games. The custom-built Stuxnet worm was designed to attack the logical environment of the Siemens S7-315 PLC at the Natanz nuclear facility in Iran. The attack sequence injected malicious code into the PLC to alter the behavior of IR-1 centrifuge cascades controlled by it.[37] Commentators ordinarily describe the effects on the PLC as direct and those on centrifuges as indirect, because the latter effects were

34. See Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Random House, 2005), chap. 17.
35. The term "industrial controller" signifies computer systems that govern processes of industrial production. It includes supervisory control and data acquisition (SCADA) systems and programmable logic controllers (PLCs).
36. See Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*.
37. For technical details on Stuxnet's destructive procedure, see Nicholas Falliere, Liam O. Murchu, and Eric Chien, "W32.Stuxnet Dossier," ver. 1.4 (Cupertino, Calif.: Symantec, February 2011).

"transmitted" via the PLC. This standard definition is nonsensical from the perspective of strategic analysis because it unnecessarily discriminates between effects exerted on an industrial controller and those on its constituent machines. In contrast, the usage proposed above assumes a more general perspective: it separates effects occurring within a unitary logical environment such as the Natanz facility from those affecting, say, Iran's ability to purify uranium—a far more useful distinction for strategic analysis. Moreover, because malware manipulates the logical unison of a computer system to execute a payload, treating effects within that system as direct and those beyond it as indirect makes more sense.[38] In short, the interesting segmentation of cyberattack effects lies at the logical, not the physical, boundary of cyberspace.

If the effects of a cyberattack produce significant physical destruction or loss of life, the action can be labeled "cyberwar," a term that should be used sparingly given that the vast majority of cyberattacks do not meet this criterion.[39] If the attack is perpetrated by a private actor for political or ideological purposes, it is an example of "hacktivism."[40] Moreover, cyberattacks can be customized or generalized. In a customized attack, the payload is designed to manipulate only machines within a specific logical habitat (e.g., Olympic Games). In a generalized attack, no machine reachable via the internet is in principle spared (e.g., the DDoS attacks that paralyzed computer systems in Estonia in 2007).

CYBER EXPLOITATION. Cyber exploitation refers to the penetration of an adversary's computer system for the purpose of exfiltrating (but not defiling) data.[41] One of the first major acts of cyber exploitation occurred in 1986 with a foreign breach of military and government computers in the United States. Another notable incident was the seizure by Chinese agents of several terabytes of secret U.S. government data in 2003. Essentially an intelligence-gathering activity, cyber exploitation relies on stealth and undetectability; thus disruption of the host system, which can lead to discovery and closure of access, defeats the purpose of exploitation.[42] One objective of exploitation may be to seize a nation's military or industrial secrets, an activity known as "cyber espionage." The technique can also be employed to

38. The standard usage can be relabeled as follows: "first-order" direct effects exerted on an industrial controller; and "second-order" direct effects influencing machine parts governed by it.
39. For a similar definition, see Nye, "Nuclear Lessons for Cyber Security?" p. 21.
40. On hacktivism as a modern form of political activism, see François Paget, *Cybercrime and Hacktivism* (Santa Clara, Calif.: McAfee, 2010), pp. 10–12.
41. See Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, p. S-1.
42. See ibid., pp. 1–7.

acquire knowledge of an adversary's computer systems to plan future cyberattacks, in which case exploitation is an element of a multistage cyberattack.[43]

Acts of cyber exploitation are often conflated with cyberattack.[44] From a strictly technical standpoint, this makes sense. In cyber exploitation, the target computer system is itself subjected to "attack," because access to privileged data usually requires aggressive measures to overcome computer defenses—hence the tendency for the conflation of terms within the technical community. From a tactical perspective, moreover, differentiating cyber exploitation from cyberattack can be difficult because both rely on the presence of a vulnerability and the ability to manipulate it; only the nature of the payload, which may not be immediately evident to the defender, varies. Further, a multistage cyberattack by an "advanced persistent threat" may involve preliminary rounds of exploitation to gain knowledge of the target,[45] further obscuring the two forms of action. These technical and tactical ambiguities, however, should not conceal an essential difference: cyber exploitation and cyberattack invite very different policy and legal consequences. As a form of espionage, exploitation by itself does not exert adverse direct effects and is not prohibited by international law; in contrast, a high-impact cyberattack could constitute a use of force or even an armed attack under treaty obligations. The use of unmanned aerial vehicles (UAVs) highlights the difference. Similar to cyber artifacts, UAVs can be employed to conduct remote sensing or they can be fitted with Hellfire missiles to strike ground targets (or both). Like a computer operator, a defender on the ground may not know the precise nature of the weapon until the operation is well under way. Yet it would be senseless—politically, legally, and strategically—to label the use of a UAV for strictly reconnaissance purposes a "drone attack." Fusion of the terms cyber exploitation and cyberattack could, however, produce such misidentification. From the perspective of international security, therefore, the common conflation of labels inhibits rather than aids understanding of the cyber issue.

The protection of military, industrial, and commercial secrets from cyber ex-

43. See David D. Clark and Susan Landau, "Untangling Attribution," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), pp. 25–40.

44. See, for example, Alexander Klimburg and Heli Tirmaa-Klaar, *Cybersecurity and Cyberpower: Concepts, Conditions, and Capabilities for Cooperation for Action within the EU* (Brussels: European Parliament Directorate General for External Policies of the Union, Policy Department, April 2011), p. 5.

45. The term "APT" refers to an actor (such as a large state) able to penetrate an adversary's computer systems persistently and successfully.

ploitation is a key preoccupation of national security policy. Nevertheless, cyberattack poses potentially greater dangers to international security, because the threshold of proven cyberattack effects has been rising steadily in recent years—it now includes physical destruction. In addition, the new weapons pose enormous defense challenges while disturbing interstate strategic stability. Whether security scholars grasp these implications of the cyber danger for international security depends on their ability to break free from their preconceptions as to what constitutes a serious threat.

