Chapter Six

Mutual Restraint in Cyberspace

Cyberspace—shorthand for the capabilities and content of computer networking—meets the criteria for a domain in the Sino-American strategic relationship. Both the United States and China are heavily digitized and critically dependent on computer networking for their prosperity, knowledge, and security. At the same time, each is able to penetrate, foul, and crash networks on which the other side depends, and each is continuously improving its ability to do so. Against the sort of large and sophisticated attacks that both China and the United States are capable of conducting, network defense can be exceedingly costly and yet still be inadequate. Consequently, each nation is vulnerable to great harm from the other in and through cyberspace. Yet it is unrealistic to expect either to forego capabilities to attack computer networks, which go hand in hand with capabilities to defend them, and traditional negotiated arms control of such capabilities is plainly impractical.

Because this mutual vulnerability in cyberspace will only get worse, China and the United States should be interested in reciprocal restraint in at least the most damaging kinds of attacks on at least their most important networks. Rather than rely predominantly on defense, deterrence based on the threat of retaliation for network attacks could undergird restraint in cyber war and thereby improve cyber security. Thus, cyberspace could become another domain in which the United States and China together manage and reduce strategic vulnerability—despite, yet also because of, their respective offensive capabilities.

Notwithstanding such logic, the complexity of computer networks, their myriad uses, and the many ways of interfering with them could make reciprocal restraint in cyberspace markedly more difficult than in the nuclear and space domains. The notion of deterrence based on mutual restraint presupposes that it is possible to define and in turn agree on the kinds and scale of network intrusion that qualify as an attack and that could warrant retaliation. Lack of clarity and understanding about the threshold for retaliation may invite mischief, cause miscalculation, and weaken deterrence. Moreover, the possibility of the attacker concealing its

identity could militate against retaliation, the credible threat of which is key to deterrence—the bedrock for mutual restraint. Still, because China and the United States can harm one another so much by large network attacks, and because defense against such attacks is so hard, both should have an incentive to pursue the idea of mutual restraint in cyberspace.

Unlike the nuclear and space domains, cyberspace is obviously not all strategic. For instance, a large swath of bandwidth is for entertainment; while this may bring pleasure to hundreds of millions of Chinese and Americans, neither nation would be seriously hurt by its interruption.[1] In contrast, networks that enable financial, transport, commercial, communications, industrial, utility/power, and government/administrative functions, not to mention those that support intelligence and military missions, are critical for national productivity, cohesion, progress, and security. So is the Internet itself, on which many sectors and users rely for important functions. Major attacks on these precincts of cyberspace can be considered strategic; attacks on lesser ones cannot.

Having made this distinction between strategic and other networks, one wonders why either the United States or China, as states, would attack functions in the other's nonstrategic cyberspace.[2] In any case, threats to unimportant networks need not preoccupy the U.S. and Chinese governments. The two can and should concern themselves with the need for mutual restraint in strategic cyberspace, where the potential to suffer national harm is greatest, the motivation to inflict such harm strongest, and the benefit of mutual restraint clearest.[3]

While the distinction between strategic and nonstrategic networks is reasonable conceptually and also necessary for progress toward mutual strategic restraint in cyberspace, these two subdomains cannot be completely partitioned. The interconnectivity among networks—so complex that it is not entirely understood—means that an attack on unimportant networks can infect important ones (and vice versa). But this does not argue against focusing mutual restraint on strategic networks. The notion of restraining all attacks on all networks is as impractical as it is utopian, yet to abandon the goal of restraint regarding strategic networks because they are not hermetically isolated from nonstrategic ones would be to make the utopian the enemy of the good.

Thus, although the demarcation between strategic and nonstrategic cyberspace is blurred, subjective, and porous, this need not preclude deterrence and restraint where they matter most. Defining and agreeing on a precise threshold of strategic cyber attack, akin to detonating a nuclear weapon or destroying a satellite, are neither possible nor necessary. As long

as there is a *substantially* shared view of what is strategic—something a Sino-U.S. strategic dialogue could address—the lack of an exact threshold could foster more restraint, not less.

It is also important to recognize at the outset that cyberspace, unlike nuclear and space domains, is largely the realm of nonstate entities, including unfriendly ones that would attack Chinese or American strategic networks if they could. This makes determining the origin of a cyber attack and the identity of the attacker that much more difficult. Moreover, the network paths that attacks take often transit intermediate countries, especially if the attacker wishes to cover its tracks. These nonstate and transnational aspects of cyberspace make it harder to take to task countries from or through which nonstate cyber attackers may operate, compounding the difficulty of establishing deterrence and thus mutual restraint across a large family of cyber threats. Indeed, blaming attacks on rogue hackers operating from their territory is a predictable deflection for state attackers.

The presence of nonstate hackers should not and does not absolve sovereign states of responsibility to control actions originating on their soil that can harm other sovereign states.[4] A good analogy is terrorism, where a state that is recognized as sovereign over territory from which terrorists operate internationally is responsible not merely for refraining from supporting the terrorists but also for actively defusing the threat they pose. This is not to argue that it is right for governments to attempt to tightly control cyberspace and those who use it; rather, it means that governments are obligated at least to try to curb domestic activities with deleterious international effects, be they cyber or other activities. Given its authoritarian political system and intrusive state security apparatus, it should be easier for China than the United States to meet this fundamental responsibility. In any case, if either China or the United States were to claim incompetence in controlling attacks from or through their countries, the answer should be not to cede cyberspace to trans-state attackers but to cooperate against them. Rather than an insurmountable obstacle to Sino-American restraint in cyberspace, the nonstate threat could be a subject of Sino-American cooperation in cyberspace.

Even those segments of cyberspace that are strategic are fraught with complexities and ambiguities that could encumber the pursuit of mutual restraint. Keeping this in mind, this chapter looks at U.S. and Chinese vulnerabilities and capabilities in cyber war, in both civilian and military domains. It then examines the relationship between offense and defense to see if the offense dominance that characterizes the nuclear and space domains applies in cyberspace as well. Further, it considers whether and

under what conditions deterrence can actually work in cyberspace, given the uncertainties in identifying the source of an attack.

If mutual deterrence in cyberspace appears at least theoretically possible, a number of questions still need to be considered before applying it in the Sino-American case: What conduct, above what threshold, can and should be deterred? Can cyber warfare be decoupled from conventional warfare? What norms, policies, and behavior are needed to support mutual restraint in strategic cyberspace? Does cyber deterrence cover allies? Can Sino-American restraint and cooperation in cyber warfare be extended to others? These issues are tackled in the pages that follow.

Vulnerability and Capability

The United States has not suffered any major damage from attacks on segments of cyberspace that are strategic, as defined here. The Internet and other critical systems have proven resilient; users are increasingly vigilant when serious viruses, worms, and other network attack agents have appeared. Computer network protection has become a government priority.[5] Leading information technology firms are working to make their products more secure. A cyber protection industry is flourishing. The most serious penetrations of sensitive U.S. national security networks, publicly attributed to be the work of Chinese intelligence services, have been essentially espionage—unwelcome, but not debilitating or, for that matter, especially hostile, given the norms of international spying.

The absence of major cyber attacks on critical U.S. networks may mean that subtle deterrence is already working. Perhaps China has chosen not to move from computer network exploitation to computer network attack out of fear of U.S. retaliation. In any case, the Chinese evidently have not found themselves in circumstances in which the advantages of disrupting or degrading U.S. strategic networks would outweigh the risks of retaliation, political condemnation, or economic sanction. China and the United States have not had a serious confrontation since President Clinton sent two aircraft carriers into the Taiwan Strait to signal U.S. willingness to defend Taiwan. One can speculate about whether a crisis of that order today would produce a Chinese cyber attack.

Although the United States has not suffered a major cyber attack, there is evidence of the mounting danger of attacks too sophisticated to defeat, too broad to isolate, and too damaging to tolerate—attacks of the sort that well-resourced and technically capable nation-states like China, Russia, and a few others can conduct. Moreover, as noted, there may be logic to conducting such an attack on strategic U.S. computer networks, especially in the

context of a wider crisis or conflict. Aside from nuclear attack (unthinkable), homeland terrorism (unthinkable except by terrorists), and ASAT weapons (nascent), the United States presently has no other obvious strategic vulnerabilities. A growing chorus of high officials and credible strategists describes cyberspace as the soft underbelly of U.S. security.[6]

One of the factors contributing to growing concern about strategic cyber attack is the expectation of a death toll of zero. Of course, the harm from cyber war, and the main argument for mutual restraint, is chiefly in economic terms. Broadly speaking, the damage from cyber war could be on the same order as that from "violent" strategic attack. Government estimates of the impact of potential cyber attacks on the U.S. economy range from $70 billion to over $900 billion (see table 6–1).[7]

Sector	**Estimated Cost (In U.S. $Trillions)**
Electric power	0.3–0.4
Oil and gas	0.1–0.4
Telecom/Internet	0.4–0.7
Banking and finance	0.9–1.3
Water and sanitation	0.1–0.1
Chemical industries	0.3–0.6
Air transport	0.1–0.3
Ground transport	0.3–0.6
Health care	1.0–2.2
Total	**3.7–6.9**

Table 6–1. Economic Cost of Cyber Attack by Sector

An enemy, if undeterred by the threat of retaliation, might think that damage on this scale (but with no casualties) is the best way to stop U.S. intervention abroad or weaken U.S. will in a conventional conflict. Moreover, such damage can be visited at negligible cost to the attacker. Add to this the potential to disrupt U.S. military operations by attacking U.S. C^4ISR networks, and cyber attacks loom as a tempting option, given U.S. superiority in other categories of force and the possibility that the attacker's identity can be concealed.

