CHAPTER 1

Cyberpower and National Security:
Policy Recommendations for a Strategic Framework

Franklin D. Kramer

CYBERPOWER is now a fundamental fact of global life. In political, economic, and military affairs, information and information technology provide and support crucial elements of operational activities. U.S. national security efforts have begun to incorporate cyber into strategic calculations. Those efforts, however, are only a beginning. The critical conclusion of this book is that the United States must create an effective national and international strategic framework for the development and use of cyber as part of an overall national security strategy.

Such a strategic framework will have both structural and geopolitical elements. Structural activities will focus on those parts of cyber that enhance capabilities for users in general. Those categories include heightened security, expanded development of research and human capital, improved governance, and more effective organization. Geopolitical activities will focus on more traditional national security and defense efforts. Included in this group are sophisticated development of network-centric operations; appropriate integrated planning of computer network attack capabilities; establishment of deterrence doctrine that incorporates cyber; expansion of effective cyber influence capabilities; carefully planned incorporation of cyber into military planning (particularly stability operations); establishment of appropriate doctrine, education, and training regarding cyber by the Services and nonmilitary elements so that cyber can be used effectively in a joint and/or multinational context; and generation of all those efforts at an international level, since cyber is inherently international and cannot be most effectively accomplished without international partners. Achieving these goals will require greatly expanded efforts by the United States in terms of people, resources, and partnerships. The potential of cyber is so great, and the costs of failing to accomplish these goals so significant, that a truly national effort must be undertaken.

Preliminaries: Understanding Cyber

Creating a strategic framework for cyber requires both understanding what cyber is now and having a sense of where it is going in the future.

Definitions

Cyber can be defined in many ways. One recent study found 28 definitions of *cyberspace*. Accordingly, one of the most important lessons in this realm is to recognize that definitions should be used as an aid to policy and analysis, and not as a limitation on them. In the context of this book, *cyber* is used to encompass technical, informational, and human elements. Daniel Kuehl defines *cyberspace* as an operational domain framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internetted information systems and their associated infrastructures.[1] That definition is broad and technically focused but is a useful platform from

which to begin discussion. As one looks at different elements of cyberpower, the Kuehl definition provides a common base for analysis, but other aspects will tend to be added or emphasized, and the technical definition will be less critical to the development of policy and strategy. By way of examples:

- cyber influence activities will include the Internet as well as radio, television, communications such as cell phones, and applications for all
- cyber military activities will include network-centric operations, computer network attack and exploitation, geopolitical influence operations, and security
- cyber security will include not only technical issues such as viruses and denial-of-service attacks, but also human matters—such as insider deception as well as normal human mistakes—and the problems of governance, both national and international.

The policymaker who faces the cyber world needs to do so with the under- standing that the arena is very broad and, as discussed below, still developing. For some policy issues, that breadth will need to be continuously maintained; for analysis of others, the focus will be narrowed. Furthermore, there needs to be recognition that there is often overlap between what might initially be considered different areas of cyber. For example, while some military communications structures are physically differentiated from civilian communication structures and run by separate software and people, others rely partially or entirely on civilian networks, riding on civilian infrastructure or using civilian protocols such as Internet transmission control protocol/Internet protocol (IP). To make good judgments about cyber issues, policymakers need to understand the scope, purpose, and effects of the cyber realm in connection with the strategic issues being reviewed.

The Cyber Future: Strategy in a Dynamic Context

Cyber has a number of characteristics that suggest its future may differ importantly from its present. Policymakers must, therefore, establish cyber strategy in a dynamic context—not knowing what the future will be, but nonetheless creating structures, processes, and people sufficiently flexible to adapt to change. Cyber is malleable because, although it exists in the physical world of electrons, transmission capabilities, and computers, it is a manmade creation subject to the power of human invention.

The degree of change that the fundamentally manmade aspect of cyber can create is considerable. By way of comparison, cyber is certainly not the first important human construct subject to major alteration—money would be a significant example. In recent years, money has led a highly dynamic existence. Among many instances, new currencies such as the euro have been created, new instruments such as financial derivatives have been widely used, and new flows of funds worldwide have become an important part of the global dynamic.

Like money, cyber is highly dynamic. In classic business analysis, an *S* curve often shows the rate of growth, with the high slope at the bottom indicating rapid change. Cyber currently is in such a period of rapid technological, organizational, and other change.

One of the reasons for such change is that, at least in parts of the cyber arena, the barriers to entry are low. At the moment, the message content of cyber rides on transmission capabilities that are not constraining, at least not in the civilian world—in short, lots of people

can use cyber for lots of things at a reasonable price (the issue of transmission capability, usually put in terms of band capacity, is more significant in the military arena). Similarly, the development of applications, including negative applications for launching various types of cyber attacks, is a relatively low-cost endeavor, allowing numerous entities to develop important new capacities. Each of these factors is enhanced by the speed of transmission and the widespread penetration of cyber throughout the world. The broad context for the policymaker is that in making judgments, "facts" about cyber, which are true today, may be altered significantly in the future—and such a prospect of changed facts may well alter what would be the most appropriate judgments. Indeed, one of the fundamental issues for policymakers will be when to take steps that will affect changes in facts.

With the understanding of the breadth of cyber and its dynamic nature, we can turn to 10 key policy issues that will affect the establishment of a strategic framework for cyberpower in a national security strategy.

Structural Issues

Security

The cyber world is not secure. Each level of cyber—physical infrastructure, operational software, information, and people—is susceptible to security breakdown, whether through attack, infiltration, or accident.

