CHAPTER 13
Deterrence of Cyber Attacks

Richard L. Kugler

CAN THE UNITED STATES hope to deter major cyber attacks on itself, its military forces, and its allies? Creating a cyber deterrence strategy is important because such attacks are becoming increasingly likely, because they could cause serious damage to America's information networks and beyond, and because fully defending against them is problematic. If adversaries could be deterred from launching them, the United States would face fewer risks from them.

Although the U.S. Government is well aware of the dangers posed by cyber attacks, currently it does not have a well-developed or publicly articulated strategy for deterring them. Most likely, not all cyber attacks can be deterred, but if the biggest and most dangerous attacks could be prevented, this alone would be an important accomplishment. Exactly how can cyber attacks be deterred? What would be the key components and calculations of a cyber deterrence strategy? What capabilities and action agendas would it require? These important questions are addressed here.

This chapter offers a perspective that rejects the view, held by some observers, that the "attribution problem"—the difficulty of identifying actual or potential attackers—wholly paralyzes any attempt to think fruitfully about a cyber deterrence strategy. To be sure, there will be cases in which some cyber attackers successfully conceal their identities and thereby frustrate attempts to apply deterrent and retaliatory mechanisms against them. But they do not constitute the entire universe, or even the most important subset, of potential cyber attackers. In the coming years, there is likely to be a growing number of important cases—ones, for example, involving big powers such as China and other nation-states—in which adversaries use the threat of cyber attacks (or actual attacks) as a means to a larger political end or to exert coercive leverage on the United States. In these circumstances, the adversaries will be willing to make their identities known, or alternatively, their identities can be reliably inferred from the surrounding strategic circumstances. Deterrence mechanisms can be applied to such "attributable" attackers. This chapter focuses on how to develop and apply a deterrence strategy to this category of cyber attackers.

The following pages advance several core arguments. First, the prospect of major cyber attacks should not be seen in isolation, but in the context of larger global security affairs. Although some cyber attacks might be mounted purely for the purpose of damaging the United States, other attacks could be launched by adversaries whose political and strategic agenda extends beyond the cyber domain; in addition to allowing their identities to be determined, this larger context can set the stage for determining how multifaceted U.S. efforts to deter them can be forged. Second, endeavoring to deter cyber attacks is a matter both of assembling the physical capabilities for defending against them and of employing offensive capabilities—cyber, diplomatic, economic, and military tools—for inflicting unacceptable damage in retaliation. Equally important, cyber deterrence also involves a psychological and cognitive component: like other forms of deterrence, it requires the capacity to influence the motives, cost-benefit calculations, and risk-taking propensities of adversaries, in order to convince them that launching a cyber attack would not serve their interests and objectives and that the costs and risks would outweigh any sensible calculation of benefits. Assembling a proper combination of motivational instruments and physical capabilities to serve this purpose lies at the heart of forging a modern-day strategy for cyber deterrence. A one-size-fits-all approach to deterrence will not work because of the multiplicity and diversity of potential adversaries and cyber attacks, and because U.S. goals and actions may shift from one situation to the next. As a result, the United States will need a strategy of "tailored" cyber deterrence that treats each category of potential adversary, type of attack, and type of U.S. response on its own merits.

This chapter begins by portraying how official U.S. Government documents treat cyber threats and the role of deterrence in dealing with them. Then it briefly discusses the ways in which the United States is vulnerable to cyber attacks and how contemporary global security affairs are giving rise to cyber threats. Against the background of lessons from how deterrence theory evolved during the Cold War and how it operates today, the chapter then develops a general model for deterring cyber threats, based on deterrence that is tailored to influence the motivations and psychology of different cyber adversaries. An analytical section reviews the key strategic requirements of cyber deterrence strategy, including declaratory policy, situational awareness, command and control, defensive cyber security, a wide spectrum of offensive capabilities for retaliation, interagency cooperation, cooperation with allies and partners, and cyber deterrence metrics. Issues that will require further research and analysis are identified. The chapter concludes by presenting a spectrum of options for pursuing cyber deterrence.

Overall, this material articulates an underlying theme: that the United States can realistically hope to create a cyber deterrence strategy that works, perhaps not perfectly, but well enough to make a big difference and that offers considerably greater security from cyber threats than exists today. Creating such a rewarding and affordable strategy, however, will require concerted thought and coordinated actions of the sort that have characterized deterrence since it first appeared as a strategic concept over 50 years ago.

Cyber Deterrence Strategy in Official U.S. Documents

Deterrence of cyber attacks is discussed in some key U.S. strategy documents. *The National Strategy to Secure Cyberspace,* issued by the White House in February 2003 in response to the prospect of growing cyber threats, articulates three broad goals: to prevent cyber attacks, to reduce U.S. vulnerability to them, and to minimize damage and recovery time.[1] However, it contains little on how to prevent cyber attacks. In terms of deterrence, it only says briefly that a U.S. response might not be limited to criminal prosecution of cyberspace criminals and that the United States reserves the right to respond in an appropriate manner. A companion document, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (issued in February 2003), articulates a similar focus on physical protection of the U.S. homeland from new-era threats, not deterrence of cyber threats.[2] The same applies to the *National Strategy for Homeland Security.*[3]

Among other U.S. strategy documents, the most important is the *National Security Strategy of the United States of America*, issued by the White House most recently in March 2006.[4] It outlines nine strategic goals ranging from defeating terrorism and preventing proliferation of weapons of mass destruction (WMD) to working with allies and partners while supporting the spread of democracy and a prosperous world economy, but it devotes little discussion to cyber threats. Discussing institutional reforms to the Department of Defense (DOD), it notes that U.S. security faces traditional, irregular, catastrophic, and disruptive challenges; cyber threats are classified as disruptive threats, along with threats from space, biotechnology, and directed energy weapons. The document instructs DOD to build a transformed military force posture that will provide tailored deterrence of a wide spectrum of future threats, including terrorist attacks in the physical and information domains, but it provides no guidance for shaping such deterrence.

The *National Defense Strategy of the United States of America* released in March 2005 identifies four broad goals: assurance, dissuasion, deterrence, and defeat of adversaries for the purpose of protecting the U.S. homeland; securing global freedom of action; strengthening alliances; and fostering favorable security conditions.[5] In order to achieve these goals, it calls for an active, layered defense rather than a passive or reactive strategy against traditional, irregular, catastrophic, and disruptive challenges, including cyber threats. It states that the top U.S. security priority is to dissuade, deter, and defeat those who seek to harm the United States directly, especially extremists who use WMD. It briefly mentions cyber threats but provides no guidance on how to deter them. Neither does *The National Military Strategy of the United States of America* issued by the Chairman of the Joint Chiefs of Staff in 2004.[6] This document is meant to provide strategic principles and operational guidelines for using and building U.S. military capabilities, including ones for homeland defense. While calling for high-technology, networked, and modular forces for full-spectrum dominance, it gives only cursory attention to cyber threats or to strategy for deterring them.

The 2006 Quadrennial Defense Review (QDR) charts future directions for improving U.S. military forces, under the rubric of capability-based planning, for a wide variety of situations.[7] It mandates agility, responsiveness, and battlefield domination. It does provide some useful guidance on dealing with cyber threats. In its section on homeland defense, it notes that the populace, territory, infrastructure, and space assets of the United States are increasingly vulnerable, not only to WMD, but also to electronic or cyber attacks. It declares that DOD "will maintain a deterrent posture to persuade potential aggressors that their objectives in attacking would be denied and that any attack on U.S. territory, people, critical infrastructure or forces could result in an overwhelming response." This statement was intended to underscore deterrence of new-era threats in general; cyber deterrence is explicitly part of the overall strategic calculus. However, the QDR provided no specific guidance on how cyber deterrence could be achieved, or on how requirements for U.S. forces and other instruments of power might be affected.

Current planning for U.S. military operations is greatly influenced by Joint Operating Concepts (JOCs), such as the one on deterrence operations.[8] This 2006 JOC presents a rich conceptual framework for thinking about deterrence in general, and therefore figures prominently in the discussion below of a general model for cyber deterrence. Although it clearly acknowledges cyber threats, however, it says less about deterring them than about deterring use of WMD and similar threats from rogue powers, terrorists, or near-peer competitors.

An official document with specific relevance is the 2007 *National Military Strategy to Secure Cyberspace*.[9] This document is still classified, but official DOD statements have indicated that it calls upon national security planners to:

- improve capabilities for attack attribution and response;
- improve coordination for responding to cyber attacks within the U.S. national security community; and
- foster the establishment of national and international watch-and-warning networks to

detect and prevent cyber attacks as they emerge.

Although these statements identify required capabilities for national strategy, they do not amount to a cyber deterrence strategy in themselves.

This brief review of official U.S. documents shows that the dangers posed by potential cyber attacks are officially acknowledged, along with the need for responsive capabilities and the desirability of deterring such attacks. However, a cyber deterrence strategy has not yet been articulated and released, at least publicly. A great deal of effort has been devoted to preparing strategic frameworks for defense and security planning, and therefore many of the basic ingredients for a cyber deterrence strategy already exist. The task is to bring them together to create a cyber deterrence strategy. The next section suggests why.