The Shape of the Cyber Danger

Some skeptics argue that the cyber peril is overblown, contending that cyberweapons have no intrinsic capacity for violence and do not alter the nature or means of war. This strategy to puncture the perceived threat inflation works by conceptual fiat: because the method of harm lacks similarities with interstate armed conflict, by definition there can be no such thing as cyber "war."

In a sense, the skeptics are correct. The cyber revolution—as far as we can tell—has not fundamentally changed warfighting. At the same time, this skepticism, grounded in traditional thinking about war and peace, fails to acknowledge the broader agenda of international security studies, which encompasses issues such as protection against nonmilitary foreign threats and the ability of nonstate actors to inflict economic and social harm. The Clausewitzian philosophical framework misses the essence of the cyber danger and conceals its true significance: the virtual weapon is expanding the range of possible harm and outcomes between the concepts of war and peace, with important consequences for national and international security. Of course, the impact of cyber technology on military affairs is an important concern and, for some thinkers, will be a starting point of theory—but it is not a point of terminus. An appraisal of the cyber danger in its fuller dimensions is therefore needed. Three main factors underscore this danger: (1) the potency of cyberweapons, (2) complications relating to defense, and (3) the potential to disturb international order.

THE POTENCY OF CYBERWEAPONS

A unique feature of a cyberattack is its virtual method. To reach its target, a weapon traditionally had to traverse a geographic medium—land, sea, air, or outer space. Upon arrival, it inflicted direct material harm. The cyber revolution has dramatically altered this situation. Malware can travel the information

surface and obeys the protocols of TCP/IP, not the laws of geography.[46] It is little constrained by space and obliterates traditional distinctions between local and distant conflict. The payload, too, is an intangible: it operates through complex coding, which means that the weapon's "charge" is not the most proximate cause of damage. Instead, the infliction of harm requires a remote object—such as an industrial controller—that can be manipulated. The use of weaponized code, nevertheless, can have potent effects on the political and social world.

To date, cyber instruments have produced no fatalities, though their potential for doing so is widely recognized. Based on extrapolations of a cyberattack simulation conducted by the National Academy of Sciences in 2007, penetration of the control system of the U.S. electrical grid could cause "hundreds or even thousands of deaths" as a result of human exposure to extreme temperatures.[47] Such an attack would be all the more damaging because, at least initially, officials would be unable to detect the source of the problem. Other calamitous cyberattack simulations involve the derailment of trains transporting hazardous chemical materials or the contamination of public water supplies.[48]

Until recently, the ability of cyber artifacts to damage physical facilities remained entirely in the realm of theoretical speculation. Olympic Games changed that. The direct effects of this operation, as revealed in a report by the International Atomic Energy Agency, included the decommissioning of approximately 1,000 centrifuges at Iran's Natanz facility during a three-month period. The indirect effects of the attack are subject to dispute, but they were almost certainly greater than this figure suggests. Indeed, the most powerful effect may have been psychological. Discord and mistrust within Iran's nuclear establishment, arising from paranoia that a rogue scientist was among its ranks, and fears of intrusion elsewhere in the nation's cyber archipelago, may have slowed Iran's ability to acquire the bomb by as many as two years—significantly longer than the time required to replace the impaired centrifuges.[49]

The use of cyberweapons, however, need not result in physical destruction to pose a serious danger to society. Even if a cyberattack lacks intrinsic vio-

46. TCP/IP signifies the suite of communications protocols that govern data transmission via the internet.
47. National Research Council of the National Academies, *Terrorism and the Electric Power Delivery System* (Washington, D.C.: National Academies Press, 2012), p. 16.
48. See Barack H. Obama, "Taking the Cyberattack Threat Seriously," op-ed, *Wall Street Journal*, July 19, 2012.
49. See David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks against Iran," *New York Times*, June 1, 2012.

lence because the execution of code is a remote as opposed to proximate cause of injury, the effects can still cause serious economic and social harm. "It may not be a bomb coming down our middle chimney of our house," Jonathan Zittrain explained, "but it could be something that greatly affects our way of life."[50] Or as Chairman of the Joint Chiefs of Staff Gen. Martin Dempsey stated, "The uncomfortable reality of our world is that bits and bytes can be as threatening as bullets and bombs."[51] The Estonian and Georgian cyberattacks, according to NATO's Supreme Allied Commander Europe, Adm. James Stavridis, provide a "glimpse of this future [of conflict]" by demonstrating the potent indirect effects of nonviolent and generalized cyberweapons.[52] The DDoS attacks on Estonia in 2007 froze the country's government and financial activities for approximately three weeks.[53] Because there was no physical wreckage or loss of life, the label of cyberwar does not apply. At the same time, the incident was far more than just a "large popular demonstration," as Thomas Rid portrays it;[54] rather, the cyberattack in Estonia represents a wholly new type of social and economic disturbance. Three factors explain why traditional analogies of political disturbance do not apply: (1) the perpetrators resided mostly outside the affected territory; (2) the attack procedure crossed more than 100 national jurisdictions via the internet with awesome speed; and (3) identifying and punishing the perpetrators proved very difficult because of Moscow's refusal to provide forensic assistance to Estonian investigators, who possessed log files of affected machines revealing that many of the culprits had operated out of Russia.