There have been numerous evaluations of the U.S. infrastructure, including the electric grid and the transmission elements of cyber itself. Vulnerabilities of those infrastructures to both kinetic and cyber attack are well documented. By way of example, *The National Strategy to Secure Cyberspace* states:

> By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser- secured sites on the interconnected network of networks also present potentially significant exposures to cyber attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products.[2]

The breadth and capacity of cyber attacks is likewise well documented. Periodically, significant virus or denial-of-service attacks are featured in the media. Whether publicized or not, the annual number of attacks is extremely large, and they often occur against significant targets. For example, the Government Accountability Office has stated, "Significant information security weaknesses continue to place federal agencies at risk. . . . In 2006, agencies reported a record number of information security incidents to US-CERT [Computer Emergency Readiness Team]—the DHS [Department of Homeland Security] unit responsible for collecting such information."[3]

Cyber is hardly the first system subject to attack and breakdown. The monetary system is susceptible to counterfeiting, fraud, and robbery, yet it obviously is widely relied upon. The fundamental questions for the cyber policymaker are what level of protection is appropriate and whether and how it may be achieved.

In evaluating the level of protection that seems appropriate, an important immediate question is whether the level might be differentiated by use and user. The United States already makes such a differentiation in protecting its military and intelligence capabilities, with some built on entirely separate networks.

A second fundamental issue is how to reach the appropriate balance between exploiting the positive aspects of cyber versus accepting the risk that costs may arise as a consequence. To put it another way, increased functionality has often been associated with increased vulnerability—for example, increasing the number of sites one visits on the Internet, which broadens the access and usefulness of the Internet, concomitantly increases the likelihood that a virus will be downloaded onto one's computer. In making such an evaluation, the consequences of the risks need to be assessed—not only the probabilities but also the lasting costs. Taking down the electric grid for a day would be costly and arguably unacceptable, but taking it down for a year would be unquestionably catastrophic.

The U.S. Government is well aware of these issues and is taking steps. The Department of Homeland Security has the governmental lead, and, as recent newspaper reports have indicated, the Department of Defense (DOD) through the National Security Agency is enhancing its efforts to protect critical governmental networks. Nonetheless, as the Government Accountability Office has annually reported, the protection of government cyber is wholly inadequate, and the private sector is at least equally and often more vulnerable. The continuing nature of this well-recognized problem derives from a combination of the difficulties of effective response, prioritization, and determining who should decide upon the appropriate security measures.

To deal with these concerns, we recommend that the Federal Government take a more directive approach to ensuring cyber security, for both governmental and private cyber. Specifically, we prescribe a two-step approach to addressing vulnerabilities. First, a differentiation should be made among *indispensable*, *key*, and *other* cyber capacities. *Indispensable* cyber would include critical military and intelligence capacities and other capacities that the Nation could not afford to lose for even a short time. *Key* cyber would include critical functionalities that could not be lost for any length of time but for which short-term workarounds might be available, and functionalities whose exploitation (as opposed to loss) by adverse parties would have consequences for the Nation. Included in this category might be the electric grid and certain critical financial networks (although a determination would have to be made whether they need to be in the *indispensable* category), as well as capacities such as the defense industry that are necessary for key work for military and intelligence functions. The great bulk of cyber would fall into the *other* category, but that categorization would still involve a higher degree of security requirements.

Second, for each of the three categories, appropriate security measures would be required or encouraged. For indispensable cyber, the government would provide security, including monitoring for attacks, providing protection, and generating responses as appropriate, including the possibility of reconstitution or the establishment of redundancy. For

key cyber, the government could require certain levels of security protection and could itself provide monitoring, response, and support. For other cyber, the government could require and/or encourage security through regulation, incentives, information, and coordination (such as working more closely with software vendors). In this necessarily large category, differentiations could be made among the sizes of businesses and the nature of users.

The cyber security situation that the United States currently faces is reminiscent of the early days of the environmental protection movement. Affirmative action by the Federal Government was required (as by the Clean Air and the Clean Water Acts), and a level playing field had to be maintained to be fair to industry. In our view, a comparable effort is now required for cyber. The executive branch and Congress should generate a full program to deal with the problem of cyber security.

A differentiated security program ought to be proposed by the executive branch and presented to Congress for full review. Hearings should take place with executive branch, industry, and individual participation. From such an effort a framework can be created for appropriate regulatory establishment of security arrangements, including appropriate allocation and/or sharing of costs. This effort should be given high priority by the Executive and the Congress.

Human Capital and Research and Development

Cyber is a manmade construction and one that particularly relies on human ingenuity and technological capacity. For the United States to maintain leadership in the cyber world, both individual capacities and research and development (R&D) must be maintained at the highest levels. Doing so in a changing cyber world will require a substantially enhanced governmental effort.

On the human capacity side, two fundamental and related changes have occurred. The first is that countries other than the United States and its traditional partners are graduating numerous students in the science, technology, engineering, and mathematics (STEM) fields. In China and India, the annual number of STEM graduates is considerably greater than in the United States and Western Europe, though there are important differences in quality. The second change is that these STEM personnel in other countries have the capacity to do work that is currently being done in the United States, putting a significant number of (and perhaps potentially nearly all) U.S. STEM personnel in competition with offshore workers.[4]

There are substantial disputes about whether there are enough U.S. graduates in the STEM fields and about the impact of the offshoring of STEM capacities that has already occurred or may occur in the future. There is, however, no dispute that the United States needs to maintain a vibrant STEM capability to maintain its technological capacities and its global leadership position.