Thus, while attacks on U.S. networks have not yet risen to the strategic level, they could.[8] For now, however, we have to rely analytically on what is publicly known about third-party strategic cyber attacks to get a

feel for motivations and effects. It is widely believed that agents of the Russian state conducted or orchestrated large-scale attacks on the computer networks of Estonia in reprisal for removal of a Soviet war memorial, and then on those of Georgia, in concert with a Russian mechanized invasion.[9] These cases serve as a reminder that although cyber threats come in all sizes and with many motivations, threats from large and technically advanced states motivated by national security interests are the most formidable, most difficult to stop, and most damaging.

While extrapolating analytically from just two cases can only be done with caution, the exercise is illuminating. Estonia is particularly advanced in its reliance on data networking; for example, banking there is done almost entirely on line. Therefore, the effects of attacks on Estonia, which were severe if temporary, provide a glimpse of the possible effects of attacks on U.S. networks. Depending on the cyber weapons used and the targets, scale, and duration of attack, critical U.S. networks and associated functions could be degraded for days or weeks. In addition to the major shock this would have on U.S. markets and production, it could shake, though not necessarily break, American resolve in a crisis. It could also have secondary and longer term economic repercussions (including on the global economy). At least a would-be attacker could reasonably expect such effects.

The alleged Russian attacks on Estonia and Georgia may be indicative in several respects. First, strategic attacks are more likely to occur in an international crisis or conflict than out of the blue. This may help to explain why the United States has not experienced its "cyber Pearl Harbor." (U.S. opponents in conflicts since the end of the Cold War—Serbia, Iraq, the Taliban—have hardly been masters of cyber war.) Also, it implies that the United States would have time to prepare itself and its networks for attack as a crisis developed, and perhaps to take preventive or preemptive action. Second, these two cases suggest that attributing an attack to a likely attacker is far from hopeless. Like counting angels on pinheads, experts point out alternative explanations for the Estonia and Georgia attacks, but the circumstantial evidence points to at least state complicity, and thus sovereign responsibility. Third, Russia was obviously not deterred, perhaps because neither Estonia nor Georgia could have inflicted very damaging retaliation. Fourth, there was no known strategic retaliation against Russian networks for the Estonia or Georgia attack, so Russia (and others) may not feel deterred from launching new attacks.

Thus, the sparse data we have on strategic cyber warfare suggest that:

- a strategic cyber attack on the United States is more likely to be in the context of an international crisis or outright conflict than a "bolt from the blue"
- the absence of an attack to date could mean only that there has been no crisis to precipitate it
- a large and sophisticated attack is most likely to come from a capable state
- circumstances, including the presumed attacker's behavior before and after an attack, could aid in identifying the source
- the attacker, though vulnerable itself, probably expected no major retaliation
- a perceived risk of U.S. retaliation could be a decisive factor in the adversary's decision to attack.

While these inferences are not definitive, they do illuminate a most likely case. A state like Russia or China with the capability to launch a strategic cyber attack against the United States is less likely to do so absent a crisis or if it expected retaliation against its strategic networks. By this reasoning, the United States should strive to present the opposite of the Estonia and Georgia circumstances to any state contemplating an attack—briefly stated, a strong prospect of retaliation more costly to the attacker than the cost of not attacking.

Closely related is the possibility of a foreign attack on networks vital to U.S. *military* preparedness and operations. Again, this would presumably be in connection with a crisis or conflict, and thus with warning. Given the overlap between military and civilian networks, such an attack could escalate to general cyber warfare involving all sorts of critical national networks. While such a path to Sino-American strategic cyber war is, by definition, no more probable than a Sino-American crisis that would precipitate it, it bears especially careful analysis because it could stand in the way of agreement on mutual restraint or else could cause such restraint to fail in a crisis.

Chinese and U.S. vulnerability in cyberspace differs because of differences in the two countries' stages of economic development, their integration into the world economy and the data networks that enable it, and their political ability to endure serious economic dislocation caused by major cyber attack. At present, China is somewhat less dependent on computer networks than the United States for critical functions and has a

somewhat more self-contained and secure communications infrastructure. Consequently, the Chinese might believe they have more to gain than to lose from resorting to cyber war.

But the Chinese are becoming more reliant on cyberspace (see figure 6–1). While this depicts only Internet users—a figure skewed by China's large population—it is also the case that China's productivity, trade and investment, competitiveness, cohesion, and national security all depend increasingly on computer networking. As a result, and to the extent the Chinese fear U.S. cyber attack, China's interest in mutual restraint should grow. Moreover, when taking into account the risk that economic reversals could cause political upheaval, China may become more sensitive than the United States to the effects of strategic cyber war.

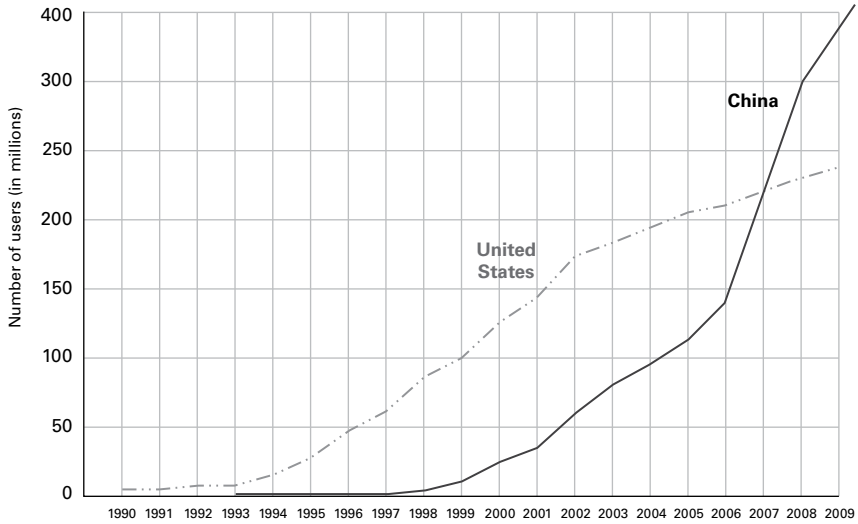

Figure 6–1. China's Internet Usage (1990–2009)

The link between Chinese economic development and dependence on computer networking is clear and strong. China's aggregate growth is tightly bound to increasingly sophisticated production of more complex goods for global markets. This has required both industrial division of labor and integration into international distribution systems in components, subassemblies, and finished goods flowing into and out of China.

Parallel payment and credit networks allow the transactions that make these markets work. This pattern, so essential for China's economic success, demands massive, rapid, uninterrupted exchange of data. Just as the expansion of Chinese affluence has spurred extraordinary growth in personal Internet use, the investment, manufacturing, trade, and financing that produce this affluence are demanding more data networking. China's growing dependence on cyberspace is both a consequence and a requirement of its economic success. With China's economy projected to overtake the U.S. economy in a decade or so, it will become at least as vulnerable to cyber war. Indeed, given the strong inhibitions against using nuclear weapons, the Chinese ought to be far more concerned about cyber security than about nuclear security.

Counterintuitively, for an authoritarian political system, Chinese use of cyberspace is at present mainly personal—80 percent of Internet use is at home—rather than industrial, commercial, or governmental.[10] This is a manifestation of rapid world-wide growth of Internet popularity and significantly rising income levels for most Chinese.[11] Data also indicate that this pattern is shifting toward a greater share of industrial and commercial use, which is to be expected given the complex production market networks that are propelling China's economic growth.[12]

The impact of even a temporary loss of critical networks on the Chinese economy could soon—if not already—be measured in percent of GDP, not unlike the U.S. impacts shown earlier. The fundamental reason for this is that the Chinese economy has grown more productive, more competitive, and larger as a result of internal and external *integration*. A highly fragmented economy has become networked, allowing vast improvements in efficiency, specialization, and optimization. In a country as large and diverse as China, economic integration is possible only with data networking. In addition, China's growing economic strength is the result of its integration in global trade and investment, the backbone of which is, again, data networking.

Although growth in Chinese industrial and commercial use has been slower than in personal use, it will accelerate as more Chinese enterprises integrate and operate throughout China, the region, and the world. Until recently, Chinese production for world markets has been largely a function of foreign direct investment and thus flowed through foreign corporate distribution systems, operations, supply chains, and financing. The data networking vital to these global business systems has been largely the responsibility of U.S., European, and Japanese multinational corporations.

This pattern has begun to change dramatically, as Chinese enterprises themselves accumulate the confidence, capital, and experience to become multinational—to globalize. This is readily seen in patterns of Chinese direct investment abroad, compared to foreign direct investment in China (see figure 6–2). As Chinese enterprises come to own, control, extend, and integrate operations, supply chains, distribution systems, market presence, and financing links, they will become more dependent on worldwide networking.[13]

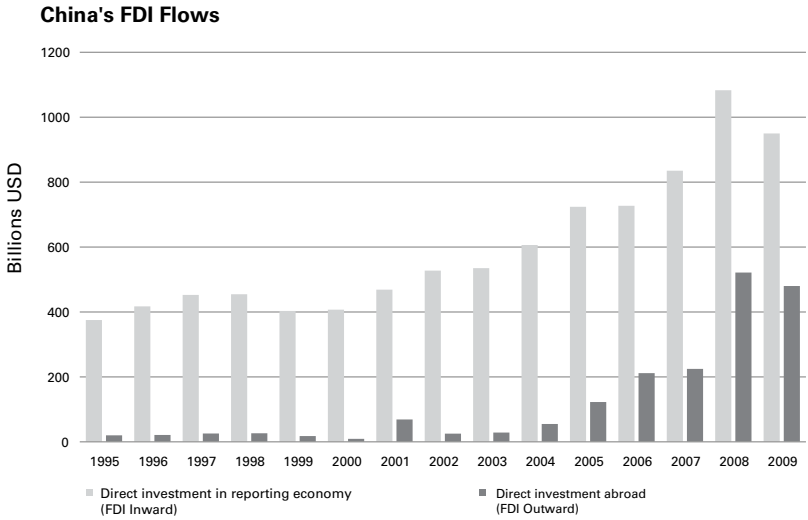

Figure 6–2. China's Foreign Direct Investment Flows

Another way to get a sense of China's reliance on data networking is to consider the importance of trade to its economy and, by extension, its political stability. China currently accounts for approximately 10 percent of total global exports, as opposed to approximately 8 percent for the United States. Trade (exports plus imports) accounts for about 40 percent of China's economy. Trade and the international commercial, financial, insurance, and logistic activities that enable it are highly communications-intensive. The implication of this is that disruption of the data that flows through business networks to and from China, even if brief, could have a large impact on Chinese trade and therefore on Chinese economic health.

