The Myth of Cyberwar

Bringing War in Cyberspace Back Down to Earth

Erik Gartzke

A blitz of media, punditry, and official pronouncements raise the specter of war on the internet. Future conflicts may well take place in cyberspace, where victory or defeat could be determined in mere "nanoseconds."[1] Secretary of Defense Leon Panetta has even warned of a "cyber-Pearl Harbor."[2] Nor are fears of cyberwar abstract speculation. Events such as the denial of service attacks against Estonian and Georgian government websites, the Stuxnet worm designed to disable Iranian nuclear centrifuges, and the recent hacking of U.S. military computer networks seem to indicate that the era of cyberwar has already arrived.

Cyberwar can be viewed as the most recent phase in the ongoing revolution in military affairs.[3] This time, however, the threat is said to be directed at the sophisticated technological civilizations of the West, rather than at desert insurgents or the leaders of rogue states with arsenals of inferior second world military hardware. Joseph Nye expresses this emerging consensus, "Dependence on complex cyber systems for support of military and economic activities creates new vulnerabilities in large states that can be exploited by nonstate actors."[4] Following this logic, the United States appears destined to be "the

Erik Gartzke is Associate Professor of Political Science at the University of California, San Diego, and Professor of Government at the University of Essex.

The author thanks Susan Aaronson, Tai Ming Cheung, Peter Cowhey, Peter Dombrowski, Eugene Gholz, Florian Grunert, Jeffrey Kwong, Jon Lindsay, John Mueller, and Heather Roff and the anonymous reviewers for comments and encouragement. Oliver Davies provided valuable research assistance.

1. Dan Kuehl, quoted by Grace Chng, "Cyber War: One Strike, and You're Out," *Sunday Times* (Singapore), July 18, 2010.
2. Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack," *New York Times*, October 11, 2012.
3. On the revolution in military affairs (RMA), see Alvin and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown, 1993); Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *National Interest*, No. 37 (Fall 1994), pp. 30–42; Andrew F. Krepinevich, *The Military-Technical Revolution: A Preliminary Assessment* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2002); Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs*, Vol. 75, No. 2 (March/April 1996), pp. 37–54; Richard Hundley, *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. Military*? (Santa Monica, Calif.: RAND, 1999); Michael O'Hanlon, "Why China Cannot Conquer Taiwan," *International Security*, Vol. 25, No. 2 (Fall 2000), pp. 51–86; and Michael G. Vickers and Robert C. Martinage, *The Revolution in War* (Washington, D.C.: Center for Strategic and Budgetary Assessments, 2004). For criticism of the RMA, see Stephen Biddle, "Assessing Theories of Future Warfare," *Security Studies*, Vol. 88, No. 1 (Autumn 1998), pp. 1–74.
4. Joseph Nye, "Cyber Power" (Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010), p. 4.

International Security, Vol. 38, No. 2 (Fall 2013), pp. 41–73, doi:10.1162/ISEC_a_00136

country most vulnerable to cyber-attack."[5] If powerful developed nations largely immune to terrestrial onslaught can have their defenses disabled and their factories idled by foreign hackers, then perhaps "Pearl Harbor" is an appropriate metaphor. One should then heed the growing chorus of warnings that the West is about to become the target, rather than perpetrator, of "shock and awe."

There is a significant fault, however, in the theme of impending cyber apocalypse: it is far from clear that conflict over the internet can actually function as war. Predictions about the nature or significance of cyberwar generally commit a common fallacy in arguing from opportunity to outcome, rather than considering whether something that could happen is at all likely, given the motives of those who are able to act. Cyber pessimism rests heavily on capabilities (means), with little thought to a companion logic of consequences (ends). Much that could happen in the world fails to occur, largely because those who can act discern no meaningful benefit from initiating a given act. Put another way, advocates have yet to work out how cyberwar enables aggressors to accomplish tasks typically associated with terrestrial military violence. Absent this logic of consequences, cyberwar is unlikely to prove as pivotal in world affairs, and for developed nations, in particular, as many observers seem to believe.

This article assesses the salience of the internet for carrying out functions commonly identified with terrestrial political violence. War is fundamentally a political process, as Carl von Clausewitz famously explained.[6] States, groups, and individuals threaten harm to deter or compel, generating influence through the prospect of damage or loss. Military force can also be exercised to maintain or alter the balance of power and resist or impose disputed outcomes. The internet is generally an inferior substitute to terrestrial force in performing the functions of coercion or conquest. Cyber "war" is not likely to serve as the final arbiter of competition in an anarchical world and so should not be considered in isolation from more traditional forms of political violence.[7] The capacity for internet coercion is further limited by some of the same factors that make cyberwar appear at first so intimidating. For threats or demands to prove effective, targets must believe both that an attack is likely to follow from noncompliance and that the attack is destined to inflict unacceptable harm. Yet, as I detail here, the need to apprise targets of internet vulnera-

5. James Adams, "Virtual Defense," *Foreign Affairs*, Vol. 80, No. 3 (May/June 2001), p. 98.
6. Carl von Clausewitz, *On War* (Princeton, N.J.: Princeton University Press, 1976).
7. Hannah Arendt wrote, "The chief reason warfare is still with us is . . . that no substitute for this final arbiter in international affairs has yet appeared on the political scene." Arendt, *On Violence* (New York: Harcourt, Brace, 1970), p. 2.

bilities to make cyber threats credible contrasts with the secrecy required to ensure an effective attack.

Given the inherent difficulty of credibly threatening cyberattacks without also compromising operational effectiveness, it will be tempting for actors to practice cyberwar rather than engage in coercive threats. Here, too, however, key limitations exist regarding what can be achieved over the internet. It is one thing for an opponent to interrupt a country's infrastructure, communications, or military coordination and planning. It is another to ensure that the damage inflicted translates into a lasting shift in the balance of national power or resolve. Cyberattacks are unlikely to prove particularly potent in grand strategic terms unless they can impose substantial, durable harm on an adversary. In many, perhaps most, circumstances, this will occur only if cyberwar is accompanied by terrestrial military force or other actions designed to capitalize on any temporary incapacity achieved via the internet. Those initiating cyberattacks must therefore decide whether they are prepared to exploit the windows of opportunity generated by internet attacks through other modes of combat. If they are not willing and able to do so, then in grand strategic terms, there are few compelling reasons to initiate cyberwar. The need to back up cyber with other modes of conflict in turn suggests that the chief beneficiaries of cyberwar are less likely to be marginal groups or rising challengers looking to overturn the existing international order and more likely to be nation-states that already possess important terrestrial military advantages. Conceived of in this way, the internet poses no revolution in military affairs but instead promises simply to extend existing international disparities in power and influence.

The remainder of this article is organized into five sections. After a brief review of the burgeoning literature on cyberwar, the subsequent section lays out the case for a logic of consequences. It is not enough to determine what could happen in a world where so much is possible. The third section applies basic insights about the nature of war to detail critical shortcomings of cyberwar as a political instrument. The Pearl Harbor attacks admirably illustrate the inadequacies of conflict in cyberspace. Section four addresses additional implications and limitations of the main argument, while the fifth section offers some concluding remarks.

Panic over the Internet: The Literature on Cyberwar

The character of war has evolved, if not regularly, then certainly at various points in history. As such, it is reasonable, even forward looking, for observers to consider what impact each new technology might have on the nature of war

and peace. Innovations such as the stirrup, steam propulsion, the airplane, and the exploding shell transformed warfare. Other changes, such as the telephone, high-rise construction techniques, and the advent of effective birth control, may have been less revolutionary than evolutionary in their military effects. A large and growing literature seeks to alert—some might say alarm—observers to the dangers of cyberwar. These studies shine much less light on how cyberspace is destined to change the nature of political conflict than on what harm it is possible to perpetrate over the internet.

Scope and scale conditions of cyberwar—cyber pessimists

For many thoughtful commentators, the size and scope of the cyberwar threat could be unprecedented. William Lynn III argues that cyberwarfare is indeed a substantial, imminent threat.[8] Those with a motive to launch an attack against the United States will soon possess the capability to do so. In this sense, cyberwarfare is unique in that opponents who utilize the strategy are not limited by financial or physical constraints. Lynn advocates a vigorous defense as the most viable and flexible strategy in cyberspace. The United States can avoid large-scale cyber calamities through the collaboration of public, private, and government-sponsored corporations. In a follow-on article, Lynn outlines a five-pillared cyberspace defense strategy, "treating cyberspace as an operational domain, like land, air, sea, and outer space; employing active defenses to stop malicious code before it affects our networks; protecting commercial networks that operate the critical infrastructure that our military relies upon; joining with allies to mount a collective cyber defense; and mobilizing industry to redesign network technology with security in mind."[9]

Treating cyberspace as an operational domain is an excellent idea, but doing so quickly reveals differences between internet conflict and warfare on land, sea, in the air, or in space. Deterring or even defending against cyberattack may prove difficult, as others have argued, but it will prove much harder still for an attacker to figure out how to benefit from internet aggression, unless cyberattacks occur in conjunction with attacks in other domains.