The cyberattacks on Georgia further demonstrate the potency of nondiscriminating cyberweapons. The attacks, which were carried out by nonstate agents including Russian criminal syndicates, occurred against the backdrop of Russia's ground incursion into Georgia in the summer of 2008. A detailed study of the case concludes that the disruption of Georgia's computer systems tactically benefited the Russians in two important ways. First, it crippled the

50. "Has the Cyberwar Threat Been Exaggerated?" debate, Intelligence Squared U.S., Washington, D.C., June 16, 2010, http://intelligencesquaredus.org/debates/past-debates/item/576-the-cyberwar-threat-has-been-grossly-exaggerated.
51. Letter from General Martin E. Dempsey to John D. Rockefeller IV, chairman, U.S. Senate Committee on Commerce, Science, and Transportation, August 1, 2012 (Washington, D.C.: U.S. Government Printing Office).
52. Donna Miles, "U.S. European Command, NATO Boost Cyber Defenses," American Force Press Service, U.S. Department of Defense, May 18, 2012, http://www.defense.gov/news/newsarticle.aspx?id=116394.
53. See President of Estonia Toomas H. Ilves, address given at the European Union Ministerial Conference on Critical Infrastructure Protection, Tallinn, Estonia, April 27, 2009.
54. Rid, "Cyber War Will Not Take Place," p. 12.

Georgian government's communications infrastructures, hindering Tbilisi's ability to coordinate domestic civil defenses. Second, it paralyzed the operations of the National Bank of Georgia, which impeded procurement of essential war matériel from private industry.[55] Although these same tactical effects could have been achieved using conventional arms, it is important to note that cyber technology offered a feasible substitute that did not directly implicate Russia's military services, was cheap and readily available to nonstate agents, and proved impervious to conventional defenses.

Traditional notions of warfare confront five difficulties in conceptualizing cyberattacks, as the above cases illustrate. First, cyberattacks lack a proximate cause of injury and may not even be violent. Second, the conception of war as the use of armed force sets a high threshold in terms of scope, duration, and intensity that cyber actions may not meet.[56] Third, the perpetrators of a cyberattack can be nonstate parties who are not typically considered subjects of international law and thus are not subject to its penalties. Fourth, an offensive cyber operation by nontraditional players, such as that conducted against Estonia, need not involve the strategic purposes of states or their militaries. Fifth, at least in the case of a generalized cyberattack, the important distinction between military and civilian targets dissolves owing to the broad diffusion of computer systems in society and their interdependencies. Two other possible analogies to cyberattacks, "sanctions" and "sabotage," are also misleading. Sanctions are an exercise in negative power: they operate through the denial of gain rather than the direct infliction of loss. Yet offensive cyberpower clearly exerts positive effects. It initiates harmful activity that otherwise would not occur and causes direct injury to the victim. The label of sabotage, which has been applied to Stuxnet,[57] is an empty concept: there is no precise definition of the term in this or other domains of conflict. Use of the term adds nothing to the resolution of the conceptual problems of cyber phenomena.

The principle of "equivalence" that underpins U.S. and NATO cyber defense policy represents an attempt to resolve the conceptual muddles attached to the cyber issue. It maintains that the direct and indirect effects of cyberattack, not its method, should determine the manner and severity of retaliation—including conventional force—but without identifying specific thresholds of

55. See U.S. Cyber Consequences Unit (US-CCU), *Overview by the US-CCU of the Cyber Campaign against Georgia in August 2008*, Special Report, US-CCU, August 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.
56. See Eneken Tikk, quoted in "Could Cyber Skirmish Lead to War?" *NBC News*, June 11, 2010, http://www.nbcnews.com/technology/could-cyber-skirmish-lead-u-s-war-6C10406234.
57. See Rid, "Cyber War Will Not Take Place."

response. The deliberate declaratory vagueness of the principle is an attempt to adapt the doctrine of "calculated ambiguity" to the peculiar conditions of the cyber domain.[58] Although it is tempting to see in this a crude treatment of cyberattacks a form of "war," the equivalence principle reflects a willingness to reinterpret and transcend, on a case-by-case basis, the limitations that traditional concepts of violence place on the retaliator. It leaves open the possibility of a forcible response even if the initial cyberattack is not construed as an act of war. As one U.S. soldier put it rather cavalierly, "If you shut down our power grid, maybe we will put a missile down one of your smokestacks."[59] The implications for international security are potentially serious: according to this principle, a cyber event can occur that does not meet the traditional definition of war but that nevertheless elicits a reprisal of commensurate severity.

In the future, war by malware may occur if a cyberattack results in a similar number of deaths or level of physical destruction as a major kinetic strike. To make sense of such an eventuality, traditional concepts of interstate warfighting are needed. The capacity of cyber arsenals to augment military force is not, however, their main contribution. Rather, the new weapons expand the available methods of harm that do not fit established conceptions of war but that may be no less harmful to national security.

The ability of a cyberattack to inflict economic and other damage without resort to traditional violence affords this virtual weapon a special utility: it expands the choice of actions and outcomes available to the strategic offense. Again, Olympic Games underscores the point. The operation was part of a broader campaign to deprive Iran of the ability to produce weapons-grade uranium. The United States and Israel agreed on this objective but differed on how to achieve it, with Israel eventually favoring airstrikes on Iranian nuclear plants. Officials in Washington agonized over the potential consequences of such a move, fearing it could ignite a regional conflagration and only intensify Tehran's resolve to obtain the bomb. The Stuxnet worm offered the two countries at least a temporary solution to their differences: it promised to deliver some of the tactical results of a military strike while avoiding certain retaliation. Thus, the fact that the direct effects of Stuxnet were not comparable to the scale of destruction possible in an air attack was the new weapon's principal

58. On calculated ambiguity in other domains of conflict, see Scott D. Sagan, "The Commitment Trap: Why the United States Should Not Use Nuclear Weapons to Deter Biological and Chemical Weapons Attacks," *International Security*, Vol. 24, No. 4 (Spring 2000), pp. 85–115.
59. Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 30, 2011.

appeal. The Stuxnet worm alone could never prevent an Iranian bomb, but it could at least delay enrichment while averting a regional war.

Tehran's response to Olympic Games, as far as is known, has been muted.[60] This demonstrates that the phenomenon of cyberattack merits strategic analysis as much for the consequences it avoids as for those it produces. Indeed, it is tempting to conclude that cyberweapons promote international security—after all, their use may avert traditional forms of war.[61] Although this argument may have some merit in specific cases, it is too simplistic as a general observation; gains to the offense produce enormous losses in defense as well as conditions for strategic instability.