China is stepping up to these dependencies by building a thick system of fiber optics and space-based communications in the region, taking a

stake in the global information infrastructure. Yet far from giving China some sort of self-contained cyberspace, the connectedness of data networks, especially those that are Internet-based, makes it increasingly vulnerable to the sort of sophisticated cyber attacks that an advanced state like the United States (or Russia) may be capable of conducting.

One would almost expect the Chinese government to have become an advocate for cyber war restraint. As it is, political and economic elites have not spoken out or made any apparent effort to muzzle PLA chatter (in the form of published articles) about the warfighting advantages of attacks on U.S. C^4ISR networks in the event of hostilities. Perhaps Chinese leaders are under the impression that China's investment in landline communications will make it invulnerable. In interviews in Beijing, the authors discovered few Chinese analysts who are aware that China's economic integration and continued growth would necessarily make it dependent on networks susceptible to attack. Progress toward Sino-American mutual restraint in cyberspace will depend on whether U.S. officials and researchers can convince Chinese counterparts that vulnerability will inevitably develop as the Chinese economy does.

As one Chinese interlocutor acknowledged, China could also suffer from secondary but sizeable damage should it attack U.S. computer networks.[14] This boomerang effect is a twist on deterrence theory (loosely akin to the self-deterring effects of the danger of jet stream–borne radioactive fallout from one's own nuclear attacks). An attacker such as China has to worry about not only the global interconnectedness of networks, but also the interdependence of the economies that depend on networks. For instance, Chinese credit card accounts are cleared through U.S. systems. The Chinese would be well advised to contemplate the effects on the Chinese economy of a strategic cyber attack on the United States even in the absence of U.S. retaliation. Of course, given the huge U.S. stake in China's economy, there is a comparable risk of substantial rebound damage from U.S. efforts to wage cyber war on China. Generally speaking, the global connectedness of cyberspace and of the economic growth it serves argues for mutual restraint—at least among major states, like China and the United States, that are both capable of and vulnerable to cyber war.

Finally, China is susceptible to political tsunamis caused by economic earthquakes. Circumstantial evidence of this comes from the regime's own strategy, which is to sustain strong per capita GDP growth to assure domestic calm. While economic damage may cause political uproar in a sturdy democracy like the United States, it does not have China's potential

for instability, with a regime whose legitimacy is wedded to national economic performance and the ability to meet rising expectations. Shocking the U.S. economy could threaten current office-holders; shocking the Chinese economy could threaten the regime itself.

Cyber war appears to have a high escalatory potential, especially if the side attacked decides to strike back in kind but with a vengeance. Compounding this problem is that electrons, worms, and viruses do not necessarily conform to human plans.[15] Again, what may begin as military cyber war could spread inadvertently, if not by design, into general cyber war. A critical question for the prospect of mutual deterrence is whether it is possible to discriminate between networks supporting military functions and systems supporting civilian functions, even if such networks rely on the same infrastructure.

In sum, Chinese economic and political exposure to large-scale network attacks should provide a basis for deterrence and an incentive to explore mutual restraint with the United States in strategic cyberspace, especially when taking into account that China could suffer secondary network and economic effects of large-scale network attacks it may conduct. Given its acknowledged vulnerability, the United States should have a similar incentive. Demarcating critical national networks—"strategic cyberspace"—is hard but not impossible. Restraint in strategic cyberspace without restraint in tactical-military cyberspace may be even harder.

Cyberspace and Sino-American Military Contingencies

The previous chapter explained that the United States is critically dependent on space-based C^4ISR to carry out its military strategy in the western Pacific, while China is increasingly dependent on it to carry out its counterstrategy. The same can be said for computer networks, which are largely space-based over the expanses of the Pacific. In addition to China's potential to disable U.S. satellites, it has the possibility of interfering with the computer networks on which U.S. readiness and operations depend.[16] Some of these networks are dedicated, isolated, and well defended. At the same time, the global cyber infrastructure that supports the Defense Department global information grid is for the most part not dedicated, not isolated, and not entirely well defended.[17] It must be assumed that the PLA would attack not only dedicated defense and intelligence networks but also any networks that enable U.S. military operations, including dual-use and less-defended ones and the Internet itself.

From fighting forces to support services, from peacetime to hostilities, the U.S. military is thoroughly networked, especially for intense, com-

plex, joint expeditionary and strike operations. Similarly, the intelligence systems that collect, process, analyze, and disseminate information vital to U.S. military readiness and combat could not function without the capability to ingest, process, and distribute data. The more formidable the enemy forces and their antiaccess capabilities, the more vital computer networking is to U.S. military success.

More specifically, in a military contingency involving Chinese forces in the western Pacific—again, a conflict over Taiwan is an appropriate example—the United States would depend on data links from intelligence collectors to give as much warning as possible of Chinese preparations to attack Taiwan and U.S. forces. USPACOM would need to direct combat forces and logistics tails as they prepare and deploy from far-flung bases and peacetime locations in and out of the region. A major operational advantage of U.S. forces is that they can be highly distributed yet function in an integrated way. But this is possible only through reliance on computer networks for command, control, and communications. Throughout hostilities, links between sensors and strike forces and among strike forces would permit tracking and targeting of Chinese forces, optimal use of weapons, and continuous assessments of their effects.

Because the Chinese intend to conduct sudden, rapid, and brief operations in order to seize the initiative and accomplish their mission before U.S. forces can stop them, U.S. data networks could make the difference between the success and failure of the U.S. response. In countering this Chinese strategy, targets of interest to U.S. strike forces are diverse and dispersed: Chinese air forces, airbases, air defenses, command and control nodes, sensors, missile launchers, surface and subsurface naval forces, amphibious forces and their staging areas, and logistics hubs and flows. Of growing concern to U.S. forces are Chinese ASBMs, along with the extended-range sensors and communications links that enable them to target U.S. aircraft carriers intervening against Chinese forces.

Chinese military strategy is not only to move suddenly and swiftly but also to degrade and delay U.S. forces en route to defend Taiwan. Of course, the Chinese would prefer to deter the United States from intervening, but that requires the ability to disable U.S. carriers. Knowing the importance of achieving their military objectives before U.S. forces can prevent it, the Chinese regard the nodes and links of computer networks that comprise U.S. C^4ISR as an inviting if not a compelling target. The same logic that attracts the Chinese to ASAT capabilities explains their interest in cyber attacks. Because they might not be confident of taking down dedicated and well-protected U.S. military and intelligence networks, they

might also target the GIG's dual-use backbone. To the extent the Chinese would want to be sure of degrading and impeding U.S. forces, they would have an incentive to target broadly rather than narrowly.[18] By design or by effect, Chinese cyber war agents could infect and affect far more than U.S. C^4ISR functions.

Of course, the United States could also launch either retaliatory or preemptive cyber attacks in such a conflict. The Chinese, owing to geographic proximity and prudent planning, have less exposed networks for supporting military operations. Theirs are largely landline and sea-bed fiber optic cables and mainland-based servers, routers, switches, and transmission systems—not entirely beyond reach of U.S. cyber attacks, but relatively inaccessible. As a consequence, even if Chinese forces are as dependent as U.S. forces on the ability to distribute data, their operations may be less susceptible to degradation than U.S. forces, even if the latter has superior cyber attack capabilities.

However, this asymmetric vulnerability will diminish as Chinese forces extend outward in peacetime and contingency operations. As Chinese networks are required to connect and direct increasingly distant and distributed Chinese forces and sensors, including spaced-based ones, the PLA will have to leave its communications fortress. The Chinese have no practical, affordable alternative to relying on existing or otherwise exposed information infrastructure in the waters and space beyond China. In sum, as PLA forces become more information-based—their stated goal—and extend into the Pacific to engage U.S. strike forces, they become more dependent on less secure computer networks. This dependence would also be manifest if dedicated military communications networks were damaged in a military conflict.

The Chinese know they must operate in more joint, integrated, and data-intensive ways, not just because U.S. forces do but also because their military strategy demands it. The Chinese have made no secret of this; indeed, they advertise their goal of informationization of warfare, which guides PLA investments and plans.[19] In a Taiwan contingency, the PLA must be able to stage and flow large land and air forces; find and target the U.S. strike fleet; target U.S. airbases in the region; attempt to gain air control over Taiwan and the Strait; operate an integrated air defense; launch short- and medium-range ballistic missiles against Taiwan and U.S. forces; place its strategic nuclear forces on alert and on the move; attack U.S. satellites and C^4ISR networks; and support these complex operations logistically, which requires liaison with local civilian officials. Again, this involves

all branches of the PLA and must occur suddenly, swiftly, and like clockwork to succeed.