To accomplish those goals, two obvious but crucial actions need to be undertaken: teachers at all levels in the STEM arena need to be recruited and rewarded on a continuous basis; and a steady pipeline of students who will work STEM problems for their productive careers needs to be maintained. Numerous ways have been proposed to accomplish those goals, but the fundamental recommendation we have is that it is time to stop talking and start acting. A joint executive branch–congressional effort that provides a high degree of certainty of

accomplishment in the human capital STEM arena will do much to help ensure continued U.S. leadership in cyber.

Maintaining human capital is not sufficient if there are not adequate resources for that capital to use. The United States has traditionally relied on specialized government laboratories to complement private industry efforts in accomplishing key national security goals. That arrangement has been operative in both the nuclear and energy areas, but in the cyber arena, no such structures have been developed, and governmental efforts are limited. For example, the Department of Homeland Security cyber R&D budget for fiscal year 2007 was less than $50 million. Similarly, as Vice Chairman of the Joint Chiefs of Staff General James Cartwright has stated, "We as a nation don't have a national lab structure associated with [cyber] so we aren't growing the intellectual capital we need to . . . at the rate we need to be doing."[5] In short, fundamental R&D activity through the combined efforts of the public and private sectors is insufficient to ensure the United States continues to develop its cyber leadership capabilities.

The needs are significant. For example, security is a major vulnerability for the United States. A structured R&D approach to security would seek to develop specific new capabilities, analyze the costs and benefits of developing and implementing alternative systemic approaches to security, and support and integrate both governmental and private efforts. Examples could include large programs to eliminate flaws from existing widely used software or to create secure, underlying operating systems. Beyond security, there could be a national program on semiconductor research, the development of integrated cyber and biological capabilities for medical treatment and other uses, and the creation of new architectures and software capacities for more effective usage of cyber.

A three-part program of establishing national cyber laboratories, substantially increasing R&D funding for governmental agencies, and enhancing private sector activities through direct contracts and incentives would significantly increase the medium and long-term capacities of the United States. At a time when other countries are advertently adding to their cyber capacities and placing them in direct competition with those of the United States, it is critically important to respond to such challenges.

International Governance

The existing international cyber governance structure is a creature of history more than of logic. It nonetheless has worked well for the United States (and the world), as cyber in all its manifestations has continued to develop. There are, however, two important factors that call for the United States to undertake a thorough review of international cyber governance.

The first is that the portion of the international cyber governance that guides the Internet is both sufficiently ad hoc and perceptually U.S.-dominated that there have been significant calls by other countries to revise the structures. Harold Kwalwasser has set forth the system in detail,[6] but the essence is that some important elements are run by private organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN). While those organizations have been quite effective, their longevity is not guaranteed. For example, in 2010, the government's contract with ICANN (which is part of the overall arrangement) comes up for renewal, and a call for change is likely at that time.

The second factor is that no effective international arrangement deals with the security

and law enforcement aspects of cyber. However, given cyber's international character, national security and enforcement efforts will necessarily be less effective than what could be accomplished by an integrated international effort. The United States, for example, has developed statutory rules against various types of cyber crimes. The European Union has organized, and nearly 30 nations have joined, a Convention on Cybercrime. However, much of the world is not covered by focused efforts, which creates a haven from which criminals can operate.

Given the probability of an international call for significant change in Internet governance and the desirability from the U.S. point of view for changes to enhance security and law enforcement, our recommendation is that the executive branch undertake a prompt and substantial review to generate an international proposal around which a consensus can be built.

Failure to create such a proposal does not mean that the United States will not face a call for change. In recent years, a number of international efforts ranging from the International Criminal Court to the land mine convention have gone forward without U.S. participation. It is likely that the current arrangements will not continue and that alternatives could end up being negotiated despite U.S. reservations. Especially because important American interests are not met by existing approaches, undertaking a review as a prelude to organizing a serious international negotiation will be important to keeping cyberspace as effective as possible.

Organization: Cyber Policy Council

The dynamic nature of cyber means that numerous issues have arisen that will need governmental consideration. The government will not always need to take action: its choices will include standing aside and letting the private sector take the lead (as has been done, for example, in the development of cyber applications), taking enabling action (through tax incentives or the creation of enabling environments, such as the development of the international governance structure for the electromagnetic spectrum), or implementing a purposive strategy in which it is substantially engaged (as it does in the military arena and could do on other aspects of cyber, such as some security).

However, there needs to be a policy organization to purposefully consider the choices the government confronts. The need is particularly acute because of the multiplicity of issues, including some already noted such as private-public interface, security, human capital, research and development, and governance, but also others such as the implications of the increased volume of traffic, the potential move from IPv4 to IPv6, net neutrality, and the nature of the U.S. global role. The problem of the multiplicity of issues is exacerbated by the numerous authorities that exist in multiple arenas working on cyber. While the government is moving to coordinate intergovernmental security arrangements, even in the security arena coordination with the private sector needs much more active consideration—and, as noted, there are a host of other issues not involved in security.

Our recommendation is to create a new organization—a Cyber Policy Council along the lines of the Council of Economic Advisors. The council would focus on policy issues that need a White House perspective, bringing together all elements of government but incorporating the Presidential perspective. Such a council could integrate or at least coordinate and review key issues. We would not recommend, at least not initially, that the council have implementing

authority; for now, that power should remain with the relevant departments and agencies. But we would give the council the authority to review budgets on cyber and to make recommendations as part of the budgetary process. The council might ultimately take a more strategic directive role (as has been contemplated for the National Counter-Terrorism Center in its area), but we would have the council work for a while before the President determined whether to make it more than a policy office.