Growing Vulnerability to Cyber Attacks in a Globalizing World

The cyber attack that was launched on Estonia in spring 2007, which allegedly originated in Russia (which its government denied), helped put the threat of cyber attacks on the front pages of newspapers everywhere. With help from the United States and Europe, Estonia recovered relatively quickly from that attack. But there is no guarantee that future cyber attacks will be confined to small countries such as Estonia or will inflict only transitory damage. Indeed, the United States is vulnerable to such attacks, and they potentially could cause widespread damage.

The damage from cyber attacks could extend far beyond the information systems that they principally affect, because so many spheres of national life depend heavily on modern information systems.[10] The U.S. military, for example, relies upon information networks, including the global information grid, to conduct modern-era combat operations.[11] Many civilian institutions, infrastructures, and essential government services are also highly dependent on the Internet and other information networks. Police, firefighters, and other emergency services providers, public health, education, transportation, banking and finance, water supply, sanitation, and energy systems all depend on computers and information networks, as do the air traffic control system, hydroelectric dams, nuclear power plants, traffic lights, water treatment facilities, and key private sector institutions such as colleges and universities, hospitals, stock markets, business corporations, shopping malls, and credit card companies. An attack on one vulnerable sector could seriously damage other sectors.

Other regions, such as Europe and democratic Asia similarly rely upon information networks and are vulnerable to their disruption. Countries embarked upon economic modernization are also beginning to use cyberspace at growing rates. The entire global economy is becoming increasingly dependent upon modern information systems. Imports, exports, and other international transactions empower growth in many modern national economies, and these rely upon global networks. Modern multinational businesses employ information networks to integrate central headquarters, production lines, and distribution systems that are often scattered across multiple countries and continents. The huge flow of global finance that takes place daily is directly dependent upon the Internet and other systems. Disruption of these activities and their information systems could damage the operations of the world economy, contributing to financial panics, recessions, and even depressions.

Cyber vulnerabilities are thus growing, while cyber attack tools and methodologies are becoming more available, and the technical capacity of malicious actors is improving.

Emerging Cyber Threats

An issue critical to cyber deterrence is understanding what kinds of actors are likely to pose cyber threats, especially threats of major disruptive attacks, to the United States, its military forces, and its allies in coming years. The ability to use cyberspace to create advantages and to influence events in other operational environments and across multiple instruments of power is spreading. Many view cyber attackers today as mainly individual hackers with purely malicious intent, or perhaps criminal groups intending to use information networks for profit-seeking. In addition, however, actors with political or ideological agendas—including terrorist groups, rogue countries, and even big powers such as China and Russia—will also pursue cyberpower and will play roles of growing importance. They may seek to use cyber threats or attacks to pursue strategic and political goals in geopolitical competition with the United States and its allies. Such cyber attacks likely would not be ends in themselves, but rather instruments of persuasion and coercion in pursuit of agendas that extend well beyond cyberspace. These actors and their activities may present bigger cyber threats than we have seen before and thus may require the attention of a U.S. cyber deterrent strategy.

Emerging trends in global security affairs will set the stage on which new and bigger threats may multiply in future years. During the Cold War, the global security structure was static and bipolar, pitting the United States and its democratic allies against the Soviet Union and its communist allies. That period was one of great danger, but bipolarity made the task of designing U.S. national security policy fairly straightforward. Waging the Cold War was difficult and costly, but it was an exercise in clarity and steadfastness rather than uncertainty, adaptability, and endless recalculation about policy basics. America's enemies were militarily powerful, but they were limited in number, their identities were firmly established, and their goals and actions were predictable—all of which facilitated the evolution of U.S. deterrence policies.

Compared to the Cold War, today's world is highly complex. Bipolarity is gone, and no permanent structure has taken its place. Instead, the world is changing rapidly in response to globalization and other information-era dynamics, which bring once-distant parts of the world into close contact with each other and draw the United States into distant regions that once were considered outside its geostrategic perimeter. The changing roles of nation-states and other actors, new political ideologies, shifting security conditions, the hotly competitive world economy, the emergence of new technologies, and transformed military forces all add to the global environment of fast-paced changes and amorphous conditions. Surprises occur frequently, major developments leap suddenly out of a dense fog of uncertainty, and even experts are unable to predict the future.

To the extent that today's international security system has a structure, its most important components have, loosely speaking, three parts. The first part is the wealthy democratic community, composed of the United States, Europe, and democratic parts of Asia, plus much of Latin America, which is mainly democratic albeit not wealthy. For the most part, this democratic community is prosperous, secure, and stable. The second part comprises the "strategic challengers," including big powers such as China, Russia, and India. With nearly one-half of the world's population and a growing share of economic wealth, these three big powers are redefining their identities on the world stage and the imprint that they want to make on global security affairs. India, a democracy with a traditionally independent foreign policy, has recently begun to draw closer to the United States and to play a constructive role in South Asian affairs. Both Russia and China are asserting themselves in global politics, but it is unclear whether they will emerge as partners or rivals of the United States, or something in between. The third part of the global structure is the "southern arc of instability" from the greater Middle East to East Asia. This huge zone is a seething cauldron of chaotic troubles, authoritarian regimes, unstable societies, poverty, turmoil, angry Islamic fundamentalism, and violence. Today's threats of terrorism, WMD proliferation, and rogue countries emerge from this zone, whose future is a big question mark. The difficult wars in Iraq and Afghanistan, the Israeli-Palestinian conflict, and the U.S. search for an effective diplomacy in the region add to the uncertainty.

Given this global structure, the dominant security agenda facing the United States is to preserve the cohesion of the democratic community, to keep relations with the big powers on an even keel, and to muster friends and allies in an effort to quell threats and turbulence along the southern arc, especially in the Middle East. In this endeavor, the United States can hope to influence events but, despite its superpower status, it cannot control the future. Today's world is being heavily shaped by two global dynamics: 10 or 15 years ago, many observers focused on hopeful neo-Kantian trends promising progress in the form of democratization, economic prosperity, and peace. Since then, however, dangerous neo-Hobbesian trends—strife, conflict, turmoil, and stalled progress—have asserted themselves in many places, especially along the southern arc of instability. While neo-Kantian trends are still operating in many ways and places, neo-Hobbesian trends have risen to equal importance. A decade or two from now, the future could witness a world enjoying greater stability if neo-Kantian trends take precedence or one descending into instability and struggle if neo-Hobbesian trends dominate.

Meanwhile, a third trend, empowerment, has gained force in recent years. Economic globalization and the information age give previously weak actors more power to act independently and influentially on the world stage, including by using cyberpower. China, for example, once poverty-stricken and inward- looking, is now on its way to becoming an economic powerhouse, able to build modern military forces and to cultivate ambitious political and strategic appetites in Asia. Some small and mid-sized countries, such as South Korea and Iran, are also deriving greater strategic power from economic growth. Also significant is that nongovernmental actors, including terrorist groups, have been empowered by the Internet and information networks to spread their influence worldwide. Such empowerment trends can help peace-minded countries to become wealthier and more stable and to play increasingly constructive roles on the world scene, but they also enable rogues, aggressors, dictators, and terrorists to pursue troublesome agendas in increasingly potent ways. For example, empowered by access to oil profits, Iran has begun to pursue a more assertive agenda, as has Hugo Chavez's Venezuela. The United States is in no danger of being eclipsed any time soon, but new actors will be able to play more influential roles in global security affairs; geopolitical dramas promise to be correspondingly more complex, and perhaps more dangerous.

Role of Cyberpower

Cyberpower contributes to the growing strength of many actors in global politics; it is a significant reason why a number of previously impoverished countries are becoming wealthier. As many countries acquire greater economic strength, owing partly to cyberpower, they will acquire greater diplomatic and political influence, allowing them to pursue more assertive strategic agendas in their regions and beyond. Mastery of modern networks will also enable some countries to acquire greater military strength by equipping their forces with tools for modern doctrine and operations, even without the expensive ground, air, and naval platforms used by the United States. The enhanced strategic clout of these countries may motivate them to seek greater influence in pursuit of their national interests.

Some countries might also pursue cyberpower as an offensive instrument of intimidation and coercion against neighbors and adversaries. As a strategic tool, cyberpower is attractive and advantageous because it can be acquired inexpensively and can be used in concert with other tools or on its own. It does not require expensive military forces to be influential and effective. Because cyberpower can provide poor countries with potential leverage that far exceeds their strength as traditionally assessed, the future may see a proliferation of cyber predators and of cyber victims too.