The Chinese should be aware that U.S. cyber attacks on increasingly important and exposed Chinese C^4ISR networks could derail their strategy, such as by damaging their ability to track, target, and attack U.S. carriers near, en route to, or at standoff range from China. Before long, U.S. cyber attacks could be as devastating to Chinese operations as Chinese cyber attacks could be to U.S. operations. A paradox—and potential trap—awaits Chinese military strategy: the more prepared PLA forces are to carry out informationized operations, the more vulnerable the PLA is to U.S. cyber war. In the context of Sino-U.S. conventional war, cyber war could leave China no better off and possibly worse off. Instead of complementing China's growing antiaccess capabilities, cyber war could undermine their effectiveness. While this scenario depends on a number of assumptions about the cyber war capabilities and vulnerabilities of both sides, the Chinese have to consider it.

Cyber war capabilities can contribute to crisis instability. Cyber attacks have little or no counterforce potential for either side, in the sense that the attacking side is no less vulnerable to cyber attacks for having conducted them. The advantage in striking first in cyberspace lies not in protecting oneself from retaliatory strikes but in degrading the opponent's C^4ISR and operations before one's own are degraded. Conversely, exercising restraint with no expectation that the opponent will do likewise could be disadvantageous. In any case, if either side is inclined to use cyber war to degrade the capabilities and performance of the other's military forces, there is logic in doing so early. Because striking early could be advantageous, there is the potential that a cyber attack could be the trigger that turns a confrontation into a conflict. The United States (or China) would likely interpret Chinese (or American) cyber attack as a prelude to physical attack.

An improbable but extremely consequential danger is that an attack by either side on the other's C^4ISR could be interpreted as intended to obstruct the ability to mobilize strategic nuclear forces. The separation of tactical and strategic C^4ISR is not a public matter. However, in the confusion of disrupted surveillance and command networks, the possibility cannot be excluded that strategic forces would at least be placed on higher alert, creating a risk of faulty calculation with incalculable results.

The Chinese would be imprudent to think that the United States would respect firebreaks in cyberspace. Whether it acts preemptively or in retaliation, the United States would have an incentive to attack Chinese

cyberspace broadly rather than narrowly on dedicated and protected Chinese military networks. Not only would this harm China's economic activity, it could also degrade the ability of the leadership to direct Chinese operations and even to communicate with the population. U.S. attacks could isolate Chinese leadership and sow confusion in the population. Chinese cyber attacks could prompt the United States to retaliate without diminishing U.S. capability to do so. The Chinese have a lot to consider before beginning cyber war.

Another feature of cyber warfare may aggravate this crisis instability: the option of subtle attacks or demonstrations. Before hostilities have begun, it might occur to one side that a mild cyber attack—a nonlethal display of one's resolve—could warn and deter the other side and demonstrate its vulnerability. Knowing this, the side attacked might well opt to escalate in cyberspace. Even more dangerous is the potential that a cyber attack intended to show resolve could be interpreted as a prelude to general hostilities, thus triggering, instead of deterring, a conflict.

It would be a gamble for either side to bet that cyber war could be controlled. Every network, whether military or dual-use, that could support military operations would likely be targeted. Networks that support intelligence collection and dissemination would be attacked, making both sides less certain about what was happening but by no means more passive in the conflict. Moreover, one side or the other might consider escalating cyber war to critical networks such as those supporting economic and financial functions, transportation, power, and state control. In sum, the existence of dual-use networks, the possibility of willful escalation, and the difficulty of controlling viruses, worms, and other infections, regardless of human plans, lead to a conclusion that limiting cyber war to the tactical military level would be hard.

Assuming neither could refrain from cyber war if the other engaged in it, U.S. and Chinese calculations of the wisdom of initiating cyber war can be summed up as linked dilemmas:

- For the United States, is it better to degrade the PLA's ability to track, target, and strike U.S. forces (especially naval) than to maintain the C^4ISR needed to operate U.S. forces effectively in the way they are meant to operate?
- For China, is it better to degrade U.S. strike operations by degrading U.S. C^4ISR than to be able to conduct Chinese strike operations against U.S. forces?

- For both, what is the better path to military success: physically striking the other's forces, or attacking the networks that enable the other side to strike one's own forces?

While Chinese strategists may currently calculate that it is better to degrade U.S. C^4ISR than to preserve their own, this could change over time. Conversely, it could be unrealistic for U.S. strategists to think it is possible to maintain undiminished C^4ISR to direct U.S. operations while striking Chinese C^4ISR capability to direct PLA operations.

Once again, these tactical military calculations have to be combined with a strong possibility that cyber war could spread from the military to other realms, with imponderable economic and political effects for both sides. It is easy to imagine how cyber war could start in a Sino-U.S. conflict but hard to see how it would end.

Offense Versus Defense

Much of the detail of U.S. and Chinese cyber warfare capabilities is secret. For our purposes, it suffices to say that the United States and China are able to break into, disrupt, and degrade each other's data networks. Those abilities range from extensive, in the case of publicly accessible and lightly protected networks, including the Internet, to challenging and limited, in the case of dedicated and heavily protected ones.

It is clear that the stronger the attack and the more capable the attacker, the harder it is to defend targeted computer networks. But is the relationship between offense and defense such that an increment of effort to defend produces no more protection, or less, relative to a comparable effort to improve offense? Is cyberspace, like the nuclear and space domains, offense dominant?

One important difference between space and cyberspace is that all satellites are inherently vulnerable, whereas not all networks are invariably so. Lone hackers can penetrate even well-protected networks, but networks can be robust (as long as the infrastructure is intact), redundant (because of automatic or readily available rerouting options), and resilient (because of the opportunity to diagnose attacks, adapt defenses, seal breaches, and restore services). These virtues can limit the scope and duration of even major disruptions.[20]

Because networks are robust, redundant, and resilient, permanent degradation and disruption are difficult, even from major cyber attacks by large and sophisticated attackers. Most experience and analysis involving disruption of services indicate network failures of days and weeks, not

months or years. Another characteristic of cyberspace is that attacks can yield information that can be used to improve defenses, even in the short term. It may be possible to adapt defense at least as quickly as to adapt offense during cyber war. Because large and unmistakable attacks carry more information than small and ambiguous ones, the former could be more conducive to diagnosis and adaptive defense than the latter.[21] In any case, the combination of attack information and availability of defensive remedies means that damage, disruption, and corruption of cyberspace may decline with time, regardless of scale.

On the other hand, the *effects* of network degradation, not the degradation itself, are what really matter. This is important in three respects. First, a large, sophisticated attack can be much harder to contain and remedy in the short term, resulting in grave and lingering damage to the economic and other functions served by the degraded networks. A small attack of the same duration could have a negligible effect. Second, the greater the short-term effects, the longer they will last. To illustrate, a brief yet total disruption of air traffic control systems may leave transportation snarled and the transportation-based economy reeling for some time, whereas a brief and minor disruption could have the effect of a passing weather front. Third, extreme defensive measures that might have to be taken in the face of a large attack, such as sealing off or shutting down threatened networks, may produce nearly as much economic harm as the attack itself. Thus, it is fair to say that the potential to cause major damage to network-dependent functions grows steeply as a function of attack and attacker size.

Figure 6–3 is a representation of a method originally derived to model the investments in cyber security by private firms.[22] It demonstrates that investments in cyber security have a diminishing marginal return per dollar spent on security. Extrapolating from it, the larger the attack, the less cost-effective defense is in preventing harmful effects.

The diminishing returns on investment in defense relative to offense are especially conspicuous when considering the disparity between "hacking" and "patching" in complexity, cost, and time required. Sophisticated network defense software contains between 5 million and 10 million lines of code; malware contains an average of 170 lines of code.[23] Protection of critical government networks typically requires standard government competition and contracting, which can take years before solutions are initiated, whereas designing an attack can be accomplished in weeks. While network defense against sophisticated attackers requires advanced

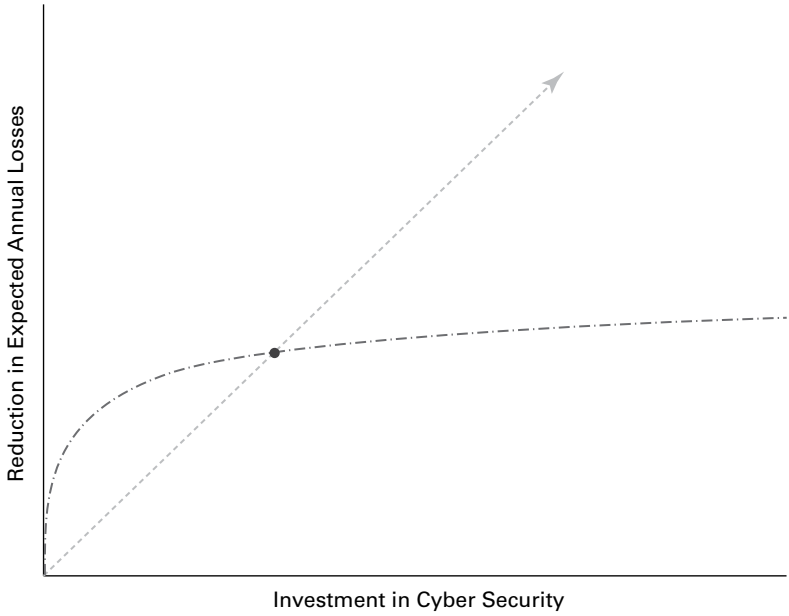

Figure 6–3. Diminishing Returns on Investment in Cyber Security

work by highly specialized firms, network attack is literally a cottage industry.

The woes of the cyber defender are compounded by the increasingly global and integrated nature of networking industries, markets, and infrastructure. Foreign components, subsystems, and whole systems (thus, hardware and software) are increasingly competitive—in price, performance, and value—and consequently are finding their way into U.S. network infrastructure. This includes formidable Chinese corporations with state connections. However difficult it may be to defend entirely made-in-America networks (an extinct species by now), the difficulty is multiplied by increasing use of foreign, notably Chinese, hardware and at least embedded software. The notion of "external" defense of networks must take into account the reality of technological integration and the attendant dangers of "internal" exploitation or disruption. At the same time, the fact of their own dependence on U.S. technology and the risks to world trade, including Chinese exports, should give Chinese political and economic leaders pause before considering or condoning an attempt to exploit for

strategic purposes China's success in U.S. network systems markets—another layer of deterrence.

