AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

[H.A.S.C. No. 110–141]

# HOLISTIC APPROACHES TO CYBERSECURITY ENABLING NETWORK-CENTRIC OPERATIONS

HEARING

BEFORE THE

TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

OF THE

COMMITTEE ON ARMED SERVICES
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

HEARING HELD
APRIL 1, 2008

U.S. GOVERNMENT PRINTING OFFICE
45–255 WASHINGTON : 2009

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

TERRORISM AND UNCONVENTIONAL THREATS SUBCOMMITTEE

ADAM SMITH, Washington, *Chairman*

MIKE MCINTYRE, North Carolina
ROBERT ANDREWS, New Jersey
JIM COOPER, Tennessee
JIM MARSHALL, Georgia
MARK E. UDALL, Colorado
BRAD ELLSWORTH, Indiana
KIRSTEN E. GILLIBRAND, New York
KATHY CASTOR, Florida
MAC THORNBERRY, Texas
ROBIN HAYES, North Carolina
JOHN KLINE, Minnesota
THELMA DRAKE, Virginia
K. MICHAEL CONAWAY, Texas
JIM SAXTON, New Jersey
BILL SHUSTER, Pennsylvania

KEVIN GATES, *Professional Staff Member*
ALEX KUGAJEVSKY, *Professional Staff Member*
ANDREW TABLER, *Staff Assistant*

# CONTENTS

## CHRONOLOGICAL LIST OF HEARINGS

2008



**TUESDAY, APRIL 1, 2008**

**HOLISTIC APPROACHES TO CYBERSECURITY ENABLING NETWORK-CENTRIC OPERATIONS**

STATEMENTS PRESENTED BY MEMBERS OF CONGRESS



WITNESSES



APPENDIX

# HOLISTIC APPROACHES TO CYBERSECURITY ENABLING NETWORK-CENTRIC OPERATIONS

---

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ARMED SERVICES,
TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES
SUBCOMMITTEE,
*Washington, DC, Tuesday, April 1, 2008.*

The subcommittee met, pursuant to call, at 3:06 p.m., in room 2212, Rayburn House Office Building, Hon. Adam Smith (chairman of the subcommittee) Presiding.

## OPENING STATEMENT OF HON. ADAM SMITH, A REPRESENTATIVE FROM WASHINGTON, CHAIRMAN, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE

Mr. SMITH. Good afternoon. I think we will go ahead and get started.

There is only going to be one set of votes today. Regrettably, it is likely to happen right in the middle of our hearing, so we will just deal with that.

As we understand, Dr. Goodman has a time constraint. Hopefully we will be able to accommodate that.

And you have someone who can sit in for you if you are forced to leave. We will try to get at least your statements in and, you know, get some questioning through and just break when we have to.

I want to call the meeting to order, first of all, welcome everybody here. I thank Ranking Member Thornberry for being here and for our witnesses.

I will do introductions, say a few brief words, and then turn it over to Mr. Thornberry for any comments he might have before taking the testimony from the witnesses.

But I want to thank Dr. Seymour Goodman, who is the Chair of the National Research Council Committee on Improving Cybersecurity Research in the U.S.

Welcome.

Dr. James Lewis, Director and Senior Fellow for the Technology and Public Policy Program at the Center for Strategic and International Studies, better known to all of us on the Hill as CSIS.

And Mr. Franklin Kramer, who is a distinguished Research Fellow at the Center for Technology and National Security Policy at the National Defense University.

Thank you for being here.

The topic of the hearing is cybersecurity, and we look forward to learning from all of you how we can better deal with it. I know what we are trying to do here and I know the effort of the Adminis-

tration and more broadly in the cybersecurity community is to have a holistic approach to what we are talking about.

Obviously, there are the basics. You don't want anybody messing with your network, and you try to set up the best firewalls and passwords and blocks to anyone getting into that network. But, as we know, that alone doesn't do the job. Our networks throughout the military are violated on probably a daily basis, if not more often, to one degree or the another, sometimes harmless, sometimes not. So we really need to develop a better strategy for preventing that.

A piece of that, obviously, is improving our technology, improving the quality of the software that we come up with to protect against our networks being invaded. But the other piece of it is that there is a human element to it too. How can we get the best and the brightest people to be working on our systems? Do we pay them enough to attract them and compete with the private sector to get them here? And then how can we also set up the physical environment where our computer networks are to make sure that we are stopping any access that way, to make sure we know who has access to those varied computers, how the passcodes are set up.

I suppose I shouldn't say this in a public hearing, but just in my own little life, I have so many security codes for so many different things, I tend to use the same one or two or three passwords. If somebody spends just a little bit of time, they could figure out what those are, and have a 33 percent chance with each guess of getting it. We don't want that same thing to be happening with some of our more secure networks.

So what we are really focused on here this afternoon, then, is the holistic approach. And we appreciate folks from out in the think-tank world giving us their ideas on how we can do that and then apply those to the Pentagon's efforts.

And, with that, I will turn it over to Mr. Thornberry for any comments he might have.

[The prepared statement of Mr. Smith can be found in the Appendix on page 29.]

**STATEMENT OF HON. MAC THORNBERRY, A REPRESENTATIVE FROM TEXAS, RANKING MEMBER, TERRORISM, UNCONVENTIONAL THREATS AND CAPABILITIES SUBCOMMITTEE**

Mr. THORNBERRY. Thank you, Mr. Chairman. And I agree with you that it is critical that we have a holistic approach. In some ways, I think some of the cyber issues are indicative of some of the future security issues we are all going to face. It is not just a military function. It is not just a governmental function. And yet it has profound implications for our national security and, therefore, requires attention from all of us.

This subcommittee, from its beginning, has spent a fair amount of time looking at information technology the Pentagon was trying to procure, including information assurance. We have gotten to the point where I believe cyber is a domain of warfare and, therefore, deserving of our attention. Our job is to try to understand where we are and why it matters and then what directions things are moving and then what we need to do about it.

I appreciate the written testimony of the witnesses, particularly where you made specific suggestions about organizational changes or policy changes, technology. People was emphasized in a number of them. This subcommittee does not have jurisdiction to solve all of those things, but it is important for us to understand all of those things. And hopefully we and other colleagues can do what is necessary to protect the country.

So I appreciate you all being here and look forward to our exchange.

Mr. SMITH. Thank you very much.

I will now begin the testimony with Dr. Goodman.

**STATEMENT OF DR. SEYMOUR GOODMAN, CHAIR, NATIONAL RESEARCH COUNCIL COMMITTEE ON IMPROVING CYBERSECURITY RESEARCH IN THE U.S.**

Dr. GOODMAN. Thank you very much.

Mr. Chairman, distinguished members of the subcommittee, thank you for the opportunity to appear before you today to discuss the subject of holistic or comprehensive approaches to cybersecurity enabling network-centric operation.

I am Sy Goodman. I am professor of international affairs and computing at the Sam Nunn School of International Affairs and the College of Computing at Georgia Tech. I recently served as chair of a committee of the National Research Council on Cybersecurity Research in the United States, and we produced a report entitled, "Toward a Safer and More Secure Cyberspace." We have a copy for all.

And I would also like to introduce—accompanying me today is Dr. Herbert Lin, who is sitting behind me. He is the chief scientist for the Computer Science and Telecommunications Board of the National Research Council. And as I have to leave around 4:15, 4:30 to go to Zurich, he may take over for me, as necessary.

Mr. SMITH. That is a long way to go.

Dr. GOODMAN. Long way to go. Just came back from Ethiopia, which was an even longer way to come.

Net-centric operations are the concept under which U.S. military forces and mission partners have rapid access to relevant, accurate and timely information and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data.

These capabilities will depend heavily on modern information technology, but commanders must be able to count on their availability when they need them, must believe that they are providing uncompromised information, and must know that adversaries do not have advanced knowledge of ensuing military activities.

My remarks will focus on the link between cybersecurity and net-centric operation. Given the need for such operations to be conducted in a secure environment, the U.S. must do at least two things.

The first could be characterized as do what you already know how to do. Many good cybersecurity technologies and practices today are not being implemented, and the widespread deployment of even relatively unsophisticated security measures can make it more difficult for an adversary to conduct a cyber attack.

The second could be characterized as learn more about how to be secure. That is, even assuming that everything known today was immediately put into practice, the resulting cybersecurity posture, though better than what we have today, would still be inadequate against today's threat, let alone tomorrow's. And I can assure you the threat is evolving and becoming more serious. Reducing this gap will require substantial and sustained investments in research.

To illustrate my description of necessary cybersecurity research, consider the story of the USS *Yorktown,* an Aegis cruiser that was the Navy testbed for Smart Ship technology in the late 1990's and an important element of the Navy's concept for network-centric operations. A widely used commercial operating system was installed on the *Yorktown* to control a variety of important shipboard applications, including navigation and propulsion. In September 1997, a crewman mistakenly entered an invalid number into a database. He thereby caused a divide-by-zero error that crashed the network, and the ship was left dead for several hours in the water.

What are some of the reasons for cybersecurity research that might be drawn from this episode? First, net-centric operations may have a very intimate connection to commercial information technology. The Department of Defense (DOD) reliance on commercial IT for all kinds of functions means that insecurities in the commercial IT base may have a potentially devastating effect on vital military operations.

Second, humans are part of any IT system. One might argue, as the Navy did at the time, that it was therefore human error that crashed the network rather than a problem with the network itself. But because cyber adversaries are likely to be smart, inducing human error is a strategy that an adversary might well employ.

Third, the testbed could have been designed to provide a backup means for controlling ship propulsion so that a crashed network would not leave the ship dead in the water. A decision to do so would not have depended on detailed knowledge of cybersecurity but, rather, on a philosophy of system design that anticipates failures and provides for ways for mitigating their impact.

Finally, the Yorktown was a testbed for new technology, and, thus, one might argue that failure should be expected. But testbeds often have a way of turning into production systems. That is, even though we build testbeds thinking that we will start over once we get serious about real-world application, in practice the design concepts from these testbeds often remain embedded in the new generation. Thus, understanding how to provide security for legacy systems is a vital dimension of cybersecurity research.