Since September 11, 2001, the public literature has commonly viewed major cyber attacks on the United States as most likely to be launched by terrorist groups, perhaps in combination with physical acts of destruction. Al Qaeda, Hamas, and Hizballah are seen as posing cyber threats, as are other terrorist groups that harbor grievances against the United States.[12] Nation-states are not yet widely feared as potential sources for such attacks, even though they are well situated to develop the tools needed to carry out sophisticated cyber attacks. Countries that are adversaries of the United States might decide to pursue this avenue in order to influence American diplomacy and military activity in their regions. Medium-sized powers that might use attacks or threats of attack as instruments of deterrence or compellence include Iran and North Korea; numerous other countries, especially across the greater Middle East, similarly view the United States as an adversary. Among the big powers, China is an obvious potential source of cyber danger. If it begins pursuing an assertive, anti-American agenda in East Asia, it might employ cyber threats or even attacks as strategic instruments. Russia also falls into this category because in recent years its government has become more authoritarian and its foreign policy more assertive and bullying. Its threats in 2007 and earlier to deny natural gas to its neighbors, such as Ukraine, suggests a growing willingness to employ techniques of coercion and intimidation that, as former Russian President Vladimir Putin said, could be expanded to include military power, including nuclear weapons, if Russia perceives a threat to its vital security interests.

A significant issue for deterrence is that because such cyber attacks can be launched largely in secret, the identities of the actors carrying them out often cannot readily be determined. For example, a cyber attack seemingly originating in China might have been launched by the Chinese government, by some unofficial group of hackers in China or elsewhere, or by terrorists in the Middle East who disguise their identities. The alleged but ambiguous Russian cyber attack on Estonia is another obvious example.[13]

Although attribution will remain a serious problem, the fear that the attribution problem wholly cripples any hope of detection and deterrence is misplaced. Many, if not most, big cyber threats or actual attacks on the United States, its military forces, or its allies are not likely to be conducted in a political vacuum. Rather, they will be conducted with an explicit political or strategic goal: as a means to an end rather than an end in themselves. They are most likely to be conducted to exert pressure, intimidation, and coercion on the United States to induce it to acquiesce in the larger agenda being pursued by the attacker. Such an attacker likely would not want to conceal its identity, because that would prevent delivery of the message and thereby dilute prospects for an acquiescent response. How could the United States be expected to buckle to such coercion if it is unable to determine the identity of the attacker and the concessions it is seeking? If the attacker makes its identity known in order to pursue its larger political and strategic agenda, it opens itself to U.S. deterrent mechanisms and retaliatory steps.

Beyond this, a U.S. cyber deterrent strategy would be a construct meant to be applied not only during actual crises, but in peacetime as well. The U.S. preparedness agenda during peacetime merely mandates that it knows the nation-states and other actors that could launch cyber attacks in future crises. Knowledge of potential future adversaries does not require real-time crisis attribution, and it could suffice to help the United States develop many core ingredients of a cyber deterrence strategy aimed at them. During the Cold War, after all, the United States possessed enough evidence of the Soviet Union's potential uses of military forces in a war to justify, in the American government's mind, creation of a deterrent strategy against the Soviet Union even though that country restrained itself from committing actual aggression. The same logic can apply to potential future cyber attackers. Yes, the United States needs concrete attribution to launch retaliatory measures in an actual crisis, but in developing peacetime cyber deterrence mechanisms and plans, its standards of proof of culpability are less demanding. It merely must decide who the potential sources of cyber attacks are, and how to pursue its deterrence agenda accordingly.

Illustrative Crisis Scenarios

Credible prospects for determining attribution of responsibility during many actual cyber attacks can be illuminated by illustrative scenarios. In the first hypothetical scenario, Iran threatens or actually uses cyber attacks to advance its interests in the Middle East, seeking to compel U.S. military withdrawal from the Persian Gulf, to assert control over the Strait of Hormuz, or to intimidate Saudi Arabia and Israel. Such an Iranian effort would not be limited to cyberpower: instead, cyber threats or attacks would probably be part of a larger campaign that would employ other instruments, such as use of declaratory policy, diplomacy, or military forces, or control of access to oil. In this scenario, the Iranian government might try to conceal its identity as a cyber attacker, but equally plausible, it might openly threaten use of cyber tools in order to strengthen its leverage and bargaining power. Even if the attacker tried to conceal its identity in the cyber realm, the source of its cyber attacks probably would not be formidably difficult to determine. Intelligence information about attacker identities can be gathered from sources beyond the cyber activities themselves: the strategic context would reveal a great deal about the attacker, and U.S. officials would be able to use technical data, all-source intelligence, and logical inference.

The second illustrative scenario is that of a North Korean effort to intimidate the Republic of Korea (ROK) into making major concessions, or even to set the stage for a military invasion of the ROK. North Korea might, for example, launch cyber attacks on the United States, Japan, and South Korea in an effort to gain leverage over all three countries. Such cyber attacks would not be conducted in isolation of other events, but would be part of North Korea's overall efforts to use diplomacy, its possession of nuclear weapons and missile delivery systems, its conventional military power, and other instruments at its disposal. If North Korea intended to conduct a military invasion of South Korea, its cyber attacks might try to blind ROK forces, delay the deployment of U.S. reinforcements from the continental United States, and degrade the combat effectiveness of U.S. military forces. Here too, North Korea might not want to conceal its identity as a cyber attacker, but might choose instead to broadcast it clearly in order to strengthen its leverage and bargaining power. Even if it tried to conceal its identity, the source of its activity in the cyber realm most likely could be determined. In such a crisis, it is unlikely that any other potential cyber attacker would choose this particular pattern of activity.

A third scenario is a hypothetical East Asian crisis in which China seeks a showdown over Taiwan in order to intimidate or even to conquer it. In such a crisis, China might resort to major cyber attacks directed against the United States, Taiwan, and Japan. Its cyber attack on the United States might be intended to deter Washington from intervention in the crisis, to prevent it from deploying air and naval reinforcements to the area, and to prevent U.S. military forces from defending Taiwan and from attacking China in event of hostilities. Here again, China's cyber attacks would not be conducted in isolation, but would be a component of its overall strategy and use of its political, diplomatic, and military power. China would have no special incentive to conceal its cyber identity at a time when it is provoking a grand showdown over Taiwan and the future of the entire East Asia security order. Instead, it would be more likely to make its cyber identity known to all of its adversaries in order to enhance its leverage over them. Even if it sought to conceal its cyber identity, it would not have much hope of success under the prying eyes of U.S. all-source intelligence.

As these three scenarios suggest, in the event of major cyber attacks by nation-states on the United States, attribution during crises might be less of a crippling problem than it is commonly presumed to be. Some cyber attacks by terrorists might also fall into this category. To be sure, some terrorist attacks might be conducted purely for vengeance and destruction and there- fore might not be directly linked to a specific political-strategic agenda that would motivate the attackers to proclaim responsibility for their actions, or that would make them obvious suspects. Yet even terrorist groups tend to have explicit political agendas such as, for example, driving the United States out of Iraq, Afghanistan, or the entire Middle East. Such an agenda could not be readily pursued by leaving the United States blind to the cyber attacker's strategic intent and demands and thus to its identity. The bottom line is that, while attribution will remain a problem that mandates development of better technical capabilities, many potentially big cyber attacks on the United States are likely to arise out of a specific strategic context, aimed at concrete goals such as altering U.S. foreign policy and defense strategy, and therefore will be possible to attribute to specific attackers. Cyber attacks of this sort fall into the category of events that can be treated by the familiar logic of deterrence.

What the United States must avoid is a crisis situation in which it is confronted by a potential or actual cyber attacker whose identity is known, but for whom the American government does not already possess a well-conceived deterrent strategy showing how it can best respond. In such a situation, the United States could be compelled to resort to improvisation, but without the time to think through the details of response mechanisms or to make the necessary preparations. As a result, it might act incorrectly or weakly in ways that produce serious reversals. By drawing upon deterrence theory, whose components are discussed below, it can reduce the dangers arising from such crisis situations and from cyber threats more generally.

Contributions from Deterrence Theory: Past and Present

What would an effective cyber deterrence theory require? A simple answer would be: strong defenses that can rebuff cyber attacks, and potent cyber offenses that can inflict massive retaliatory damage in return. Such a capability-based approach would presume, however, that cyber wars would occur in isolation from larger surrounding events and could be treated as self-contained, subject to their own logic and requirements. However, the greater likelihood is that many major cyber attacks are likely to appear as one instrument among several aimed at achieving political and strategic goals, not just inflicting damage for its own sake. They would be intended as instruments of bargaining and coercion, to deter the United States from taking actions the attackers do not want, or to compel the United States to acquiesce in the attackers' political-strategic agendas. Dealing with cyber attacks of this sort requires not just offensive and defensive capabilities to deter them in some mechanical sense; it requires, above all, the capacity to influence the motivations and psychology of the attacker, as well as a capacity to integrate U.S. cyber responses—defensive and offensive—with other instruments of national power and crisis response. For these reasons, the issue of cyber deterrence strategy cannot be separated from the rest of U.S. national security policy.