COMPLICATIONS OF CYBER DEFENSE

Security planners repeatedly warn that, in the cyber domain, the offense holds the advantage.[62] Some skeptics seek to dispel this notion by emphasizing the high costs of staging a destructive cyberattack. They cite Olympic Games to make their point: the operation required years of meticulous planning, involved a preliminary intrusion into the Natanz PLC to gain knowledge of the target, manipulated no less than six vulnerabilities in the PLC (each an expensive technical feat), and required a skilled operative in situ or close by to deliver the worm across the air gap. Moreover, once the worm's coding secrets were revealed, systems operators were able to patch the programming defects that the worm exploited, rendering knowledge of these weaknesses useless to aspiring proliferants. For these reasons, skeptics assert, the defense, not the offense, has the advantage.[63] This conclusion is only half complete: it ignores or downplays the other half of the strategic picture—the enormous costs of defense against a cyberattack. Following is a description of five such costs.

OFFENSE UNPREDICTABILITY AND UNDETECTABILITY. The use of code to achieve destructive direct effects requires the manipulation of vulnerabilities in the target's computer system. By definition, the defender is unaware of such "zero-day" weaknesses. The universe of unknown and manipulable weaknesses renders a cyberattack difficult to predict, complicating the design of measures to repulse it. Incomplete knowledge of weaknesses also hinders

60. Some officials speculate that Iran retaliated for Olympic Games with DDoS attacks against U.S. financial institutions. See Sen. Joseph Lieberman, interview on *Newsmakers*, C-SPAN, September 23, 2012.
61. See Adam P. Liff, "Cyberwar: A New 'Absolute Weapon?' The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol. 35, No. 3 (June 2012), p. 401.
62. See William J. Lynn III, "Defending a New Domain," *Foreign Affairs*, Vol. 89, No. 5 (September 2010), pp. 97–108.
63. See Rid, "Think Again."

remediation of intrusion post facto, because this requires understanding the zero-day exploits in question. Furthermore, the abundance of possible access vectors that an attacker can utilize complicates the interception of malware "in transit." Olympic Games demonstrates these points. Stealth was a genial feature of this multistage operation. The method of access, which may have involved the use of infected removable drives, was unanticipated. For three years, the Stuxnet worm and its antecedents (which acted as "beacons" for the offense) resided in the logical environment of the target PLC without the plant operators noticing their presence. Remarkably, the worm was able to mask its damaging effects from the controllers even after the attack sequence had begun. Only a few months later did the Iranians determine, with outside assistance, the source of the centrifuge malfunction.

DEFENSE DENIAL. The possibility that attack code will reside undiscovered in a defender's computer system is perhaps the most worrisome feature of the cyber strategic landscape. Residency within a logical habitat affords the invader means to deprive the defense of the ability to manage its own protection in at least two ways. One is peer-to-peer monitoring, which allows an attacker to adjust the attack sequence remotely and in real time; another is the use of an intelligent malware agent with self-adaptive capacities that enable it to learn and override defensive acts. The ability of malware to generate multiple versions of itself means that the threat variants during a cyberattack are theoretically limitless. Nevertheless, permanent breach of a computer system need not entail permanent insecurity if the defensive terrain can be organized in concentric zones of access so that the most prized nodes are quarantined from less secure compartments. This approach, however, runs counter to the very purpose of information technologies, namely, to ease transmission of data between machines. Therein lies the root dilemma of cybersecurity: an impregnable computer system is inaccessible to legitimate users while an accessible machine is inherently manipulable by pernicious code.

COMPLEX DEFENSE SURFACE. Computer systems are becoming more intricate at all stages of design and use. As software and hardware complexity rises, so do the costs of customizing weaponized code. This increases the work factor of the attacker, who requires greater resources of manpower and intelligence to tailor the payload. At the same time, the costs to the defender, who has more node interdependencies to map and greater vulnerabilities to patch, also increase. The result is a fundamental offense-defense imbalance. Whereas the attacker need understand only the procedures of entry and attack it decides to employ, the defender must continuously protect the entire network surface against the vast universe of conceivable attacks; the growing tendency to join

critical computer systems to the internet is multiplying the available points of entry for use in a customized cyberattack. Moreover, society's increasing reliance on interconnected computer systems to support basic economic and social functions is increasing the opportunities to cause harm through a generalized cyberattack. The expanding network surface provides conditions for a shock offensive or, as John Mearsheimer puts it, "the ability to choose the main point"—indeed multiple points simultaneously—"of attack for the initial battles, to move forces there surreptitiously, and to surprise the defender."[64]

DEFENSE FRAGMENTATION. The majority of critical computer infrastructures are owned and operated by private industry.[65] Thus, the challenge of cyber security is essentially one of civil defense: how to equip the private sector to protect its computer systems in the absence of government direction. This ordinarily involves passive measures, such as resiliency and redundancy (the equivalents of underground shelters and target dispersal in nuclear defense), which thicken the defensive glacis and can absorb damage from offensive hits. Yet a passive approach will pay only limited defensive returns if it is unable to implement the highest level of protection across the entire network surface. A proactive strategy, in contrast, seeks to neutralize threats before they can be carried out—for instance, by dismantling an attacker's command and control. Proactive defenses, however, are difficult to implement, not least because the authority to execute offense-as-defense rarely belongs to the operators of systems subject to attack; instead, it resides with the government and internet service providers, which may not even be aware of an attack. Such fragmentation of defense responsibilities is a limiting factor when formulating a coherent response to a cyberattack.