These comments are not intended to diminish the conceptualization of cybersecurity as a technological problem, because in many ways it is a technological problem. One of the six categories for research outlined in our report is blocking and limiting the impact of compromise. Although this category is relatively traditional, it also includes research on how to understand and contain the damage from a penetration and how to recover quickly from a successful attack. Because absolute security of an information system never can be guaranteed, research is needed so that recovery from a successful attack can be accomplished as expeditiously as possible.

But cybersecurity is not only a technological problem. This is a very important statement from a group like ours that is composed largely of some of the most serious and accomplished technical people in the country.

Consider, for example, that today a great deal of security functionality is often turned off, disabled, bypassed, underutilized or not deployed because it is too complex for individuals and enterprise organizations to manage effectively or to use conveniently. It is easy to believe that in military organizations a senior commander can simply order his subordinates to comply with all necessary security measures. To some extent, this is true. Nevertheless, under the pressure of combat operations, it is often the case that faithful execution of security procedures gives way to mistakes and the expediency of circumventing those procedures if they are cumbersome. Thus, good cybersecurity construed in purely technological terms may well be ineffective in an operational context.

Our report includes a category focused on promoting deployment and effective use of cybersecurity technologies, and this category includes research on technology that facilitate ease of use by both end-users and system implementers, incentives that promote the use of security technologies in the relevant context, and the removal of barriers that impede such use. Measures to provide incentives and to remove barriers to the use of security technologies and procedures may have legal, economic, psychological, social and organizational dimensions.

Consider also that net-centric operations, broadly writ, depend dramatically on increased access and functionality afforded by modern information technology. But increased access also multiplies the routes through which adversaries can attack, and increased functionality requires ever more complex systems that are inevitably—and I emphasize inevitably—riddled with vulnerabilities. From a security standpoint, the consequence has been that our increasing dependence on these technologies provides formerly weak adversaries with unprecedented opportunities for attacking us.

In response, we need to reduce the likelihood that an adversary will succeed in penetrating our cyber defenses and to increase the ability to recover from successful penetration of those defenses. But a third logical possibility, also addressed in the report, is to design systems so that critical activities can take advantage of advanced information technology whenever possible but do not require such technology in order to basically function.

In some cases, this may mean providing adequate backup in case the technology has been compromised. In other cases, it may mean foregoing some of the advantages afforded by network-centric operations because the risk is just too great to manage, even with backups in place.

Finally, I was asked to comment on coordination within the Federal Government of cybersecurity research. It was our impression that the scope and nature of cybersecurity research across the Federal Government were not well-understood, that no entity within the—and this is with all due respect to a lot of very good people who are working these problems within the Government. But the scope of what we were concerned with was really much larger than what some of them can basically put under their domains. And

then no entity within the Federal Government had a reasonably complete picture, including classified and unclassified, of the cybersecurity research effort that the Government supports from year to year.

The report argues for a sustained, coherent and comprehensive approach to cybersecurity research. And the lack of a mechanism for drawing this complete picture suggests that the U.S. Government is not well-organized for supporting such an approach, much less in welding the results together to comprehensively make cyberspace safer and more secure.

I thank you, and I will try to answer any questions that you may have.

[The prepared statement of Dr. Goodman can be found in the Appendix on page 30.]

Mr. SMITH. Thank you, Dr. Goodman.

Dr. Lewis.

**STATEMENT OF DR. JAMES ANDREW LEWIS, DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM AT THE CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (CSIS)**

Dr. LEWIS. Thank you for the opportunity to testify.

As you know and as we heard from Representative Thornberry, we have seen new domains for conflict emerge in the last decade. Cyberspace is perhaps the most interesting of these new domains because the cost of attack is low and because it has been an area of significant U.S. vulnerability that our opponents have exploited.

Computer networks and information technology can improve performance for both businesses and for militaries when they are used to provide better information and coordination. We are just beginning to develop the organizational structures and tactics that can make full use of the new technologies to provide informational advantage.

But at the same time, these technologies have created vulnerabilities. Our opponents have seized the opportunity presented by these vulnerabilities to engage in an extensive espionage campaign against the United States.

It is also possible that when intruders access U.S. computers to steal information, they leave something behind. We cannot say that a network that has been penetrated has been infected with hidden malware that could be triggered in a crisis.

China and Russia are the most dangerous of our opponents. China has resources and is willing to spend them. Russia has experience and skill. However, China and Russia are not the only nations interested in cyber warfare, nor are nation-states our only opponents. The emergence of a skilled cyber-crime community has serious implications for U.S. security.

While we have underestimated the risks of espionage and cyber crime, the risk of cyber terrorism is overstated. Terrorists make extensive use of the Internet, but cyber weapons are not yet sufficiently lethal to attract their use.

Last year, we crossed a threshold in cyber attacks with noisy demonstrations launched by a foreign intelligence service against Estonia and with massive sustained attacks on U.S. Government

networks and the networks of allied countries. These attacks prompted the U.S. to begin a major new initiative to secure Government networks. Many of the initiative's elements are highly classified, but we know that it allocates more money and personnel to cybersecurity and directs a number of actions by different agencies.

These are positive steps, but difficult issues remain. One such issue is coordination with the private sector. We need to rethink how the Government interacts with the private sector on cybersecurity.

Another issue is international cooperations. Attacks come over a global network. A national effort can only provide part of the solution. The U.S. will need to work with its allies and perhaps even with our adversaries to improve cybersecurity. Better international security could deter cyber crime. In some countries, criminals face little risk of prosecution. Only international cooperation will change this.

Other forms of cyber deterrence, however, are less practical. It is difficult to deter if you cannot predict the degree of collateral damage to innocent networks. It is even more difficult to deter if you do not know who is attacking. The Internet is too anonymous and too easily deceived. The attacks on Estonia highlighted the problem of anonymity. Identity management must be improved for better cybersecurity.

Federal organization, as of course you know, remains a problem. There is no agency fully responsible for cybersecurity. Better organization is crucial.

Federal organization, strategy, coordination with the private sector and allies—these and other issues remain challenges despite the progress made by the President's cybersecurity initiative.

Much can be done in the time left in the Administration, but much will be necessarily remain unfinished. Presidential transitions are a moment of opportunity. The first year of the next Administration will provide an opportunity to take the cybersecurity initiative and advance it.

To help the new Administration think about this opportunity, the Center for Strategic and International Studies has established a nonpartisan commission on cybersecurity for the 44th presidency. Our goal is to look at cybersecurity as a problem for national security. It has often been regarded as kind of a boutique issue, and I think it is time to recognize that it has moved well beyond that. We hope to develop recommendations for a comprehensive strategy for Federal systems and critical infrastructure, and we want to explore new ways the Government can engage with the private sector.

CSIS intends to make the work of the commission an inclusive process and has asked other experts and groups to participate in the development of recommendations and to make presentations on substantive issues.

To summarize, the attackers have the advantage in cyberspace. The U.S. is behind the curve. The Administration's initiative is good, but it won't be finished by the time they leave office. A new Administration will inherit both challenges and opportunities. Our hope is that CSIS can help identify some of these opportunities.

When we think about network-centric activities, the U.S. has a clear advantage, but this advantage is eroded by our uneven approach to cybersecurity. We will never have perfect security, but we can reduce the opportunities for our opponents to gain advantage against us.

I thank the committee and will be happy to take any questions.

[The prepared statement of Dr. Lewis can be found in the Appendix on page 58.]

Mr. SMITH. Thank you very much.

Mr. Kramer.

**STATEMENT OF FRANKLIN D. KRAMER, DISTINGUISHED RESEARCH FELLOW, CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY, NATIONAL DEFENSE UNIVERSITY**

Mr. KRAMER. Thank you, Mr. Chairman and members of the committee. I am very happy to be here.

Like my colleagues and like the Chairman and the ranking member, I think that cyber needs to be looked at as part of what I would call an effective national and international framework as part of an overall national security strategy.

And I think we also need to make sure that when we think about cyber, we don't simply equate it with the Internet, although that is certainly part of it. But, as people have mentioned, military networks, but also influence operations like TV and radio, cell phones, applications and the like. So it is a big world out there; it is not just an Internet world.

And we also need to think about the fact that it has changed so much in the last 10 years, we ought to be expecting that it will change a great deal in the next 10. And so whatever frameworks we create, we want to make sure that they are not constraints on the expansion of cyber but that they enhance the expansion of cyber. So it needs to be an adaptive approach rather than a static one.

On the security side, as the committee's title for this hearing indicates, I agree, it really needs to be holistic. We need to look at organization. We need to look at classic security. We need to look at R&D and funding, I think deterrence, network-centric operations and international, all of which have been suggested.

My first recommendation to the committee is that there really needs to be created within the executive branch a new organization that would take a holistic look at the cyber set of issues. It probably ought to be at the White House level. In my opinion, it ought to be something along the lines of the Council of Economic Advisors, which is a policy organization, not an implementing organization. And it ought to look at and have the ability to deal with the multiple problems, the multiple arenas, the multiple authorities, to integrate and also to integrate with the private sector.

There is no place in the Government that now does this. And in the absence of an overall approach, everyone is trying to do the best they can, but it is not coordinated. And, therefore, the sum of the parts is far less than what the whole ought to be.

If you had that organization, then you really could look at what I might call the classic security kinds of questions. And there we

all know that cyber is not secure; that is perfectly clear. The question is, how much risk do we want to take, and what is the relationship between the security and the functionality that we want to adopt?

If you think about it, the more Internet sites you go to, the greater chance you have to downloading a virus. But if you don't go to Internet sites, you don't make use of the Internet. So there is a trade-off. I mean, you need to think about that and not expect to have 100 percent security throughout, but some areas you might really want to do it.

In my opinion, where we are on cyber is a little bit like where we were in the early 1970's with respect to the environment. We know there is a problem, and we are just starting to create the framework. And I think that the Government really needs to take what I would call a much more directed approach to cyber and take, I would call it, a differentiated security approach.

There are some areas that I think are just indispensable networks; some key military networks are indispensable. We really can't afford to lose those at all for any period of time. There are other networks that I would call key—I mean, just my words—and they might be the electric grid or certain parts of the financial arena or maybe the communications grid. I mean, we have had the electric grid go down for other reasons for a short period of time, but if it went down for a long period of time, that would be catastrophic. And then the rest, if you will, of cyber, and you might differentiate between say an individual, a small business and businesses.