James Adams anticipates Lynn in arguing for a comprehensive U.S. cyberwarfare defense strategy.[10] The United States is vulnerable to attack because

8. William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, Vol. 89, No. 5 (September/October 2010), pp. 97–108.
9. William J. Lynn III, "The Pentagon's Cyberstrategy, One Year Later: Defending against the Next Cyberattack," *Foreign Affairs* (September 28, 2011), http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later.
10. Adams, "Virtual Defense," pp. 98–112.

many smaller nations and private groups will seek to gain an advantage by employing asymmetric warfare, whose impact would be felt not only in the public sector, but also in private industry.[11] The U.S. military has become increasingly dependent on new technology to dominate modern battlefields, paradoxically rendering itself more vulnerable and prone to ever-increasing incidences of potentially crippling cyberattacks. Richard Clark and Robert Knake offer early examples of cyberwar.[12] They claim that the United States has been slow to orient itself to what they argue could be a national security nightmare. Shane Courville also considers the United States to be highly susceptible to a catastrophic cyberattack, but he is pessimistic about the ability of the United States or other nations to defend themselves.[13] Cyber defense is problematic given rapidly changing technology. In particular, Courville notes that little thought has gone into exactly who manufactures computer hardware for the U.S. military.[14]

Kenneth Knapp and William Boulton point out that the limited barriers to entry in cyberwarfare leave even great powers vulnerable to a constant stream of virtual attacks.[15] As they write, "[W]ide ranges of formidable cyberweapons have become more affordable and available. . . . An attacker can build an [electromagnetic] bomb, designed to fry computer electronics with electromagnetic energy, for as little as $400."[16] The authors blame advances in cyberwar technology for heightened losses in U.S. industry: "500 U.S. companies showed an increase in reported financial losses of 21 percent, or $455.8 million, in 2002."[17]

Lorenzo Valeri and Michael Knights are also concerned about the vulnerability of U.S. military and civilian infrastructure to cyberwarfare.[18] These authors speculate that terrorists will exercise offensive information warfare, focusing on electronic commerce websites instead of national infrastructure, as the former will be significantly more accessible and might ultimately wreak

11. Ibid., p. 99.
12. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: Ecco, 2010).
13. Shane P. Courville, "Air Force and the Cyberspace Mission: Defending the Air Force's Computer Network in the Future" (Maxwell, Ala.: Center for Strategy and Technology, Air War College, 2007).
14. Ibid.
15. Kenneth Knapp and William Boulton, "Cyber-Warfare Threatens Corporations: Expansion to Commercial Environments," *Information Systems Management Journal*, Vol. 23, No. 2 (Spring 2006), pp. 76–87.
16. Ibid., p. 79.
17. Ibid., p. 83.
18. Lorenzo Valeri and Michael Knights, "Affecting Trust: Terrorism, Internet, and Offensive Information Warfare," *Terrorism and Political Violence*, Vol. 12, No. 1 (Spring 2000), pp. 15–36.

the most havoc. Attacks on commercial industry will seriously damage consumer trust in the internet, and might ultimately undermine government plans to convert services to the digital domain. Valeri and Knights emphasize that the skills needed to conduct offensive information warfare "are easily available as the Internet and exposure to information and network technologies encourages increasing technological sophistication in society."[19]

John Arquilla and David Ronfeldt seek to distinguish between actors and their roles in internet conflict.[20] Cyberwar generally involves conflicts among organized militaries, while "Netwar" consists of internet conflict that includes nonstate actors. As they explain it, "[T]he term Netwar refers to an emerging mode of conflict (and crime) at societal levels, involving measures short of traditional war."[21] Arquilla and Ronfeldt argue that "cyberwar" has become misleading with the advent of newer technology. However, while Netwar and traditional cyberwar differ in their respective forms, each is a potentially catastrophic threat.

The attribution problem and international law

It has been argued that one of the most important, and potentially menacing, characteristics of cyberwar involves anonymity. David Clark and Susan Landau highlight attribution as a critical issue that is difficult to overcome in seeking to deter cyberattacks.[22] As they argue, "Retaliation requires knowing with full certainty who the attackers are."[23] Similarly, Martin Libicki is concerned that the internet may create intractable difficulties in seeking to deter would-be perpetrators.[24] As he explains the problem, "The lower the odds of getting caught, the higher the penalty required to convince potential attackers that what they might achieve is not worth the cost."[25] Attackers are much more likely to strike if they are unlikely to be targeted in return.

The focus is again on the potential for harm, rather than on exploring the motives and operational logic of perpetrators. If internet anonymity is awkward for targets of attacks, it is also a problem for initiators. Terrorists spend as

19. Ibid., p. 20.
20. John Arquilla and David Ronfeldt, "The Advent of Netwar: Analytic Background," *Studies in Conflict and Terrorism*, Vol. 22, No. 3 (September 1999), pp. 193–206.
21. Ibid., p. 194.
22. David D. Clark and Susan Landau, "Untangling Attribution," *Harvard National Security Journal*, Vol. 2, No. 2 (March, 2011), pp. 25–40.
23. Ibid., p. 2. Targeting improves with information about perpetrators, but blanket retaliation could also prove effective, provided that punishment also touches the attackers. At the same time, no one ever possesses "full certainty." The U.S. legal standard is "reasonable doubt."
24. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Calif.: RAND, 2009).
25. Ibid., p. 43.

much time marketing their exploits as they do fighting, bombing, assassinating, and so on. Where anonymity protects an aggressor from retribution, it also dilutes credit for the deed. Vandals often "tag" their handiwork—creating an identity where none need exist—precisely because real anonymity means not receiving credit for one's handiwork. Internet vandals also brand their exploits, presumably because they wish to receive credit for their exploits, even at some risk to their anonymity.

Just as ongoing cyberattacks from unidentified sources do not give the target a way to retaliate, they also fail to provide the target with the means to acquiesce. Demands from an anonymous cyberwarrior will tend to be ignored or reneged upon once vulnerabilities are identified and addressed. Demands might also come from a source that did not, or was even incapable of, mounting a cyberattack. As with the use of identifying symbols in war, it is in an attacker's interest to "brand" its actions to most effectively elicit concessions from a target. Indeed, even if demands are complied with, an attacker will have difficulty obtaining sustained compliance, given the impossibility of demonstrating future capabilities.

Discussion of attribution problems in cyberspace also reflects a subtle but telling shift in framing. Libicki's simple calculus of deterrence, for example, involves "getting caught," something more often characteristic of crime than war. Some aspects of international relations involve anonymity. Espionage, covert operations, and certain kinds of political theft or murder function most effectively when the perpetrators are unknown, or indeed when the operations themselves remain undisclosed. Strategic or tactical advantage can also stem from anonymity and surprise in terrestrial military missions, though nations and groups often sacrifice surprise and advertise their role in contests to extract concessions or tacit or formal admission of defeat. How does one surrender to no one in particular? The advantage of anonymity will persist for peripheral forms of warfare on the internet, just as it has played a role in terrestrial competition and conflict. Most forms of political conflict, however, encourage disclosing an initiator's identity. Coercion requires attribution. Similarly, threats designed to elicit concessions or deter aggression are already problematic in physical space.[26] This "credibility problem" mirrors the attribution problem and is perhaps equally likely to make internet aggression problematic for initiators as for possible targets.

---

26. Robert Powell, *Nuclear Deterrence Theory: The Search for Credibility* (Cambridge: Cambridge University Press, 1990); and Barry Nalebuff, "Rational Deterrence in an Imperfect World," *World Politics*, Vol. 43, No. 3 (April 1991), pp. 313–335.

Several scholars also note that cyberwar creates an unparalleled legal environment, one in which even defining the scope of activities has become problematic. There has not yet been sufficient time, or perhaps the inclination, to solidify the legal standing of cyber conflict in international law. Charles Dunlap notes that democracies, in particular, have sidestepped attempts to formulate a treaty covering cyber conflict.[27] Indeed, it is inherently difficult to legally define a process when capabilities have yet to be uncovered. Cyberattacks could perhaps be looked upon as the legal equivalent to armed attacks.[28] Yet, the legal definition of armed conflict involves "significantly destructive attacks taking place over some period of time and conducted by a group that is well-organized,"[29] a set of conditions yet to be adequately demonstrated in cyberspace.

cyber salience—a balancing of perspectives

While the bulk of reactions to cyberwar emphasize dramatic dangers, some studies offer a more balanced perspective. Tim Maurer contrasts the gloomy picture provided by the bulk of writers with estimates of likely determinants of loss of life associated with a cyberattack.[30] Maurer lists the relative security of civilian infrastructure, participation of nonstate actors, and the evolution of law regarding retaliation strategies. He concludes that loss of life from cyberattacks will generally be slight. Indeed, drawing on his estimates, Maurer asserts that "a digital Pearl Harbor would cost fewer lives than the attack 70 years ago."[31]

Wesley Clark and Peter Levin anticipate an inevitable rise in cyberwarfare, one that will eventually involve broad sectors of society.[32] Populations will face "network-born disruptions of critical national infrastructure"—including terrestrial and airborne traffic, energy generation and distribution, and the financial system. The authors note, however, that the United States and other

27. Charles J. Dunlap Jr., "Perspectives for Cyber Strategists on Law for Cyberwar," *Strategic Studies Quarterly*, Vol. 5, No. 1 (Spring 2011), pp. 81–99.
28. Vinton G. Cerf, "Safety in Cyberspace," *Daedalus*, Vol. 140, No. 4 (Fall 2011), pp. 59–69.
29. Michael N. Schmitt, "Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense, and Armed Conflict," in Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy* (Washington, D.C.: National Academies Press, 2010), p. 176.
30. Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, October 19, 2011, http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar.
31. Ibid.
32. Wesley K. Clark and Peter L. Levin, "Securing the Information Highway: How to Enhance the United States' Electronic Defenses," *Foreign Affairs*, Vol. 88, No. 6 (November/December 2009), pp. 2–10.