Geopolitical Issues

Cyber is both an element of, and a support for, power—for nations, for individuals, and for other entities including businesses, nonprofit organizations, and criminals and terrorists. While "cyberpower and national security" issues could therefore be defined to include the whole scope of societal activities, in this part to create more effective analysis and recommendations, we have focused on traditional geopolitical activities—the grist of international politics, including the use of diplomacy, influence, and force by both nation-states and nonstate actors.

Two preliminary issues deserve review in this connection. First is the question of whether "cyber" is a domain, comparable to other domains—land, sea, air, and space—regularly analyzed in geopolitical contexts. Authoritative DOD publications have described cyber in similar terms as the global commons.[7] Gregory Rattray has fully compared the cyber context to other domains,[8] and the comparability clearly seems to be there. From the perspective of the policymaker, however, it is critical to recognize that nothing—repeat, nothing— follows from that conclusion alone. Being in the status of a domain is not like being in the status of, for example, marriage from which various rights and obligations flow for historic, religious, and legal reasons—for example, the right to community property in some jurisdictions. Indeed, as the community property example shows, even for true forms of status such as marriage, the rights and obligations flowing from that status need to be prescribed. Some states are community property states, some are not—yet there are marriages in each. The consequence of cyber being a domain is simply that its important implications need to be determined.

Second is the question of whether dominance—meaning overwhelming superiority—can be achieved in cyberspace. The high probability is that it cannot. By comparison to sea, air, and space, where military dominance can reasonably be sought, cyber shares three characteristics of land warfare—though in even greater dimensions: number of players, ease of entry, and opportunity for concealment.

The world's most powerful navy has only some 300 ships, there is only one geosynchronous orbit with the number of satellites limited, and a military airplane can easily cost more than $100 million, a satellite system more than $1 billion, and a warship more than $3 billion. By contrast, there are billions of cyber users around the world and untold pathways between cyber site A and cyber site B. An Internet connection costs perhaps $40 a month, a good computer can be purchased for $600 (or rented for $10 an hour), and complex software can be created by a single person or downloaded off the Internet.

The point of the complexity and low cost of much of cyber is that success in cyber will be more like success in land warfare than in sea, air, and space warfare. On land, dominance is not a

readily achievable criterion. During the Cold War, the United States and its allies had an effective land capability but did not have dominance vis-à-vis the Soviet Union. While the first phase of the 2003 Iraq War suggested land dominance, the more recent—and much longer and more costly—counterinsurgency/stability operations phase has demonstrated absence of dominance. A more realistic set of goals in land warfare is effectiveness and achieving objectives. That likewise is a sensible set of goals for cyber. The United States will engage in a cyber landscape where there are opponents, major and otherwise, who have consequential capabilities. We should seek to prevail—and apply the resources to do so—but we should expect a competitive environment, one in which the opponent maintains important capabilities. Indeed, if any further proof is required, it should be clear that if we were capable of dominance, we would have gotten rid of hackers instead of being subject to thousands of attacks and probes on a daily basis.

Network-centric Operations

Network-centric operations are a fundamental approach used by the U.S. military. We have been highly successful in their use, and substantial efforts are ongoing to expand such capacities. We strongly support those efforts but raise the following question: By focusing so heavily on network-centric capabilities, are we creating vulnerabilities that may be exploited by opponents to our substantial detriment?

Since the Gulf War of 1991, U.S. conventional warfare capabilities, which are grounded in network-centricity, have been deemed extremely powerful by virtually all who review them. For this reason, opponents are expected to attempt to use asymmetric means when engaged in conflict against the United States. Computer network attack against U.S. networks—both military and those civilian networks supporting the military—would be one type of asymmetry.

To offset such a potential problem, we recommend three specific DOD efforts, all of which would fall under the purview of achieving mission assurance— the ability to accomplish the objective despite significant opposition.

First, a review should be initiated to determine the operational vulnerability of network capacities. The review should include full red team efforts designed to determine what negative effects could be created under operational conditions and would presumably require a number of exercises. Since some important networks will be run by the private sector, it will be necessary to create a process by which such networks can be evaluated. The focus should not be just on red-teaming. On the blue side, efforts should be made to determine what workarounds and capacities exist even after networks become degraded. Networks hardly would be the first wartime systems or materiel to sustain degradation, and, in other arenas, we certainly plan to move forward despite the problems created.

Second, having assessed vulnerabilities, a determination should be made as to the most important research, development, and/or acquisition efforts necessary to overcome key vulnerabilities. To the extent that important vulnerabilities are found to exist in the private sector, a public-private approach will need to be generated.

Third, as part of both the R&D and acquisition processes as well as in future exercises, the implications of risk in cyber from potential network vulnerability need to be systematically assessed.

Computer Network Attack

The potential for cyber warfare has long been discussed, and the attacks on Estonia's cyber capabilities in 2007 made the prospects even clearer. DOD has been equally clear. As Lieutenant General Keith Alexander stated, "The focus of cyber warfare is on using cyberspace (by operating within or through it) to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability, while protecting our own."[9]

While General Alexander's goal for DOD is clear enough, a fundamental obstacle stands in its way: cyber warfare—generally called *computer network attack* (CNA) by DOD—is not integrated with other overall planning because of the highly compartmented classification that cyber activities receive. Senior military leaders have been entirely clear about the problem, with one stating: "I do not want to see the cyberspace train drive off down some dark alley and set up shop and nobody knows what the hell they've been doing. They need to be integrated."[10] Of course, as the Vice Chairman of the Joint Chiefs of Staff has said, that is difficult because of the compartmentalization/classification problem: "We make sure the recce teams don't tell the defenders what they found, or the attackers, and the attackers go out and attack and don't tell anybody they did. It's a complete secret to everybody in the loop and it's dysfunctional."[11] The negative results are clear enough, according to General Cartwright: "The geeks turn it into a special language behind a bunch of closed doors so that a warfighter has no idea how to use it."[12]