Deterrence during the Cold War

The ingredients for constructing a cyber deterrence strategy can be illustrated by briefly reviewing how deterrence operated during the Cold War and how it operates today. To be sure, the experience of the Cold War cannot be grafted onto the different realities of today, including in the cyber realm. Even so, the process by which Cold War deterrence theory was adopted—for example, awareness of the larger strategic context and adversary motives, the systematic creation of clear strategic concepts, the evolutionary development of new requirements as events changed, and the careful efforts to assemble capabilities that fulfilled these requirements—provides lessons that can be adopted if a credible cyber deterrence strategy is to be built today.

The concept of deterrence first emerged during the 1950s, when the Cold War with the Soviet Union was heating up and rapidly acquiring military components. Some observers, in hindsight, view Cold War deterrence strategy as largely shaped by the U.S. effort to build nuclear offensive forces that could inflict massive retaliation in response to a Soviet nuclear attack on the United States. This is an oversimplification: deterrence was embedded in a more nuanced approach that was entirely focused neither on military nor nuclear calculations. As it evolved during the 1950s and beyond, deterrence became anchored in political calculations aimed at influencing Soviet motivations, underpinning U.S. national defense strategy in Europe, and controlling nuclear escalation. It was isolated from neither larger strategic considerations nor the need to deal with the Soviet adversary in political terms.

Deterrence theory first appeared as part of the West's containment strategy in Europe, which aspired to keep the Soviet Union confined to Eastern Europe and to prevent it from gaining control of Western Europe. When the United States and its European allies created the North Atlantic Treaty Organization (NATO) in 1949 to strengthen their defense capabilities for countering Soviet forces, their new alliance faced a precarious imbalance of military power in Central Europe. The Soviet Union commanded a massive army that was permanently stationed in Eastern Europe, with easy access to exposed West Germany. NATO, by contrast, was able to field only a few combat divisions and air wings. It therefore turned to America's growing fleet of strategic bombers, built to carry nuclear weapons. If the Soviet Army invaded Western Europe with the intent of driving to the English Channel, the United States could launch a devastating nuclear attack not only on Soviet military forces, but also on the Soviet homeland itself. In the mid-1950s, this strategy was, in fact, based on massive nuclear retaliation, but it was not aimed at responding to a nuclear attack on the United States: although the Soviets possessed nuclear weapons, they had few long-range bombers capable of intercontinental attack. The strategy was aimed at deterring conventional attack on Western Europe by convincing the Soviet government that an invasion would not succeed and that the Soviet Union faced unacceptable risks: if it made such an attack, it would suffer losses that far exceeded any benefits that it might hope to gain.

Even at this early stage, then, deterrence theory did not exist in a political vacuum: it took account of the motives and risk-taking propensities of the adversary. Deterrence theory presumed that the Soviet Union would act rationally in a crisis, that it would be motivated by self-preservation as well as cost-benefit calculations, and that it would not launch a war in which it would inevitably suffer devastating losses. Moreover, deterrence theory, as well as the containment doctrine that was its umbrella political rationale, cautioned the United States to be careful not to threaten an unprovoked western offensive aimed at dislodging the Soviet Union from its stranglehold control over Eastern Europe. As a result, the U.S. deterrence strategy offered the Soviet Union a dual rationale for exercising restraint: whereas military aggression would result in punishing losses, maintaining the peace would allow the Soviets to preserve their principal gain from World War II, their strategic buffer in Eastern Europe. Containment and deterrence thus offered the Soviets a political and strategic bargain. They could retain de facto control of Eastern Europe if they kept their military hands off Western Europe, but if they invaded Western Europe, they would lose both Eastern Europe and their own homeland to nuclear destruction. As events would show, the Soviets were prepared to accept this bargain, and peace was preserved during a period of intense political rivalry and ideological incompatibility that easily could have erupted into full-scale war.

The U.S. deterrence strategy began to change in the 1960s. The Soviet Union started to deploy nuclear-tipped intercontinental ballistic missiles (ICBMs) that could reach U.S. targets within 30 minutes, destroying the U.S.-based bomber force on the ground. This could undermine the precarious logic of deterrence by diminishing the threat that the Soviets would face nuclear punishment if they invaded Western Europe. The United States therefore embarked on an expensive effort to deploy a large force of ICBMs and submarine-launched ballistic missiles (SLBMs) that could survive a surprise Soviet missile attack. The goal was to create a survivable second-strike retaliatory force so as to restore the credibility of retaliatory deterrence.

At the same time, the United States began backing away from its earlier emphasis on massive retaliation in the form of all-out nuclear obliteration of the Soviet Union. A main reason was that, as the Soviets deployed a survivable, second-strike missile force of their own, the United States could not hope to disarm them in a surprise attack. Mutual nuclear vulnerability had arrived. The United States therefore began crafting new nuclear warfighting doctrines that contemplated limited nuclear strikes in the early stages of a war but sought to control subsequent escalation. The threat of nuclear retaliation remained the backbone of deterrence, but ideas for actually waging nuclear war were now developed, along with theories of limiting escalation. The goal would be to halt fighting by political means before the two countries had obliterated each other.

American nuclear theorists therefore outlined a so-called “ladder of escalation” to guide how the United States should prepare to fight at each “rung,” so as to offer multiple options and flexibility and avoid domination by the Soviet Union at any step. It postulated that the escalatory process would be characterized on both sides by strategic intentions and political bargaining: each side would employ military strikes to coerce the other into submission to its political objectives. The goal of climbing the ladder gradually and purposefully was to compel the other side to back down, while keeping escalation from spiraling out of control and resulting in massive devastation on both sides. Whether an actual military conflict would have conformed to this hypothetical ladder is uncertain. Many critics doubted that the escalation process, once started, could be controlled at all, let alone in finely tuned ways, but U.S. strategy endeavored to do everything possible to bring escalation under control.

As Cold War deterrence theory matured, it was accompanied by efforts to define its military requirements and to pursue the defense programs mandated by them. In preparing its nuclear offensive forces, the United States created a "triad doctrine" in the 1960s and 1970s. The triad doctrine specified that the U.S. force posture should be composed of three legs—1,000 ICBMs, 656 SLBMs carried by submarines, and about 350 B–52 strategic bombers—each of which could survive a surprise attack and retaliate with sufficient force to devastate Soviet urban areas, so as to deter any Soviet inclination to wage a full-scale nuclear war. Beyond this, the quest for flexibility and options led to decisions to equip all three legs of the triad with accurate warheads that could be used against a range of targets other than cities. As a consequence, the U.S. triad eventually was armed with 12,000 warheads or more, enough to meet almost any need for strike options and target coverage. Meanwhile, the Soviet Union deployed its own version of a triad.[14]

While nuclear forces could deter nuclear attack, they could not reliably deter a conventional attack because the Soviets might judge that if NATO found its conventional defenses buckling, it would not risk nuclear escalation even to save Western Europe.[15] In 1967, therefore, NATO adopted a strategy of forward defense and flexible response that mandated a stronger conventional defense posture. During the 1970s and 1980s, the United States and its European allies invested major sums in conventional defenses. The Cold War ended with Western nuclear and conventional forces stronger than ever, with deterrence solidified, and with the Soviet Union facing bankruptcy partly due to its huge investments in a military buildup that brought fruitless strategic returns.

Cold War Lessons

Deterrence was a risky proposition during the Cold War, but it worked: major war with the Soviet Union was averted, and Western security was safeguarded. It worked for reasons that yield lessons for cyber deterrence. First, it worked because it was credible, and because the United States made efforts to maintain, improve, and adjust it. Second, nuclear war was not viewed in isolation from larger events, but took into account the political and diplomatic motivations of both sides. Third, U.S. deterrence strategy denied the Soviet Union any favorable prospects from aggression, while offering it reasons to conclude that remaining at peace with the West was preferable to war. As deterrence theory matured, it balanced the need of warning the adversary against the imperative of minimizing the risks of unwarranted escalation. Its emphasis on flexibility and options allowed it to respond to a range of situations. Its success was also due to the fact that the United States and its NATO allies took care to meet its military requirements, and because it was crafted to protect not only the United States, but vulnerable allies as well.

All of these lessons provide valuable insights for thinking about deterrence today, including cyber deterrence. The general principles it yields for the contemporary era include the need for focus on the political motivations and risk-taking propensities of potential adversaries, for credible deterrent mechanisms that will work even under great stress, for well-integrated capabilities that are guided by carefully crafted deterrence doctrines and that address the spectrum of challenges likely to be confronted, for flexibility and options, for integration of doctrines of retaliation and compellence with the necessity to control escalation, and for policies that protect allies along with the United States.

Modern-day Problems

What are the implications of contemporary nuclear deterrence theory for deterring cyber attacks? Deterrence theory today continues to focus on influencing the motivations and aspirations of potential adversaries by persuading them that aggression cannot succeed. The principal target of U.S. deterrence strategy has switched, however, from the defunct Soviet Union to rogue countries, terrorists, and other adversaries that menace U.S. and allied interests. While the strategy still is aimed at nuclear attacks and big conventional invasions, such as a North Korean attack on South Korea, it also seeks to deter lesser provocations, including terrorism. This emphasis on multiple adversaries and provocations has given rise to the concept of "tailored deterrence":[16] deterrence must take into account the specific predilections of each individual adversary and its conduct. The U.S. nuclear triad is now composed of offensive forces, defensive forces, and infrastructure. Today, bombers and missiles carrying precision conventional (nonnuclear) warheads figure importantly in the deterrence equation. The entire

U.S. conventional military posture is viewed as a major contributor to deterrence, as well as to the other key activities, spelled out in the National Defense Strategy, including assurance of allies, dissuasion of potential rivals from competitive provocative conduct, and defeat of adversaries in wartime.