SUPPLY CHAIN RISKS. Computer systems increasingly rely on off-the-shelf and offshore manufacturers for components, introducing vulnerabilities into the supply chain. Foreign agents or private contractors could preload software and hardware components with malware, whether for attack or exploitative purposes. In 2009 Britain's Joint Intelligence Committee warned that Chinese-stocked components of British Telecom's phone network could be preloaded with malware or zero-day weaknesses, giving Beijing the ability to interrupt the country's power and food supplies. A "sleeper" payload of this kind could be remotely executed to achieve a preferred outcome in a future diplomatic or military crisis. In 2012 the U.S. House of Representatives Intelligence Commit-

64. John J. Mearsheimer, *Conventional Deterrence* (Ithaca, N.Y.: Cornell University Press, 1983), p. 26.
65. For instance, more than three-quarters of U.S. electrical power is supplied by private utilities.

tee warned that machine parts supplied by Huawei, a Chinese company founded by a former officer of the People's Liberation Army, could be used to exfiltrate data from government computers. Protection against such supply chain risks requires government- and industrywide coordination, yet such efforts have barely commenced.

None of the above observations is axiomatic: we are only at the early stages of the cyber phenomenon. In combination, however, they underscore the immense disadvantages of defense against cyberattack. Nothing in the available historical record suggests that defensive costs are low or diminishing—certainly not Olympic Games, a case cherished by skeptics who challenge the common wisdom of offense dominance. The enormity of the defender's challenge is convincingly illustrated by the successful penetration of computer systems at Google and RSA, two companies that represent the quintessence of technological ability in the current information age.[66]

The thesis of defense dominance misses an essential truth: the offense-defense equation is relative; thus the absolute measurement of offensive costs has meaning only in reference to the expenses of the defender.[67] At most, the current high price of mounting a high-impact cyberattack limits the ability of traditionally weak players to harness cyberspace for asymmetrical gain. It does not eliminate the significant tactical advantages of a possessor of advanced code. Moreover, the absolute costs of cyberattack are possibly diminishing. "What was considered a sophisticated cyber attack only a year ago," warned Ian Lobbain, chief of Britain's Government Communications Headquarters, "might now be incorporated into a downloadable and easy to deploy internet application, requiring little or no expertise to use."[68] Former Director of Central Intelligence George Tenet summarizes the defender's anguish: "We have built our future upon a capability we have not learned how to protect."[69]

DISTURBANCES TO STRATEGIC STABILITY AND INTERNATIONAL ORDER

A third manifestation of the cyber danger concerns the potential for global disorder. As Chairman of the Joint Chiefs of Staff Adm. Michael Mullen once re-

66. In 2010, Google announced that sophisticated Chinese agents had breached its systems, and in 2011, unknown parties compromised RSA's authentication products. This was followed by attempts to penetrate computers at Lockheed Martin, an RSA client.
67. See Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies*, Vol. 4, No. 4 (Summer 1995), p. 665.
68. Brian Groom, "Ministers Warn on Threat from Cyber Attacks," *Financial Times*, September 4, 2012.
69. Robert O'Harrow Jr., "Understanding Cyberspace Is Key to Defending against Digital Attacks," *Washington Post*, June 2, 2012.

marked, "We're going to have a catastrophic [cyber] event. Some of these tools already being built"—not least by the Pentagon—"are going to leak or be sold or be given up to a group that wants to change the world order, and we're incredibly vulnerable."[70] Admiral Stavridis voiced a similar concern. "In the world of cyber, we are at the beach at Kitty Hawk," he observed, referring to the advent of aviation in 1903. "We are just at the beginning," he went on. "We don't have 100 years [of experience] in cyber [conflict]. . . . We have to take steps today to bring order to [this] chaotic world."[71] The argument of this section—that cyber technology is exerting a limited but observable influence on regularized patterns of interstate rivalry—elaborates on such apprehensions and draws important observations for theory.

Concerns over global chaos lead—inevitably—to a theme familiar to the theoretician: the nature and requirements of order under conditions of international anarchy—most important, the stability of strategic interactions among states. Everyone knows that international politics transpires in the absence of a constraining authority, which produces incessant rivalry and occasional violence among actors competing for security. The interesting feature of anarchy, however, is not the recurrence of conflict—that is obvious—but its regularity. Although conceptions of national interest differ, even quarrelling states recognize the need to preserve order in their security relationships. This recognition underpins states' acceptance of common elementary goals (e.g., survival) as well as rules and principles of conduct; it helps to sustain the constancy of anarchic interactions and makes the permanent "state of war" tolerable because its contests for security are in the main regularized.

The revolutionary impact of technological change upsets this basic political framework of international society, whether because the transforming technology empowers unrecognized players with subversive motives and aims or because it deprives states of clear "if-then" assumptions necessary to conduct a restrained rivalry. The first factor, the concern voiced by Admiral Mullen above, contributes to fundamental instability in security relationships: a condition where the appearance of nontraditional or dissatisfied players undermines strategic stability. The second factor, alluded to by Admiral Stavridis, can produce instrumental instability, whereby accidents and misinterpretation of the new technology destabilize the dealings even of rational state adversar-

70. Alexander Fitzpatrick, "Cybersecurity Experts Needed to Meet Growing Demand," *Washington Post*, May 29, 2012.
71. Donna Miles, "Stavridis Spotlights Top National Security Issues," American Force Press Service, U.S. Department of Defense, March 15, 2012, http://www.defense.gov/news/newsarticle.aspx?id=119538.

ies.[72] The advent of the atom bomb, for instance, proved transformative only in the second sense: it elevated the horrors of war and disturbed the interstate strategic equation without altering the basic Hobbesian framework that defines how nuclear states compete for survival. Ongoing efforts to deprive terrorists and rogue states of the bomb, in contrast, are motivated by a desire to avert a nuclear revolution of the first order. In short, more important than the nature of a new weapon are the nature of its possessor and the purposes that instigate its use.