We do not mean to say that investment in computer network defense is pointless: it is indispensable against less sophisticated, more numerous, and hard-to-deter threats; it raises the barriers to more sophisticated threats; and in any case, it is vital to restore network functionality and service in the event of attack. Given enough time to adjust, offense may not be dominant over defense. Still, the effects of offense can dominate defenses in the short term and can increase sharply with the size of the attack and attacker. So it is crucial to consider deterrence based on fear of retaliation.

Cyber Deterrence

Whether the United States and China can agree on mutual restraint in strategic cyberspace depends heavily on whether they can be mutually deterred from making at least some classes of attacks, even in wartime. This begs the question of whether deterrence works in cyberspace—whether a would-be network attacker with something to be gained by attacking can nevertheless be persuaded not to attack because retaliation risks outweigh expected gains.[24]

History's starkest example of effective deterrence, between the United States and the Soviet Union in the nuclear domain, was elegantly simple and empirically stable: two unmistakable adversaries with tight control of their weaponry, each capable of retaliation with expected consequences that no rational leader would judge acceptable, and with no significant defense (apart from a counterforce first strike, which does not apply in cyber war). The very term *mutual assured destruction* connoted the shared cataclysmic results of general nuclear war. The result was reciprocal deterrence, self-organized though reinforced by common concepts, tight control, negotiated arms control, and transparency.

Cyber deterrence is anything but elegant. Thanks to the ubiquity and dynamics of information technology, cyber war, like cyberspace itself, would be highly complex, fluid, and unpredictable. Who has access to what networks? How is this changing? Who has what capabilities? Who is interfering with whom? Is a foreign power responsible for a given attack by a foreign adversary? Which one? With what weapons? To what end? Will defenses work? What new technology is around the corner? Moreover, the expected consequences of even large network attacks could be mild and fleeting compared to nuclear war, implying that fear of retaliation would contribute less to the strength of deterrence. The contrast between nuclear

and cyber deterrence is reason not to apply wholesale the tenets of the former to the latter.

That said, the ambiguities that characterize cyberspace do not argue against exploring how deeper theories of deterrence, which transcend nuclear weapons, could be applied in some conditions—perhaps to Sino-U.S. cyber war. Most classes of cyber attackers—for example, nonstate actors and rogue states with little to lose—probably cannot be deterred by the threat of cyber retaliation. The source of lesser attacks and identity of the attackers may be difficult to determine. Consequences may be more annoying than devastating. Network defense may be adequate to contain if not prevent such attacks, reducing the importance of a threat of retaliation. Thus, deterrence is neither assured nor essential for most network attacks and attackers.

Yet the fact that deterrence does not apply against *every* network threat does not mean it does not apply to *any*. Even if adequate network protection is possible against most attackers, it might not be against all. Even if many network attackers are themselves not vitally dependent on data networking and thus unlikely to be bothered by the threat of retaliation, some might be. For our purposes, cyber deterrence need not apply generally: it need only apply to Sino-U.S. cyber war.

Beyond simple logic that some cases may not prove all cases, two factors suggest that deterrence might work under some conditions. First, states that pose the largest and most damaging network threats, for which defense is least promising, may themselves be dependent on networks and thus susceptible to threats of retaliation. Second, those posing such threats are unlikely to carry them out except in a crisis or conflict, which could help identify the attacker.

Generally speaking, deterrence is indicated when five conditions are satisfied:[25]

- adequate defense is infeasible or unaffordable
- the scale of expected harm makes it important to prevent attack
- means of powerful retaliation exist
- the enemy has more to lose from retaliation than to gain from attacking
- the attacker is identifiable *enough* to support a credible threat of retaliation.

The first two conditions make deterrence necessary; the third, fourth, and fifth make it possible.

This study finds that these conditions fit the case of Sino-American cyber war, albeit with important qualifications. The first two conditions have already been addressed. If large-scale and sustained attacks were made against strategic networks on which the United States relies—for example, those that enable financial transactions, powergrid management, telecommunications, transportation, national intelligence, or military operations—defenses are unlikely to be adequate to prevent large and lasting harm. This does not mean that efforts to defend against major network attacks are pointless; indeed, even an imperfect defense is more important against infrequent major attacks than frequent minor ones. Better defended U.S. networks may increase the adversary's costs and difficulties and reduce its prospective gains from attack. However, for at least the days and weeks following a major attack, network defense alone cannot be counted on to avoid serious national damage.

The third condition—means of powerful retaliation—has also been addressed. The United States has the means to retaliate strongly for a Chinese attack, regardless of the scale of the attack and damage done (because there is essentially no counterforce). The same could be said for Chinese retaliation for a U.S. cyberstrike. The United States and China have ways to communicate a credible threat of retaliation, which is as much a matter of will and intent as it is of capabilities.

The fourth condition—the attacker's vulnerability in cyberspace—has also been addressed, at least where China and the United States are concerned. Vital functions of each, as well as their economic stability, could be badly if temporarily disrupted, with lasting effects. In the Chinese case, this danger is compounded by uncertainty about how segments of the population would respond to the crisis to their material conditions and future. These dangers would be weighed against expected gains from launching a cyber attack or expected harm that might come from not doing so. The stakes for the United States could be high—for example, the loss of some forces (aircraft carriers) and failure to prevent China from forcibly gaining control of Taiwan. For China, the stakes could be even higher—a crushing defeat by the United States, failure to reunify the country, and a setback in China's quest to become a great power. For these reasons, cyber deterrence might not work. Yet the fact that one cannot be certain that the threat of retaliation will prevent cyber attack does not argue against a cyber deterrence strategy.

There is an important, if imperfect, correlation between the ability of states to conduct large and damaging cyber attacks and their vulnerability to harm from cyber attacks. Generally speaking, sophistication in computer

networks and systems is both a byproduct of heavy reliance on cyberspace and a prerequisite for advanced cyber war capabilities. The anomalous cases are states with little use for computer networks yet advanced attack capabilities and, on the other hand, states with heavy use of computer networks but no competence in cyber warfare (the latter obviously do not matter in cyber deterrence). Figure 6–4 shows some examples of where particular states may fall on these two axes. While these are purely notional, they do illustrate that the states that may most need to be deterred, by virtue of capability, may also be susceptible to deterrence (by virtue of connectivity).

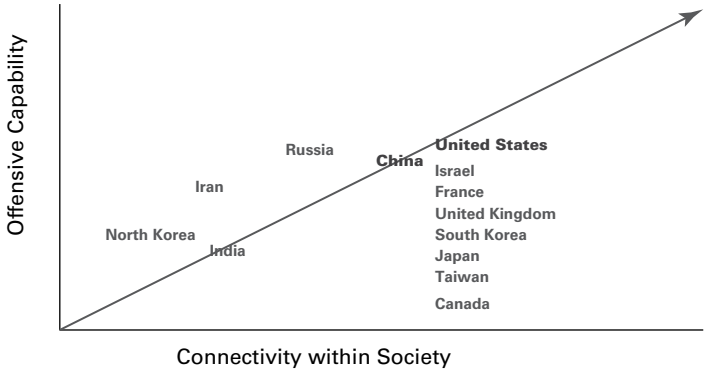

Figure 6–4. Cyber Attack: Offensive Capability Versus Vulnerability

As to the fifth condition, the credibility of the threat to inflict unacceptable retaliatory damage depends *to some extent* on knowing against whom to retaliate. Skeptics of cyber deterrence point out that network attacks can be hard to trace with enough confidence to retaliate.[26] This is true, but several factors mitigate this problem. First, the possibility of tracing an attack is greater if the attack reveals capabilities of a sort and scale possessed by only a few candidates. All else being equal, devastating attacks are more traceable than mild ones.

In this regard, only a few nation-states, including the United States and China, and no nonstates currently have the ability to overwhelm network protection and do enough harm to critical national functions to be considered strategic, as defined here. While the United States and China are obviously capable of lesser attacks, the primary aim of mutual restraint would be at the high end of the scale. The greater the scale, sophistication,

and effects of attack, the fewer the possible attackers other than China (or, from China's perspective, other than the United States).

As to which of the few capable candidates is the actual attacker, it is likely that one state would have a more apparent motive than others to attack. A crisis might provide the clearest indicator of motive and thus of the attacker. Intelligence would likely reveal clues, such as military preparations. Actual hostilities would constitute a smoking gun (metaphorically and literally). In the unlikely event of a bolt-from-the-blue strategic cyber attack, the immediate aftermath would undoubtedly produce indicators of purpose. The Estonia and Georgia attacks both furnished strong if circumstantial evidence of Moscow's complicity.

In general, deterrence is more likely to work against states than nonstates because the latter have less to lose and are less vulnerable to retaliation. In cyber deterrence, there is the added challenge of identifying a nonstate attacker. Because nonstate actors could become able, as well as motivated, to conduct large attacks, this represents a potential hole in cyber deterrence: hard to defend against but also hard to deter. However, while this could in time make identification more problematic, it does not argue against trying to deter the large-state threat.

Even if identifying the attacker from the nature and context of the attack is inferential and not absolutely certain, it may be good enough. Keep in mind that the purpose of deterrence is to prevent attack, thus obviating the need for retaliation. It follows that certainty about an attacker's identity is the wrong standard by which to judge whether the United States should seek cyber deterrence. Would a state that was capable of a severe network attack on the United States but was also vulnerable in the event of retaliation want to count on the inability of the United States to identify it with certainty as the attacker, or on the United States to refrain from retaliating if less than certain as to the attacker? Would the Chinese, in the midst of a crisis with the United States, gamble that the United States would have enough doubt about the perpetrator of a large cyber attack that it could not retaliate?