If you think about those three different elements, for the indispensable areas, I think the Government needs to provide the security. It needs to do the monitoring, it needs to create the possibility of response, it needs to create resilience, it needs to do reconstitution. It does the whole nine yards. For something I would call key, you are going to have a public-private involvement. So you have to work closely there, but the Government might also provide some of the security and provide some of the monitoring and the like. And then for the rest, the Government can encourage and incentivize and the like.

Now, as soon as you get into the private sector, you are immediately going to have very important privacy and civil liberty questions which this committee and other committees in the Congress have raised. So there really needs to be a dialogue on this with industry, with the American people, with the executive branch. And this committee could start that dialogue.

But the upshot of what I am saying is that we really need to think that we are going to spend some time—and it will take several years, just like it did with the environmental area—to create the statute, the regulations and the framework that would allow you to appropriately protect the indispensable, the key and the other networks.

Part of what you need to do to do that, I think, is to create what I would call national cyber laboratories. We don't really have those now. We have national laboratories for nuclear. We have national laboratories for energy. We ought to have national laboratories for cyber. It is a whole new world, and we ought to think about it. Pri-

vate sector does a lot of good research, very good research, but it is focused, appropriately, on the profit motive, because that is what the private sector is about. The DHS's cyber R&D budget for last year was less than $50 million. That is really not quite enough.

So I would suggest a three-part approach, where we increase funding to agencies like the DHS, more funding for R&D, we incentivize the private sector and use them for Government-type research, but we also create a national laboratory-type structure. And, again, I think this committee could think about that.

We ought to also, as you think about security, not to only think about the defense. We have spent a lot of time thinking about deterrence, and I think that deterrence is more possible in the cyber arena than most people think. And I think there are four things that I would propose for you.

First of all, one shouldn't think about cyber deterrence as just cyber versus cyber. I can't think of anything really relatively more dumb than if somebody attacks you, to go and burn out his computer. He is going to have a second computer on his desk. What we really need to think about is deterrence in the context of overall deterrence—political, military, economic and cyber—and then think about what the appropriate responses would be.

We need to differentiate state from nonstate actors, because a state actor normally acts for political movies, and you can think about ways to deter those political motives.

We would probably want to think about different thresholds. If it is a very large attack, we are certainly going to respond strongly, and we should respond strongly. A smaller attack, perhaps it is a law enforcement opportunity.

And then, as was already raised, we really need to do work on attribution. I think we are a little better than some people think we are, but there is no question whatsoever that we need R&D on attribution. And we also need a governing structure, an international structure that allows for attribution and also a framework in which to respond. So, for example, what is NATO going to do if there is an armed attack? Estonia was a wake-up call, but what about the next time? How are we going to deal with these things?

A number of people have already raised the network-centric operations problem. We rely on it. I was in the Defense Department twice for President Clinton's Assistant Secretary for International Security Affairs. I couldn't possibly more strongly support network-centric operations. But it does create a vulnerability. It means that people can have asymmetric attacks against us.

So what should we do about that? I think we need to do a lot more red teaming, vulnerability assessments. I think we need to figure out how to do what I would call blue teaming. How do you operate degraded? Cyber is not the first area where we would think that we would operate in less than perfect conditions, and we need to figure out how to operate with which you might call mission assurance. And, as has already been suggested, research and development on this area is very important; building that concept of vulnerability into the acquisition cycle and deciding which risks one wants to take and which risk one wants to avoid and making that requirement. And, again, this committee could raise that kind of question.

And the last point I would make is the international point. There is no point in thinking about cyber from a national point of view, because cyber simply isn't just national. It is national, but it is national integrated into the international arena.

So we need to do a number of things. I mentioned NATO already. We need to create a dialogue about what constitutes an attack within the meaning of the treaty or even not within the treaty but just, what should NATO do? There is going to be some statements about cyber made at the summit that is ongoing right now, but those are just first steps, so we really need to do more.

We need to think about an international governance structure. The current governance structure for cyber, particularly the Internet, is historical but not logical. There are a lot of countries who are pushing at that governance structure. That is not a reason to change it; it has actually worked well for us. But they will push at it, and we don't have a good structure to support us in the security arena. We don't have a good structure to help on the law enforcement side. We might want to expand, for example, the European Convention on Cyber Crime, have more countries develop it. So the last point I would make is that we need to think about cyber internationally.

With that, let me finish, Mr. Chairman, and I would be happy to answer your questions.

[The prepared statement of Mr. Kramer can be found in the Appendix on page 65.]

Mr. SMITH. Thank you, Mr. Kramer.

Before we take questions, we did have a statement for the record submitted by the Director of Defense Information Systems Agency. Without objection, we will put that into the record for the hearing.

[The information referred to can be found in the Appendix on page 81.]

Mr. SMITH. With that, I want to award the members of the committee for showing up. And I will pass, actually, on my questions. And Mrs. Gillibrand is first on our side, so I will yield my time to her to ask the first questions.

Mrs. GILLIBRAND. Thank you, Mr. Chairman.

I liked your idea of a national laboratory for cybersecurity. Is that consistent with having a Cabinet-level position for cybersecurity, or would that be done separately?

Mr. KRAMER. I think you could do the two in parallel. In other words, the national laboratories, say, for energy are actually run, to some extent, by universities, but you still have a Cabinet-level Energy Department.

I think what you would want to think through is you would want to look at the places, some of which were mentioned, where work is being done and decide whether the best way to do it is to expand on current activities or do you really want to create a whole new activity. And you might—I am going to make a guess here—you would probably end up using some of what already exists and then creating some new ones. And I probably wouldn't just have one; competition is usually good.

Mrs. GILLIBRAND. Because right now I think the majority of our research and development is through the armed services, particularly through the Air Force right now. So would this be something

we are doing in complement with the Air Force? Or would it be something that would be done instead of? Please give me more detail about what you envision would be your ideal scenario.

Mr. KRAMER. I love the Air Force. I don't think—and it has created the Cyber Command, but it is early days. And I think that a lot of people are doing a lot of efforts and particularly at——

Mrs. GILLIBRAND. Would you consolidate that all under this one Cabinet position?

Mr. KRAMER. I wouldn't. I think what I would be inclined to do, as I said, is create laboratory—I am going to call them communities, maybe like Los Alamos or Livermore and the like. But in parallel to those kinds of activities, I would also probably have the more functional efforts by the services that would be more focused on, if you will, the applications.

And one of the reasons, at least from my perspective, is because we don't really know all of the places where we are going to go and we don't really know necessarily how to get there. I mean, Dr. Goodman and his group proposed a very extensive program of research and development. I would like to have a lot of people work on that.

Mrs. GILLIBRAND. Uh-huh. In terms of if—well, you have all briefed various aspects. Obviously, there is the military concerns of cybersecurity and attacks from either a state actor or a nonstate actor. And that has separate questions of whether we have to adjust the laws of armed conflict to reflect these types of attacks and how we would retaliate. And you raised those questions, which I would like to perhaps hear more about your views.

But the other types of attacks, whether it is on civilian targets, such as our electric grid, such as our water systems, such as any chemical plant or nuclear plant or any infrastructure, to the extent that work is now being done solely under the military, is your view that the reason why you have this Cabinet-level position so that you would have another avenue for addressing not only research and development but for creating plans of action for national security on, perhaps, areas that are not necessarily typically under the purview of our military; they are not more under the purview of Governors and States and civilian control issues?

Mr. KRAMER. And the Department of Homeland Security (DHS), as you know, has a substantial role in cyber protection. So it really is a combination, in some sense, of the military and DHS.

But the short answer to your question is yes. The reason I would like to have an overall look at it is because I don't think that we are really taking, to use the committee's word, a holistic look. And I think the only place you can do that is if you have someone that has the Presidential perspective and then can focus on where resources need to go—we don't have infinite resources—and how they might coordinate and the like.

For a time, there was an office in the National Security Council that did some of this, and I just think that there needs to be a White House perspective.

Mrs. GILLIBRAND. Uh-huh. In terms of, you know—I would like, Dr. Goodman and Dr. Lewis, your thoughts on these as well—in terms of their idea about having public-private relationships, particularly perhaps the R&D stage, over the next 5 years, where we

are trying to get the brightest minds in the entire country focused on cybersecurity, defensive postures and the other issues that have been brought up, if you do that, what would be your top recommendations about how to do that and how to be able to keep the security levels that are necessary?

You know, one thing I have been challenging our military leaders on is, how do you expect to recruit the minds and the young folks that are coming out of these great engineering universities around our country to join the military, to have a military training and mission to do this kind of work?

And so one obvious answer is you recruit but you also create public-private partnerships in the meantime to get the best minds. Just quick thoughts on that, and then I have to return it to the Chairman.

Mr. KRAMER. Want to jump in there?

Dr. LEWIS. Go ahead.

Dr. GOODMAN. There is a very broad range of possible answers to what you have asked. Let me just bring up a couple of examples of how to respond to the range of questions that you have.

The fact of the matter is that, in this country and in most of the world, these enormous infrastructures that we will collectively call cyberspace are largely owned and operated by the private sector. Most of the vulnerabilities, in the sense of users being vulnerable and introducing perhaps inadvertently vulnerabilities, are also from the public sector. Our governments, not just the U.S. Government, are really smalltime players in a cyberspace that includes 1.5 billion users on the Internet alone worldwide, and it comes to ground in 200 countries. And the only thing growing faster and that is more extensive are the 3 billion users of cellular telephony in the world. And, again, even in countries that have very weak private sectors, the private sectors really own and operate, and they may be even foreign companies.

So what can governments do in this regard? There are analogies in other areas that have not been very well-pursued, and they have to be pursued very carefully because the dimensions of cyberspace and the range and number of stakeholders is so great and they don't share, sort of, common vulnerabilities or interests.

But we have, throughout other emerging technologies that have caused problems from a safety and security standpoint, we have fairly successfully brought these things into a kind of satisfactory level by what might be described as required mandates from Government. Not strong forms of regulatory control, as we had, for example, when AT&T ran the national carrier; in fact, that is disappearing from most of the world's telecom. But the analogy that I like is, the carnage on highways has at least been partially brought into satisfactory levels with, if you like, required mandates for seatbelts and airbags.