The cyber domain is a perfect breeding ground for political disorder and strategic instability. Six factors contribute to instrumental instability: offense dominance, attribution difficulties, technological volatility, poor strategic depth, and escalatory ambiguity. Another—the "large-N" problem—carries with it fundamental instability as well.

OFFENSE DOMINANCE. For the reasons enumerated in the preceding section, cyberspace is an offense-superior domain. This poses instrumentalist obstacles to the preservation of strategic stability among state rivals. Most notably, it exacerbates the security dilemma in three ways.[73] First, the recognition of offense superiority has instigated an arms race as states seek to avert strategic upsets in the new strategic arena.[74] Cyber arms verification, the chief prerequisite of successful arms control, confronts enormous challenges—not least the intangibility of cyberweapons, which complicates their detection. At present, no international limitations exist on the production of offensive cyber artifacts, and no such regulatory framework has yet been foreseen. Second, the perceived advantages of offensive use elevate the chances that those in possession of the new capability will actually employ it. Adversaries of the United States will have taken note of the tactical and strategic returns paid by Olympic Games; they may consider similar policy adventures in the future. Third, attempts to redress the defensive gap with "active defenses," a class of proactive measures that involves preemption or prevention of cyberattack by infiltrating or disrupting an opponent's computer systems,[75] obscures the offense-defense

72. For a discussion of strategic instability in the nuclear context, see Graham T. Allison, Albert Carnesale, and Joseph S. Nye, eds., *Hawks, Doves, and Owls: An Agenda for Avoiding Nuclear War* (New York: W.W. Norton, 1985), chap. 1.

73. A classic analysis of the problem is Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167–214.

74. According to some accounts, the fifteen largest militaries are developing advanced cyber weapons systems. See Editorial Board, "A New Kind of Warfare," *New York Times*, September 9, 2012.

75. On active defenses, see U.S. Department of Defense, *Department of Defense Strategy for Operating in Cyberspace* (Washington, D.C.: U.S. Department of Defense, July 2011), p. 7, http://www.defense.gov/news/d20110714cyber.pdf?.

boundary in weapons systems. Consequently, defensive actions may be misconstrued as overt attacks and produce pressures for an accidental exchange of blows.

ATTRIBUTION DIFFICULTIES. Authentication of the source of a cyberattack is ordinarily difficult.[76] Five characteristics of cyber conflict contribute to this problem. First, the ease of proliferation of cyberweapons means that, except in case of the most sophisticated offensive actions, the number of possible assailants is large. Second, proving the identity or location of any one of these assailants can be a huge challenge, because cyberspace affords an attacker an inordinate degree of anonymity. Third, where attribution is possible, it may not be of the right kind to organize a punitive response. Knowing the IP address of an attacking machine—the most basic form of technical attribution—does not necessarily reveal the identity of its human handler and, even if it does, this does not mean that the identity and motives of the sponsoring party will be divulged.[77] Fourth, because malware crosses multiple jurisdictions with ease, obtaining forensic evidence in the aftermath of an attack will be difficult without effective international cooperation. Fifth, even if all of these complications are resolved, it is still possible that attribution will not be prompt enough for timely retaliation. By the time their identity is known, the perpetrators may have relocated beyond the ability of the victim to respond. The most important strategic consequence of the attribution problem is that it weakens deterrence by reducing an assailant's expectation of unacceptable penalties.[78] Moreover, because reprisal to a cyberattack in the absence of convincing attribution incurs legitimacy costs for the retaliator, acceptable options following a failure to deter may be limited.

TECHNOLOGICAL VOLATILITY. The technology itself is a third destabilizing factor: cyberweapons are so novel and the vulnerabilities they seek to manipulate so inscrutable as to impede interpretation of probable effects of their use. Put simply, it is difficult to know how pernicious code will behave. The very short life cycle of advanced malware strains (many of which can be updated almost instantly upon release) contributes to this problem. Another difficulty concerns collateral damage. A poorly customized cyber artifact can

76. Others have analyzed this problem in detail. See, for example, Clark and Landau, "Untangling Attribution."

77. Herbert S. Lin, "Some Interesting Aspects of Cyberconflict for Discussion," presentation at the Harvard Kennedy School, Cambridge, Massachusetts, February 8, 2012.

78. On cyber deterrence, see Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), pp. 55–76.

cause far-reaching effects beyond the intended target if it infects a large number of third-party machines. The customization of malware only partly resolves the problem of unintentional civilian harm. Although the scope of possible direct effects may be reduced, the indirect consequences can still be enormous if the affected computer systems support essential social and economic activities. These indirect effects may be difficult to model or predict. A single brief interruption of stock-trading platforms, for instance, could produce little impact, or it could exert psychological effects that undermine public confidence in the entire financial system. Another related difficulty is the potential for "blowback": the possibility that the negative effects of a cyberattack will be felt by the attacker, whether through the self-propagative tendencies of malware (causing direct effects on home computer systems) or through cascading economic damage (indirect effects on the home society).[79]

POOR STRATEGIC DEPTH. A fourth destabilizing factor is the short time a defender has between the detection and impact of a cyberattack. The speed of cyberweapons eliminates temporal limitations to the infliction of harm. The new capability pushes the upper speed of weapons systems from Mach 20 (the speed of the fastest intercontinental ballistic missiles) to the velocity of electrons. Consequently, the interaction domain of cyber conflict unfolds in milliseconds[80]—an infinitesimally narrow response time for which existing crisis management procedures, which move at the speed of bureaucracy, may not be adequate. Traditional precedents that regulate the role of government agencies in the conduct of national defense can be difficult to interpret in a cyber emergency. And even where the necessary tactical action is known, the ability of operational and command structures to implement it may not exist. To illustrate, the U.S. National Security Agency has authority to retaliate against foreign-based cyberattacks, but it may lack access to forensic data necessary to tailor a timely response if such information resides in private computer systems or in foreign jurisdictions. The implementation of automated "tactical fires" can go far toward restoring strategic depth, but by removing the human agent from the response procedure, it introduces unknown risks of inappropriate reaction.