The remedy (and our recommendation) for this problem is to reduce classification and to enhance integration of CNA with other planning. This has not been done previously out of concern that knowledge of DOD capabilities would allow potential adversaries to take offsetting measures in advance. However, with other capabilities such as electronic warfare, which have great similarity to computer network attack, we have been able to offset those problems. While specific electronic warfare techniques have higher classification, general capabilities have lower classification and are fully accessible to planners. Moreover, capabilities that can be discussed at the conceptual and engineering levels are entirely unclassified, as even a quick review of the numerous DOD publications on electronic warfare will demonstrate. While potential adversaries will know that we have such capacities in general, that will hardly come as a surprise inasmuch as significant capacities for computer network attack can simply be downloaded off the Internet, attacks (in the thousands) occur each day, and hacking is discussed regularly (in both constructive and nonconstructive ways) in both open literature and private groups. To put it bluntly, we are kidding ourselves when we undertake to classify CNA in the fashion that we do—and, more importantly than kidding, we are harming our own capacity to use CNA to the extent it deserves.

Deterrence

Cyber attacks—hacking of various kinds—are a fact of modern life. Nation-states, such as China, have been publicly accused of hacking for espionage purposes, and nonstate actors, such as criminals and terrorists, likewise have substantial capabilities. The steady state of modern life is that thousands of intrusions occur each day, some with important

consequences. More ominously, there are concerns that attacks could be undertaken for geopolitical purposes by states or nonstate actors that would have far greater negative impact than has thus far occurred. The capacity to deter such attacks would be enormously valuable.

Cyber deterrence has been considered challenging because of the difficulty of attributing the source of cyber attacks. While attribution unquestionably is a consequential issue, we believe that deterrence in the context of cyber is a viable strategy and one on which the United States ought to embark much more advertently. The components of such a strategy would consist of the following elements, some of which would require development as discussed below.

First, any approach to deterrence of cyber attacks needs to be considered in an overall concept of deterrence, not as a separate cyber arena. Such an effort would use a combination of potential retaliation, defense, and dissuasion. It would be based on all elements of national power so that, for example, any retaliation would not necessarily be by cyber but could be by diplomatic, economic, or kinetic—or cyber—means, depending on the circumstances. Retaliation, when and if it occurred, would be at a time, place, and manner of our choosing.

In generating policy, some important differentiations could be consequential. State actors generally act for classic geopolitical aims and often are susceptible to classic geopolitical strategies. Retaliation of various sorts might be more available against state actors, and dissuasion likewise might be more effective. By contrast, nonstate actors could be less susceptible to classic geopolitical strategies (though indirect strategies, such as affecting the country in which they are based, may have impact). Cyber defense, law enforcement, and, for terrorists, classic counterterrorist techniques may be most effective.

One important question is whether there is a threshold at which more significant responses become appropriate. It bears restating that there are a great many intrusions already ongoing, and responses to them have not been dramatic. In analyzing this issue, it may be useful to separate what might be termed *high-end* attacks from *low-end* attacks. If one hypothesized a serious attack that rendered, for example, military or key financial systems inoperative, the probability would be that an extremely robust response would be appropriate. A state actor that undertook a high-end attack should certainly understand that the United States could carry out a countervalue response that would not be limited to a response on cyber assets. The potential of a response against the high-value elements of a state should add considerably to deterrence. Likewise, it should be clear that an attack in the context of an ongoing conflict, whether against a state or a nonstate actor, likely will receive a very significant response. Dealing with cyber actions by an actor with whom we are militarily engaged, such as al Qaeda or the insurgents in Iraq, seems different than dealing with a new problem where force has not already been used.

On the other hand, even if, for example, it was clear that an identity theft ring was being operated out of a particular country, law enforcement and diplomatic responses probably would be used. The degree of damage generally would not be deemed sufficient to require a significant response. Such restraint, however, might not always be appropriate in circumstances that usually are the province of law enforcement. Historically, some instances of criminal behavior have led to consequential U.S. efforts, such as the 1989 invasion of Panama and the capture, trial, and incarceration of its president for drug trafficking. Moreover, an effective response against criminal use of cyberspace could add credibility to the prospect of a response against other actors.

One important difference between high-end and low-end attacks might be that attributing

the high-end attack to its source would be easier. Because states normally act for geopolitical reasons, a high-end cyber attack by a state probably would occur in a context in which it might be possible to determine the source. Nonetheless, attribution is a significant challenge, and a major part of a deterrence policy will be to create greater capabilities to assist in attribution. Those efforts should include developing more effective technical means, such as monitoring and intrusion devices as well as traceback and forensic capacities, and it might involve other technical efforts such as new architectures, protocols, and types of servers and routers. In addition to technical responses, intelligence capabilities and law enforcement capabilities might be expanded. An important element of deterrence will be expanding protection beyond governmental entities. We have recommended a differentiated response to security, and a vital component will be to make the appropriate private networks "hard targets."

Finally, inasmuch as cyber is inherently international, working with the international community will be indispensable to generating effective deterrence of both high-end and low-end attacks. At the high end, a common approach will be important to establish the international framework that will help end the conflict on the most desirable terms to the United States. Likewise, allies and partners may have important technical and other capabilities to help enhance retaliation, defense, or dissuasion. At the lower end, greater cooperation will advance law enforcement and diplomatic capacities.

