Statement of Franklin D. Kramer
before the
House Armed Services Committee
Subcommittee on Terrorism and Unconventional Threats
April 1, 2008

Mr. Chairman and Members of the Committee:

Thank you for the opportunity to testify on the subject of cyberpower and national security. I am appearing today in my individual capacity. Most specifically, although I have worked on an extensive study on “Cyberpower and National Security” in conjunction with the Center for Technology and National Security Policy at the National Defense University, my testimony is only my own and not that of the Center, the National Defense University nor the Department of Defense.

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. United States national security efforts have begun to incorporate cyber into strategic calculations. Those efforts, however, are only a beginning. The critical point of my testimony is that the United States should create an effective national and international strategic framework for the development and use of cyber as part of an overall national security strategy. That is an effort that this Committee and the Congress should undertake with the Executive Branch—and, since cyber has fundamental private sector components ranging from infrastructure to privacy concerns, it is an effort that must reach out to the American people.

Let me make two foundational points, and then propose eight areas for policy review, with my own recommendations.

Foundationally, a first key point is to recognize that cyber can be defined in many ways. One recent study found 28 different 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. Cyber encompasses not only technical aspects—computers, communications infrastructure and the like, but also informational and human elements. There is a tendency to think of the

Internet as equating to cyber—but while the Internet is part of cyber, so are military network centric operations, and so are influence activities including television and radio, communications such as cell phones, and applications for all. So when discussing cyber security, that subject is not at all limited to technical issues such as viruses and denial of service attacks, nor even to human matters--such as insider deception or normal human mistakes—nor even to the problems of governance, both national and international. Rather, cyber security is best thought of as part of national security—geo-political and economic, of which technical security is only a limited, though important, part.

The second key foundational point is that cyber has a number of characteristics that suggest that its future may importantly differ 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 changeable because it is a manmade creation subject to the power of human invention. The broad context for the policymaker is that in making judgments, "facts" that 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 that foundational context, let me turn to key policy issues, and separate them into what might be called "structural" issues—those that affect the cyber world broadly--and "geo-political" issues, the more classical subjects of national security.

A. Structural Issues

1. Organization—Cyber Policy Council

The first structural issue that needs consideration is how will the government organize itself to deal with the problems of cyber. The dynamic nature of cyber means that numerous issues have arisen and will continue to arise 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 to implement 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).

There needs, however, to be a policy organization to consider in a purposeful fashion the choices the government confronts. That is particularly true because of the multiplicity of issues, ranging from private-public interface, security, human capital, research and development, and governance to others such as the implications of the increased volume of traffic, the potential move from IPv.4 to IPv.6, net neutrality, and the nature of the United States global role. The problem of the multiplicity of issues is exacerbated by the multiple authorities that exist in multiple arenas working on cyber. While the Executive Branch is taking steps to coordinate intergovernmental security arrangements, even in the security arena coordination with the private sector needs much more active consideration—and there are a host of other issues not involved in security.

My first recommendation, therefore, is that there should be created 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. It could also be a central place to interact with the Congress.

I would not recommend, at least not as it is first established, that the Council have implementing authority, instead leaving that for now with the relevant departments and agencies. But the Council should have the authority to review budgets on cyber and to be able to make recommendations as part of the budgetary process. Ultimately, it might be that the Council took a more strategic directive role (as has been contemplated for the National Counter-Terrorism Center in its area), but the Council should work for a period of time before it was determined whether to make it more than a policy office.

The Council could also review the important issue of whether there should be created a government "cyber corps." Such a group could be joint and multidisciplinary—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 the departments and agencies. But whether to have a cyber corps probably cannot be determined until the government itself has developed a more structured and thorough approach to cyber.

Now let me turn to several key issues the Council would focus on.

2. Security

The first issue is obvious: classic cyber 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.

The fundamental questions for the cyber policymaker are what level of protection is appropriate and whether and how that may be achieved.

In evaluating the level of protection that seems appropriate, an important immediate question is whether such levels might be differentiated by use and user. The United States already makes such a differentiation in protecting its military and intelligence capabilities—some being 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 risks that costs may arise as a consequence. Or, to put it another way, increased functionality has often been associated with increased vulnerability—a simple example would be that 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 just the probabilities but also the lasting costs. Taking down the electric grid for a day would be high cost and arguably not acceptable, but taking it down for a year would be catastrophic beyond question.

To deal with these concerns, my recommendation is that the federal government needs to take a more directive approach to ensuring cyber security, both for governmental and for private cyber. Specifically, I recommend a two-step approach of 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 simply could not afford to lose for even a short period of time. "Key" would include critical functionalities that could not be lost for any length of time, but for which short-term work-arounds might be available, or functionalities whose exploitation (as opposed to loss) by adverse parties would have consequential effects 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 first "indispensable" category), as well as capacities such as the defense industry which is necessary for key work for military and intelligence functions. "Other" would include the great bulk of cyber, but, as described below, that categorization could still involve a higher degree of security requirements.