ESCALATORY AMBIGUITY. Traditionally, an international crisis could be averted through confidence-building measures such as established signaling procedures and diplomatic "hotlines." Failing that, common rules and norms could

79. See Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, pp. 2–32.
80. John C. Mallery, "Models of Escalation in Cyber Conflict," presentation at the Workshop on Cyber Security and Global Affairs, Budapest, May 31–June 2, 2011, http://es.slideshare.net/zsmav/models-of-escalation-and-deescalation-in-cyber-conflict.

still provide a minimum measure of expectations and moderating behavior. These safety valves disappear when dealing with a cyberattack. Signaling becomes murky; channels of communication break down or vanish; shared norms are rudimentary or unenforceable; and the identity, motives, or location of an attacker may not be known. Moreover, the tactical and strategic ambiguities of the related technology impede attempts to design escalatory models for the full spectrum of conceivable cyber conflict. The absence of clear "conversion tables" to orient interpretation of the equivalence principle could prompt an excessive response from a victim of an attack; lack of agreed standards of proportionality may produce further unreasonable counterresponses; and all the while, the lack of confidence-building measures could hinder attempts to de-escalate or terminate the crisis. What may begin as a low-intensity cyber exchange could intensify into a major showdown, possibly of conventional proportions. Such a crisis could be set in motion by cyber exploitation if the defender misconstrues it as a step in preparation for attack and instigates a preemptive blow.

"LARGE-N" PROBLEM. Low barriers to entry mean that the cyber domain features a variety of relevant players, ranging from states to private organized groups and individuals.[81] This can upset strategic stability in three ways, the first two of which are instrumental. One problem involves cooperation difficulties among unitarily rational states. As the number of cyber-capable states rises, the transaction and information costs of cooperation among them increase; there is less heterogeneity in discount rates for future payoffs (which raises the chances of a defection spiral); and the punishment of defection itself becomes a collective-action problem.[82] Second, the rising number of players in the domestic cyber establishment can impede the ability of states to act as coherent units. Although the United States has operated a unified cyber command since 2009, the first steps to standardize cyber operations across the combatant commands and their respective cyber outfits began only in mid-2012.[83] In the civilian domain, it is possible, according to Secretary of Homeland Security Janet Napolitano in remarks made in 2012, that private industry will be authorized by the government to conduct its own proactive measures.[84] Moreover, some countries—notably, Russia and China—

81. For a discussion of this phenomenon, see Nye, *The Future of Power*, chap. 5.
82. A classic study of this problem is Kenneth A. Oye, ed., *Cooperation under Anarchy* (Princeton, N.J.: Princeton University Press, 1986).
83. See Zachary Fryar-Biggs, "Panetta Green Lights First Cyber Operations Plan," *Defense News*, June 6, 2012.
84. Joseph Menn, "Hacked Companies Fight Back with Controversial Steps," Reuters, June 18, 2012.

increasingly employ cyber "militias" to prepare and execute hostilities. Such use of civilian proxies provides states plausible deniability if they chose to initiate a cyberattack, but it also risks instigating a catalytic exchange should the lines of authority and communication break down or if agents decide to act alone.

A third, deeper source of instability stems from the dispersion of power away from governments. While states remain the most powerful cyber players, they are not alone; the new technology empowers a variety of nontraditional actors such as religious extremist groups, political activists, criminal syndicates, and individuals. The cyberattacks against Estonia and Georgia demonstrate the ease with which civilian culprits can use the new weapons to exert economic and tactical effects outside their borders. Even lone agents can generate astonishing impact. A virus created in 2000 by a disaffected Filipino teenager infected one in ten machines worldwide, causing billions of dollars in economic losses and forcing the closure of computer networks at the Pentagon. Secretary of Defense Panetta warned of far worse scenarios, stating that militant groups could use cyber instruments to derail trains transporting hazardous chemicals or to contaminate the water supplies of large cities.[85] Cyber conflict, therefore, can fit four basic agent frames: (1) state-to-state, in which one state targets another state's strategic computer assets, such as in Olympic Games (this category includes the use by government of obedient civilian proxies); (2) private-to-state, which includes cyberattacks by militant groups or "patriotic" hackers such as in the Estonian case; (3) private-to-private, involving an exchange of cyber blows between nonstate entities such as private companies (a possible contingency of Secretary Napolitano's consideration); and (4) state-to-private, in which a state attacks the private computer systems of another nation, possibly for commercial or other economic gain.

The diversity of potential cyber adversaries and the possibility of cooperation among them establish conditions for fundamental instability; rather than hew to the familiar logic of interstate rivalry, cyber phenomena are likely to strain established theoretical models of security competition. Analysts must grapple, in effect, with two distinct but interrelated "states of nature," each of which may exhibit its own peculiarities: the traditional one of states locked in familiar contests for security but featuring a largely untested weapon whose use is difficult to model and regulate even among rational contenders; and a chaotic "global" system comprising nontraditional actors who may not

85. See Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, October 11, 2012.

accept or even understand the delicate political framework of anarchic international relations.[86]

The greatest test of international relations theory may well be its ability to assess instances of convergence and collision between these two universes. On the one hand, the wide diffusion of cyber technology enables new modes of cooperation between state and nonstate players who share certain goals and adversaries. An example of this phenomenon is the reported collusion between Iran and company insiders at Saudi Aramco to incapacitate tens of thousands of the firm's machines in 2012. There is also the danger of collision, however: a cyber event in which nonstate cyber activity encounters the high stakes of interstate competition. The cyberattacks that were conducted by nonstate actors to freeze financial activity in Estonia prompted officials in the capital, Tallinn, to consider invoking NATO's collective defense clause, a move that would have embroiled the Alliance in a major crisis with Moscow. Contamination of the preference pool with nontraditional players can impede the ability of states to maintain the restrained stability of their relations. States have demonstrated reserve in the use of cyberweapons against each other, as illustrated by the United States' decision in 2003 not to attack computer systems in Iraq for fear of causing indiscriminate effects and setting dangerous precedents for future action. Nontraditional players, however, may not be so inhibited: they may use the new technology in ways that disrupt habitualized interstate rivalries, perhaps initiating a catalytic event that instigates a military showdown.[87]

Thus, a dangerous separation of power and diplomacy is occurring. Even if problems of instrumental instability in the cyber domain were soluble through intergovernmental agreement—a Sisyphean task thus far—private culprits could still unsettle the interstate equilibrium by defying the consensus. Overall, concerns about the possibility of global chaos voiced by practitioners may be overstated, but they contain the germ of an important truth about the contemporary cyber danger.