Since the Cold War ended in 1990, deterrence has continued to work in some places but seems to have failed in others. It failed to prevent Iraq from invading Kuwait in 1990, Serbia from invading Kosovo in 1999, or al Qaeda from using Afghanistan to launch its attack on the United States in 2001. Deterrence has not prevented North Korea and Iran from pursuing nuclear weapons, nor has the presence of large U.S. military forces in Iraq and Afghanistan prevented adversaries from waging guerrilla wars aimed at destabilizing both countries.

Such problems have led many observers to conclude that deterrence theory is inadequate against present-day U.S. adversaries that range from rogue countries to terrorists. Is the problem that the United States does not have a properly conceived deterrence theory, or is it that today's adversaries are more willing to take dangerous risks, and pay heavy prices, than was the Soviet Union during the Cold War? If the success of deterrence could be taken for granted during the Cold War, it cannot be taken for granted today. It has become a variable, not a constant, in the strategic equation. Some threats are harder to deter than others. Recognition of this disturbing reality makes the task of designing an effective cyber deterrence strategy both more necessary and more difficult.

Towards a General Model of Tailored Cyber Deterrence

Given the troubled track record of recent years, can deterrence—including cyber deterrence—be accomplished against multiple potential adversaries with assertive agendas? Some observers argue that modern-era aggressors cannot be deterred, on the grounds that they are not rational: that they are not influenced by the same cautionary mechanisms that motivate normally sensible actors. However, *rationality* is a relative term: while some of today's actors may not be rational by U. S. standards, this does not mean that they are wholly irrational.

Although they may perceive high potential payoffs in a confrontation with the United States, and this may lead them to think and act boldly, they are not necessarily oblivious to potential damage and the pain that they may suffer in return. Even today's actors with malevolent agendas tend to be governed by explicit motives, goals, and awareness of costs and risks. This is certainly true of nation-states, and it also applies, to varying degrees, to nonstate actors. Even terrorist groups are motivated not just by ideology and hatred, but also by strategic goals and self- preservation. The decision calculus of such actors may be influenced by U.S. deterrence mechanisms, even cyber deterrence. Cyber attacks are often regarded as not deterrable because they are "free rides"—the attacker has an expectation of impunity—but this calculus could be changed by creating expectations that cyber aggression might be an uncertain or costly act.

No cyber deterrence strategy can hope to be airtight to prevent all minor attacks. However, a strategy can increase the chances that major cyber attacks can be prevented; this could protect the United States and its allies not only from a single major attack but also from serial cyber aggressions and resulting damage. A worthwhile goal of a cyber deterrence strategy would be to transform medium-sized attacks into low-probability events and to provide practically 100 percent deterrence of major attacks.

A cyber deterrence strategy could contribute to other key defense activities and goals, including assurance of allies, dissuasion, and readiness to defeat adversaries in the event of actual combat. The goal of dissuading adversaries is crucially important. Thus far, the United States has not been noticeably forceful in stating its intentions to deter major cyber attacks and, if necessary, to respond to them with decisive force employing multiple instruments of power. Meanwhile, several countries and terrorist groups are reportedly developing cyber attack capabilities. Dissuasion of such activities is not an easy task: it requires investment in technical capabilities as well as building an internal consensus to employ these capabilities. If some of these actors can be dissuaded from entering into cyber competition with the United States and its allies, the dangers of actual cyber aggression will diminish.

How would a cyber deterrence strategy operate, and how can its potential effectiveness be judged? Deterrence depends on the capacity of the United States to project an image of resolve, willpower, and capability in sufficient strength to convince a potential adversary to refrain from activities that threaten U.S. and allied interests. As recent experience shows, deterrence can be especially difficult in the face of adversaries who are inclined to challenge the United States and otherwise take dangerous risks. In cases of failure, deterrence might well have been sound in theory but not carried out effectively enough to work. The aggressions of Saddam Hussein, Slobodan Milosevic, and al Qaeda might not have been carried out had these actors been convinced that the United States would respond with massive military force. These aggressions resulted because of a failure to communicate U.S. willpower and resolve, not because the attackers were wholly oblivious to any sense of restraint or self-preservation, nor because the logic of deterrence had lost its relevance.

A general model of cyber deterrence provides a strategic framework for thinking about tailored deterrence. Such a model is the DOD JOC for deterrence operations, which emphasizes employing instruments of deterrence to affect not only the physical capacities of potential adversaries, but their psychology and motivations as well. The model specifies ends, ways, means, and analytical procedures.

Ends, Ways, and Means

The goal of a cyber deterrence strategy would be to influence an adversary's decisionmaking calculus so decisively that it will not launch cyber attacks against the United States, its military forces, or its allies. Coordinated actions reduce the chances for attacker success, so that the dangers, costs, risks, and uncertainties of a cyber attack are perceived to outweigh any expected success, benefits, or rewards. In the case of an adversary who seeks to use threats of cyber attacks, or actual attacks, to coerce the United States into conduct that would serve its larger interests and goals, a cyber deterrence strategy will work if the adversary judges that this attempted coercion would not succeed and that the attack would provoke U.S. retaliation, resulting in a net strategic setback for the would-be attacker. For example, if Iran were to contemplate cyber attacks to try to coerce the United States into making political concessions in the Persian Gulf and Middle East, it might be deterred from this course if its decisionmakers were to judge that the cyber attack would not physically succeed in inflicting the desired damage; that even if the attack succeeded, the United States would not make the desired concessions; or that the United States would be likely to retaliate in ways that inflict unacceptable damage on Iran in return, in the cyber realm or elsewhere.

The same strategic calculus applies to Chinese use of cyber threats and attacks, as well as actions by other plausible adversaries in the cyber domain. Potential U.S. counteractions in such situations are encapsulated in the three principal ways of pursuing deterrence articulated in the JOC model: deterrence by denying benefits, deterrence by imposing costs, and deterrence by offering incentives for adversary restraint.

Deterrence by denying benefits entails credibly threatening to deprive the attacker of the benefits or gains being sought: convincing it that a cyber attack will not achieve its goals. Deterrence by imposing costs entails credibly threatening to impose costs, losses, and risks that are too painful to accept, thus convincing the adversary that punishment would outweigh any expected successes. Deterrence by encouraging restraint means convincing the adversary that not attacking will result in an acceptable, attractive outcome.

These three deterrence mechanisms can be employed singly, but they are likely to work best when they are combined in mutually reinforcing ways. Potential cyber adversaries may not be unitary actors dominated by a single strategic calculus; decisionmaking may be influenced by multiple actors, such as different parts of a foreign government or terrorist network, that have differing priorities and tolerance for risk. Together, these three mechanisms can influence multiple actors in different ways and to different degrees, enhancing the prospects that the decision will be to reject cyber attacks.

Deterrence by denial or by imposing costs can, in principle, both be carried out purely within cyberspace. For example, the United States could seek to deter cyber attacks both by building strong cyber defenses and by employing cyber offensive capability for retaliatory attack on the information networks of the adversary. This narrow focus may not, however, be appropriate for most strategic confrontations in which cyber attacks are used to pursue larger political and strategic objectives. In such cases, the U.S. strategic calculus of cyber deterrence will need to be broader, too. Efforts to deny benefits will need to focus not only on protecting U.S. cyber networks, but also on ensuring that cyber attacks, even if physically successful, could not compel the United States into making the political concessions being sought. In other words, U.S. cyber defenses must be not only technical but strategic as well.

The same calculation applies to deterrence by imposing costs: the United States might choose to retaliate purely in the cyber realm by taking down enemy information networks, but it can maximize deterrence by applying a full set of other mechanisms—political, diplomatic, economic, and military— to increase the strategic pressures, costs, and risks to adversaries. Indeed, these other instruments may be more potent than cyber retaliation against adversaries that lack sophisticated information networks and thus would not be especially bothered by cyber counterattacks. Retaliatory options must be more than purely cyber; they should be multifaceted and strategic in character.

Encouraging adversary restraint necessitates sophisticated handling of strategic confrontations and crisis management. As a general proposition, cyber deterrence will not work if the adversary is faced with the imminent prospect of total defeat and destruction regardless of whether it launches a cyber attack. For example, a rogue country faced with the imminent prospect of U.S. invasion and conquest has little incentive to refrain from a cyber attack, while it has many incentives to launch one in order to deter, hamper, or exact retaliation for a

U.S.invasion. Such an adversary has something to gain and nothing to lose by pursuing offensive cyber warfare. An adversary that may judge itself better off by refraining from cyber warfare, even if it is involved in strategic rivalry, competition, or outright warfare with the United States, can be deterred. Just as deterrence theory during the Cold War required the United States to contemplate how to give the Soviet Union better options than initiating or escalating a nuclear war, cyber deterrence theory requires awareness of adversary interests, and offering adversaries more attractive options than engaging in a mutual effort to destroy each other's information networks and infrastructures. This will be easiest where strategic conflicts are limited and subject to diplomatic resolution. It will be harder to carry out with implacable adversaries that are pursuing duels to the death with the United States.