People came up with technologies that were clearly going to be useful. The private sector resisted both technologies very seriously. The Government and lots of private people not vested in the industry saw to it that some very reasonable required mandates were passed that smooth out the problems of competitive advantage by insisting that everybody have these things. They didn't turn out to

be all that expensive. And they have arguably made a huge difference with regard to safety in the automobile world.

We have some analogies in the telecommunications world. We have some, if you would like, regulations——

Mr. SMITH. I am sorry, Dr. Goodman. I wanted to get a couple more questions in before we buzz for our votes.

Dr. GOODMAN. Oh, okay. In any case, let me make two comments. One is that some very thoughtful mandated requirements—I won't use the word "regulation" because it is usually too strong—can probably be put together to really make a significant difference.

Second, with regard to getting good people in the Government, there is, in fact, a major NSF program, and I am the PI for this at Georgia Tech, called Scholarship for Service that attracts some very, very capable people from around the country, students who acquire typically a master's degree, with specialties in cybersecurity. And the program has created cybersecurity programs. And these people very willingly have to have at least a 2-year obligation with Government. And so far, most are sticking with it. It is a great way to get good people in Government, and it is not hard to find people who want to serve.

Dr. LEWIS. Can I throw in three quick words, Mr. Chairman? It will be real quick.

Public-private partnership, you have got a couple of models you could look at. You have something that used to be called the National Institute for Strategic Technology Acquisition and Commercialization (NISTAC). It was at DOD. It is a coordination between the big service providers and the Government. Another model would be the North American Electric Reliability Corporation (NERC) and the Federal Energy Regulatory Commission (FERC), what they do with energy.

But something you could also look at that might fall under this committee's jurisdiction is acquisitions. And DOD is doing some interesting stuff in using its acquisitions to drive better cybersecurity. Part of the new initiative is something called the Federal Desktop Core Configuration. This came out of Air Force, and it mandates a more secure desktop. So there are some areas where we have existing models that would be useful, some of which come out of DOD.

Mr. SMITH. Okay.

I really have to try to move on.

Mr. Thornberry.

Mr. THORNBERRY. Mr. Chairman, I would yield to Mrs. Drake for any questions she may have.

Mrs. DRAKE. Thank you. I will be quick so maybe we can get another one before we go vote.

First of all, thank you all for being here. And I think this is a topic that is so timely, and you have given us a really good overview of it.

My question is, what are we doing today? Is it within each different agency—Homeland Security, FBI, CIA, DOD, here within Congress? Is everybody doing their own thing? And is it all different? Or is this agency you talked about, Director of Informational Services, are they spearheading trying to bring it together?

I mean, I know you have proposed this new group to do it. But what are we doing today?

Mr. KRAMER. The DHS has the lead, the Department of Homeland Security. And there—although it is a classified program, I don't want to go into it here—there has been a new initiative that newspapers have talked about. So I think there is an effort to be more combined.

But I think the long and the short of it is that the agencies are not working as well together as they ought to be. And every year the GAO puts out a report, for example, on how well at least the GAO thinks that the agencies are doing in terms of security. And, speaking loosely, everybody fails.

Mrs. DRAKE. Okay.

Thank you, Mr. Chairman.

Dr. GOODMAN. May I make a quick response to that that is in some ways more fundamental?

The basic architecture and organizational and service structure of the Internet in particular but lots of these networks and cellular telephony fundamentally pushes defense to the end-users. And so it makes not only the kinds of organizations that you have in Government basically forced to think first and foremost of defending themselves, but it makes all of us—Mr. Smith mentioned that he has some problems, perhaps, defending his own computers. That is true of all of us.

And this is fundamental in the architecture and the service-providing infrastructure that we have out there. Defense is pushed to the end-user. The end-user has to fend for itself, whatever organizations or people that are involved.

And given the growing sophistication of the kinds of attacks and attackers that there are out there, we are all, including all the members of my committee, increasingly unable to defend ourselves against the sophisticated, innovative attacks that are taking place out there.

Mrs. DRAKE. Dr. Lewis, did you want to comment?

Dr. LEWIS. I think the ball game has changed a lot in the last couple of months, and so we probably need to take a look at that. There is a lot more coordination.

I would have said the Director of National Intelligence has a major role in this. And there has been a little bit of a turf fight between DOD, DNI, DHS. I think that is resolved, but I don't know.

So we are better than we were would be the short answer.

Mrs. DRAKE. Thank you.

Mr. SMITH. I think one of the questions I have had—we certainly see the threats. This all over the place. There are a lot of systems to protect, a lot of threats coming from a lot of different directions. We haven't yet here had a big catastrophic attack. And I think that is perhaps one of the things that sort of lulls us.

Because a lot of the suggestions that you are talking about come into a lot of money. And I think if we are going to be setting up labs that are for cybersecurity, if we are going to be setting up a new agency, I envision something sort of like the National Counterterrorism Center where someone is pulling it all together, looking at all the threats and then working with DHCs, we are talking a

lot of money. And if we are going to sell people on that, we have to get over the fact that, as of yet, you know, despite all the weaknesses we have talked about, we have not yet been severely struck.

Am I wrong about that, first of all? And second of all, why? What is the answer to that, given all the vulnerabilities that we hear about repeatedly, not just in this hearing but elsewhere?

Dr. LEWIS. We are looking at the wrong things. We got off to a bad start 10 or 15 years ago by thinking this would be an electronic Pearl Harbor. So people are still looking for flames and buildings blowing up. That is not going to happen. It may happen in the future. The real crisis, though, has been the loss of intelligence, the loss of information, the information and intelligence successes. And I think we have had some major failures in the last year or two, even more, that I would qualify as creating the kind of crisis you are looking for. It is a different kind of Pearl Harbor, but we have had serious problems that we can't ignore any more on the intelligence side.

Mr. SMITH. Dr. Goodman.

Dr. GOODMAN. A quick response to that is, ask yourself, who are the most capable people of benefiting from doing malicious things on the Net, or the Nets? And the answer is that it is probably, at least so far, not in their best interest to have caused any kind of catastrophic failure. They are doing extremely well, whether it is criminals, whether it is foreign intelligence agencies and what have you——

Mr. SMITH. Gathering information.

Dr. GOODMAN [continuing]. With things the way they are, whether they are making money, whether they are conducting their own business through these networks. We have set up a wonderful infrastructure for them to operate in their own best interests, and they are doing wonderfully well out there. Why would any of them, at least under current kinds of conflict situations—maybe if there is a serious war with China or what have you, this could change—but why would any of them want to bring it down?

Mr. SMITH. The question would be al Qaeda and the terrorists that would want to cause us as much economic damage as possible, so if they could hit our network and take it down, causing us massive economic damage, they would want to do that, I would presume.

Unfortunately, we have to go vote. And I have a heart to stop shortly after 5 o'clock. We have three votes. We should be able to be back here before 4:30. I will come right back after the last vote. Any other members who want to come back, I thank them for their patience.

Thank you.

[Recess]

Mr. SMITH. I think we will go ahead and get started. I don't know how many other members will be back this late in the afternoon. I have some questions, I am sure Mr. Thornberry does as well; so we will take a stab at that. And actually, if you could just identify yourself for the record, standing in for Dr. Goodman there.

Mr. LIN. My name is Herb Lin, Chief Scientist from the Computer Science and Telecommunications Board of the National Research Council.

Mr. SMITH. Welcome. Thank you for joining the panel. Actually, I will go ahead and yield to Mr. Thornberry, if for no other reason than because I haven't had a chance to look back down at my notes.

Mr. THORNBERRY. Well, I haven't found my notes. They sort of disappeared while we were gone. Not that they were all that great a thing, but—I don't know, I made several notes while we were going, and they seem to have disappeared.

Let me ask this. Has any of you all's organizations looked at the question I think that Ms. Gillibrand asked about the authorities—Title 10 authorities and perhaps Title 50 and other things on cyber—and had any suggestions on what Congress ought to begin to think about when it comes to what constitutes an attack on our Nation; what is the proper, you know, role of the military, et cetera, et cetera? Has anybody gone down that trail yet?

Dr. LEWIS. We actually came up with a list that I can share with the committee of the various laws, including the laws covering DOD, that affected cybersecurity. It was, unfortunately, a long list. If I remember, we felt like we didn't finish it, but we had three pages, including Title 10, a lot of authorities. And one of the things I hope we can do is go through and figure out where the authorities need to be deconflicted.

One the things that has come up several times in discussions I have had with other people is the need for some sort of doctrine, a cyber doctrine for the U.S. And you know, knowing DOD as you do, you know that there is doctrine for everything. We don't have a national cyber doctrine. So that might be a useful place to look at. But deconflicting the authorities is really going to be complicated because——

Mr. THORNBERRY. That is the easy part, deconflicting. To make sure the authorities are there for the advancements, I think that is even harder.

Mr. SMITH. Yeah. I want to dive in there, because what is something that really strikes me as challenging about this from your testimony in the cybersecurity arena is sheer volume. You talk about coming up with sort of a national—I forget the word you used, "strategy" or——

Dr. LEWIS. Strategy.

Mr. SMITH. It was something you had just said a moment ago. And I guess the problem I have with that is, you know, there are so many systems out there that are different. And also the talents of the people that you have working on those systems are different. And how you are going to set up your network is going to have to match both; both the talents and the relative technology IQ, if you will, of the people working there and the systems.

I mean, are we in a situation in cybersecurity where it sort of defies an overarching plan and a centralization? And you can correct me if I am wrong here, but I am thinking in a National Counterterrorism Center sort of model where we had all these organizations engaged in counterterrorism and intelligence gathering, but there was a concern about stovepiping and no sort of comprehensive strategy. Well, once al Qaeda emerged as a central threat it is like, okay, anybody affiliated with them, we are tracking those targets, we can put the National Counter Terrorism Cen-

ter (NCTC) up top, have them keep track of that stuff, and it has worked reasonably well.

I just wonder in the cyber arena is there just such a sheer volume of vulnerabilities and areas here that it defies that sort of central coordination?