Second, for each of the three categories, appropriate security measures would be required or encouraged, some measures to be undertaken by the government. For the "indispensable" category, the government would provide security, including such activities as monitoring for attacks, providing protection, and generating responses as appropriate, including the possibility of reconstitution or the establishment of redundancy. For the "key" cyber, the government could require certain levels of security protection, and could provide part, including the possibility of, for example, monitoring, response, and support. For the "other" category, 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, last group, differentiations could be made among types of businesses (e.g., large and small) and among nature of user.

The cyber security situation currently faced by the United States is not unlike the early days of recognizing the issue of environmental protection. 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. A comparable effort is now required for cyber. However, in the cyber world, the situation is even more complicated--any security program immediately presents extremely important and challenging privacy and civil liberties questions. Such issues must be directly faced, and a full dialogue undertaken with the American people.

A “differentiated security” program ought to result only from joint full consideration by the Executive Branch and the Congress working together to create a 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, and the protection of privacy and civil liberties. This effort should be given high priority by the Executive and the Congress.

3. Human Capital and R&D

Cyber is a manmade construction, and one that particularly relies on human ingenuity and technological capacity. To maintain leadership in the cyber world for the United States demands that both individual capacities and research and development be maintained at the highest levels.

To accomplish those goals, it seems to me that two obvious, but crucial actions need to be undertaken: first, teachers at all levels in the science, technology, engineering and mathematics fields need to be recruited and rewarded on a continuous basis; and a steady pipeline of students who will work such scientific and technological problems for their productive careers needs to be maintained. Numerous ways have been proposed to accomplish those goals—but the fundamental recommendation I have is that it is time to stop talking and start doing. This Committee could lead a joint Executive Branch-Congressional effort to enhance scientific and technological human capital and by doing so would do much to help ensure the United States’ continued leadership position in cyber.

Maintaining human capital is not sufficient if there are not adequate resources for that capital to utilize. The United States has traditionally relied on specialized government laboratories to complement private industry efforts to accomplish key national security goals. That has been true 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 research and development budget for FY 2007 was less than $50 million. Similarly, as the Vice-Chairman of the Joint Chiefs of Staff 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.” In short, there is not sufficient fundamental research and development activity through the combined efforts of the public and private sectors to ensure the United States continues to develop its cyber leadership capabilities.

I do recognize that the private sector conducts significant and highly valuable cyber research. The private sector, however, is understandably motivated significantly by the profit motive, 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.

A three-part program of establishing national cyber laboratories; very significantly 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.

4. Governance

The existing 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 which call for the United States to undertake a thorough review of cyber governance.

The first is that the portion of the 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.

The second is that there is no effective international arrangement that deals with the security and law enforcement aspects of cyber. Given, however, cyber’s international character, national security efforts as well as the development of enforcement will necessarily be less effective than could be accomplished by an integrated international effort.

Given the probability of an international call for significant change in Internet governance and the desirability from the United States point of view for changes to enhance security and law enforcement, this Committee could lead an effort, working with the Executive Branch, to generate an international proposal around which a consensus can be built. Undertaking a series of hearings to explore governance issues would be a good first step toward establishing such a consensus.

B. Geo-Political Issues

In addition to structural issues, cyber presents certain key geo-political issues. Last year, I testified to this Committee on the issue of strategic communications so I will not rehearse those comments. Instead, let me focus on four other important issues.

1. Deterrence

Cyber attacks—hacking of various kinds—are a fact of modern life.

Cyber deterrence has often been thought very difficult because of the difficulty of attribution of the source of cyber attacks. While there is no question that attribution is a consequential issue, nonetheless 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:

First, any approach to deterrence of cyber attacks need to be considered in an overall concept of deterrence—not as a separate cyber arena. Such an effort would utilize 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 diplomatic, economic or kinetic—or cyber—depending on the circumstances. Retaliation, when and if used, would be at a time, place and manner of our choosing.

Second, in generating the policy, some important differentiations could be consequential. State actors generally act for classic geo-political aims, and are susceptible to classic geo-political strategies in many instances. Retaliation of various sorts may be more available against state actors, and dissuasion likewise more effective. By contrast, non-state actors may be less susceptible to classic geo-political strategies (though indirect strategies, such as affecting the country in which they are in, may have impact). Cyber defense, law enforcement, and, for terrorists, classic counter-terrorist techniques may be most effective.