To accomplish both high-end and low-end goals, the United States will want to lead a variety of efforts, including assuring that the North Atlantic Treaty Organization (NATO) treaty is understood at a minimum as including high-end attacks as a matter of treaty consequence; developing binding law enforcement mechanisms, possibly modeled on the European Union Convention on Cyber-crime; and generating a new international regime that provides internal guidance, as well as requirements for cooperation, for all countries—potentially modeled on United Nations Security Council resolutions undertaken in the light of the 9/11 attacks. As a critical element in undertaking such action, significant policy and legal review will be imperative to determine relevant constitutional and statutory considerations (including the possibility of revising statutes) and generate an effective international diplomatic strategy. Ultimately, it may be worthwhile to expand the current limited U.S. declaratory policy regarding cyber, but such a decision should await the results of any review.

In sum, the United States needs a much more robust cyber deterrence policy than it has. Such a policy will include both generating capabilities and undertaking political action.

Influence[13]

Cyber influence is an ongoing source of power in the international security arena. Although the United States has an enormous cyber information capacity (estimated to produce annually about 40 percent of the world's new, stored information and a similar share of telecommunications), its cyber influence is not proportional to that capacity. For example, a British Broadcasting Corporation poll of some 26,000 people in 24 countries (including the United States) published in 2007 stated that the "global perception of the U.S. continues to decline," with the populace of only 3 of the 24 countries surveyed saying the United States had a mainly positive impact on world affairs.[14] The mismatch between U.S. information capabilities and the actuality of U.S. influence is obvious.

Impediments to American cyber influence include the vastness and complexity of the international information environment, the multiplicity of cultures and differing audiences to which communications must be addressed, the extensiveness and significance of contending or alternative messages, and the complexity and importance of using appropriate influential messengers and message mechanisms.

Enhancing the influence of the United States in cyberspace will require a multifaceted strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers. To improve in these areas, the United States must focus on actions that include discerning the nature of the audiences, societies, and cultures to which messages will be delivered; increasing the number of experts in geographic and cultural arenas, particularly in languages; augmenting resources for overall strategic communications and cyber influence efforts; encouraging long-term communications and cyber influence efforts along with short-term responses; and understanding that successful strategic communications and cyber influence operations cannot be achieved by the United States acting on its own—allies and partners are needed both to shape our messages and to support theirs.

To accomplish those ends, U.S. policymakers can undertake a variety of specific actions. First, and perhaps most important, greater focus must be placed on the nature of audiences and of the societies and cultures into which cyber-transmitted messages will be delivered. The intended recipients need to be clear. For example, in the context of a counterterror effort, there likely will be a difference among messages to populations at large—those who do not support terrorists, those who are terrorist sympathizers, those who are active supporters of terrorists, and those who are terrorists. Moreover, those varying audiences might well be reached by different types of communications—for example, television for broader audiences and Web sites for potential terrorist recruits. In this context of differentiated messaging, a further consideration needs to be an understanding of the types of persons who have influence with the message recipients and the types of contexts in which that influence will be most effective.

Second, it will be necessary to increase the number of experts in geographic, cultural, and linguistic arenas. Such expertise can help build a societal/cultural map of influencers, key communications nodes, and cultural patterns to guide strategic communications and influence operations. Added to these cultural experts should be experts in psychology and marketing who can help generate messages and ensure that communications are effective. Finally, experts are needed in the use of television, radio, the Internet, and cell phones. In short, an interdisciplinary approach is required.

Third, leaders must realize that while there may be a consistent base message, that message will be presented in multiple theaters. These areas will differ significantly, and to be effective, messaging should likewise differ. For example, the society, culture, and influential persons in Indonesia are significantly different from those in Pakistan, and both are significantly different from those in Egypt. It is also worth noting that the Internet has created coherent, nongeographic communities. Numerous studies and reports document the Internet's effectiveness in transmitting messages that sympathize with, give support to, and recruit for terrorist efforts. The Internet must be a focused arena for strategic communications and influence operations.

Fourth, greater resources must be given to overall strategic communications and influence

efforts. For example, expanding the capacities of the Broadcasting Board of Governors, Embassies, and other outlets of the State Department would be enormously valuable. As noted, the Internet is a key mechanism. The State Department runs Web sites, but a broader and more multifaceted Internet strategy—both globally and regionally—would be highly desirable. The Government Accountability Office has found that while Embassy posts are supposed to have a strategic communications plan, they are generally ineffective and lack focus and resources.[15] Enhancing U.S. Government capabilities is a critical requirement.

Fifth, long-term communication efforts must be encouraged along with short-term responses. It is possible to change attitudes over time. As an example, consider the American attitude toward smoking, which has transformed significantly over the last 30 years. In the battle of ideas, the U.S. Government is seeking a long-term change—and so there is a need to adopt long-term policies. Transmitting messages over DOD Web sites and the Web sites Southeast European Times and Magharebia, which provide news, analysis, and information, is a productive, long-term approach that will not affect attitudes immediately but can have significant consequences over time.