A cyber deterrence strategy will also need to be aware of thresholds. Cyber attacks can come in many different shapes and sizes, and they will not all merit the same response. Some attacks may be too minor to worry about. Others may merit a retaliatory response, but the degree of that response will depend upon the degree of provocation.

What about the means—the instruments—for pursuing cyber deterrence? A cyber deterrence strategy aimed at handling multiple threats and differing situations cannot rely primarily on any single instrument. It must be able to employ multiple instruments that offer a wide range of response options, that can be packaged and repackaged to serve the specific goals being pursued, and that allow the United States to deal with dynamically evolving situations of complexity. Multiple instruments might be used singly or in combination. Single instruments may be effective against weak adversaries, but multiple instruments are likely to be needed against ambitious, assertive opponents. For each situation, the instruments of retaliation must enable the United States to act credibly and powerfully.

Both cyber defenses and cyber offenses are part of deterrence strategy, but they are not the whole solution or even the most important component of it. In some situations, U.S. cyber defenses may be ineffective, but the United States might choose not to respond with a cyber counterattack. The most effective response to some cyber attacks may be political and economic, perhaps isolating the attacker from the global community, mobilizing nation-states to treat it as a pariah, or imposing economic sanctions. These could inflict more painful penalties than any cyber counterattack. U.S. military strikes might even be carried out, perhaps in retaliation for a truly devastating attack on U.S. information networks, or as part of major combat operations against enemies. Much depends on the identity of the attacker, the nature of the potential attacks, and the nature of a proper response. The United States needs to be able to respond flexibly, to have a portfolio of options that provide adaptability, and to be capable of employing multiple instruments in whatever combination makes best sense for the situation at hand.

Analytical Procedures

The general deterrence model, as derived from the JOC on deterrence operations, offers six analytical steps for pursuing each case of cyber deterrence in peace, crisis, and war:

1. specify the deterrence objectives and the strategic context
2. assess the strategic calculus of adversary decisionmakers
3. identify desired deterrence effects on adversary conduct
4. develop and assess courses of action designed to achieve desired effects
5. develop plans to execute deterrence courses of action and to monitor and assess adversary responses
6. develop capacities to respond flexibly and effectively as the deterrence situation evolves.

These six steps reflect the demands and challenges of achieving tailored deterrence of cyber attacks. Tailored deterrence recognizes that U.S. goals and objectives may vary considerably from one situation to the next, necessitating different types of responses. Thus, step 1 defines U.S. purposes for cyber situations. Step 2 recognizes that, because not all adversaries are the same, the United States must specify the adversary being encountered, the strategic context of the encounter, and the decision calculus being employed by the adversary. Each of the three types of adversaries likely to be faced—near-peer rivals, middle-sized rogue countries, and terrorist groups—would bring different psychologies and motives to confrontations with the United States, as well as different attitudes toward goals, stakes, actions, perceptions of U.S. willpower and resolve, risk-taking propensities, and handling of uncertainties.

Steps 3 and 4 are both critical and challenging. Step 3 entails identifying the desired effects of deterrence on adversary conduct; in step 4, then, courses of action to produce these effects are developed and assessed. Generally, when deterrence has succeeded in the past, the United States was skillful at identifying how its courses of action would produce effects that could influence the motivations and behavior of adversary governments in the desired ways. When deterrence has failed, it was usually because the U.S. Government failed to assemble a portfolio of declaratory policies and actions that strongly influenced the perceptions and motives of the adversaries. In these cases, the problem was not that the United States was blind to the need to send strong deterrence signals, but that it sent the wrong signals, which failed to have the desired effects because they did not credibly signal the will and the capability of the United States.

Because many cyber attack situations will be part of larger geopolitical confrontations, determining how to send credible cyber deterrence signals will entail carrying out multiple actions that, in turn, will need to be embedded in broader U.S. activities aimed at achieving other purposes. When the United States acts weakly in the eyes of adversaries, it may unintentionally signal that cyber attacks can be carried out with impunity or will not be met with a decisive response. However, when the United States acts powerfully in handling a larger crisis that goes beyond the cyber realm, it could risk burying its cyber deterrence signals in a plethora of other activities, thus leading the adversary to overlook or misinterpret them. Beyond this, U.S. actions that powerfully influence one set of adversaries may have little impact on other adversaries, who might be influenced by an entirely different set of measures. For some adversaries, a simple warning might be deterrent enough; for others, a cyber response, or powerful use of other instruments as well as a cyber response, might be appropriate. For some, however, the only effective response might be the use of military power or other non-cyber instruments. For such reasons, cyber deterrence requires that the United States develop its skills in figuring out how to influence each adversary and how to act accordingly.

Step 5, developing plans, and step 6, developing capacities (discussed below), are also important. Plans determine the crucial details of how multiple instruments are to be blended together in a cyber crisis; they also reduce the risks of serious errors in judgment if complex actions had to be cobbled together on the fly. Execution plans are needed for precrisis situations and the initial stages of actual crises, and also for the various stages in which a cyber crisis might unfold, such as a small probing cyber attack, a larger but still limited attack, and so on up the ladder of escalation. This cyber escalation, in turn, might be part of a sequence of political and military steps aimed at bringing pressure on the United States. Thus, a cyber deterrence strategy needs to master the ladder of cyber escalation as well as the other ingredients of cyber crisis management.

Tailored cyber deterrence requires more than realizing that potential adversaries will differ from each other, will harbor different perceptions and motivations, and will employ cyber attacks with differing agendas in mind. It also requires realizing that U.S. goals and objectives will vary from one adversary and situation to the next, that diverse responses may be needed in order to have different types of effects, and that crisis response plans must provide the capacity to act both strongly and effectively. Many cyber attacks will not occur in a vacuum, but instead will arise in a larger context that necessitates multiple U.S. responses in addition to those aimed at ensuring cyber deterrence. Because each cyber situation is likely to be unique, applying tailored deterrence to the cyber domain promises to be complex and challenging.

Strategic Requirements for Cyber Deterrence Assets and Capabilities

Because a cyber strategy of tailored deterrence must deal with diverse threats, multiple assets and capabilities will be needed. This necessitates a persistent, wide-ranging U.S. Government effort. Key requirements and priorities for achieving an effective capability to carry out a cyber deterrent strategy include:

- a clear and firm declaratory policy spelling out the U.S. intention to deter cyber attacks
- high global situational awareness that is attuned to the full spectrum of potential cyber threats and the circumstances in which they might arise
- good command and control systems that permit coordinated multiregional and homeland responses to cyber threats
- effective cyber defenses that protect both U.S. military forces and the U.S. homeland with a high priority for defending key infrastructure
- a wide spectrum of counter–cyber offensive capabilities, including cyber attack and other instruments for asserting U.S. power in order to enforce deterrence before, during, and after crises
- well-developed U.S. interagency cooperation and collaboration with allies and partners including those in Europe, Asia, and elsewhere
- cyber deterrence methodologies, metrics, and experiments that can help guide the

planning process.

Each of these requisites of an effective cyber deterrence policy is examined in this section.

Strong Declaratory Policy

The goal of deterrence of cyber attacks is already stated in some official U.S. documents, but a case can be made for a stronger and clearer U.S. declaratory policy. A good place to present it would be in the next National Security Strategy. The declaratory policy should provide a credible, convincing explanation of why the United States takes cyber threats seriously, why it would regard a major cyber attack as potentially an act of war against it, and the intention of the United States to respond with decisive actions, possibly including force. The declaratory policy should leave no doubt in the minds of potential adversaries that any cyber attacks on the United States would fail to achieve their goals and that the attackers would suffer unacceptable costs, damages, and risks in return. A U.S. declaratory policy for cyber deterrence needs to be firm, but it also needs to be balanced, sending the right messages regarding possible responses to cyber attack and avoiding inflammatory statements that could contribute to escalation of cyber conflicts. The QDR of 2006 asserts that the deterrent posture should be capable of mounting an "overwhelming response." While this statement clearly is appropriate for major cyber attacks that could cause massive disruption, not all cyber attacks will fall into this category. Some might be smaller, yet still large enough to merit a U.S. response of some magnitude. Above all, the U.S. response should be tailored to the situation. Based on this principle, U.S. declaratory policy could endorse a cyber deterrence strategy of "tailored, decisive, and proportional response."