Dr. LEWIS. What I have thought in the past, speaking for myself now, is there is this, you know, huge profusion of different networks, different technologies, different actors. You can do a couple things, though. The first is there are some networks that are more important than others—and you heard that, I think, in Mr. Kramer's testimony—the financial network, the telecom network, the electrical grid; maybe the fuel supply, the Petroleum Oil Luricants (POL) pipeline, government services like DOD. So you can narrow it down and say if those networks continue to operate, we will be able to continue to function as an economy and our military capabilities won't be badly damaged. So focusing in on key networks would be a good first step.

The second part is, you know, I do think you can come up with a strategy. The strategy has to be linked. And I think that was implicit in all our remarks. It has to be linked to some new organization. And the stovepiping problem, you are very familiar with it from DOD. This is why we had the Department of Defense and then why we had Goldwater-Nichols, and now we have tried it with DHS to break stovepipes, put them all in one place. Tried it with the Director of National Intelligence (DNI). So you can rate the effectiveness of those attempts differently, but I think we need to make a similar kind of attempt for cybersecurity. How do we get people to work, you know, across agency boundaries, and whether that is a Cabinet office or something else?

Mr. SMITH. Mr. Kramer, you are shaking your head as he is speaking.

Mr. KRAMER. Going to the Title 10, Title 50, I mean I dealt with that, so to speak, in real life when I was in the government. I think on that there have been some advances. And you are going to have—presumably you are going to have classified hearings, or have had classified hearings, and that will come right up.

But there are efforts, substantial efforts to deal with that issue. But I do think, I do think we have made progress in terms of what I am going to call—I keep calling it classic security, you know, the defensive side of security, the new initiative. Again, you are going to have hearings on these, I presume.

One thing I think that would make a big difference which would help is if a lot of aspects of cyber were either declassified or substantially reduced in classification. This is an area in which I think it is wildly overclassified. And if one compares cyber to electronic warfare, which is not all that different, but cyber is normally way up here in classification, electronic warfare has some programs that are up there, but a lot that are just sort of what I call secret level classified, and a lot of principles and the like that are not actually classified at all, and it makes it a lot easier to integrate that both into military operations and to have people talk about it.

So again, something I would encourage the committee to look at, and you know, obviously, the Vice Chairman, for example, the current Vice Chairman is obviously very interested in this issue, and

he is someone who I have talked to about the classification issue, and I would encourage you to do it.

Mr. SMITH. Okay.

Mr. THORNBERRY. I wanted to ask the two of you all, I thought Mr. Kramer's differentiation of the networks that are most valuable, where the government has a responsibility to actively defend versus a lesser network where the government has less, versus—makes some sense to me. And I think, Dr. Lewis, you implied in your last answer that probably that does.

But I want—you know, you always hear whatever it is, 94 percent of the network is in private hands. That doesn't mean all 94 percent is of equal value to the security of the Nation, which is where we are coming from here. But I wonder if you agreed with that idea of having tiers and different levels of responsibility for those tiers.

Dr. LEWIS. Well, the tiered idea makes a lot of sense because there are some things that—you know, the electrical network is the best example. If the electricity goes off, nothing works. So we have a responsibility, the government has a responsibility to ensure that it continues to supply power.

What the complicated part is that there are so many different agencies that currently have some piece of making sure the electrical power grid continues to deliver. You have got the Department of Energy, you have got the Nuclear Regulatory Commission, you have got the State commissions. You get into a very complicated—you have got DHS to some extent—complicated situation where each of them say, You should do something. They don't always say the same thing.

There are a few other networks, you know, financial, where you know you have multiple regulators. So that is one of the issues for us is multiple laws, multiple requirements, multiple regulators for these few crucial networks. And working through that is going to be very difficult.

Mr. LIN. I think from the perspective of the National Research Council (NRC) report, we say that it is really hard to make—although the separation into tiers of different responsibilities may make some conceptual sense—it is hard to make that separation operationally. I mean you know, my dad's personal computer is on a public—you know, is connected to an Internet service provider that will be used in a botnet attack against something critical. And so being able to separate them cleanly is kind of a problem.

Mr. THORNBERRY. Yeah. And I guess, Mr. Chairman, that leads me to the other part of this. I think you have each in the testimony talked about the international—need to have international. So does that mean—because it is hard to separate, particularly with the Internet, does that mean we are put in a position of defending the whole global Internet? How does geography interface with this need to have greater international cooperation?

Mr. KRAMER. Can I jump in on this? I think one of the things I think is really important is to recognize that just because we can't do everything doesn't mean we can't do some things, and also that this is going to be an incremental-type approach of improvement. We built the Internet. And again I want to say it is not just the Internet. It is networks, if you want to call it that. Cell phones

and the like are very important in some countries. We didn't build them thinking about vulnerability. We built them thinking about functionality. And now we are sort of trying to redo it.

There are some ways to make improvements. And again, I happen to use the environmental laws notion as an analogy. That is to say in 1970 we didn't have pretty much anything. By 1985 we had had a lot, and it worked all right.

The NRC used the example of, you know, required mandates. I think there is a lot that can be done. And when you go over to the international arena, the more that you can bring in other countries, the more opportunities you have. But it certainly is not the case that you are going to get a perfect world. But you could do things like, for example, limit down the number of gateways or put Supervisory Control and Data Acquisition (SCADA) systems on a different kind of—I am going to call it computer, so to speak, network or router or the like. You could do a lot.

Mr. THORNBERRY. Things that would not compromise technology.

Mr. KRAMER. Right. In fact, you can use some advanced technologies to do different things. But one of the problems I think that conceptually occurs is people recognize that there are so many problems that they sort of in a certain sense throw up their hands. I think everyone agrees there are a lot of problems. So the issue is okay, you know, let's take the first step.

Mr. SMITH. We talked a little bit how to coordinate this and the different ways to do that and get the stovepiping issue. And I don't think any of you had recommended, you know, the creation of a new cybersecurity agency. I think you talked about creating national laboratories that focused on cybersecurity, which I think makes a great deal of sense.

So you are satisfied that, you know, basically using United States Strategic Command (STRATCOM) as sort of the center right now, and then coordinating out from there, that we don't need some new bureaucracy; we just need to work within the ones we have, better.

Dr. LEWIS. Well, I have thought about this a little bit. And first of all, I don't think we need to go back to a czar. I usually don't think the word "czar" is in the Constitution.

Mr. SMITH. Right. Bad rep at this point, too.

Dr. LEWIS. That's right. This is a real national security problem now. It is not a boutique issue. For me that means it should be in the National Security Council (NSC). And so we need a senior director, we need an office, we need somebody who can provide the same sort of coordination we have for intelligence or military matters or proliferation. That would be one solution.

Mr. SMITH. And you think NSC is a better place than DOD?

Dr. LEWIS. I do. Because you have at least seven agencies that think they own the majority of this problem: DHS, Energy is involved, Justice, FBI. Who else has the power to coordinate? DOD? I think it has to be at the White House.

Mr. KRAMER. Can I just—I did recommend a new organization. And I said it as an analog to the Council of Economic Advisers. You happened to use the NCTC example. Could be that. That is a little bit more implementing. The reason I didn't put it in my head in

the NSC is because I think cyber is bigger than security, and certainly bigger than security from the defensive side.

There is a huge aspect of cyber with respect to influence, a huge aspect of cyber using it for, say, enhancing stability operations, a positive side. There are just the issues of net neutrality, pure technology, and the like.

So you could have—you know, exactly where the agency goes, I don't want to get all bent out of shape over that. But the reason I suggested a cyber council as opposed to just putting it in the NSC is because we should deal with all these issues' breakdown, but the impact has to be the same.

With respect to the DOD itself, I mean the DOD's reorganized on cyber and STRATCOM itself about three times in the last 2 years. So they are working hard. I would encourage the committee to keep talking to them a lot, because I don't think they even think they have the right answers yet, but they are trying to find them.

The new cyber command for the Air Force, how does that relate to STRATCOM, which is a combatant command? Not clear. What is the Army's role, the Navy's role, the Marines' role? Not clear. Everyone is working hard, but I think there is a lot to be talked about with the committee.

Dr. LEWIS. The reason I thought the NSC was better is because when you create some of these new bodies—this is a debate we need to have—they end up being peripheral, they end up being sidelined. They end up being—you know, the drug czar, you know, and the offices over there on——

Mr. SMITH. They end up being another stovepipe basically as opposed to a coordinator, except in rare situations. And that is why I keep coming back to——

Mr. KRAMER. The point is well taken. I think this is one of these issues that should be talked out. But there is no—if we created a better overall office in the NSC as opposed to the Kramer suggestion about the cyber council, I would be very happy.

Mr. SMITH. And again, it is a major challenge, because if you are looking at the counterterrorism threat or—I forget the organization you mentioned earlier—it is more narrow in scope. Every single department of the government at every single level has multiple networks and goes into the big broad Internet as well. So there is, you know, really no way to sort of round them all up and put them under one umbrella. There has to be, I would think, a certain strategy that takes into account the autonomy that is going to come with that and try to have people work within their own framework. That is all I have got.

Mr. Thornberry.

Mr. THORNBERRY. This is the unanswerable question, I guess. But the thing I am struggling most with cyber is how fast it changes. I think every morning when I turn on my computer I get a new virus update. Just pretty much every day. When you look at charts of changing and computing power, you know, those are steep lines. And what I grapple with is how in the world can a giant bureaucracy as cumbersome and stovepiped as it is, even if there are improvements made, keep up with that level of change?

In cyber you don't really even have time for human intervention in carrying out operations at least. Things move so quickly. And it

just seems to me one of the challenges we face is how to make this agile and adaptable at the appropriate pace. I don't know if that is a question or a concern. But government is not that way, anyway. And how we do that in this field may be one of our biggest challenges.

If you all have suggestions on how to do it, I would love to hear them.

Mr. LIN. In the National Research Council (NRC) report we basically took that one on and said that top-down priority setting isn't going to work in this area, at least in the research domain. And we thought that there had to be some priority setting, but it ought to be done by the people who were closest to the technical understanding of the threat; that is, the program managers and the like. We just didn't see any way that a top-down organization could meaningfully set priorities here that wouldn't be overtaken in months.