Sixth, we must fully appreciate that facts speak louder than words. Some policies generate considerable opposition, and strategic communications and influence operations are not panaceas that can overcome all real-world actions. In the earliest planning stages, the communications consequences of actions must be discussed. In conflicts such as those in Iraq and Afghanistan, the impact of violent activities will significantly change the worldviews of not only those immediately impacted but also those who are indirectly affected and those to whom those effects are communicated. Every battle commander in these irregular wars soon finds out that the communications battle is critical—because the center of gravity for success is the population. But all too often, our commanders have to learn this on the ground. Especially in this globalized world of instant communications, tactical actions can have strategic consequences. Cyberspace is a creative and cultural commons defined by information, perception, cognition, and belief, and it is becoming the preeminent domain of political victory or defeat. Increased support for training and resources for cyber-enabled communications will be critical elements of effective counterinsurgency and stability operations. Communication—to one's supporters, to the population at large, and to the opposition—is of crucial importance. The government needs resources and training for our people on these issues, and these must be undertaken not only by DOD, but also in a joint DOD-State context.

Seventh, the U.S. Government should not expect success at strategic communications and influence operations acting on its own. Rather, it should use an alliance and partnership approach, both to expand capacities and to increase effectiveness. In the business world, it would be the rare American company that would seek to enter another country without the guidance and support of local business, whether as partners, joint ventures, or advisors—and often as all three. In military and diplomatic arenas, our allies and partners are recognized as enormous sources of strength. In the strategic communications and influence operations arena, we need to develop those alliances and partnerships, both to shape our own messages and support theirs.

Stability Operations[16]

Cyber, through information and information technology, can increase considerably the likelihood of success in stability operations—if engaged as part of an overall strategy that coordinates the actions of outside interveners and focuses on generating effective results for the host nation. Properly used, cyber can help create a knowledgeable intervention, organize complex activities, and increase the effectiveness of stability operations by integrating them with the host nation. The critical decision for policymakers is to utilize on a systematic and resourced basis the capabilities that cyber provides.

The benefits from adopting such an approach are substantial. First, proper use of cyber can help create a "knowledgeable" intervention. Even before the intervention, and certainly as it progresses, the interveners will need information of many kinds about both planned and ongoing respondent activities and about the host nation. An information strategy supported by information technology provides an opportunity to share information among the stability operations respondents themselves. This cooperation will facilitate the generation of a common approach and can help in the effective use of scarce resources.

A second key benefit of a cyber-supported strategy will be the help it provides in organizing complex activities. Normally, a stability operation will be undertaken on a countrywide basis. For even the smallest countries, this means a significant geographic area, with all the difficulties of maintaining connectivity. The intervention also will undoubtedly be of some duration, and cyber will be valuable to maintain an updated approach as conditions on the ground change.

The third key benefit from cyber will come from the ability to use distributed information to integrate the stability operations respondents with the host nation. The objective of a stability operation is not a "good intervention" but rather an "effective host nation" as a result of the intervention. To accomplish this difficult task, given that the host nation is likely fragmented, disrupted, and ineffective, the interveners need to stay connected to the host nation so that the results are adopted and adoptable by the populace on whose behalf the effort is being undertaken. An effective cyber strategy would involve the host nation (likely in numerous manifestations) in the ongoing activities of the intervention.

The fourth benefit is to integrate the host nation and make it more effective. Effectiveness can be enhanced by using cyber capacities to identify key requirements and target scarce resources. Host nation capacity can also be created by the use of cyber. Government operations can be reestablished with the proper use of information technology. Both the information systems and the training to use them will be required, but information capacity often can be generated far more quickly than other infrastructures—and can enable other effective actions.

Five key elements are required to generate an effective cyber strategy for the United States to use in stability operations. The first requirement is for the U.S. Government to make the fundamental decision that such a strategy is a mandatory element of all stability operations. That is no small statement because the reality is that the United States has never—in any of its many stability operations—made such a decision. But the rationale for such a conclusion is clear: information and information technology are crucial elements to the success of stability operations.

Although the problems of stability operations go far beyond military, the second

element of an effective cyber strategy recognizes that, doctrinally, the military requires a cyber strategy as part of the planning and execution of any stability operation. Accordingly, in both joint and Service documents—plans and the rules and guidance for their development and execution—a cyber strategy is a required element.

The third element of a cyber strategy for the U.S. Government for stability operations is to establish partnerships with key stability operations participants in advance. It is important to emphasize the word *key*. It is not possible, and would not be effective, to try to establish partnerships with all of the many players who would take part in a stability operation. But there are some very key parties who would regularly be involved and participate in planning.

The fourth element of an effective cyber strategy is to focus on the host nation. Establishing host nation effectiveness cannot be overemphasized—it is the main goal. Informing host nation decisionmaking, enhancing governmental capacities, and supporting societal and economic development are all crucial elements of an effective cyber strategy. However, when cyber technology is considered, efforts with respect to the interveners too often are emphasized as compared to creating effectiveness of the host nation. This is backward. An effective cyber strategy is one that makes the host nation effective. Nothing else will do. Thus, a critical element of the strategy is a cyber business plan for the host nation and an intervener support strategy that aims to enable the host nation business plan.

In sum, policymakers can substantially enhance U.S. capabilities in stability operations by adopting a cyber strategy as part of the overall effort.

Doctrine, Organization, Training, Materiel, Logistics, People, and Finance

The concept of doctrine, organization, training, materiel, logistics, people, and finance is a DOD construct intended to ensure that an activity is looked at in its full dimensions. Cyber needs such a review by DOD because as a new activity, it has generated a host of initiatives that need to be better coordinated. In general, we applaud the various actions taken, such as the designation of U.S. Strategic Command (USSTRATCOM) to have authority over cyber or the Air Force's decision to have a new cyber command. But there are numerous open questions that need consideration, and a significant internal review should lay them out for decision. Among the key questions are:

- What should be the relationship between cyber efforts and information operations, and does the latter need redefinition?
- How should USSTRATCOM relate to the regional commands in practice?
- What component commands should be established to support USSTRATCOM, and should they all perform the same functions?
- How should the Joint Information Operations Command relate to the public diplomacy activities of the State Department?
- What should the role of cyber be in exercises, both Service and joint, and does there need to be greater interagency exercising?
- What education and training should personnel involved in cyber receive, and what career paths should be developed?
- What cyber research and development should DOD engage in, and how should that be conducted?