Of course, deterrence *might* fail, a large attack *might* occur, and the United States *might* be unable to identify the attacker with enough confidence to retaliate. In that case, deterrence might be weakened for the future. But this is no reason for the United States to forego the advantages of deterrence against a Chinese (or other) strategic cyber attack. The same reasoning can be applied to the Chinese as they consider how to restrain the United States from such attacks on China.

Figure 6–5 depicts notionally why deterrence may work even with a lack of certainty about the identity of an attacker. As the likelihood of attri-

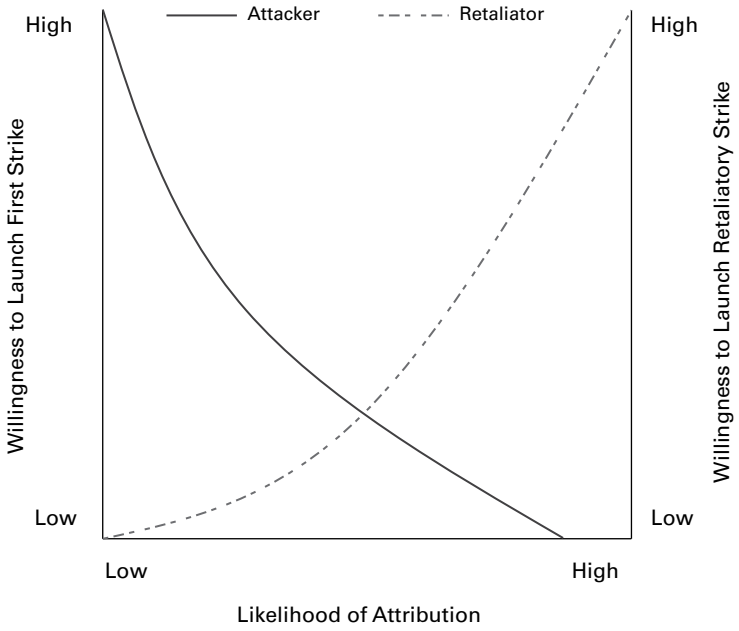

Figure 6–5. Deterrence in the Cyber Domain

bution increases, the side attacked ("retaliator") grows increasingly confident of retaliating against the actual attacker. Meanwhile, the attacker loses confidence that it will not be identified and thus escape retaliation. The attacker does not know for certain how likely it is to be identified or how confident the attacked side must be before deciding to retaliate. Assuming that retaliation would be extremely punishing—outweighing the gains of

	NO	YES
NO	■ Attacker is invulnerable to retaliation ■ Attacker is unknown ■ Defense is possible	■ Attacker is invulnerable to retaliation ■ Attacker is unknown ■ Defense is inadequate
YES	■ Attacker is vulnerable to retaliation ■ Attacker could be known ■ Defense is possible	■ Attacker is vulnerable to retaliation ■ Attacker could be known ■ Defense is inadequate

Table 6–2. Cyber Deterrence: Possible Versus Necessary

attacking—the attacker is unlikely to depend on not being identified *or* the attacked side will retaliate only if absolutely sure of the attacker's identity.

In sum, it appears that there are at least two important cases where cyber deterrence is both necessary and possible—China and the United States, vis-à-vis each other—and thus a basis for Sino-American mutual restraint in strategic cyberspace. Table 6–2 summarizes why and under what conditions cyber deterrence is both necessary and possible. The Sino-U.S. case falls into the possible-and-necessary quadrant.

Thresholds and Firebreaks

Our use of the concept of strategic cyberspace begs the question of what the threshold of that domain is. This is important if there is to be some common understanding about the field in which the United States and China expect restraint from the other.

This question does not arise in connection with the nuclear domain, where any use of a nuclear weapon crosses the well-understood nuclear threshold. The preceding chapter defined the threshold as denying the other side's access to and use of space. Such precision is impossible in cyberspace. Nevertheless, it is important to address the threshold problem if there is to be reciprocal restraint in cyberspace, for intrusions occur routinely and at very low levels. Rather than a single boundary, there are several dimensions along which strategic and nonstrategic cyberspace can be distinguished. None provides either/or indicators, but together they describe what we mean.

One dimension is the severity of an attack's effects, whether they are intended or not. Either an attack that is intended to cause grave national harm but fails or one that is not intended to cause such harm but does so could be considered strategic. This raises again the question of what is meant by national harm. The theft of information, such as what occurred to Google (allegedly at the hands of agents of the Chinese state), while colossal, did not substantially harm the United States. It is also possible to intrude into government networks, even sensitive ones, and yet not intend or cause harm. The most important example is intelligence collection. The exfiltration of secrets from government computers via the networks that link them is hardly friendly, but it is designed to be unnoticed and thus not to disrupt or damage. Although it may have national security implications, like any form of intelligence collection, it occurs often and is hard to restrain. It is, de facto, allowed by international "rules of the game." Apart from network defense, the penalty for the theft of national secrets

by another sovereign state is typically to steal that state's secrets, which may be happening anyway and therefore is not retaliation.

Another dimension is to define *strategic* according to the functions of the networks that might be attacked. It is possible, though not simple, to distinguish networks according to their strategic importance, the criterion being their bearing on national well-being, such as networks often referred to as critical to the economic, physical, and societal well-being of the country and its people. Examples include weather information, air traffic control systems, stock market and interbank transactions, health information, utilities, e-commerce, and government functions. Massive disruption of email could also be critical. Nonstrategic functions include entertainment and advertising. Such distinctions are not static; for instance, social networking tools might first have been regarded as amusement but increasingly are the main media of communities of great importance to the users and to society in general.

Even if a distinction between strategic and nonstrategic cyberspace can be settled, an equally confounding and consequential matter is the boundary of cyber war as an aspect of military hostilities. The more seamless the technical link—or operational transition—from tactical-military to strategic-civilian cyber war, the harder it will be to prevent the former from leading to the latter. In the absence of an escalatory firebreak, mutual strategic restraint in the cyber domain would require a complete ban, in effect, on military cyber attacks below the strategic level. Conversely, a firebreak would permit cyber attacks by armed forces on armed forces during hostilities without undue risk of disruption of networks on which the well-being of civilian populations depends.

The concept of firebreaks figured importantly in American nuclear deterrence theory and Cold War strategy. The most salient was the distinction between battlefield use of tactical nuclear weapons—for example, in Europe—and general intercontinental exchange of strategic nuclear weapons, the former potentially engulfing U.S. troops and NATO Allies but not the U.S. (or Soviet) homeland. The implication was that it was better to confine nuclear war once begun. However, such Allies as the Germans preferred that their homeland not be thought of merely as a nuclear battlefield by the superpowers. Moreover, the United States and its Allies agreed that the Soviets should be offered no assurance that nuclear war would stop at the tactical nuclear firebreak, lest deterrence be weakened. Consequently, for most of the Cold War, the United States tried to erase rather than accentuate a nuclear firebreak. It chose to stress the possibility of escalation over the need to prevent escalation.

In cyberspace, it is not obvious that a firebreak is even theoretically possible, given how connected networks tend to be and the fact that military and civilian networks utilize a largely common infrastructure. If a firebreak is possible, it is important to ask whether it should be favored in the interest of preventing escalation or instead be avoided in the interest of strengthening deterrence by posing the danger of escalation, general cyber war, and economic catastrophe. This issue is critical because of the potential utility, if not inevitability, of military cyber attacks in the event of Sino-U.S. hostilities.

Both the PLA and the U.S. military now regard offensive and defensive network warfare as integral to regular warfare. Against a formidable opponent capable of large-scale, high-intensity combat involving joint forces, the U.S. and Chinese militaries might be considered negligent if they failed to target the C^4ISR networks of the other and to plan for their own to be attacked. After all, military cyber warfare descends from electronic warfare, which is as old as military use of radio and radar and never considered illegitimate. To suggest that attacks on C^4ISR should be proscribed in the same way the use of chemical and biological weapons has been or the way nuclear warfighting and space warfare could be is as unrealistic as it is impractical.

This presents a serious conundrum. As noted, military and civilian networks overlap, in the sense that they use common infrastructure. Moreover, there could be operational military rationales to attack civilian networks that can support large and far-flung combat operations.[27] To make the problem even more complex, cyber targeting is not yet so refined that the effects can be foreseen or controlled with confidence. Once networks of economic and civilian importance are disrupted by one side, retaliation by the other must be expected. Herein lies the risk that military cyber war would lead to general cyber war.

This study has been consistent in the conviction that mutual deterrence is a sine qua non of mutual restraint. Yet there is insufficient reason to think that either China or the United States will be deterred from initiating cyber attacks on military C^4ISR networks if armed conflict were to occur. Indeed, there could be an incentive to conduct such attacks before the enemy does in order to gain tactical advantage. Considering current U.S. conventional military advantages, the PLA has all but declared its intent to exploit this U.S. vulnerability. And as Chinese military capabilities improve in general and come to rely more on C^4ISR in particular, U.S. military interest in promptly disabling Chinese networks will likely grow. As a result, while both countries may be deterred from starting strategic

national cyber war, neither may be deterred from starting tactical military cyber war.

Yet given the improbability of a bolt-from-the-blue strategic cyber attack by China or the United States on the other, the greatest danger of general cyber war is that it could be triggered by a military cyber war in an intense crisis or armed conflict. Hostilities between U.S. and Chinese armed forces may be unlikely; however, there could be strong temptations to strike preemptively in cyberspace, perhaps as the first shot in a conflict. Yet if cyber war between the United States and China is permissible—indeed, probable—during armed conflict, mutual restraint would only apply to a peacetime surprise attack, which is barely plausible. Thus, the danger of escalation from military to general cyber war provides one of the most powerful incentives for mutual restraint. Sino-U.S. agreement not to conduct cyber attacks on military networks even in the course of combat operations is not realistic and, if reached nevertheless, is unlikely to be believed or respected. Therefore, a cyber war firebreak is very desirable—for both countries.