Mr. KRAMER. You know, one of the things, to take an analogy and go to the financial structures, we have an enormously adaptive financial set of markets—not doing so well this past couple of weeks, but in general really enormously adaptive and flexible. And yet they do have regulation. And maybe they need more and maybe they don't. I don't know. That is one of the questions you all will be debating.

But we were able to create some useful regulation, FDIC, Fed, SEC, et cetera, even though the specifics of how the operation runs is, I am going to call it "distributed." In that case it is the market. But nonetheless. So I think it is possible to create some central vision and direction, and then distribute out the capacities.

So, for example, on the particulars of what is the best research in a particular area, I am sure Dr. Lin knows a lot more than I do and so, you know, he is probably right. But I am pretty doubtful that any particular set of scientists would be able, better than a set of policymakers, to step back and say what are the biggest issues that we are facing as policymakers? So you are going to need to integrate the two is, I guess, what I would say.

Mr. SMITH. I was going to ask a question about the money side of this. As I mentioned earlier, a lot of these things, certainly setting up laboratories and implementing some of these programs—and even recruiting, you know, better talent—pay is certainly going to be a factor, not the only factor, but one. But within our given systems, then, do you see opportunities where, without increasing the budgets, we could move the money around and get more for the money we are already spending? I ask that for obvious reasons, because those are policy changes we can make as opposed to, gosh, if you gave us $10 billion we could do a lot more. And I am sure that is true. But we have a real tight budget situation.

Mr. KRAMER. You know, one of the questions is which kinds of money are you giving me to move around? In other words, is it just cyber money we are moving around or is it other money? Because one of the questions you will want to ask yourself——

Mr. SMITH. Either one is fine.

Mr. KRAMER. I suspect that within the overall amounts of money that are available for national security, we could create a—we could and I would say we should create a somewhat higher priority

on various aspects of cyber. Again not just—for my money, not just the technical sides of security, although I think that is important, but also some of the organizational—some of the people and the like that we have talked about. And sure, there is no free lunch; $10 billion is just not automatically available. I understand the committee doesn't have it, and so we really do have to do trade-offs.

Dr. LEWIS. We need to start reprioritizing how we look at threats. And though there are some threats, and I won't say which ones, that maybe were important 20 years ago, 15 years ago, and we now would have to say maybe cyber is a more important priority and maybe money should flow from older programs to cyber. And that is always a painful decision. But if you look at the size of the Defense budget and if you look at the size of the Intelligence budget, you ought to be able to scrape up—one should be able to scrape up more money for these kind of activities.

And I think it is getting people to realize there is a real threat, there has been real damage, and we need to do a little more. To their credit, the Administration is trying to do that. And I think, you know, you can get a classified briefing on their money. I think it was a 12 percent increase for cybersecurity this year, 12 or 15. And that is good. But it just—one year is not enough. So where would you take this from?

Mr. SMITH. And we are actually—I think we are getting a classified briefing tomorrow morning at 8:45. I forget; who is that, DOD?

Mr. LIN. There is one other possible shifting that you could do, which is that if you look at the amounts devoted to research, and Dr. Kramer mentioned it earlier, about the size of the DHS budget for R&D, if you look at the amounts devoted to patching systems versus the amounts devoted to research, that is way, way, way outbalanced. Lots more, lots more on the patching systems side and very little on the research side.

Mr. SMITH. Right.

Dr. LEWIS. What you might hear tomorrow, too, is the Air Force in particular—I think it was a guy named John Gilligan who used to be the Chief Information Officer (CIO), realized he was spending a lot of money on patching—came up with this idea, what they now call the Federal desktop core configuration that cut his costs on the patching side. And so one thing we can ask is—that was just for one, that was for operating systems. There are probably other opportunities to move out of the Band-Aid approach to a more strategic direction. And that is where you could get a little more money.

Mr. SMITH. Absolutely. Well, thank you all very much for your testimony. Sorry about the interruption. I appreciate the information, and look forward to continuing to work with all of you. This is certainly going to be a major focus of our committee. It was last year. And we will look for any ideas and any ways to improve our cybersecurity approach. Thank you for the information.

[Whereupon, at 4:55 p.m., the subcommittee was adjourned.]

# A P P E N D I X

APRIL 1, 2008

**PREPARED STATEMENTS SUBMITTED FOR THE RECORD**

APRIL 1, 2008

**Statement of Terrorism, Unconventional Threats and Capabilities Subcommittee Chairman Adam Smith**
**Opening Statement**
**Hearing on Cybersecurity**

April 1, 2008

"Good afternoon. Today the Terrorism, Unconventional Threats and Capabilities Subcommittee will hear testimony regarding Holistic Approaches to Cybersecurity Enabling Network Centric Operations. This is an area of our national defense that is not fully understood, especially with regards to the costs of a cyber attack, and I appreciate our panel sharing their expertise with us today.

"As our forces move closer to the vision of network-centric operations, it's absolutely crucial that we make proper investments in cybersecurity. Net-centric warfare depends not only on the operation of network connections and infrastructure, but on being able to trust the information being shared across the networks in question. That means we have to not only protect highly vulnerable physical choke-points of global network infrastructure, but also take into account factors such as the potential security vulnerabilities posed by outsourcing of coding functions to overseas contractors, as well as the 'human factor' – weak passwords, vulnerability to social engineering, and the like.

"We also have to understand the nature of the battlefield. Unlike traditional physical battlefields, cyberspace is not neatly divided into friendly space and hostile space. Our operations share space with our interagency partners, allies, hostile states, criminal entities, terrorist communities, and hackers with too much time on their hands. Unlike traditional weapons of mass destruction, we have very limited abilities to prevent the proliferation of damaging weapons in this sphere of operation; once a tool is invented and made available online, it is available to anyone.

"As with other areas that touch on DoD's technology policies, we need to take a hard look at our personnel recruitment incentives as well as our acquisition policies. We need the best and the brightest working for us, and that means our incentive packages have to be competitive with the private sector.

"We also need the best technology as quickly as possible, and that will mean reexamining our acquisition policies. Know-how and technological capabilities are the only ways to stay ahead of the curve when anyone with connection to the Internet can potentially disrupt our operations.

"This subcommittee is committed to making sure our policies support a robust information defense while balancing legitimate privacy concerns. In addition, we'd be interested to hear from our panel on areas of existing law that might have been written for a pre-Information Age era and that should be revisited to ensure we are not constrained by laws that did not anticipate the emergence of net-centric operations.

"Again, I want to thank our panel and Ranking Member Thornberry, as always, for his bipartisan work on this subcommittee."

**Written Testimony of**

**Dr. Seymour Goodman**

**Chair, Committee on Improving Cybersecurity Research in the United States**

**Computer Science and Telecommunications Board**
**National Research Council**

**Before the**
**Subcommittee on Terrorism, Unconventional Threats and Capabilities**
**Armed Services Committee**
**U.S. House of Representatives**

**April 1, 2008**

Mr. Chairman, distinguished members of the Subcommittee: Thank you for the opportunity to appear before you today to discuss the subject of holistic approaches to cybersecurity enabling network centric operations.

My name is Seymour Goodman, and I am professor of international affairs and of computing, at the Sam Nunn School of International Affairs and the College of Computing at the Georgia Institute of Technology. I recently served as chair of a committee of the National Research Council on cybersecurity research in the United States; this committee produced a report entitled "*Towards a Safer and More Secure Cyberspace*." The National Research Council is the operating arm of the National Academy of Sciences, National Academy of Engineering, and the Institute of Medicine of the National Academies, chartered by Congress in 1863 to advise the government on matters of science and technology.

According to the Joint Chiefs of Staff, net-centric operations are the operational concept under which U.S. military forces and mission partners have "rapid access to relevant, accurate, and timely information, and also the ability to create and share the knowledge required to make superior decisions in an assured environment amid unprecedented quantities of operational data."[1] It goes without saying that access to such information and the ability to create and share information are capabilities that will depend heavily on modern information technology. (A number of NRC reports address matters related to net-centric operations in a naval context, including *FORCEnet Implementation Strategy* (2005), *C4ISR for Future Naval Strike Groups* (2006), and *Network-Centric Naval Forces: A Transition Strategy for Enhancing Operational Capabilities* (2000).)

[1] CONNECTING THE WARFIGHTERS, Joint Net-Centric Operations (JNO) fact sheet, J-6, available at http://www.jcs.mil/j6/c4campaignplan/JNO_fact_sheet.pdf.

But in order to leverage these capabilities effectively, commanders must be able to count on their availability when they need them, must believe that they are providing trustworthy and uncompromised information, and must know that adversaries do not have advance knowledge of ensuing military activities. Moreover, all of these things must be true in the face of an adversary wanting to compromise these capabilities. Ensuring the availability, integrity, and confidentiality of information are the classical goals of cybersecurity, and high-confidence authentication is often added to this list.

My remarks will focus on the link between cybersecurity and net-centric operations.

Given the need for net-centric operations to be conducted in a secure environment, two thrusts are necessary. The first could be characterized as "do what you already know how to do." There is much that is known about cybersecurity technologies and practices today that is simply not put into practice, and even the widespread deployment of relatively unsophisticated cybersecurity measures can make it more difficult for an adversary to conduct a cyberattack.

The second could be characterized as "learn more about how to be secure." That is, even assuming that everything known today was immediately put into practice, the resulting cybersecurity posture—though it would be stronger and more resilient than it is now—would still be inadequate against today's threat, let alone tomorrow's. Reducing this gap—a gap of knowledge—will require both traditional and unorthodox approaches to research.

Traditional research is problem-specific, and there are many cybersecurity problems for which good solutions are not known. (A good solution to a cybersecurity problem is one that is effective, is robust against a variety of attack types, is inexpensive and easy to deploy, is easy to use, and does not significantly reduce or cripple other functionality in the system of which it is made a part.) Research will be needed to address these problems.

But problem-by-problem solutions, or even problem-class by problem-class solutions, are highly unlikely to be sufficient to close the gap by themselves. Unorthodox, clean-slate approaches will also be needed to deal with what might be called a structural problem in cybersecurity research now, and these approaches will entail the development of new ideas and new points of view that revisit the basic foundations and implicit assumptions of security research.