As part of the review, we have two recommendations. First, we believe cyber needs to be regularly integrated into exercises, both through red teams and otherwise, since the cyber world is the real world we face. Second, just as we have nuclear and energy laboratories, we believe there need to be government "cyber laboratories." The precise mechanics can be determined, but the critical point is that there needs to be focused and substantial government research on cyber. We recognize that the private sector conducts significant and highly valuable cyber research. The private sector, however, is understandably motivated by profit, and there are issues that government needs to address because the appropriate level of effort will not be generated through market activity alone. The government can, of course, rely in part on the private sector for such R&D, as it does in other national security areas. However, creation of government cyber laboratories will establish the ability to delve deeply into key questions under government control in a way that cannot always be accomplished through the contracting process.

Finally, in connection with the DOD review, we think that a government "cyber corps" should be considered. Such a group could be joint and multi-disciplinary—and probably should be looked at as a potential interagency approach. Operationally, a cyber corps could integrate influence, attack, defense, and exploitation in the operational arena—and could help support those efforts in particular, more specialized agencies.

The Need for International Action

The nature of cyber itself and the discussions thus far should make it readily apparent that cyber cannot sensibly be considered solely on a national basis. Cyber in many of its manifestations is a creature of globalization, and it needs to be analyzed and reviewed with an international framework and international consequences in mind. The fundamental issues are the same internationally as they are from the U.S. perspective—including security, governance, uses in geopolitical context, and others—and their solutions will require, or at least be enhanced by, international actions.

Three international issues call out for immediate action. First, the 2007 cyber attacks on Estonia should make clear that NATO needs to undertake a comprehensive review of its cyber policies. The review would include the obvious question of when an "armed attack" in terms of the treaty has occurred, and whether the treaty or its interpretation needs to be revised to include the ability to act jointly. But the review should also raise the issue of whether NATO has the appropriate security arrangements for its forces to allow for secure interconnectivity and for its nations to protect them from outside harm. Moreover, the review needs to determine whether NATO has the proper capacity for deterrence (retaliation, defense, and dissuasion). Finally, it needs to analyze NATO capacity to use cyber in stability operations and for influence. In short, a major NATO effort concentrating on cyber is called for.

Second, international influence and international public diplomacy need to be strengthened. A battle of ideas is likely to continue in the 21st century. The United States will need significant international support to prevail. Third, the international governance structure for cyber needs to be strengthened. In the law enforcement arena, greater cooperative measures need to be created. In the overall governance area, there undoubtedly will be a major review. Cyber offers important prospects for individuals, organizations, and governments. But it will require

forceful steps to ensure that its potential is best fulfilled. Accomplishing the major recommendations of this study will go far toward enabling that end.

---

[1] For example, see chapter 2 in this volume, "From Cyberspace to Cyberpower: Defining the Problem."

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

[3] Gregory C. Wilshusen, director, Government Accountability Office, "Information Security: Persistent Weaknesses Highlight Need for Further Improvement," testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives (April 19, 2007), GAO–07–75IT, 2.

[4] Committee on Prospering in the Global Economy in the 21st Century, *Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Future* (Washington, DC: The National Academies Press, 2007), 16. There are disputes over the numbers, though China, India, and other countries are certainly graduating increasing numbers of science and engineering students. See Gary Gereffi et al., "Getting the Numbers Right: International Engineering Education in the United States, China, and India," *Journal of Engineering Education* 97, no. 1 (January 2008), 13.

[5] General James E. Cartwright, USMC, comments at Air Force Association Air Warfare Symposium, February 8, 2007, accessed at <www.afa.org/events/aws/post_orlando/ scripts/Cartwright_Printer.asp>.

[6] See chapter 21 in this volume, "Internet Governance."

[7] Department of Defense, *The National Defense Strategy of the United States of America* (Washington, DC: The Pentagon, March 2005), available at <www.au.af.mil/au/awc/ awcgate/nds/nds2005.pdf>, 15.

[8] See chapter 10 in this volume, "An Environmental Approach to Understanding Cyber-power."

[9] Keith B. Alexander, "Warfighting in Cyberspace," *Joint Force Quarterly* (Issue 46, 3d Quarter 2007), 60.

[10] Ronald Keys, quoted in *Defense News*, February 26, 2007, 8.

[11] Cartwright.

[12] Ibid.

[13] This section was derived from chapter 14 in this volume, "Cyber Influence and International Security."

[14] British Broadcasting Company, "'Listen More' is World's Message to U.S.," World Service Poll, January 23, 2007, available at <http://news.bbc.co.uk/2/hi/americas/6288933.stm>.

[15] Jesse T. Ford, director, International Affairs and Trade, "U.S. Public Diplomacy, State Department Efforts to Engage Muslim Audiences Lack Certain Communication Elements and Face Significant Challenges," testimony before the Subcommittee on Science, the Departments of State, Justice, and Commerce, and Related Agencies, House Committee on Appropriations, GAO–06–707T (Washington, DC: U.S. Government Account- ability Office, May 2006), 21, available at <www.gao.gov/new.items/d06535.pdf>.

[16] This section was derived from chapter 16 in this volume, "I-Power: The Information Revolution and Stability Operations."