There are at least two ways conceptually to establish a firebreak. One is to stipulate that the need for mutual restraint in strategic cyberspace extends to any military cyber operations that have the *potential* to infect and crash civilian computer networking, including civilian functions that rely on dual-use infrastructure. This approach can be derived from established norms against harm to civilians or uses of force that are disproportionate to what the opponent has committed. However, apart from the fact that such norms tend to be ignored when they may interfere with achieving victory, this approach rules out so much of military cyber war as to be nearly as unrealistic or incredible as a complete ban.

Another approach is to rely on the risk of escalation to impart prudence to military cyberspace, without proclaiming it to be governed by mutual restraint, strictly speaking. This would mean exercising exceptional caution in treating military cyber attacks as a low-risk alternative to physical force. Such caution would demand especially tight civilian control over cyber attacks even during war. In this regard, it is worth borrowing from nuclear escalation theory and practice, to which the United States and, as far as we know, China both conform: orders to release nuclear weapons must come from top political leadership. Although applying such control to cyber attacks may seem constricting to military commanders, the dangers and consequence of escalation to general cyber war suggest a need for if not chief-of-state decision authority, than at least senior political authority and strict rules of engagement.

Such an approach would treat cyber war as fundamentally indiscriminate. Because of the prevalence of dual-use network infrastructure, even if the purpose is to disrupt military networks that enable enemy forces, the effects of a cyber attack might be to disrupt networks that enable international banking, transportation, or other communications on which civilian societies rely. As noted, the United States and other governments have a way to control the use of indiscriminate weapons: they do not delegate authority to use these weapons down the military chain of command or, if they do, it is to use them only when the risks of unwanted or collateral effects, such as harm to civilians, are low. The more likely and consequential the potential effects, the higher the decisionmaking level required to authorize their use. For instance, higher authority is required to use conventional weapons on a military target that is near a civilian population, the destruction of which could do harm to civilians, than if there were little or no such danger.

This same principle could be applied to cyber war. Thus, an attack on a network that is dedicated to supporting enemy forces and completely partitioned from other networks could be authorized at a lower level than an attack on one that could also harm nonmilitary functions or noncombatants. Whereas military commanders could take small risks, political leaders would have to decide whether to take big ones, defined as presenting a nontrivial chance of affecting civilian-commercial networks. Using such delegation protocols, the danger of escalation from tactical to strategic cyber war could be managed without completely tying the hands of military commanders faced with enemy forces utilizing military computer networks.

Protocols for delegation of authority to conduct tactical cyber attacks on military networks could be designed to take into account the general state of alert in a crisis. Just as the United States has a system of graduated defense conditions that grants increasing authority to military commanders as circumstances warrant, it could adopt a system of graduated cyber conditions. For now, however, there should and will be a bias in favor of centralized political control except when the risk of unintended civilian consequences is clearly low, even—or especially—in wartime.

A technical capability to improve discrimination in cyber war could also help within such a framework. As techniques for cyber attack are refined, the key to making cyber war less indiscriminate is intelligence. With expansive and excellent knowledge of the workings of a potential adversary's computer systems—a tall order, to be sure—a state with sophisticated cyber war capabilities could target military but not civilian networks, even if they use the same infrastructure. To illustrate, a given server

can support multiple networks, both military and civilian, each with its own software characteristics and identifiers. Destroying that server by, say, dropping a bomb on it would obviously disrupt all the networks being supported. However, dropping a virus into the server, with the benefit of excellent intelligence, could infect only the targeted network, perhaps a military one but not a civilian one.

With imperfect intelligence, there would be a risk that the attack would infect more than the target network. However, when combined with the procedures for delegating authority just described, such targeting would provide a way to manage risks of collateral damage and unintentional escalation. By improving discrimination and instituting appropriate decisionmaking control, it may be possible to achieve mutual restraint in attacking critical ("strategic") cyberspace without expecting a prohibition on tactical cyber war during hostilities, which is not practical, not believable, and not in the interest of the United States.

Returning, then, to the question of the boundaries of strategic cyberspace for purposes of mutual restraint, a possible Sino-U.S. approach would be to:

- agree that mutual strategic restraint applies to attacks on networks with the intent or potential of doing serious economic, civilian, or other national harm
- agree that restraint should apply to attacks on military and intelligence networks in peacetime (apart from cyber spying)
- agree that at no time should networks critical to civilian and economic well-being be subject to attacks, except in retaliation
- acknowledge jointly that the risk of escalation demands caution, discrimination, and control in wartime military cyber attacks
- apply strict delegations of decisionmaking authority regarding military cyber attacks, based on the risks of civilian and other collateral harm
- begin a dialogue, involving both civilian leaders and military commanders, to share concerns and intentions and to avert misperceptions and miscalculation.

Resting on the strength of mutual deterrence, such undertakings could reduce the dangers of Sino-American strategic cyber war.

This matter of authority to engage in cyber war is receiving attention within the U.S. Government, evidently with a view toward avoiding unwanted consequences of the sort laid out above. There recently has been

some public reporting on guidelines to U.S. military commanders in connection with cyber war. In a nutshell, "the military must seek presidential approval for 1) a specific cyber assault on an enemy, and 2) the option to weave cyber capabilities into U.S. warfighting strategy." The United States can defend itself by blocking cyber intrusions and taking down servers in another country and has the right to pursue attackers via cyberspace net.[28]

Such provisions are consistent with the proposition that cyber attacks ought to be regarded as potentially indiscriminate, at least for now. Unless and until the firebreak concept developed here becomes technically and operationally reliable, the bias should be toward tight civilian control at the highest level. We expect and suggest that further thought be given to two issues: how such guidance is to be followed in the event of hostilities, once Presidential authority has been granted; and whether the principle of Presidential control can withstand pressures to engage in cyber operations as an integral aspect of 21st-century warfare, especially as potential adversaries expand their use of computer networking to support combat against U.S. forces. Broadly speaking, it seems that the United States is still in the foothills of solving the dilemma posed by the dual objectives of enabling U.S. forces to succeed while also avoiding escalation up to and including general war in cyber space.

Elements of Practical Cyber Deterrence

Cyber deterrence requires a country committed to it to address several matters: offensive capabilities, legitimacy of the threat to retaliate, declaratory policy, consistent behavior, adequate control, security of allies, and international cooperation. While these are addressed from the U.S. perspective in the pages that follow, the prescriptions apply more or less also to China on the assumption that mutual restraint in cyberspace would be symmetrical.

Any country's external use of force is constrained by international law and norms, starting with the United Nations Charter. The right of self-defense is widely understood to include deterrence and thus threats and acts of retaliatory force, within limits.[29] Less clear is the right to escalate in retaliation, which is disproportionate by design. The threat of escalation can be important for deterrence. Throughout the Cold War, the United States relied on the threat of escalation, including first use of nuclear weapons, to deter Soviet aggression in Europe; it justified this as inherent in the right of self-defense (including of allies). In cyberspace, Chinese leaders would presumably be more leery of PLA proposals to initiate cyber attacks to disrupt U.S. military operations if given reason to fear that the U.S.

response would not be limited to military forces and could damage China's own critical national networks.

Related to escalation is the issue of civilian consequences. The U.S. Government is known to have struggled with the civilian impact of cyber war, especially if waged against networks that affect a population's well-being.[30] Of course, the fact that network attacks can harm noncombatants does not call for a higher standard than for physical attacks. From the Civil War to two World Wars to Vietnam to Iraq, the United States has waged war in ways that affect civilians, while not failing to assert that industrial, infrastructure, and enemy leadership targets are legitimate because they enable enemy warmaking. Although the weaponry differs in cyber war, norms of proportionality and minimizing harm to civilians are essentially the same.

A third normative question is whether an unprovoked or initial cyber attack constitutes international aggression—an act of war. The answer must reflect the potential destructiveness of cyber warfare. It also should apply the same standard to the enemy as to oneself. If it is considered aggression, as it ought to be if the intention or effect is substantially destructive, an enemy attack would justify whatever is permissible under the right of self-defense, including both cyber and physical responses.

In this light, resorting to cyber war only in response to cyber attack would add legitimacy to the threat and act of retaliation and thus strengthen deterrence. Given its myriad other forms of power and its dependence on vulnerable networks, the United States should favor such a norm. However, networks have become so integral to military operations, for the United States and China alike, that the United States is highly unlikely to foreswear attacks on networks that enable operations of the PLA.

As an alternative, the United States could take the position that military aggression, whether physical or electronic, justifies cyber attacks. This would rule out a cyber no-first-use policy. But it would amount to a pledge not to wage cyber war unless aggression has been committed—unless hostilities have begun. If inclined toward such a pledge, the United States should make it contingent on a reciprocal one from China. Doing so would reduce the risk that China would conduct cyberstrikes preemptively or in a crisis before any shooting occurs.

In essence, U.S. policy could be as follows:

- The United States opposes aggression in the form of computer network attacks and regards such attacks as acts of war.
- It reserves the right of self-defense by responding to such attacks and will maintain the capability to retaliate in order to deter.

- The laws of war governing the obligation not to harm civilians apply in cyberspace.