nations are doing a great deal to mitigate the threat. The United States has pledged a reported $30 billion by 2015 as part of the Comprehensive National Cyber Security Initiative. In addition, Clark and Levin note lessons learned from previous attacks. The most effective electronic security strategy must operate under full disclosure. Experts in academic, industrial, and governmental sectors must quickly collaborate on a mitigation strategy. Yet, Clark and Levin also acknowledge that "electronic security works best when it is autonomous, adaptable, distributed and diversified."[33]

Stephen Walt argues that a critical preliminary task is to separate out different dangers grouped under the common rubric of "cyber-warfare."[34] For Walt, cyberwarfare consists of four distinct issues: degrading an enemy's military capabilities, penetrating networks to shut down civilian infrastructure, web-based criminal activity, and cyber espionage. These four issues help to frame cyberwarfare as an evolving, nuanced set of issues, each amenable to its own cost-benefit analysis. Thomas Rid argues that cyberwar is not really war because it fails to conform to conventional definitions of conflict.[35] Rid's chief point—mirroring in an interesting manner Maurer's argument—is that cyberwar is not sufficiently violent or casualty-producing to be considered war. As such, cyberwar is a misnomer. This perspective risks becoming a purely academic exercise, however, if cyber conflict eventually supplants military violence as the ultimate arbiter of international politics. Cyberwar does not need to be war to make war obsolete. Instead, it must fulfill the existing functions of terrestrial warfare if it is to rival the utility of existing forms of conflict. As I argue below, the internet is extremely unlikely to substitute for, or serve as an alternative to, earthbound warfare.

Contrasting Vulnerability and the Nature of Threats

It has become an article of faith among those attentive to questions of security or technology that cyberspace is a new domain where the old rules of warfare no longer apply. Cyberspace could constitute a hidden back door, enabling opponents of the Western-dominated world order to undermine the hard-won terrestrial advantages of the established powers. History makes clear that technological innovations or new modes of organization eventually topple every

33. Ibid., p. 6.
34. Stephen M. Walt, "Is the Cyber Threat Overblown?" *Foreign Policy*, March 30, 2010, http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown.
35. Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol. 35, No. 1 (February 2012), pp. 5–32.

hierarchy.[36] The United States and other nations have already begun expensive reforms designed to prepare for war over the internet, while some civil liberties have been curtailed on the grounds that cyberwar may well constitute the next existential threat.

Yet, it is far from clear that the internet is transformational in military terms, let alone revolutionary. Lacking information about whether developments are radical or merely incremental, it may make sense to adopt a few guidelines that will help to determine whether there is cause for panic. A reasonable level of caution is usually provided by our own common sense. Most readers will lock their doors at night, for example, and refrain from handling large sums of cash in a dark alley. Imagining what others could do to injure each of us, however, can quickly descend into paranoia. It is not reasonable to believe that someone is intent on mischief simply because it is possible for them to inflict harm.

Even in the safest of societies, individuals, groups, and entire communities are subject to an enormous variety of potential hazards. Much could be done to impinge on each of us, even though few of these possibilities are ever exercised, or experienced, with any regularity. The physical world hosts a multitude of venues for extremely unlikely accident or disease. A small number of people prefer to remain indoors rather than risk being struck by lightning or struck down by botchulism. Still, individuals with these concerns may merit more attention from psychiatric professionals than from military planners. Being vulnerable will be novel to no one living in our modern, highly integrated world. Indeed, the capacity to hurt is so ubiquitous in densely populated portions of the globe that blood would coat the streets if it were not true that relatively little relationship exists between the capacity to attack and the actual prospect that one will be invaded, assaulted, or otherwise done in.[37]

Just about anything is possible. Someone may have put poison in your Corn flakes at breakfast. Terrorists may have singled you out for vengeance, or you might just become one of the unlucky few who are in the wrong place at the

36. On political order and technological change in world affairs, see Robert Gilpin, *War and Change in World Politics* (New York: Cambridge University Press, 1981); William H. McNeill, *The Pursuit of Power: Technology, Armed Force, and Society since* A.D. *1000* (Chicago: University of Chicago Press, 1984); Martin van Creveld, *Technology and War: From 2000* B.C. *to the Present* (New York: Free Press, 1989); Emily O. Goldman and Leslie C. Eliason, eds., *Diffusion of Military Technology and Ideas* (Stanford, Calif.: Stanford University Press, 2003); and Keir A. Lieber, *War and the Engineers: The Primacy of Politics over Technology* (Ithaca, N.Y.: Cornell University Press, 2005).

37. The current fascination with vampires (in popular culture) and zombies (among academics) illustrates the basic point. Aggression becomes endemic if harm has an intrinsic payoff (e.g., human beings are food). Vampires and zombies threaten not just individuals but the whole of civil society, because interdependence/specialization requires that vulnerability not equal insecurity.

wrong time. When a commuter steps outside to start her car or to catch the bus, it is impossible to be certain that no truck will jump the curb and that every asteroid will remain in its usual orbit. And yet, despite endless potential for injury or death, few of us have chosen to harden our living rooms against cruise missile attack or immersed ourselves in real-time plots from NASA charting the trajectories of space detritus. In dealing with known unknowns, we became comfortable with not being protected. California homeowners typically do not carry earthquake insurance, for example, even though "the big one" is an eventuality. We do so because security is expensive; being indemnified against unlikely events may literally not be worth the effort. One could buy that bulletproof vest listed on Ebay, but then how often would it prove fashionable at the office or in the classroom? The probabilities of esoteric catastrophe are by their nature minute. Unlikely events are unlikely, and so most of us go about our business, paying little attention to the potential menace from the skies or, for that matter, from one another.

Governments face similar realities. Many threats are conceivable, but relatively few actually materialize. A holistic approach to security involves assessing risks, and then allocating finite resources to address tractable threats, making the largest improvements in protection or, conversely, the greatest increases in influence.[38] Every dollar spent on national defense must be taken from objectives such as improving education, building or repairing infrastructure, or paying down the debt. Only extremely affluent (or paranoid) populations pay the price of pursuing protection from the most exotic hazards. More to the point, protection is inevitably incomplete, and comes with its own consequences, including other forms of insecurity. The risk of attack is never zero, given that a potent defense or deterrent endangers the security of others.[39]

If violence is ecological, why do human beings not live in consummate fear? Most of us are safe because the multitudes capable of causing us harm have little interest in doing so. For the most part, violence does little that potential perpetrators view as worth their while. Humanity is protected by an invisible

---

38. The distinction between security and influence is often missed or misrepresented in policy debates. For example, although discussions often center on protecting the American people (security), much of U.S. defense spending actually purchases discretion abroad (influence).

39. On the security dilemma, see John Herz, "Idealist Internationalism and the Security Dilemma," *World Politics*, Vol. 2, No. 2 (January 1950), pp. 157–180; Robert Jervis, "Cooperation under the Security Dilemma," *World Politics*, Vol. 30, No. 2 (January 1978), pp. 167–214; Randall L. Schweller, "Neorealism's Status-Quo Bias: What Security Dilemma?" *Security Studies*, Vol. 5, No. 3 (Spring 1996), pp. 90–121; and Charles L. Glaser, "The Security Dilemma Revisited," *World Politics*, Vol. 50, No. 1 (October 1997), pp. 171–201.

shell of indifference or inefficaciousness. The stranger coming toward you on a busy city street could swing out his arm, catching you under the chin. He could be carrying an Uzi, which in a fit of rage will leave you and other passersby on the pavement in a pool of intermingling fluids. Yet, you are probably not going to die a violent death in the next minute, or at any other time. The potential for violence is both ubiquitous and seldom realized because striking out, though often possible, does little to benefit the violator. The use of force is costly, risky, and mostly unproductive. When we learn of violence, our natural inclination is to ask "why?" Like a police detective, we seek a motive. Violence requires a cause. When, on occasion, we cannot identify the logic behind a perpetrator's choice of a target, the experience is remarkable, and considerably puzzling.

Most of us are capable of seriously injuring others, but for the most part we fail to exercise our capabilities because there is no positive reason to strike. A driver behind the wheel of an automobile can cause enormous damage or loss of life, and yet pedestrians walk in front of stopped vehicles at an intersection, with little care or attention to the fact that a tap of a toe on the accelerator is all it takes to end their lives. The mere capacity to harm is just not a very good predictor of aggression, because the potential for harm is everywhere but seldom practiced. Few of us are likely to be the target of attack, and so each of us can greet the day with minimal anxiety, to say nothing of personal security, not because we are thoroughly protected, but because causing harm is usually inconvenient, unnecessary, or pointless for potential perpetrators. Attacking us (or others) serves no purpose.

The internet makes it possible to interact with people just about anywhere on the globe as easily, or even more easily, than conversing with the neighbors next door. Initial attention to the mobility of cyberspace focused on the potential for good, but convenience also overcomes barriers to conflict. The supply of targets for cyber acts of aggression is certainly huge relative to the supply of perpetrators of physical violence. Viewed in this way, it is remarkable that cyberspace has yet to become exclusively the domain of fraud, identity theft, and other acts of predation, interspersed only with pornography and the occasional Nigerian emailer looking to deposit millions in your bank account. Yet, if the internet makes it easy to reach out and touch others, it in no way makes those contacts profound. Casual attempts to undermine one's welfare abound, but it is with equal casualness that we ignore the bulk of spam or internet sites marketing lapsed software. Predation continues unabated on the world wide web, but if it is easy to reach us, contact is all the more superficial.