High Global Situational Awareness

Global situational awareness will be a key requirement for a cyber deterrence strategy. In particular, five types of knowledge are necessary: identification of potential cyber threats around the world, including state and nonstate actors; assessment of the motives, value structures, goals, perceptions, and calculations that different adversaries might bring to the use of cyber attacks, including attacks that are part of broader strategic campaigns aimed at damaging U.S. interests; appraisal of the calculations, judgments, and external pressures that might lead potential adversaries to refrain from launching cyber attacks; awareness of the cyber assets, capabilities, and vulnerabilities that potential adversaries might possess or acquire; and use of all-source intelligence for attributing the source of cyber attacks in crisis situations where attribution is possible.

Especially important for carrying out deterrence is situational awareness of the psychology and motivations that might lead potential adversaries to launch cyber attacks; their attitudes toward benefits, costs, and risk-taking propensities; and the calculations that might lead them to refrain from such attacks. This requires gathering intelligence on the adversaries and developing awareness of how U.S. deterrent actions might affect others' behavior in peace, crisis, or war. The U.S. Intelligence Community must be involved in gathering this information, and it must work closely with U.S. policy agencies in order to evaluate the likely consequences of various courses of action for convincing adversaries to exercise restraint by refraining from committing cyber aggression and from escalating in a crisis. Accurate intelligence on the cyber attack capabilities and activities of potential adversaries is also necessary, to gauge U.S. vulnerabilities, as well as adversary vulnerabilities to U.S. counteraction. Determining the identity of potential attacks requires both technical means and human sources of intelligence.

Effective Command and Control

Preparedness is critical to an effective cyber deterrence strategy and to crisis management. A cyber attack on the United States, especially during an ongoing regional crisis with strategic interests at stake, could impose significant demands on the U.S. command and control system. Simultaneously, the United States would need to orchestrate its cyber defenses at home, to employ counter–cyber actions against the adversary, and to coordinate its cyberspace activities with other instruments of power and actions to manage events that could be taking place anywhere in the world. Beyond this, the United States might have to coordinate its responses to two cyber adversaries at the same time. For example, multiple combatant commands within DOD would need to coordinate their actions, inside as well as outside of the cyber realm, along with homeland defense agencies, the national security interagency community, and U.S. diplomatic activity abroad. Improvements in this arena seem necessary.

Stronger Cyber Defenses

Cyber defenses capable of protecting U.S. information networks are needed both to reduce potential vulnerabilities to cyber attack and to help deter potential attackers. If adversaries conclude that cyber attacks cannot attain their goals of damaging U.S. information networks, they will be less inclined to incur the costs and risks of launching them. Many observers judge that the United States is too vulnerable to cyber attacks. This weakens U.S. hopes for effective deterrence. Improvements in U.S. cyber defenses are thus needed for both defense and deterrence.

The National Strategy to Secure Cyberspace of 2003 sought to foster a partnership between government and the private sector. It outlined five major priorities for strengthening U.S. cyber defenses, along with specific recommendations in each area, many of which remain current. First, it called for a national cyberspace security and response program, establishing the Department of Homeland Security as the main point of contact for cyberspace security efforts with industry. It recommended improvements to cyberspace analysis, warning, information-sharing, major incident management, and national-level recovery efforts.

As a second priority, it called for a program for reducing the national cyberspace security threat and vulnerability. Major recommendations included improved criminal prosecution of cyber attackers, the adoption of improved security protocols and more secure router technology for the Internet, and improved computer software security.

The third priority identified was a national cyberspace security awareness and training program. It recommended improved Federal, state, and local efforts to promote awareness of cyber security, education programs in elementary and secondary schools, and efforts to improve awareness by small businesses and home computer users regarding antivirus software and firewalls.

A fourth priority was to secure government cyberspace with Federal efforts to strengthen the security of computers, software, and information networks, coupled with parallel efforts by state and local governments.

The strategy called, fifth, for national security and international cyberspace security cooperation. Recommendations included improving counter–cyber intelligence and attribution capabilities as well as closer cooperation with foreign governments and multinational organizations in pursuing cyber security.

Preferential defense of the most crucial information networks is a high priority for enhancing cyber deterrence. Safeguarding the information networks of the U.S. military, along with U.S. Government information networks, is clearly critical. Priority efforts to safeguard networks that operate key areas of the domestic infrastructure make sense, too. An example is the electrical power grid, loss of which could have a cascading effect in damaging other key parts of the U.S. economy.[17]

Multifaceted Counter–Cyber Offensive Capabilities

Because America's defenses cannot realistically be made impregnable against major cyber attacks any time soon, creation of offensive retaliatory capabilities is an essential component of a cyber deterrence strategy. Retaliation could be needed to help deter "bolt-out-of-the-blue" attacks confined to cyberspace, or threats of cyber attack during periods of rising political tensions, or major cyber attacks during intense crises or actual shooting wars. Retaliation could take many forms. It could mainly take the form of cyber retaliation against an adversary's networks; this might be launched quickly after an attack began, or later if time is needed to identify the attacker or to create the proper conditions for acting effectively. Retaliation might also include diplomatic, political, or economic responses, or the use of military force. As a general rule, confrontations with adversaries that are strategic in nature, and are focused on regional security affairs elsewhere in the world, are especially likely to require a blend of retaliatory instruments that are embedded in a larger framework of U.S. actions and that extend well beyond the cyber domain.

A major challenge will be to tailor responses to help achieve the specific deterrence goals being sought. A cyber deterrent strategy will require developing a portfolio of capabilities and actions that can be combined to form effective offensive responses tailored to the situations at hand. This requires not only creation of physical capabilities but also development of a wide spectrum of offensive response plans to avoid the risks associated with improvising in a crisis.

Interagency Cooperation and Collaboration with Allies and Partners

A cyber deterrence strategy would be carried out in multiple domains, requiring careful coordination. Strong U.S. interagency cooperation is therefore needed, especially among the intelligence agencies, which are responsible for identifying cyber threats; the homeland security agencies, which handle domestic priorities; and the national security community, which handles external policies. Within the national security community, close cooperation between DOD and the State Department would be needed at home and abroad. The more such agencies collaborate, the stronger the cyber deterrence strategy will be.

Collaboration with allies and partners is also important. Because they are potentially vulnerable to cyber attacks, cooperation in pursuing a cyber deterrence strategy can help reduce their vulnerabilities, as well as the risk that threats of attack against them could be used by adversaries to pressure the United States to make strategic concessions. Multinational cooperation can also increase the pool of assets and capabilities that could be mobilized to deal with cyber attacks. Cooperation with European allies, which already is starting to take place, is especially important.[18]18 An issue worth examining is whether security collaboration for a cyber deterrence strategy can take place within NATO, which provides the best transatlantic institution for handling threats to its members. It could be argued that a major cyber attack against the United States or its European allies could qualify as an Article 5 contingency that would mandate a strong NATO response in the cyber realm or outside it. If such a judgment is reached, the likelihood of being able to employ NATO increases significantly, but much would depend upon the attitudes of Britain, Germany, France, and other major European allies. Multilateral collaboration with such key Asian allies as Japan, South Korea, and Australia also makes strategic sense. Indeed, collaboration for the purpose of creating a strong cyber deterrence strategy might help set the stage for pursuing broader Asian collective defense and security planning.

Metrics and Experiments

Development of analytical methods and metrics for assessment should be part of any effort to create a cyber deterrence strategy of tailored response. The essence of cyber deterrence—the ability to influence the motives and calculations of potential cyber attackers—requires subjective evaluations and qualitative techniques, but that does not mean that assessment is impossible. Analytical studies might endeavor to calibrate the likely deterrence effects of alternative strategies and capabilities on different types of potential cyber attackers and the situations in which their attacks might occur. Simulation exercises and other experiments could also help build usable knowledge.

Issues for Further Analysis

Efforts to develop an effective cyber deterrence strategy will require further analysis of a number of thorny issues, including developing declaratory policy for multiple audiences; providing better net assessments of adversary cyber capabilities and U.S. vulnerabilities; addressing the attribution problem; learning to deal with nonstate actors; addressing the threshold problem; dealing with intrawar deterrence and control of escalation; and providing extended deterrence coverage and dealing with attacks on third parties. This section briefly outlines each of these issues.

Declaratory Policy for Multiple Audience

During the Cold War, shaping declaratory policy was relatively easy because the United States was dealing mainly with one audience, the Soviet Union, whose motives and aspirations were relatively well known. In the current era, the United States will need to deal with multiple adversaries and wider audiences as it shapes a cyber deterrence strategy. These actors possess differing perceptions, motives, and calculations, and they are likely to be influenced by differing types of U.S. deterrent actions. Thus, the types of U.S. policies to deter one type of adversary may differ from those needed to deter another adversary, with varying degrees of soft and hard rhetoric or of positive incentives and punishing responses. This challenge cannot readily be solved by trying to fine-tune each public declaratory statement so that it somehow addresses all potential adversaries. Instead, the United States will need to use a combination of public and private diplomacy to convey tailored, focused messages to each adversary. Doing so will require Washington to develop a better capacity to communicate with foreign audiences, a challenge that applies to many issues far beyond the cyber realm.