To motivate my description of necessary cybersecurity research, consider the story of the U.S.S. Yorktown, an Aegis cruiser that was the Navy testbed for "smart ship technology" in the late 1990's. As you know, the Aegis system has been an important element of the Navy's concept for network-centric operations. A widely used commercial network operating system—Windows NT—was installed on the Yorktown to control a variety of important ship-board applications, including navigation and

propulsion. In September 1997, a crewman mistakenly entered an invalid number into a database. He thereby caused a "divide-by-zero" error that crashed the network—and the ship was left dead in the water for several hours.

What are some lessons for cybersecurity research that might be drawn from this episode?

- Net-centric operations may have a very intimate connection to commercial information technology. Indeed, the day has long since passed when the DOD can rely on custom-built information technology—and its reliance on commercial IT for all kinds of functions means that insecurities in the commercial IT base may have a potentially devastating effect on vital military functions.

- Humans are part of any IT system. One might argue, as the Navy did at the time, that it was therefore "human error" that crashed the network rather than a problem with the network itself. But because we assume that cyber-adversaries are smart and highly motivated, inducing human error is a strategy that an adversary might well employ.

- A decision could have been made to provide a back up means of controlling ship propulsion, so that a crashed network would not leave the ship dead in the water. A decision to do so would not have depended on a detailed knowledge of cybersecurity as cybersecurity is traditionally construed, but rather on a philosophy of system design that anticipates failures and provides for ways of mitigating and containing their impact.

- The Yorktown was a testbed for new technologies, and thus one might argue that failures should be expected. True enough, but the argument is incomplete. Testbeds often have a way of turning into a legacy base—that is, even though we built testbeds and experimental applications thinking that we can throw them away when we "get serious" about an application that will be deployed for real, in practice the design concepts from these testbeds and experimental applications often remain embedded in the new generation. This reality suggests that understanding how to provide security for legacy systems is a vital dimension of cybersecurity research.

These comments are not intended to denigrate the conceptualization of cybersecurity as a technological problem, because in many ways, it is a technological problem. One of the six categories of needed research outlined in our report is *blocking and limiting the impact of compromise.* This category is relatively traditional, including the design and development of secure information systems and networks that resist technical compromise. Somewhat unusual in the topics for inclusion in this category was the need for research to understand how to contain the damage from a penetration, how to lock down a system under attack, and how to recover quickly from a successful attack. Because absolute security of an information system never can be guaranteed, that

research is needed so that recovery from a successful attack can be accomplished as expeditiously as possible.

But it would be a bad mistake to conceptualize cybersecurity as only a technological problem. Indeed, we found in our work that areas ranging from anthropology, sociology, design, economics, law, psychology, human factors, and organizational theory were relevant to cybersecurity.

Consider, for example, a proposition that very few cybersecurity experts would deny—the most effective security measures or technologies provide very little benefit if they are not deployed in operational systems, and even if they are deployed, they provide very little benefit if they are not used, or even worse, misused or bypassed by users because they are not well understood or they interfere with getting work done. Today, a great deal of security functionality is often turned off, disabled, bypassed, and not deployed because it is too complex for individuals and enterprise organizations to manage effectively or to use conveniently.

It is easy to believe that in military organizations, a senior commander can simply order his subordinates to comply with all necessary security measures—and to some extent, this is true. Nevertheless, under the pressure of combat operations, it is often the case that faithful execution of security procedures gives way to the expediency of circumventing those procedures if they are cumbersome. Indeed, you might want to inquire whether the use of secure STU-III telephones increases or decreases at the onset of combat operations.

Such reasons suggest that cybersecurity construed in purely technological terms may well be ineffective in an operational context. Thus, our view of necessary cybersecurity research includes a category focused on *promoting deployment and effective use* of cybersecurity technologies. This category includes research on technologies that facilitate ease of use by both end users and system implementers, incentives that promote the use of security technologies in the relevant contexts, and the removal of barriers that impede such use. Measures to provide incentives and to remove barriers to the use of security technologies and procedures may have legal, economic, psychological, social, and organizational dimensions.

The NRC report also covered four other categories of necessary research:

- *Enabling accountability*. This category includes matters such as remote authentication, access control and policy management, auditing and traceability, maintenance of provenance, secure associations between system components, intrusion detection, and so on. In general, the objective is to hold anyone or anything that has access to a system component—a computing device, a sensor, an actuator, a network—accountable for the results of such access. An example of research in this category is attribution. Anonymous attackers cannot be held responsible for their actions and do not suffer any consequences for the harmful actions that they may initiate. But many computer operations are inherently

anonymous, which means that associating actors with actions must be done explicitly. Attribution technology enables such associations to be easily ascertained, captured, and preserved. At the same time, attribution mechanisms do not solve the important problem of the unwittingly compromised or duped user, although these mechanisms may be necessary in conducting forensic investigations that lead to such a user.

- *Deterring would-be attackers.* This category includes legal and policy measures that could be employed to penalize or impose consequences on cyberattackers, and technologies that support such measures. In principle, this category could also include technical measures to retaliate against a cyberattacker. One illustrative example of research in this category would facilitate the prosecution of cybercriminals across international borders. Many cybercrime perpetrators are outside of U.S. jurisdiction, and the applicable laws may not criminalize the particulars of the crime perpetrated. Even if they do, logistical difficulties in identifying a perpetrator across national boundaries may render him or her practically immune to prosecution. Research is needed to further harmonize laws across many national boundaries to enable international prosecutions and to reduce the logistical difficulties involved in such activities. Other illustrations are provided in the main text of the report.

- *Crosscutting problem-focused research.* This category focuses elements of research in the above categories onto specific important problems in cybersecurity. These include security for legacy systems, the role of secrecy in cyberdefense, coping with the insider threat, and security for new computing environments and in application domains.

- *Speculative research.* This category focuses on admittedly speculative approaches to cybersecurity that are unorthodox, "out-of-the-box," and also that arguably have some potential for revolutionary and nonincremental gains in cybersecurity.

The committee also examined the lack of substantive progress in closing the gap between the nation's cybersecurity posture and the cyberthreat. Indeed, it observed that after more than 15 years of cybersecurity reports pointing to an ominous threat, and more than 15 years in which the threat has objectively grown, there is not a national sense of urgency about cybersecurity.

The committee concluded that the lack of adequate action in the cybersecurity space could be largely explained by three factors:

- Past reports have not provided the sufficiently compelling information needed to make the case for dramatic and urgent action. If so, perhaps it is possible to paint a sufficiently ominous picture of the threat in terms that would inspire decision makers to take action. Detailed and specific information is usually more convincing than information couched in very general terms, but

unfortunately, detailed and specific information in the open literature about the scope and nature of the cyberthreat is lacking. Many corporate victims of cyberattack, for example, are reluctant to identify themselves as being victims for fear of being cast in a bad light relative to their competitors.

- Even with the relevant information in hand, decision makers discount future possibilities so much that they do not see the need for present-day action. If that is the case, then nothing short of a highly visible and perhaps ongoing cyber-disaster will motivate actions. Decision makers weigh the immediate costs of putting into place adequate cybersecurity measures, both technical and procedural, against the potential future benefits (actually, avoided costs) of preventing cyber-disaster in the future—and systematically discount the latter as uncertain and vague.
- The costs of inaction are not borne by the relevant decision makers. The bulk of the nation's critical infrastructure is owned and operated by private-sector companies. To the extent that these companies respond to security issues, they generally do so as one of the risks of doing business. But they do much less to respond to the threat of low-probability, high-impact (i.e., catastrophic) threats, although all of society at large has a large stake in their actions.

Although these observations were made regarding information technology outside the military sphere, I believe that they—and especially the last two factors—are highly relevant to DOD cybersecurity issues as well.

One might also consider the fact that net-centric operations, broadly writ, depend on dramatically increased access and functionality afforded by modern information technology. But increased access also multiplies the routes through which an adversary can attack us, and increased functionality has required ever more complex systems that are inevitably riddled with vulnerabilities. From a security standpoint, the consequence has been that our increasing dependence on these technologies provides formerly weak adversaries with unprecedented ways of attacking us.

To address these vulnerabilities, the report suggests that we need to reduce the likelihood that an adversary will succeed in penetrating our cyber-defenses and to increase the ease of recovering from successful penetrations of those defenses. But a third logical possibility, also addressed in the report, is to design systems so that critical activities can take advantage of advanced information technology when appropriate and possible but do not require such technology in order to function. In some cases, this may mean providing adequate means for backup in case the necessary IT is unavailable or under attack; in other cases, it may mean foregoing some of the advantages afforded by network-centric operations because the risk is just too large to manage even with backups in place.

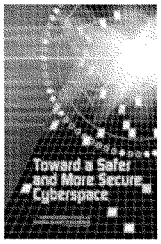
Finally, I was asked to comment on coordination within the Federal government of cybersecurity research, which our report addressed. It was our impression that the scope and nature of cybersecurity research across the federal government were not well understood, including by government decision makers, and that no entity within the

federal government had a reasonably complete picture, including classified and unclassified, of the cybersecurity research efforts that the government supports from year to year. To illustrate the issue, in 2004, the President's Information Technology Advisory Committee, backed by the National Coordination Office for Networking and Information Technology Research and Development, was able to determine the DARPA investment in cybersecurity research and development (R&D) for FY 2004 only within a factor of about four (that is, PITAC determined that figure to be between $40 million and $150 million).

Our report argues that an effort to develop a complete picture should distinguish clearly between research and development, including both classified and unclassified R&D; disaggregate (and publish) government-wide budget figures associated with different areas of research focus; and track budget figures from year to year. Further, the report argues for a sustained, coherent, and comprehensive approach to cybersecurity research, and the lack of a mechanism for drawing this complete picture suggests that the U.S. government is not well-organized for supporting such an approach.

Thank you. I will try to answer any questions you might have.

http://www.nap.edu/catalog/11925.html
We ship printed books within 1 business day; personal PDFs are available immediately.