The bulk of internet traffic is benign. Cyberspace has not made life more

dangerous for the multitudes. There are crimes on the internet, but it is unclear whether these have increased the overall crime rate. Internet crime often substitutes for crimes that would have been committed in terrestrial space nevertheless. Perhaps even more to the point, much of internet fraud and cyber violence is intrinsically tied to the physical domain; much of the harm initiated on the internet eventually gets perpetrated in more conventional ways.

The safety from predation that mass populations achieve as a result of numbers and anonymity is denied political institutions and their representatives. Organizations and certainly countries have personnel and property that can be targeted with violence. How might this shift in the nature of the target affect the risk of cyberattack? Once again, we must inquire not about what could happen but why individuals, groups, or nations might act.

Nations and organizations can be attacked through the internet, just as they have long been attacked in physical space. The ease with which such attacks can be perpetrated is an obvious, and much discussed, phenomenon. Physical space has always been an important barrier to conflict.[40] Even today, the single best predictor of interstate conflict is contiguity.[41] Lowering the cost to transmit an attack, however, only increases its appeal if the attack is also capable of achieving the actor's desired ends. Beyond numbers and anonymity, the main factor protecting individuals is even more potent for institutions; how force will produce the desired change is often unclear. Cyberattacks can be appealing as political acts only to the degree that they affect the decisions that organizations and sovereigns make with and without cyber violence. Because understanding how cyberwar can (and cannot) influence politics is largely the same as understanding how conventional military violence acts on politics, I turn next to a brief discussion of the nature of terrestrial warfare.

War and Peace in the Internet Age

U.S. Defense Secretary Leon Panetta returned to the theme of a cyber "Pearl Harbor" more than once. In his Senate confirmation hearings, then Central

---

40. See Kenneth Boulding, *Conflict and Defense* (New York: Harper and Row, 1962) concerning the "loss of strength gradient." Halvard Buhaug and Nils Petter Gleditsch show that the relationship, though weaker in recent decades, remains in effect. See Buhaug and Gleditch, "The Death of Distance?: The Globalization of Armed Conflict," in Miles Kahler and Barbara Walter, eds., *Territoriality and Conflict in an Era of Globalization* (Cambridge: Cambridge University Press, 2006)
41. Paul R. Hensel, "Territory: Theory and Evidence on Geography and Conflict," in John A. Vasquez, ed., *What Do We Know About War?* (New York: Rowman and Littlefield, 2000), pp. 57–84; and Paul Senese, "Territory, Contiguity, and International Conflict: Assessing a New Joint Explanation," *American Journal of Political Science*, Vol. 49, No. 4 (October 2005), pp. 769–779.

Intelligence Director Panetta noted, "I have often said that there is a strong likelihood that the next Pearl Harbor that we confront could very well be a cyber attack," adding that, "This is a real possibility in today's world."[42] No event in the twentieth century has done more to realign U.S. public opinion than the Japanese attack on Pearl Harbor, which mobilized the nation psychologically for entry into World War II. The analogy may be apt, but almost certainly not for the reasons contemplated by Secretary Panetta. The situation in 1941 serves as a basis for comparison and a point of departure in examining cyberwar. To understand why a cyber Pearl Harbor is not as threatening as it sounds, it helps to review what the air raids on December 7, 1941, were meant to accomplish and what they achieved.

Before exploring Secretary Panetta's Pearl Harbor analogy, however, I first discuss the nature of war and how key attributes of warfare function or fail via the internet. States and nonstate actors make war to further their interests when incompatibilities exist between those interests, and when alternative methods of conflict resolution are deemed ineffective or inefficient. Although many conflicts are conceivable, most potential wars do not occur because the participants recognize that threats or uses of force are futile. Only some acts of violence are likely to achieve the objectives for which political actors strive. If the futility of violence discourages the bulk of terrestrial conflict, it is an even larger concern in cyberwar.

A BRIEF LOOK AT THE LOGIC OF WAR

The theory of war provides two basic mechanisms for the expression of political interests through physical violence. First, force can be used to punish or compel, indirectly affecting the state of the world by harming an enemy to make it do something that it would not do otherwise, or alternately discouraging change by raising the price of aggression. Just about everyone from parents to police and prime ministers seems to grasp the intuition behind creating consequences to modify behavior. Second, force can be used to conquer, directly imposing one's will by capturing and controlling inhabitants or resources contained in a given physical space. One thing that the recent "Occupy" movement shared with the U.S. military was the conviction that denial can prove effective if exercised for a sufficient period of time.[43] The ability to conquer or

42. U.S. Senate Committee on Armed Services Hearing to Consider the Nomination of Hon. Leon E. Panetta to be Secretary of Defense, June 9, 2011, Washington, D.C., http://www.armed-services.senate.gov/Transcripts/2011/06%20June/11-47%20-%206-9-11.pdf, p. 25.

43. The whole question of denial/conquest depends on whether a target is likely to acquiesce. The British have occupied Scotland for centuries, with some success. They occupied Ireland for just

compel can, in turn, be used to achieve these objectives through actual force (offense or defense), overt threats (deterrence or compellence), or the shadow of war (e.g., diplomacy).[44]

During the Cold War, the two superpowers could easily have annihilated each other, along with much of the rest of the world. Yet, vast nuclear arsenals remained dormant, and the prospect of mutual harm even led to the peculiar stability of mutual assured destruction. Again, the mere capacity to hurt tells us relatively little about the actual advent of violence, even though the potential in the Cold War was extraordinary and mutual assured destruction, by its nature, meant that devastation could not be prevented. Indeed, it was this mutual vulnerability that many credit with the Cold War remaining cold.[45]

In contrast, Japan kept even its own diplomats in the dark about its plans to attack U.S. bases in the Philippines and Hawaii because it could not share information about its intentions with U.S. officials without fatally weakening the effectiveness of such a plan.[46] President Richard Nixon reportedly threatened to restart the Christmas bombing campaign against Hanoi to expedite the talks for ending U.S. involvement in the Vietnam War. The threat could be made under any circumstances, but it was more credible given that Hanoi had recently been attacked and the consequences of renewed heavy bombing were also clear. Whether force is threatened or carried out depends on whether threats can be made without degrading the instruments of military advantage. Revelation of the ability to harm can prove sufficiently compelling to cause a target to make concessions or to alter the target's behavior. Conversely, if threatening an enemy makes an eventual attack less effective, then the temptation may be to strike rather than threaten.

Experts on cyber security have failed to draw the same conclusions from the inability to protect that strategists drew from the Cold War. It is true that mutual assured destruction may not exist in cyberspace, as it did in the post–World War II terrestrial world. Whether the internet is a different kind of strategic setting, and what this means in terms of what can and cannot be

---

about the same length of time with very little lasting political effect. Perhaps days or decades are unlikely to succeed when centuries often prove insufficient.

44. Geoffrey Blainey, *The Causes of War* (New York: Free Press, 1973); and James D. Fearon, "Rationalist Explanations for War," *International Organization*, Vol. 49, No. 3 (Summer 1995), pp. 379–414.

45. John J. Mearsheimer, *Conventional Deterrence*, (Ithaca, N.Y.: Cornell University Press, 1983); and Kenneth N. Waltz, "Nuclear Myths and Political Realities," *American Political Science Review*, Vol. 84, No. 3 (September 1990), pp. 731–745.

46. Branislav Slantchev, "Feigning Weakness," *International Organization*, Vol. 64, No. 3 (Summer 2010), pp. 357–388. and Erik Gartzke, "Globalization, Economic Development, and Territorial Conflict," in Miles Kahler and Barbara Walter, eds., *Territoriality and Conflict in an Era of Globalization* (Cambridge: Cambridge University Press, 2006), pp. 156–186.

accomplished—offensively or defensively—remains to be shown. Although the Cold War is remembered as the ideal deterrence environment, strategic thinkers and government officials struggled with how they could exercise influence in such a world. The mere potential for imposing harm did not imply that harm would be imposed, or even that, when imposed or threatened, nations would respond in an obliging manner. Few could doubt in retrospect that citizens and leaders on both sides of the iron curtain felt vulnerable, especially during the first decade or so of the nuclear era. It does not follow, however, that a heightened sense of insecurity was reflected in actual behavioral conflict. Whether warfare in cyberspace will depart radically from previous patterns, or will mimic, in part or in whole, familiar patterns of conflict from earlier eras, will depend on the degree to which the strategic logic of cyberwar is able to accommodate the objectives of political actors in contemplating or exercising coercion.

Nor do students of cyberwar seem much preoccupied with the implications of Nixon's Hanoi bombing campaign. The threatened use of force is intended in this, and in most other instances, to alter behavior through the prospect of long-term damage. To the degree that damage can be quickly and easily repaired, there is not much leverage in raising such a threat. Conversely, details harmful to attackers or to the effectiveness or potency of attacks are typically concealed from an opponent, even when this information would significantly increase the credibility of coercive threats. Flight plans, bomb loads, and electronic countermeasures used by U.S. B-52s, for example, were not shared with Hanoi, because this would have compromised the capacity of U.S. forces to carry out Nixon's threat.