Providing Better Net Assessments of Capabilities and Vulnerabilities

An essential issue is knowing how capable adversaries are of launching major cyber attacks and how vulnerable the United States is to such attacks. Many observers postulate that multiple actors are developing expert attack capabilities in this arena, and that U.S. information networks are highly vulnerable to them. Embracing this assumption is a prudent response to an issue clouded by many technicalities. However, the fact that the United States has not yet been subjected to a major crippling cyber attack may indicate that adversary capabilities and

U.S. vulnerabilities are not so great as many fear. Further analysis of this issue is needed because it affects not only future threats, but also how future U.S. cyber deterrence strategy and response options should take shape. During the Cold War, U.S. deterrence strategy did not fully take shape until sophisticated net assessments of the nuclear and conventional military capabilities of both sides had been done. For example, a combination of static techniques and dynamic computer models helped shed analytical light on both nuclear competition and the conventional military balance in Europe. Comparable analyses of capabilities and vulnerabilities in the cyber domain will be needed for a mature and effective U.S. cyber deterrence strategy.

Addressing the Attribution Problem

Earlier, this chapter argued that the perpetrators of many major cyber attacks would likely be identifiable through use of all-source intelligence and strategic reasoning. While this judgment suffices to justify initial efforts to establish a cyber deterrence strategy, it does not mean that we can ignore the critical need to develop better technical attribution capabilities so that the sources of all attacks can be identified. In the cyber realm, attribution is far more difficult than in the realms of nuclear and conventional forces. Perhaps this problem will lessen as better technical means are developed, and as the United States becomes better at employing all-source intelligence to sort out the identity of attackers promptly. Pursuing improved capabilities in this arena is a high-priority goal.

Learning to Deal with Nonstate Actors

Although nation-states seem likely to be the main source of major cyber attacks on the United States, major or minor attacks might also come from nonstate actors, such as al Qaeda, Hamas, Hizballah, and other terrorist groups, or ethnic groups and other political actors whose memberships cut across state boundaries. Their motives and aspirations could be quite different from those of nation- states: they might be more influenced by ideology and anger, and they might be more willing to take risks and to engage in provocations. Whether such groups can be deterred from employing cyber attacks is an open question, but it is not a hopeless proposition: they will typically be pursuing political agendas in order to advance their interests, and they will therefore be vulnerable to counterpressures. In order to carry out a tailored cyber deterrence strategy, the United States will need to learn how to influence such actors. Further research and analysis in this area are an important requirement.

Addressing the Threshold Problem

Cyber attacks can range from small attacks that cause minor damage to very large attacks that can inflict massive damage. It is hard to point to any specific threshold of potential cyber damage below which U.S. strategy should discount an attack, but above which an attack should trigger concern for deterrence, coupled with the possibility of retaliatory response. The ladder of escalation contains many rungs of ascending provocation and damage, each of which could merit a response, of increasing intensity. A U.S. cyber deterrence strategy might be shaped to identify decisive, proportional responses at each rung of the ladder, rather than trying to specify a single threshold that separates nonresponses from strong responses.

Dealing with Intrawar Deterrence and Control of Escalation

While deterring the launching of cyber attacks is a critical imperative, equally important is deterring escalation once a cyber conflict has begun. Some adversaries, for example, might start with a small attack and then gradually scale up to the point at which the United States comes under intense pressure to buckle to the attacker's wishes. Such escalation could happen if U.S. responses at the low rungs of the escalatory ladder are not strong or decisive enough to convince the adversary to desist. If control of cyber escalation is lost, major damage could be inflicted on the United States and its allies. To a degree, this risk can be reduced by preferential defenses aimed at thoroughly safeguarding critical military and governmental networks and by building redundancy into other important networks whose temporary loss could be a calamity. Even so, taking steps such as offensive countermeasures and otherwise holding enemy targets at risk to discourage adversaries from escalating seems likely to be critically important. While no rules exist that guide cyber escalation, a balance will need to be continually struck between responding too lightly, in ways that do not persuade the enemy to desist, and responding too harshly, such as with a massive U.S. retaliation that might provoke a similar counterstrike. U.S. responses, including military responses, might take place in the cyber realm or outside it. The United States will need to learn how to wage cyber conflicts that are strongly affected by escalation dynamics and by the need to preserve deterrence in settings short of all-out war.

Achieving Extended Cyber Deterrence

A final thorny issue is determining how to achieve extended cyber deterrence coverage of allies, and how to deal with other third parties that might be menaced by cyber attacks. Adversaries might choose to attack U.S. allies in Europe and Asia either to coerce them into altering their foreign policies or to exert indirect pressure on the United States to modify its policies. To reduce this risk while preserving alliance cohesion, extended deterrence coverage of these allies, as well as a measure of protection for other friendly countries, may well become an important priority for a U.S. cyber deterrence strategy. Whether this goal can be achieved, and how it can best be pursued, are crucial questions. What types of U.S.

commitments might become necessary? Apart from calling for closer multilateral collaboration, answering these questions is not easy, but further research, analysis, and thinking will help produce answers, just as they helped forge extended nuclear deterrence coverage during the Cold War.

Toward a Spectrum of Cyber Deterrence Options

A cyber deterrence strategy is needed because the United States, its military forces, and its allies are vulnerable to major attacks against information networks. Such a strategy should employ a general model or framework from which tailored actions can be created in response to differing threats, situations, and U. S. objectives. As it assesses the need for a cyber deterrence strategy, the United States has a range of options. A limited cyber deterrence strategy would rely mainly on security and defensive measures to achieve its goals, seeking only a gradual, evolutionary improvement in its offensive capabilities. This would be the least demanding and easiest to execute but offers the lowest promise of success. A more ambitious strategy would make robust use of both defenses and offenses and would seek major, rapid improvements in its offensive capabilities. This option is more demanding and harder to execute but could offer better results by combining emphasis on defensive and offensive capabilities. A highly ambitious strategy would not only strengthen U.S. capabilities quickly, but also pursue major improvements in integrated, collaborative planning with allies and partners. This option would be the most demanding and hardest to execute, especially because mobilizing broad international collaboration would be difficult, but it would offer the biggest payoffs because it involves greater U.S. collaboration with allies and partners.

Deciding which of these options to choose requires an appraisal of desirability and feasibility: what the emerging strategic situation mandates, which of the options does the best job of producing an effective strategy, and what the traffic will bear in terms of political consensus and budgetary affordability.

The United States cannot afford to risk drift in this arena. The alternative to a thoughtfully crafted strategy of deterrence is growing vulnerability of America's vital information networks. By contrast, the potential payoff of a well-conceived cyber deterrence strategy is considerably greater security than exists today.

[1] The White House, *The National Strategy to Secure Cyberspace* (Washington, DC: The White House, February 2003).

[2] The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, DC: The White House, February 2003).

[3] The White House, *The National Strategy for Homeland Security* (Washington, DC: The White House, February 2003).

[4] The White House, *The National Security Strategy of the United States of America* (Washington, DC: The White House, March 2006).

[5] Department of Defense, *The National Defense Strategy of the United States of America* (Washington, DC: The Pentagon, March 2005).

[6] Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, DC: The Joint Chiefs of Staff, 2004).

[7] Department of Defense, *2006 Quadrennial Defense Review Report* (Washington, DC: Department of Defense, February 2006).

[8] Department of Defense, *Deterrence Operations, Joint Operating Concept* (Washington, DC: Department of Defense, December 2006).

[9] *The National Military Strategy to Secure Cyberspace* (classified), issued by Department of Defense in early 2007.

[10] See, in this volume, chapter 7, "Information Security Issues in Cyberspace," and chapter 23, "Cyberspace and Critical Information Protection: A Critical Assessment of Federal Efforts."

[11] See, in this volume, chapters 10–13 on military uses of cyberpower.

[12] For analysis of the motivations and actions of terrorist groups, see Jessica Stern, *Terror in the Name of God: Why Religious Militants Kill* (New York: Ecco, 2003).

[13] The cyber attack on Estonia in May 2007 was attributed, but not with certainty, to hackers within Russia: The Russian government has denied any involvement in the attacks, which came close to shutting down the country's digital infrastructure, clogging the Web sites of the president, the prime minister, Parliament and other government agencies, staggering Estonia's biggest bank and overwhelming the sites of several daily newspapers. 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>.

[14] The Soviet Union had more ICBMs and SLBMs than the U.S. force posture, but fewer strategic bombers; ultimately it deployed about 2,400 launchers and 10,000–12,000 warheads.

[15] For details, see Richard L. Kugler, *Commitment to Purpose: How Alliance Partnership Won the Cold War* (Santa Monica, CA: RAND, 1993).

[16] Tailored deterrence is a central concept of current U.S. deterrent strategy, and is discussed in detail in the *Deterrence Operations, Joint Operating Concept*.

[17] See chapter 23 in this volume, "Cyberspace and Critical Infrastructure Protection: A Critical Assessment of Federal Efforts."

[18] The official NATO Web site provides a valuable source for tracking NATO activities across the full spectrum of preparedness measures.