Conclusion

This article has offered a conceptual framework for the study of adversarial cyber phenomena in the field of international security. It has argued that ignor-

86. For a discussion of a similar point in relation to globalization, see Stanley Hoffmann, *Chaos and Violence: What Globalization, Failed States, and Terrorism Mean for U.S. Foreign Policy* (Lanham, Md.: Rowman and Littlefield, 2006), chap. 1.
87. On catalytic cyberattacks, see Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, p. 9-8.

ing the dangers that cyberweapons pose domestically and internationally inhibits future intellectual progress in the field. What may now seem a "revolutionary" technology will eventually become the new "conventional." Either there will be an exhaustive effort to integrate the new technology into our theories or there will be theoretical exhaustion. Equally important, sound theory can assist practitioners in the reevaluation of strategic axioms on which the efficacy of security policy ultimately rests. Scholars have a duty to decipher the meaning of the cyber revolution—if only to dispel the misperceptions of decisionmakers about its consequences for policy.

The cyber issue influences international relations theory in three general ways that cyber studies can immediately begin to address. At the most basic level, it touches on foundational theory, that is, scholars' understanding of basic concepts such as anarchy and order, which orient the formulation of research questions and guide the quest for satisfactory answers. In this respect, the preceding analysis suggests that the peculiar features of cyber phenomena may give impetus to two intellectual trends. One relates to the content of our substantive concerns—an ongoing conceptual shift that privileges security, broadly defined, over strict notions of war or military defense.[88] It is important to understand that cyber technology is expanding the range of possible harm beyond traditional conceptions of war and that it poses new challenges for national and international security. Another trend involves the field's current state-centric prejudices. Within the field of international security studies, conceptions of system and order typically—and at times exclusively—center on states and competition among them. To be sure, this frame applies to much of the cyber issue; insofar as it does not, however, future study will require consideration of the negative influences that nonstate players may be able to exert on states and their relations with other states. Cyber studies requires a willingness to evaluate the cyber issue in its interstate as well as in its global dimensions—especially the points at which the two universes converge and collide.

Second, scholars must open their theoretical toolkits to model, explain, and, where possible, predict adversarial cyber relationships. This task may involve incorporating cyber phenomena into major existing theoretical paradigms, such as the balance of power or institutional theory, each of which may yield distinct explanatory models. Empirical analysis, however, could also yield more narrowly focused theorization: the formulation of orderly

88. See Steven E. Miller, "*International Security* at Twenty-five: From One World to Another," *International Security*, Vol. 26, No. 1 (Summer 2001), pp. 7–8.

propositions that account for precise occurrences within the dataset, such as the use of code to destroy Iranian nuclear centrifuges and the regional consequences of pressing for such a course.

Third, in addition to elucidating empirical cyber events, scholars can guide the design of policies to affect them. Some theorists may resist the extension of scholarship in this manner. The pressures of decisionmaking, however, leave practitioners little time for strategic interpretation, further elevating the need for cyber studies. The quandaries of strategy are urgent. Does declaratory ambiguity deter cyberattacks or merely increase the chances that the prospect of retaliation will be underrated? What dangers does a policy of cross-domain deterrence that includes escalation to conventional force pose for the management of a cyber crisis? What signaling procedures and confidence-building measures could halt a cyber exchange involving nonstate actors from accelerating beyond the ability of states to control it? With what mechanisms can private actors be co-opted into the cyber establishment so that it can leverage civilian resources for strategic gain? The academy has a duty to apply and adapt its theories in the assessment of such policy conundrums.

Some observers perceive the information age as a veritable revolution in human affairs. Few questions in future cyber studies will be more important than that of determining the extent to which the present era represents a new phase in international relations—whether patterns of security competition will be significantly altered or whether they will continue essentially the same, albeit with new instruments at actors' disposal. One of the main conclusions of this study contravenes what historical experience seems to suggest: unlike previous technological transformations, the cyber revolution is influencing the tendencies of anarchic international politics, rather than merely altering the strategic dealings of states; that is, the cyber domain exhibits both fundamental and instrumental forms of instability. Given its lack of purposive regularity and absence of stable or known logics of interaction, the present cyber condition deviates from the routinized patterns of competition that characterize much of international anarchy. A central task of scholarship, therefore, will be to formulate concepts and propose policies that can impose on the chaotic cyber domain the necessary measure of stability to render its contests not just orderly but also "ordinary."

The cyber revolution is still incipient; conclusions about its implications for theory and practice are necessarily provisional. It remains open to question whether the related technology demands a greater order of change in our thinking about international security than did previous technological revolutions. We may discover that the challenge to our theories is not much larger

than, for example, the advent of the telegraph in the nineteenth century. Conversely, the need for new concepts could be far greater, given societies' growing reliance on cyberspace and its usefulness in the propagation of threats.

In sum, the conceptual apparatus of international security may yet absorb emergent cyber phenomena—or it could become a relic in need of redevelopment. But whatever the cyber revolution signifies, it is detrimental to the intellectual progress and policy relevance of the field to continue to avoid its central questions.