Nations, groups, or individuals with the ability to inflict harm must ask not just how much can be inflicted at what cost, but also what is to be achieved through force, and whether these ends are justified compared to the price and availability of other, typically cheaper, mechanisms. Force, or the threat of force, is useful as punishment to the degree that the harm imposed is substantial and durable. Damage that can be quickly or easily undone will not do much to deter or compel, but it will alert an enemy to vulnerabilities in its defenses, and certainly also antagonize an opponent, increasing the risk of counterattack and general hostility. The threat or exercise of physical conquest can be effective provided the perpetrator finds it worthwhile to engage in the costliest form of politics. Here, again, the simple ability to act aggressively is not itself sufficient to predict aggression. The United States could probably conquer Canada if it chose to, and yet Canada remains free and independent. Most states, groups, and individuals persist in peace because they can conceive of

no benefit from force, even if violence, and victory, are feasible. The mere ability to cause harm over the internet does not suffice to predict that cyberwar will substitute for terrestrial conflict, or even that it will be an important independent domain for the future of warfare.

WARFARE IN CYBERSPACE

Beyond questions of means and motive, two basic features make cyberwarfare different from other types of conflict. First, much of the damage contemplated by cyberwar is in all likelihood temporary. The assumption among many cyber pessimists that the potential for creating harm is sufficient to make cyberspace a suitable substitute for, or indeed alternative to, terrestrial conflict is incorrect. Shutting down power grids, closing airports, or derailing communication could be tremendously costly, but most damage of this type will be fixed quickly and at comparatively modest investment of tangible resources. Regardless, damage of this type is sunk. Losses experienced over a given interval cannot be recovered whatever one's reactions and so should not have much direct impact on subsequent policy behavior. Harm inflicted over the internet or any other medium will matter politically when it alters the subsequent balance of power, or when it indicates enemy capabilities that must be taken into account in future plans. Because cyberwar does not involve bombing cities or devastating armored columns, the damage inflicted will have a short-term impact on its targets.[47] To accomplish politically meaningful objectives, cyberattacks must contribute to other aspects of a more conventional war effort. And to affect the long-term balance of power, for instance, cyberwar must be joined to other, more traditional, forms of war.

Temporary damage can be useful under two circumstances. First, compromising or incapacitating networks might give an enemy valuable tactical, or even strategic, advantages. An opponent that cannot shoot, move, resupply, or communicate will be easier to defeat. Nonetheless, the advantaged party must still act through some medium of combat to seize the initiative. Notions that cyberattacks will themselves prove pivotal in future war are reminiscent of World War I artillery barrages that cleared enemy trenches but still required the infantry and other arms to achieve a breakout. Whether an actor can benefit from cyberwar depends almost entirely on whether the actor is able to

47. In the 1970s, the so-called neutron bomb promised high casualties with minimal damage to physical structures. It might be tempting to think of cyberweapons as anti-neutron bombs, because they damage infrastructure, leaving people largely unharmed. Yet, this is also a key limitation of cyberwar, as damage is temporary and far from complete.

combine a cyberattack with some other method—typically kinetic warfare—that can convert temporary advantages achieved over the internet into a lasting effect. In the parlance of war, internet attacks produce a "soft kill" that is valuable only when attackers prosecute follow-on attacks with traditional military force or permanently weaken an enemy in some other way.[48]

The notion of a devastating surprise attack is a particularly baroque aspect of cyberwar paranoia, and is certainly frightening to the degree that such scenarios are accurate. Yet, the idea of a surprise internet attack is misleading and relies on a fundamental misconception of the role of internet-based aggression. Modern warfare seldom allows any one element of combat to prove pivotal. Instead, it is the ability to combine elements into a complex whole that increasingly distinguishes the adept utilization of force.[49]

The archetype of modern, combined arms warfare is the blitzkrieg, where the lethality and decisiveness of conventional military violence is enhanced by actions designed to disrupt the enemy's military and civilian infrastructure. An important element of blitzkrieg was the use of terror weapons, such as the Ju 87 "Stuka" dive bomber, to sow panic, causing enemy populations to flood roads and railways, thereby crippling transportation grids needed by the defense. Yet, fear is temporary and in the absence of substance, subsides. The Stukas were effective only as long as Germany held other military advantages over its enemies. Similarly, unless Stuka attacks were accompanied by a ground attack or an invasion, their role as terror weapons was largely redundant. Stukas contributed little to Germany's effort to subdue Great Britain, for example. Stuka units experienced heavy casualties when engaged against a sophisticated air defense and were eventually removed from service in the Battle of Britain. The hubris of Luftwaffe Commander in Chief Hermann Göring in promising victory while exploiting just one domain (the air) was precisely that he exaggerated the effectiveness of a new technology in isolation from other elements of an integrated offense.

There is no reason to believe that cyberwar will be any more useful as an isolated instrument of coercive foreign policy. An attack that causes temporary harm will inevitably be followed by countermeasures and heightened vigilance, as has happened, for example, in Estonia in the aftermath of the 2007 attacks. For cyber aggression to have lasting effects, a virtual attack must be

48. Nonlethal weapons have similar functionality. Immobilizing an enemy with sticky foam works until it does not; nonlethal weapons are effective only if they are followed up by other actions, such as physical restraint or redeployment of forces away from the immediate area.
49. Stephen Biddle, *Military Power: Explaining Victory and Defeat in Modern Battle* (Princeton, N.J.: Princeton University Press, 2004).

combined with physical intervention. Knocking out communications or power infrastructure could cause tremendous disruption, but the ability to quickly recover from such attacks implies that the consequences for the balance of national power would be negligible. The need to follow virtual force with physical force to achieve lasting political consequences suggests that the application of cyberwarfare independent of conventional forms of warfare will be of tertiary importance in strategic and grand strategic terms. If one cannot foresee circumstances where the terrestrial use of force is plausible independent of cyberwar, then cyberwar is also unlikely to constitute a fundamental threat.

A second element of the logic of cyberwar has to do with influence. Rather than attacking directly, an actor can use the potential to harm (deterrence or compellence). The ability to shut down the U.S. energy grid, say, might be used to compel U.S. officials to refrain from aggressive policies or actions, or to persuade the United States to make diplomatic concessions. Yet, the problem with the standard deterrence or compellence logic in the context of potential cyberattacks, as I have already pointed out, is that revealing a given set of cybercapabilities heavily degrades their usefulness. Deterrence and compellence are therefore marginal as "pure" actions in cyberspace. Indeed, concerns that nations will not be able to deter cyber aggression amount to recognition that neither will cyber threats prove very effective as threats or inducements. Again, actions in cyberspace can be combined with initiatives in physical space, but this just reinforces the fact that, rather than a distinct form of conflict, cyberwar is basically tied to conventional forms of warfare.

Imagine for a moment that a foreign power has hacked into the communications systems of the United States or another major Western power. Imagine further that this foreign power can disable cellular phone systems or military radio networks more or less at will. The foreign power could threaten its target with this capability, but obviously the leadership of the target state must be skeptical of such a threat, because the foreign power could easily be bluffing. Proof of the capacity to damage the target nation is needed, but such evidence would, in turn, jeopardize the potency or effectiveness of the cyberattack, allowing the target to address some or all of its vulnerabilities or adopt to countermeasures.

Contrast this scenario with the revelation in the 1990s that the United States had developed radar-evading "stealth" aircraft. Knowledge by foreign powers that a confrontation with the United States would necessarily involve the risk of attack by stealthy fighters and bombers in no significant way lessened the military effectiveness of these weapons systems, given that countermeasures to stealth technology have been slow to develop. Stealth technology thus

serves as an excellent deterrent/compellent, because it can be used to coerce an opponent without sacrificing much of its military value. The "perishable" nature of capabilities in cyberwar means that advantages generally yield time-bound deterrent or compellent threats, and thus create little in the way of leverage for states that have, or plan to invest in, cyberwar assets. Deterrent/compellent threats work best when they are tied to capabilities that are not much affected by enemy knowledge of the capabilities, whereas the opposite is true for capabilities that are compromised by the revelation of forces, technologies, or attack plans.

Offensive cyber advantages are thus "use and lose" capabilities. Revealing the capacity to harm via the internet typically also means tipping the enemy off to vulnerabilities that can be remedied or compensated for, while inflicting harm seldom has a durable effect on the balance of power. "Use and lose" capabilities cannot compel or deter, because convincing evidence of the capacity to inflict harm is itself useful information in nullifying the threat. If instead cyberwar is waged rather than threatened, then the temporary nature of cyber harm dictates that an enemy follow internet attacks with more kinetic action. Otherwise, the use of cyber force is punitive, even provocative. As such, cyberwar remains adjunct to terrestrial force unless some way is found for cyberattacks to permanently alter the balance of power.

The Myth of a Cyber Pearl Harbor

The air strikes on December 7, 1941, against U.S. military instillations in Hawaii and in the Philippines were an important tactical and even strategic victory for Japan. Yet, the attacks, as is now widely understood, were a prodigious failure in grand strategic terms, setting up a nearly inexorable path to Japanese defeat and surrender.[50] Officials on both sides recognized this almost immediately. When informed of the attack, Adm. Isoroku Yamamoto is said to have offered this stark commentary, "I fear all we have done is to awaken a sleeping giant and fill him with a terrible resolve."[51] Leaders in Washington could not be bothered even to give war in the Pacific first priority, focusing the might of the nation instead on war in Europe.