Third, 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 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 very significant attack that rendered, for example, military or key financial systems inoperative, the probability would be that a very significant response would be appropriate. A state actor who undertook a “high end” attack should certainly understand that the United States could undertake a “counter value” 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 significantly to deterrence. Likewise, it should be clear that an attack in the context of an ongoing conflict, whether against state actor or non-state actor, likely will receive a very significant response. Dealing with cyber actions by Al Qaeda or the insurgency in Iraq, against which we are militarily engaged would seem to be 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, it probably would be the case that law enforcement and diplomatic responses would be used. The degree of damage generally would not be deemed to be sufficient to require a highly significant response. Such restraint, however, might not always be the case in circumstances that are usually are the province of law enforcement. Historically, some instances of criminal behavior have led to very consequential United States efforts, such as the 1989 invasion of Panama and the capture and subsequent trial and incarceration of its president for drug trafficking. Moreover, a very effective response against criminal use of cyber potentially would add credibility to the prospect of a response against other actors.

Fourth, one important difference between high end and low end attacks may be that it will be easier to attribute the high end attack to its source. Because states normally will act for geo-political reasons, a high end cyber attack by a state likely will occur in a context in which it may be possible to determine the source. Nonetheless, attribution is a significant challenge, and an important part of a deterrence policy will be to create greater capabilities to allow for attribution. Those should include developing more effective technical means, such as monitoring and intrusion devices as well as trace-back and forensic capacities, and it might involve other technical efforts such as new architectures, new protocols, and new 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. As I have recommended, this will require a differentiated response to security, and an important element of deterrence will be to ensure making 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. That is true for both high end and low end attacks. At the high end, a common approach will be important as is true of all conflicts 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 NATO treaty is understood at a minimum as including high end attacks as a matter of treaty consequence; developing binding law enforcement mechanisms perhaps modeled on the European Union Convention on Cybercrime; and perhaps 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, it will be important for there to be a significant policy and legal review to determine relevant constitutional and statutory considerations (including the possibility of revising statutes), and generating an effective international diplomatic strategy. Ultimately, it may be worthwhile to expand the current relatively limited United States 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 deterrence policy with respect to cyber than it currently has. Such a policy will include both generating capabilities and undertaking political action.

2. Stability Operations

Cyber, through information and information technology, can significantly increase 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 utilized, cyber can help create a knowledgeable intervention, organize complex activities, and integrate stability operations with the host nation, making stability operations more effective. The critical decision for policymakers is to decide to utilize on a systematic and resourced basis the capabilities that cyber provides. Three actions would help create an effective cyber strategy for stability operations.

First would be to recognize the need for including cyber as part of the planning and execution of any stability operation. Accordingly, in both civilian and military efforts—and specifically in joint and Service planning documents—a cyber strategy element would be required.

The second element of a cyber strategy for stability operations is to pre-establish partnerships with key stability operations participants. It is important to underscore the word “key.” It is not possible, and would not be effective, to try to establish pre-existing partnerships with all of the many players who will be involved in a stability operation. But there are some very key players who will regularly be involved and who would participate in planning.

The third element of an effective cyber strategy is to focus on the host nation. Cyber can be utilized to inform host-nation decisionmaking, to enhance governmental capacities, and to support societal and economic development. Those are all crucial elements of an effective stability operations strategy.

This Committee could play an important role in the development of a cyber stability operations strategy as it works with the Executive Branch in the development of an overall strategy for irregular challenges.

D. Network Centric Operations

Network-centric operations are a fundamental approach of the United States military. We have been highly successful in their use, and substantial efforts are ongoing to expand such capacities. I 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? Certainly, as has widely been discussed, opponents are expected to attempt to use asymmetric means when engaged in conflict against the United States. Computer network attack against United States networks—both military and those civilian networks supporting the military—would be one potential type of asymmetry.

To offset such a potential problem, three specific efforts by the Department of Defense could be undertaken—all of which would come under the heading of how to achieve "mission assurance," i.e. 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 work-arounds 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.

This Committee could play an important role by working with the Department of Defense to generate the necessary focus on how to deal with the asymmetric risks posed by cyber.

4. The Need for International Action

It should be readily apparent from the nature of cyber itself and the discussions thus far 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 United States perspective--including security, governance, uses in geo-political context and others—and their solutions will require, or at least be enhanced by, international actions.

There are three international issues which call out for immediate action. First, the 2007 cyber attacks on Estonia should make clear that the North Atlantic Treaty Organization needs to undertake a comprehensive review of its cyber policies. The review would include the obvious question of when has an “armed attack” in terms of the treaty 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, as discussed above). Finally, it needs to analyze NATO capacity to use cyber in stability operations and for influence, also as discussed above. I understand some useful first steps will be put in place at the NATO Summit which will occur this week. While those steps are warranted, they are limited, and a major NATO effort concentrated on cyber is called for.

Second, international influence and international public diplomacy need to be strengthened. There likely will continue to be a major battle of ideas in the 21st century. The United States will need significant international support to prevail, and cyber can be a key element, as I testified to this Committee last year.

Third, as discussed above, 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 major prospects for individuals, for organizations and for governments. But it will require advertent steps to ensure that its potential is best reached.

Thank you for the opportunity to testify, and I look forward to your questions and the opportunity for discussion.