Behavior will speak at least as loudly as declaratory policy. Two behaviors that could undermine cyber deterrence vis-à-vis China are attacking Chinese networks other than in retaliation for Chinese attacks, and failing to retaliate for Chinese attacks. The greater the difference in consequences for China between attacking and not attacking the United States, the stronger the deterrence. Moreover, for the United States to attack Chinese networks absent Chinese attacks would strengthen the hands of those Chinese who argue for an aggressive cyber warfare policy and weaken those who argue that China is better off showing restraint. Conversely, U.S. failure to retaliate could undercut the credibility of deterrence insofar as the potential attacker is given reason to think that retaliation will not occur.

Such a posture is the opposite of frequent lesser network interference. It requires purposeful decisionmaking. The need for calibrated and consistent strategic behavior reinforces the need for strong civilian control, in both the United States and China. A clear distinction must be made between the technical competence to create and employ cyber weapons and the authority to determine whether, when, against whom, and for what ends to use them. Because it requires strategic behavior and is a matter of war and peace, cyber deterrence must be managed by proper authorities in the same way all other international uses of force are: politically accountable civilian officials of the executive branch and designated military commanders, with proper Congressional oversight. The United States is moving in this direction with the creation of U.S. Cyber Command (under U.S. Title 10 and the Secretary of Defense) alongside the National Security Agency (under U.S. Title 50 and the Director of National Intelligence).

The existence of security commitments to U.S. allies (and hypothetically to Chinese allies) may appear to further complicate an already difficult domain. But the cyber security of allies need not and should not be different than their physical security, at least not where destructive cyber warfare is concerned. For starters, a serious cyber attack on a NATO Ally should cause Article V of the Washington Treaty to be invoked; anything less would invite Russia to attempt again the sort of attacks it allegedly sponsored against Estonia (a NATO Ally) and Georgia. By extension, U.S. commitments to the security of Japan, South Korea, and other treaty Allies in Asia should include the option of U.S. retaliation for Chinese cyber attack. Thus, any agreement by the United States and China to show

restraint toward the strategic cyberspace of the other must include at least treaty Allies.

Finally, Sino-American mutual restraint in cyberspace could be extended to cooperation against common third-party threats in that domain. Both countries have two sets of cyber security concerns: high-end state threats, and all other state and nonstate threats. For the former, deterrence is necessary and feasible; for the latter, it is less necessary and less feasible. U.S. and Chinese security against all other state and nonstate cyber threats could be improved through Sino-American cooperation, whether in bilateral or multilateral settings. At a minimum, exchanging information on potential attackers and attacks, notifying alerts, and extraordinary measures would be worthwhile, as gaining wide acceptance of mutual strategic restraint in cyberspace. While such cooperation is not essential for mutual restraint, it would be a natural and beneficial supplement.

Conclusion

China and the United States are both beginning to grasp the grave harm that could come from strategic cyber war. Their respective offensive capabilities in this domain, the difficulty of defense against large cyber threats, and thus the fear of retaliation can be the foundation for mutual deterrence. While this could be left as a de facto condition or tacit understanding, it is better to make it a matter of agreement on mutual restraint in initiating strategic cyber war, including tight political control of any military cyber attacks in the event of armed conflict. Such agreement could be bolstered by continuing discussion of thorny definitional issues and possible concrete cooperation.

The United States should be interested in pursuing an accord along these lines, though with its eyes open about the ambiguities and pitfalls. But it should do so as part of a wider approach, covering nuclear and space domains as well. As with restraint in space, the United States should not accede definitively to China's position on no first use of nuclear weapons if the Chinese reject the larger concept of mutual strategic restraint and its application to cyberspace.

These ideas might be more appealing to the United States than to the Chinese. The United States is the stronger military power, and it is more vulnerable than China to the effects of cyber war—for now. But China is becoming highly dependent on computer networks and more exposed to their disruption, and it has no more hope of complete network defense than the United States has. Perhaps Chinese leaders have the foresight to appreciate the value of mutual strategic restraint in cyberspace, and the clout to overrule objections from Chinese warfighters. In

the meantime, they can be sure that the United States will not accept inferiority in offensive cyber war capabilities and that China's vulnerabilities in this domain will only get worse.

Notes

[1] An intriguing question is how important Web-based social networking might be or become for either the United States or China, given its remarkable importance in marshaling and unifying citizens on a large scale in the recent democratic revolutions in the Arab world. Of course, it is more likely that the Chinese government would interfere with social networking in China than that the U.S. Government would. For this analysis, we will not treat it as "critical."

[2] Perhaps for probing or to send a non-harmful signal. But such examples do not negate the point.

[3] Lest such a distinction between strategic and nonstrategic networks be taken as a green light to attack the latter, each country should consider its own vulnerability throughout cyberspace before conducting or condoning cyber war at any level or on any target.

[4] A basic Westphalian principle, which the Chinese above all would appreciate.

[5] For further discussion, see National Security Council, "The Comprehensive National Cybersecurity Initiative," available at <www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>; "Remarks by the President on Securing our Nation's Cyber Infrastructure," May 2009, available at <www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>; National Security Council, "The Cyberspace Policy Review," available at <www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf>.

[6] Dennis C. Blair, "Annual Threat Assessment of the U.S. Intelligence Committee for the Senate Select Committee on Intelligence," Office of the Director of National Intelligence, 2010; Spencer Michels, interview with Michael Hayden, "Hackers Force Internet Users to Learn Self-Defense," *PBS News Hour,* August 11, 2010; Michael McConnell, "Cybersecurity: Next Steps to Protect Our Critical Infrastructure," statement before the Committee on Commerce, Science, and Transportation, Washington, DC, February 23, 2010, available at <www.fas.org/irp/congress/2010_hr/cybersec.pdf>.

[7] Scott Borg, "How Cyber Attacks Will Be Used in International Conflicts," presentation at *USENIX Security '10 Technical Symposium,* Washington, DC, 2010.

[8] The attack on Google was not strategic for two reasons. First, the purpose of the attack was to exfiltrate data, not to degrade the systems. Second, the network that was attacked was not of national importance.

[9] "Marching Off to Cyberwar," *The Economist,* December 4, 2008, available at <www.economist.com/node/12673385>; Mark Landler and John Markoff, "Digital Fears Emerge After Data Siege in Estonia," *The New York Times,* May 29, 2007, available at <www.nytimes.com/2007/05/29/technology/29estonia.html>.

[10] China Internet Network Information Center, "Statistical Report on Internet Development in China," 2009.

[11] Before assuming that personal Internet use in China will subvert the state, note that much of it is nationalistic—questioning the government not for being too strong at home but for being too weak abroad. So far, at least, the threat of cyber dissent has not caused the government to shut down Internet use, only to block any political excesses.

[12] Investment in WiFi is shifting from telecom and end-users to institutions. See Analysys International, *The Market for Wi-Fi® in China: Opportunities, Enablers and Challenges* (Beijing: Analysys International, June 2006), 24.

[13] "Being Eaten by the Dragon: Chinese Takeovers," *The Economist,* November 13, 2010, 81.

[14] Interview with Chinese expert, Beijing, December 2010.

[15] It appears to be the case that while Stuxnet was meant to target Iranian nuclear facilities, it infected the SCADA systems in several different countries.

[16] Electronic attacks on the data networks connected to space-based sensors and space-based communications could be considered either counter-space or cyber war. Because we are defining counter-space as attacks on satellites themselves, we will consider such electronic attacks as cyber war.

[17] The alternative, a cluster of U.S. defense and intelligence networks that are totally, globally isolated, would be prohibitively expensive and virtually impractical.

[18] One U.S. cyber expert makes the point that crude (and relatively indiscriminant) methods such as distributed denial-of-service attacks against U.S. military logistics networks could be an effective tool. Mulvenon, "PLA Computer Network Operations."

[19] Information Office of the State Council of the People's Republic of China, *China's National Defense in 2008* (Beijing: Information Office of the State Council of the People's Republic of China, January 2009), 11.

[20] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND, 2009), 57–59.

[21] This might be especially true in a military conflict, where the imperative to prevail might result in the use of all availability capabilities, including ones previously reserved or used sparingly to avoid compromising their effectiveness.

[22] L.A. Gordon and M.P. Loeb, "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5, no. 4 (November 2002), 438–457.

[23] William Lynn, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* (September–October 2010).

[24] Deterring cyber attack by other means, such as physical attack, is possible. However, that possibility does not negate the possible merits of mutual cyber deterrence, at least as an option.

[25] For purposes of this book, we concentrate on deterrence by the threat of retaliation and not "deterrence by denial," that is, by better defense. The latter presents the attacker with only the risk of failure, whereas we are interested here in the question of presenting risks worse than failure.

[26] Some examples include Libicki; Richard Harknett, John Callaghan, and Rudi Kauffman, "Leaving Deterrence Behind: War-Fighting and National Cybersecurity," *Journal of Homeland Security and Emergency Management* 7, no. 1 (2010); Richard Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (Autumn 1996); and Stephen Blank, "Can Information Warfare be Deterred?" in *Information Age Anthology,* Volume III: *The Information Age Military,* ed. David S. Alberts and Daniel S. Papp (Washington, DC: Command and Control Research Program, 2001), 125–157, available at <www.dodccrp.org/files/Alberts_Anthology_III.pdf>.

[27] A good analogy might be bombing interdiction campaigns that target dual-use transportation nodes (bridges, highways, rail switching stations) to prevent military forces and supplies from moving to the front.

[28] Lolita C. Baldor, Associated Press, June 24, 2010.

[29] There is a somewhat metaphysical debate about whether mutual assured destruction is consistent with the rules of law, given the civilian cataclysm implied. But this has never had any real impact on nuclear doctrine.

[30] For more discussion on the Kosovo controversy, see Tonia Voon, "Pointing the Finger: Civilian Casualties of NATO Bombing in the Kosovo Conflict," Washington College of Law, American University, 2001, available at <www.wcl.american.edu/journal/ilr/16/voon.pdf?rd=1>.