The Japanese decision to strike at the United States was a calculated gamble, balancing the imperatives of seasonal weather patterns and the impending de-

50. "From a strategic point of view, Pearl Harbor was one of the most spectacular miscalculations in history." Ian W. Toll, "A Reluctant Enemy," *New York Times*, December 7, 2011.
51. Documentary evidence for the famous quotation is not available. Although widely referenced, it may be apocryphal. It certainly summarizes Yamamoto's views, however.

cline in power projection capabilities for the resource-starved empire with the realization that much was being staked on a complex plan linking the conquest of oil fields in Southeast Asia with a temporary shift in the regional balance of power in the Pacific.[52] With almost no indigenous sources of iron, rubber, and especially oil, Japan was dependent on foreign-held reserves to feed its factories and allow it to sustain its occupation of Manchuria and war in China. The U.S. embargo led Japanese officials to consider stark alternatives. Either Japan must relent and withdraw its forces from East Asia, or it would have to capture oil-rich regions in the south. This, in turn, put Japan in direct conflict with the United States. The Japanese plan was to blunt U.S. naval and military capabilities temporarily, long enough to prepare a defense in depth in the western Pacific and present the United States with a fait accompli, one that would compel the Americans to submit to a compromise, a negotiated settlement that would end the war.

The prospect of an impending and significant relative decline in power and optimism about the potential benefits of a "bounce" giving Japan a temporary advantage in the region were critical elements of Japan's decision to go to war. Importantly, Japan underestimated the psychological impact that the Pearl Harbor raid would have in mobilizing U.S. public opinion. Japanese commanders also overestimated the damage they could inflict on U.S. forces.[53] The surprise assault famously failed to catch the U.S. aircraft carriers in port. It was this inability to impair U.S. naval airpower that seemed to vex Yamamoto the most. Even allowing for Japanese optimism and error, however, Tokyo was reluctant to act against the United States prior to the end of 1940, when events in Europe laid bare Dutch holdings in Asia and dramatically weakened the ability of British forces in the region to resist.

Tactical or strategic surprise is useful as a temporary force multiplier; an attack such as that on U.S. and European forces in December 1941 could shift the balance of power in Japan's favor for a time, but the real value of a surprise attack is what it allows an assailant to accomplish subsequently. An attacker can exploit the effect of surprise to prepare a more effective defense or, alternately,

---

52. Louis Morton, "Japan's Decision for War," in Kent Roberts Greenfield, ed., *Command Decisions* (Washington, D.C.: Center of Military History, Department of the Army, 2000).

53. Evidence of this is reflected in subsequent efforts by the Imperial Japanese Navy to realize the original strategic objective. Midway, in particular, was an elaborate trap, masterminded by Yamamoto, to locate and destroy the remaining U.S. carrier force in the Pacific. See, for example, Gordon W. Prange, *Miracle at Midway* (New York: Penguin, 1983); Jonathan Parshall and Anthony Tully, *Shattered Sword: The Untold Story of the Battle of Midway* (Herndon, Va.: Potomac, 2007); Mitsuo Fuchida, *Midway: The Battle That Doomed Japan* (New York: Ballantine, 1986); and Craig L. Symonds, *The Battle of Midway* (New York: Oxford University Press, 2011).

to prosecute additional offensive action against the target or others. By itself, a surprise attack has limited utility, precisely because surprise fades in time.

Japanese war planners anticipated the temporal nature of advantages gleaned from the Pearl Harbor attack. It was hoped that Japan would be able to secure critical resources in the south, fortify its gains in depth, and wait out the American onslaught.[54] At no time did Japan seriously consider unlimited war with the United States. Indeed, Japanese planners recognized the impossibility of directly defeating the United States.[55] In the months after December 7, the United States mainland was open to attack. Japanese forces landed in the Aleutian Islands, and Japanese submarines shelled a few isolated coastal communities, but there were never any serious plans to carry the war to the continental United States.[56]

Now suppose that Japanese officials recognized from the outset that they would not be able to target the U.S. carriers or other U.S. military assets with permanent destruction. Instead, imagine (not very plausibly) that Japanese dive bombers and torpedo planes were fitted with special "delay bombs" that, unlike delay fuses, would simply disable a ship for hours, days, or possibly weeks, rather than permanently, or at least for months or years. Faced with this altered reality, Japanese officials and military planners would have been forced to contemplate a very different war, one that they would almost certainly have preferred not to initiate. In effect, Japan would have had to choose to precipitate total war, as surprise attacks themselves would not do much to diminish or delay a military response from the United States. The only value one could anticipate from a surprise attack, then, would be if it facilitated a follow-up invasion of the U.S. mainland. This is the basic shortcoming of cyberwar. Because cyberattacks involve temporary "soft kills" of a target's military capabilities and civilian infrastructure, the point of the attack is largely nullified if an attacker cannot reasonably be expected to accompany internet aggression with terrestrial strikes designed to make permanent short-term damage to a target's security capabilities.

No foreign military force is capable of subduing the United States, now or in

54. Louis Morton writes, "Japan planned to fight a war of limited objectives and, having gained what it wanted, expected to negotiate for a favorable settlement." Morton, "Japan's Decision for War," p. 110.

55. Admiral Yamamoto's other famous quotation, which was meant as an ironic reference to total war with the United States, claims, "To make victory certain, we would have to march into Washington and dictate the terms of peace in the White House." The private letter from Yamamoto to Ryoichi Sasakawa is quoted in Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: McGraw-Hill, 1981), p. 11.

56. The invasion of the Aleutians was a feint to distract attention from the attack on Midway.

the foreseeable future, with or without the assistance of a phenomenally successful coordinated cyberattack. If cyberwar is unlikely to allow a foreign power to permanently overtake U.S. or allied capabilities, and if temporary damage is useful only when practiced in conjunction with more conventional military operations, then an opponent must plan and evaluate its use of cyberwar in relation to its complementarity to terrestrial combat, not as a fully independent method of force. If instead a cyberattack is carried out in which conventional force is either ineffective or not contemplated, then an attack of this kind fails to serve a meaningful grand strategic purpose, degrading neither the target's longer-term capabilities nor its resolve.

Unless cyberwar can substitute for a physical surprise attack, there is no reason to believe that it will be used in place of conventional modes of warfare. Nor is it clear why an attacker would choose to strike over the internet, unless a conventional surprise attack is also planned and when it is expected that the combination of cyber and terrestrial aggression will yield a decisive advantage to the attacker. If it is difficult to imagine a particular nation being attacked by traditional methods of warfare, even with the benefit of surprise, then it is hard to see how that nation might be fundamentally threatened by warfare conducted over the internet. Indeed, the connection between internet aggression and traditional forms of military force imply an unfashionable prediction: cyberwar should be particularly appealing to capable states confronting weaker opponents. Rather than threatening to overturn the existing world order, cyberwar may perpetuate or even increase current military inequality.

Additional Implications of Cyberwar

If cyberwar functions not as an independent domain, but as part of a broader, coordinated military action, then the conventional military balance is the best indicator of where the most important threats exist in cyberspace. Thus, unless someone believes that economically and militarily advanced nations are in danger of physical attack from a foreign power, the threat of cyberattack cannot be treated as particularly serious in political terms. Most experts view an attack that subdues U.S. military capabilities and subjects the U.S. mainland to a foreign power as remote, even fanciful, for example. To the degree that powerful states are immune to conventional attack, cyberattacks are at most a nuisance and not a fundamental threat.

Ironically, the greatest threat posed by cyberwar may be to those states and actors that are thought to be insulated, the same actors that are currently vulnerable to conventional terrestrial aggression. Cyberwar is not a revolution in

military affairs in strategic (military) terms, nor is cyberwar likely to prove revolutionary in political terms, by threatening or transforming existing global or regional power structures. In this sense, cyberwar appears to be reactionary, reinforcing the advantages of states that already possess significant terrestrial military advantages. The need to prosecute cyberattacks with more kinetic forms of force, and the perishability of cybercapabilities in the face of revelation, mean that nations with capable militaries are best equipped to exploit the type of damage that cyberwar inflicts, even as they are better able to credibly threaten cyberattacks and to "reveal and replace" a given capability to target an enemy's cyber vulnerabilities. This new mode of warfare, most feared by technologically advanced states, may pose greater grand-strategic challenges to the technologically backward or weak, something that has not been considered previously.

This is not to say that the sophisticated computer-dependent nations of the West are immune to attack. The United States and other advanced countries are certainly vulnerable to internet aggression. Instead, the consequences of this harm will prove ineffectual, because the ability to alter the balance of power in regional or world affairs or to exploit capabilities is present only for those nations and interests that already possess considerable international influence. We would all like to live in a world where no one could harm us even if someone fervently wished to do so. To the degree that this is not possible, a useful second best is for others to possess disincentives to inflict injury or death, even if they still can. An inability to exploit temporary opportunities created by cyberwar is a disincentive to conduct concerted internet attacks. In contrast, powerful nations continue to possess both the ability and interest in intervening in the developing world, even if they do so only episodically.

Existing examples of cyberwar illustrate and reinforce this counterintuitive conclusion. Attacks on Estonian websites, which appear to have originated in Russia, pitted a tiny nation against a considerable military and economic power. The ability of Russian leaders to exploit effects of the attack, not just on the internet but through military and diplomatic pressure, ensured that the impact was much more potent than if equivalent attacks were carried out against Russia by nonaligned hackers. Similarly, the Stuxnet worm, which was apparently designed and unleashed by the United States or Israel, was more effective because of the U.S. advantage in conventional and nuclear military capabilities. The dynamic would have been far different if instead Iran had been able to counter the Stuxnet attack with aggressive military action.[57]

57. For a discussion of the politics and technology behind Stuxnet, see Jon Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol. 22, No. 3 (August 2013), pp. 365–404.

The Russian invasion of Georgia/South Ossetia is perhaps the clearest example of the kind of combined terrestrial-cyber conflict conceived of here. As one commentator described it, "This appears to be the first case in history of a coordinated cyberspace domain attack synchronized with major combat actions in the other warfighting domains (consisting of Land, Air, Sea, and Space)."[58] Because they allow for exploitation of the temporary effects of surprise and asymmetry highlighted in other studies of internet warfare, cyberattacks will be most efficacious when the conventional military balance already favors an attacker.[59]

An open question exists in any crisis about how far competitors are willing to escalate, but an ability to counter cyberattack with other, more kinetic forms of military violence serves alternately to deter or to facilitate the use of cybercapabilities, giving those nations with terrestrial military power yet another option that, even if available to their opponents, may prove extraordinarily dangerous to practice. As we see today with U.S. drone attacks and Special Operations raids on foreign sovereign territory, the power to do much more ensures that an opponent maintains a level of discretion in its response to provocation. Few can doubt the reaction of the United States, for example, if Pakistan attempted to mount a commando raid in suburban Baltimore, say, to assassinate a local resident. Nations that can physically punish others for transgressions in any domain, electronic or otherwise, are better able to operate in all domains. Once one distinguishes between simple vulnerability and actual threats, terrestrial capabilities become pivotal in determining who exercises cyberwar.

Even if cyberattacks are available to weaker actors, their effectiveness will be stymied where these actors lack the ability to prosecute advantages generated by cyberwar, and where weakness in more traditional modes of diplomatic, economic, or military competition ensure that these actors are exposed to countermeasures. The intractable nature of vulnerabilities ensures that cyberwar will not fundamentally transform either war or world affairs. Despite a dependence on high technology, developed countries will find that they can better exercise cyberwar as a political tool. Attacks against prosperous Western powers, if well publicized and the source of considerable anxiety, will turn out to be less consequential. While other technological or social changes

58. David M. Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, Vol. 6 (January 2011), p. 2.

59. For skepticism about the coercive effect of cyberpower, see John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly*, Vol. 5, No. 2 (Summer 2011), pp. 95–112. Sheldon's perspective relies on induction from recent cases, rather than on a theory of the role of cybewar as part of a modern integrated military.

may well transform contemporary hierarchies, cyberwar will most likely function more to perpetuate than to undermine existing inequalities of influence.

THE ADJUNCT ROLE OF CYBERWAR

Because war on the internet is adjunct to more conventional forms of fighting, a cyberattack is extremely unlikely to prove pivotal in conflicts involving capable states or their partners. Still, cyberwar could be used by and against forces in the field, a valid and possibly important concern. A common approach to evaluating the implications of new technologies for war and peace involves the offense-defense balance. Proponents of offense-defense theory focus on material or, alternately, on cognitive/informational factors that they believe will lead to increased military aggression.[60] Nations or time periods that experience or perceive offensive advantages will be associated with more war, whereas the opposite is said to happen when innovations or circumstances favor the defense. There is considerable skepticism about the empirical validity of offense-defense theory, as well as about the ability of researchers to isolate the factors leading to offense or defense dominance.[61] Even if there were nothing controversial in the application of offense-defense theory, it would still be challenging to draw conclusions about the impact of cyberwar on the general appeal of warfare, given that cyberwar is new, and given that cybercapabilities are not the only factors influencing the offense-defense balance. In evaluating the impact of cyberwar, it would be valuable, however, to know whether the internet systematically favors attackers or defenders.

Robert Jervis proposed a framework for understanding technology-induced instability that seems well suited to explaining the externalities of cyberwar for

60. For perspectives and coverage of the debate concerning offense-defense theory, see George H. Quester, *Offense and Defense in the International System* (New York: John Wiley and Sons, 1977); Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca, N.Y.: Cornell University Press, 1984); Ted Hopf, "Polarity, the Offense-Defense Balance, and War," *American Political Science Review*, Vol. 85, No. 2 (June 1991), pp. 475–494; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security*, Vol. 22, No. 4 (Spring 1998), pp. 5–43; Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security*, Vol. 22, No. 4 (Spring 1998), pp. 44–82; and Karen Ruth Adams, "Attack and Conquer?: International Anarchy and the Offense-Defense-Deterrence Balance," *International Security*, Vol. 28, No. 3 (Winter 2003), pp. 45–83.

61. For several different criticisms of offense-defense theory, see Jack S. Levy, "The Offense/Defense Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly*, Vol. 28, No. 2 (June 1984), pp. 219–238; Jonathan Shimshoni, "Technology, Military Advantage, and World War I: A Case for Military Entrepreneurship," *International Security*, Vol. 15, No. 3 (Winter 1991), pp. 187–215; and Yoav Gortzak, Yoram Z. Haftel, and Kevin Sweeney, "Offense-Defense Theory: An Empirical Assessment," *Journal of Conflict Resolution*, Vol. 49, No. 1 (February 2005), pp. 67–89. For a rebuttal of some of these critiques, see Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies*, Vol. 4, No. 4 (Summer 1995), pp. 660–691.

the broader question of conflict among states.[62] As James Fearon makes clear, however, offense-defense theory also needs to distinguish between advantages gleaned from initiating disputes and those from acting aggressively, should war occur.[63] Fearon further notes a more general tendency to confuse the shifting offense-defense balance with changes in the balance of power. Offense dominance implies that states are more likely to prefer attack rather than defense regardless of the prevailing balance of forces. Weaker states seldom prevail under any circumstances.

Imagine first that cyberwar is defense dominant. This does not seem all that likely, and in fact contradicts the prevailing view in the literature. Still, suppose that information infrastructures are more readily defended than attacked. In such as world, the balance of power would favor those states that could most effectively orchestrate military command, communications, logistics, and intelligence through the internet or similar types of networks. Even if this imagined cyber world is defense dominant, it does not follow that terrestrial conflict is also defense dominant. The relative immunity of networks to attack could lead to a reluctance to use conventional force, or it could increase incentives to act aggressively, depending on whether secure networks are more important for defenders or attackers. The standard military answer is that command and control are more critical for the offense, as commanders have more need to directly control their forces in the attack. If so, then perhaps cyber defense dominance is actually destabilizing, because it increases the ability to attack and (slightly) decreases the ability of defenders to prevail. Conversely, if, as many contend, cyberspace is offense dominant, then this should tend to weaken offensive operations in the physical world, making terrestrial conflict more defense dominant.[64]

This basic conception assumes dichotomous conditions of network vulnerability that do not reflect actual wartime dynamism. It may take time to disable networks. If so, then there is a first-mover advantage that could prove more critical than the defense dominance created by the heightened need among attacking forces for effective command, control, communications, computers, and intelligence. Advantages may follow from starting early in cyberwar. Striking first could also prove valuable if disabling an opponent's internet reduces the enemy's ability to retaliate. Given that a state projecting

62. Jervis, "Cooperation under the Security Dilemma."
63. James D. Fearon, "The Offense-Defense Balance and War since 1945," typescript, University of Chicago.
64. I am grateful to Eugene Gholz for raising the issue of offense/defense cyber dominance.

power benefits from being able to choose the time and place of its attack, the first-strike advantage might be more important for victory than the pacifying effect produced by offense dominance in cyberspace.

Regardless of whether the internet increases or decreases incentives to attack, cyberwar is likely to continue to favor the strong against the weak. This is not to say that cyberattacks will not have an effect, only that they are extremely unlikely to be strategically decisive. A capability to address cyber threats is useful, but planning for cyberwarfare must occur within the larger framework of recognition that this new domain is evolutionary rather than revolutionary. There will not be a cyber Pearl Harbor, except possibly when and if a foreign power has decided it can stand toe-to-toe with conventional U.S. military power.

CYBERTERRORISM

The terrorist attacks of September 11, 2001, generated a sense of insecurity in the Western world: How can governments protect their citizens in an age where the enemy is concealed and where an attack may come at any time or place? The temptation has been both to treat terrorism as an existential threat (because it is frightening) and to assume that the best response is a vigorous defense. Yet, as I have argued, one of the most effective mechanisms of protection is not to remove capabilities, but to puncture resolve, foremost by ensuring adversaries that their objectives will not be realized. A vault does less to deter bank robbers than the presence of countermeasures (die packs, numbered bills) that deny criminals the fruit of their plunder, even when they successfully complete the crime. Terrorism is a marginal business, not because airports and diplomats are too well protected or because guns or bombs are hard to come by, but because most people, even if very unhappy, do not believe that bombings, hijackings, or assassinations will effect positive change. Incapable of achieving their objectives directly, terrorists seek to mobilize fear and to cause overreaction, mechanisms that mobilize the targets of terror to assist in accomplishing terrorist objectives.

The resort to cyberwar by terrorists does not imply that cyberterrorism is an important threat to national security, any more than the appeal of the lottery to the poor or financially desperate implies that the odds of winning are inversely tied to one's income. Desperation leads to desperate measures, an indication in fact that such measures probably will not succeed. In this sense, the rise of cyberterrorism may say more about rigidity and impotence between agent and structure than about either in isolation. Cyberterrorism may be relatively ineffective, not unlike terrorism generally. Nevertheless, terrorists may

adopt cyberwar even though internet attacks are unlikely to sway national policies or public opinion. The adoption of a particular method of attack by terrorists does not mean that their actions represent a critical threat, any more than crime and corruption are considered issues of national security. Most societies treat the latter activities as distinct from national security, not because they are not important or fail to harm people, but because they do not directly threaten the state. Unless attackers have the ability to prosecute temporary advantages through physical force, it is not clear whether cyberterrorism requires an elaborate or concerted national security response.

Terrorism is a form of compellence. Lacking the ability to impose their will on others, terrorists rely on the prospect of harm to influence a target's behavior. Indeed, because their ability to harm is limited, the terrorist relies on psychology (fear and uncertainty) to multiply the impact of relatively finite capabilities on opposing populations or states. Cyberwar is arguably especially poorly suited to the task of fomenting terror. In particular, in addition to the problems in credibly threatening cyberattacks that have already been discussed, it is difficult to see how internet attacks will be able to instill the quality of fear needed to magnify the terrorist's actions. How terrifying is a cyberattack? No one will be happy when the power goes out or when one's bank account is locked down, but attacks of this type evoke feelings of anger, frustration, even resignation, not terror. Terrorism relies on generating a particularly visceral emotion (the "terror" in terrorist), one not likely to be effected through the actions of cyberwarriors, at least not directly. The old journalistic adage that "if it bleeds, it leads" implies the need for graphic trauma and lurid imagery. The very attributes that make cyberwar appealing in the abstract—the sanitary nature of interaction, the lack of exposure to direct harm, and strikes from remote locations—all conspire to make cyberterrorism less than terrifying. White collar terrorists are probably not going to prove any more effective, and perhaps may prove less, at shaping hearts and minds than the traditional model.

This is even more the case with long-duration, low-intensity conflicts that are a key component of both non-Western attempts at resistance and Western efforts to protect the status quo international order. From the perspective of the insurgent, asymmetric warfare has never been about attacking to diminish an opponent's strengths, but is instead focused on maximizing one's own strengths by targeting enemy weaknesses.[65] Insurgency seeks out kinetic close

65. Mao, Zedong, *On Guerrilla Warfare* (New York: Praeger, 1961).

physical combat where sophisticated technology is at its least effective (and decisive). Damaging the technology may draw an enemy into direct contact, but it might also cause that enemy to withdraw and reschedule operations. Mobility dominates every battlefield for this very reason. Internet attacks in the midst of close contact make little sense, as it is here that the comparative advantage of cyberwar (distance and asymmetry) is least potent. The ability of internet-dependent armies to perform in superior ways on existing dimensions means that this is generally a process of leveling, not revolution.

Cyber espionage

By far the most compelling scenario for the transformation of political conflict through the internet, and the one that makes new headlines daily, involves the use of the internet for espionage. As events such as the disclosure of an enormous number of classified documents through WikiLeaks illustrates, it may become increasingly difficult for states to hide details of their capabilities and plans from individuals, groups, and other nations.

States have always sought information about prospective opponents. Successful espionage creates significant advantages, but also challenges. For most of history, spying was physical. An agent had to enter enemy territory to obtain information about the capabilities or intentions of a foreign group or power. The products of espionage were equally tangible. Spies brought back documents, captives, tallies, or other materials designed to inform their masters and demonstrate the veracity of their claims. This made spying risky. Espionage required an overt act that could itself precipitate war. Evidence of spying could form the casus belli for an attack by a target of espionage against the perpetrator. Even if it did not lead directly to a contest, where agents were found, and what they were looking for, revealed sensitive information. For these reasons, counterespionage is itself as much about spying as it is about preventing espionage. Of course, captured spies also fared poorly, as international norms offer none of the protections afforded to conventional combatants.

The internet makes it possible for the spy to telecommute.[66] Information can be collected without leaving the territory of the sponsoring state, making it difficult to deter or capture cyber spies. A spy's affiliation can also be concealed, so that the target is uncertain whether espionage indicates a prelude to war, threats from specific states, specific formal national objectives, or even whether espionage actually occurred. At the same time, cyber spies face their own challenges. Indeed, the detection of cyber spies may be easier than con-

66. Telecommuting and the paperless office are two other myths of the internet age. It is possible that telecommuting may be no more successful for spies than for anyone else.

ventional espionage, given computer forensics and the trail left when accessing files.

One of the perennial challenges for political decisionmakers in dealing with any form of espionage is what to do with the information collected. Acting on covert knowledge is tempting, but often this will also tip off the target and lead to countermeasures. Even more fundamentally, the challenge to analysts is to interpret the significance of information, not something that the internet makes easier, particularly given the quantity of materials likely to be involved. Critical facts may even be obscured among masses of trivial details, protection not unlike the anonymity provided by mass humanity that shelters most of us, something that is only possible given the mountains of information in the internet age.

Conversely, the single most dramatic impact of the cyber world on political conflict may well come in the form of transparency. Nations may find that they can no longer sustain jealously guarded secrets. The phenomenon of classification that led large portions of government activity underground may find itself "outed," not by alien spies or terrorists, but by groups devoted to the idea that airing national secrets makes it more difficult for governments to connive against one another, or to scheme against their own people.

There is considerable reason to believe that reducing secrecy will led to a decline in warfare, even if some nations are made worse off in terms of relative power. The conceit of sovereigns is that secrets can be kept indefinitely. This has never been true. Code breaking in both world wars exposed German and Japanese operational plans to exploitation by the Allied commanders. Similar results may have shadowed opponents during the Cold War. The problem of course was that espionage that unearthed enemy secrets also had to be kept secret, because there were advantages to knowing something that an enemy did not know that the opponent knew. Espionage did not reduce the prospect of war as much as it affected who was likely to win, because those in the know were able to exploit relationships and win contests. Today, nations may find it increasingly difficult to imagine that their secrets are safe, even if they are. In addition to "nonprofit" espionage that publicly discloses state secrets, the ubiquity and success of "for profit" spying in the internet age must make nations consider the possibility that security is inherently porous. Secrets are not sacrosanct, making it more difficult to carry out the conspiracies so often associated with coercive politics. War will still occur, but surprise in war will be increasingly difficult to achieve, in turn reducing at least part of the motivation behind the use of coercive military force. With fewer surprises, identifying bargains that competitors prefer to the costly exercise of war becomes easier.

Conclusion

In war, tactics must serve strategy and strategy must serve grand strategy. Students of cyberwar have yet to explain how the internet can host meaningful political conflict, precisely because it cannot serve the final arbiter function that has for millennia been the purview of physical violence. The tendency among pundits of cyberwar has been to focus on tactics and possibly strategy, showing that harm is possible without explaining how the harm generated is likely to shape the product of political differences. In the absence of this logic of consequences, the internet becomes an adjunct domain to more traditional forms of warfare. Cyberwar is an evolving dimension of war and a source of concern, but in grand strategic terms, it remains a backwater. A failure to focus on grand strategy is an all-too-familiar by-product of the war on terror, where the objective has been to harm and not be harmed, rather than to effect meaningful changes to the disposition of world affairs.

It would be absurd to infer that there is no role for the internet in twenty-first-century conflict. The internet will be affected by conflict, just as is the case with every other domain in which individuals, groups, and societies interact. Indeed, the real message for soldiers and politicians is that cyberwar involves a broadening of the dimensions of warfare, rather than a narrowing of future conflict. In most cases, the internet is not a viable, free-standing venue for the pursuit of national interests. It would be surprising if a country intent on attacking another nation failed to carry out preparatory or simultaneous attacks of target's defense capabilities via the internet. It would be even more surprising if an aggressor successfully substituted cyberwar for conventional, tangible forms of conflict. This is the conceit of Nikolai Kuryanovich, former member of the Russian Duma: "In the very near future, many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers."[67] Mr. Kuryanovich continues, "[A] small force of hackers is stronger than the multi-thousand force of the current armed forces."[68] Surely, a country with thousands of soldiers and hundreds of hackers would be inclined to use both.

By itself cyberwar can achieve neither conquest nor, in most cases, coercion. Russian military planners obviously understood this in preparing to invade

67. Cited by Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters*, Vol. 38, No. 4 (April 2009), p. 60. Korns and Kastenberg reference Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, December 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.
68. Ibid.

Georgia, not just with an army of hackers, but with tanks. Indeed, the tanks appear to have done more for Georgian insecurity than anything accomplished by information soldiers. The threat of cyberwar cannot deter or compel particularly effectively either, except possibly in the short term, and only with the consequence that an attacker will have forfeited the potential to exploit a given set of vulnerabilities in the future. Cyberwarfare will most often occur as an adjunct to conventional warfare, or as a stop-gap and largely symbolic effort to express dissatisfaction with a foreign opponent. It is best to discuss cyberwar in these contexts, not as an independent, or even alternative form of conflict, but as an extension of the logic already expressed in combined arms battle. Because in most cases cyberwar cannot achieve the objectives that have historically prompted nations to commit to tangible military violence, "cyberwar" is only warfare in the context of terrestrial forms of interstate threats or force.

Even the most successful forms of cyberwar (such as cyber espionage) do not presage much of a transformation. Just as innovations in artillery and small arms made fighting in close formation untenable, militaries, governments, and societies will adapt. It would be ludicrous to suggest to modern infantries that the massing of fires would be best achieved if they stayed in formation while on the march or in the assault. Contemporary field commanders have become comfortable with the idea that perimeters are partial or temporary, that air-land battle (and naval warfare for a longer time) necessarily involves not fronts, but mobility; not frontal attack, but maneuver. Similar concepts will pervade discussions of cyberwar. Static security is insecurity. It does not follow, however, that being vulnerable means one will be attacked, or that there is much that can be done to prevent aggression if it is initiated. Security in the modern world, terrestrial and cyber, is a function more of the motives of opponents than of the ability to attack. Nations or groups that strike through the internet in minor ways may be ubiquitous. Those that threaten critical national security goals will be rare if for no other reason than that cyberwar is not really war in grand strategic terms. In this regard, the next Pearl Harbor is much more likely to occur in Hawaii than in cyberspace.