**Toward a Safer and More Secure Cyberspace**

Seymour E. Goodman and Herbert S. Lin, Editors,
Committee on Improving Cybersecurity Research in the United States, National Research Council

ISBN: 0-309-66741-0, 328 pages, 6 x 9, (2007)

**This PDF is available from the National Academies Press at:**
**http://www.nap.edu/catalog/11925.html**

Visit the National Academies Press online, the authoritative source for all books from the National Academy of Sciences, the National Academy of Engineering, the Institute of Medicine, and the National Research Council:

- Download hundreds of free books in PDF
- Read thousands of books online for free
- Explore our innovative research tools – try the "Research Dashboard" now!
- Sign up to be notified when new books are published
- Purchase printed books and selected PDF files

**Thank you for downloading this PDF. If you have comments, questions or just want more information about the books published by the National Academies Press, you may contact our customer service department toll-free at 888-624-8373, visit us online, or send an email to feedback@nap.edu.**

**This book plus thousands more are available at http://www.nap.edu.**

Copyright © National Academy of Sciences. All rights reserved.
Unless otherwise indicated, all materials in this PDF File are copyrighted by the National Academy of Sciences. Distribution, posting, or copying is strictly prohibited without written permission of the National Academies Press. Request reprint permission for this book.

THE NATIONAL ACADEMIES
*Advisers to the Nation on Science, Engineering, and Medicine*

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# Toward a Safer and More Secure Cyberspace

Seymour E. Goodman and Herbert S. Lin, *Editors*

Committee on Improving Cybersecurity Research in the United States

Computer Science and Telecommunications Board

Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL *AND*
NATIONAL ACADEMY OF ENGINEERING
*OF THE NATIONAL ACADEMIES*

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
**www.nap.edu**

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

Support for this project was provided by the Defense Advanced Research Projects Agency (award number N00174-03-C-0074), the National Science Foundation (award number CNS-0221722), the National Institute of Standards and Technology (contract number SB1341-03-C-0028), the Department of Homeland Security through the National Science Foundation (award number CNS-0344585), the National Academy of Engineering, the National Research Council Fund (no award number), and F. Thomas Leighton and Bonnie Berger Leighton. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the organizations, agencies, or individuals that provided support for the project.

*Back cover:* Summarized in the right-hand column of the chart is the new mind-set advocated in this report as essential to achieving a more generally secure cyberspace.

**Library of Congress Cataloging-in-Publication Data**

Toward a safer and more secure cyberspace / Committee on Improving Cybersecurity Research in the United States, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences, National Research Council of the National Academies ; Seymour E. Goodman and Herbert S. Lin, editors.
p. cm.
Includes bibliographical references.
ISBN 978-0-309-10395-4 (pbk.) -- ISBN 978-0-309-66741-8 (pdf) 1. Computer security. 2. Computer networks--Security measures. 3. Cyberterrorism--Prevention. I. Goodman, Seymour E. II. Lin, Herbert. III. National Research Council (U.S.). Committee on Improving Cybersecurity Research in the United States.
QA76.9.A25T695 2007
005.8--dc22
2007037982

This report is available from
Computer Science and Telecommunications Board
National Research Council
500 Fifth Street, N.W.
Washington, DC 20001

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Copyright 2007 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# THE NATIONAL ACADEMIES

*Advisers to the Nation on Science, Engineering, and Medicine*

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

**www.national-academies.org**

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

**COMMITTEE ON IMPROVING CYBERSECURITY RESEARCH IN THE UNITED STATES**

SEYMOUR (Sy) E. GOODMAN, Georgia Institute of Technology, *Chair* (from August 2006)
JOEL S. BIRNBAUM, Hewlett-Packard Company, *Chair* (until August 2006)
DAVID AUCSMITH, Microsoft Corporation
STEVEN M. BELLOVIN, Columbia University
ANJAN BOSE, Washington State University
BARBARA FRASER, Cisco Systems, Inc.
JAMES GOSLER, Sandia National Laboratories
WILLIAM GUTTMAN, Carnegie Mellon University
RUBY B. LEE, Princeton University
FERNANDO (FRED) LUIZ, Hewlett-Packard Company (retired)
TERESA F. LUNT, Palo Alto Research Center
PETER G. NEUMANN, SRI International
STEFAN SAVAGE, University of California, San Diego
WILLIAM L. SCHERLIS, Carnegie Mellon University
FRED B. SCHNEIDER, Cornell University
ALFRED Z. SPECTOR, Independent Consultant
JOHN WANKMUELLER, MasterCard International
JAY WARRIOR, Agilent Laboratories

*Staff*

HERBERT S. LIN, Senior Scientist and Study Director (from September 2005)
CHARLES N. BROWNSTEIN, Study Director (until September 2005)
KRISTEN BATCH, Associate Program Officer
JENNIFER M. BISHOP, Program Associate (until November 2006)
JANICE M. SABUDA, Senior Program Assistant
TED SCHMITT, Consultant



Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

JOSEPH F. TRAUB, Columbia University, *Chair*
ERIC BENHAMOU, Benhamou Global Ventures, LLC
FREDERICK R. CHANG, University of Texas, Austin
WILLIAM DALLY, Stanford University
MARK E. DEAN, IBM Almaden Research Center
DEBORAH ESTRIN, University of California, Los Angeles
JOAN FEIGENBAUM, Yale University
KEVIN KAHN, Intel Corporation
JAMES KAJIYA, Microsoft Corporation
MICHAEL KATZ, University of California, Berkeley
RANDY H. KATZ, University of California, Berkeley
SARA KIESLER, Carnegie Mellon University
TERESA H. MENG, Stanford University
PRABHAKAR RAGHAVAN, Yahoo! Research
FRED B. SCHNEIDER, Cornell University
ALFRED Z. SPECTOR, Independent Consultant
WILLIAM STEAD, Vanderbilt University
ANDREW J. VITERBI, Viterbi Group, LLC
PETER WEINBERGER, Google, Inc.
JEANNETTE M. WING, Carnegie Mellon University

*Staff*

JON EISENBERG, Director
KRISTEN BATCH, Associate Program Officer
RADHIKA CHARI, Administrative Coordinator
RENEE HAWKINS, Financial Associate
MARGARET MARSH HUYNH, Senior Program Assistant
HERBERT S. LIN, Senior Scientist
LYNETTE I. MILLETT, Senior Program Officer
DAVID PADGHAM, Associate Program Officer
JANICE M. SABUDA, Senior Program Assistant
TED SCHMITT, Consultant
BRANDYE WILLIAMS, Program Assistant
JOAN D. WINSTON, Program Officer

For more information on CSTB, see its Web site at http://www.cstb.org, write to CSTB, National Research Council, 500 Fifth Street, N.W., Washington, DC 20001, call (202) 334-2605, or e-mail the CSTB at cstb@nas.edu.



Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# Preface

In the past several years, cybersecurity has been transformed from a concern chiefly of computer scientists and information system managers to an issue of pressing national importance. The nation's critical infrastructure, such as the electric power grid, air traffic control system, financial system, and communication networks, depends extensively on information technology (IT) for its operation. Concerns about the vulnerability of this infrastructure have heightened in the security-conscious environment after the September 11, 2001, attacks. National policy makers have become increasingly concerned that adversaries backed by substantial resources will attempt to exploit the cyber-vulnerabilities in the critical infrastructure, thereby inflicting substantial harm on the nation.

Today, there is an inadequate understanding of what makes IT systems vulnerable to attack, how best to reduce these vulnerabilities, and how to transfer cybersecurity knowledge to actual practice. For these reasons, and in response to both legislative and executive branch interest, the National Research Council (NRC) established the Committee on Improving Cybersecurity Research in the United States (see Appendix A for biographies of the committee members). The committee was charged with developing a strategy for cybersecurity research in the 21st century. To develop this strategy, the committee built on a number of previous NRC reports in this area, notably, *Computers at Risk* (1991), *Trust in Cyberspace* (1998), and *Information Technology for Counterterrorism* (2003).[1] Although

[1]National Research Council, 1991, *Computers at Risk*, National Academy Press, Washington, D.C.; National Research Council, 1998, *Trust in Cyberspace*, National Academy Press, Washington, D.C.; National Research Council, 2003, *Information Technology for Counterterrorism: Immediate Actions and Future Possibilities*, The National Academies Press, Washington, D.C.



Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



these reports were issued some years ago, the committee found that they contained valuable points of departure for the present effort. In addition, the committee undertook a set of hearings and briefings that provided information about present-day concerns and responses to those concerns. The report of the President's Information Technology Advisory Committee on cybersecurity—*Cyber Security: A Crisis of Prioritization*—which lays out a research agenda and makes recommendations on how to implement it, provided a useful point of departure as well.[2]

Box P.1 contains the full charge to the committee. The committee's survey of the current cybersecurity research landscape is described in Appendix B. As requested in the charge, Section B.5 contains a survey of the research effort in cybersecurity and trustworthiness to assess the current mix of topics; Sections B.4 and B.6 address level of effort, division of labor, and sources of funding; Section B.3 addresses quality. The issue related to the timescales of cybersecurity research is addressed in Section 10.2.2. Structural dimensions of a program for cybersecurity research are addressed in Section 3.3.

Two elements in the committee's statement of task were not fully addressed. First, although Part II provides general guidance regarding appropriate areas of programmatic focus, this report does not provide a detailed explication of research priorities within or among these areas (that is, the research areas meriting federal funding). The reason, explained at greater length in Section 3.4.4, is that in the course of its deliberations, the committee concluded that the nation's cybersecurity research agenda should be broad and that any attempt to specify research priorities in a top-down manner would be counterproductive. Second, the study's statement of task calls for it to address appropriate levels of federal funding for cybersecurity research. As discussed in Section 10.2.2, the committee articulates a specific principle for determining the appropriate level of budgets for cybersecurity research: namely, that such budgets should be adequate to ensure that a large fraction of good ideas for cybersecurity research can be explored. It further notes that the threat is likely to grow at a rate faster than the present federal cybersecurity research program will enable us to respond to, and thus that in order to execute fully the broad strategy articulated in this report, a substantial increase in federal budgetary resources devoted to cybersecurity research will be needed.

It is important to delineate the scope of what this report does and to

[2]President's Information Technology Advisory Committee. February 2005. *Cyber Security: A Crisis of Prioritization*, National Coordination Office for Information Technology Research and Development, Washington, D.C.; available at www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



specify what it does not do. The committee recognizes that cybersecurity is only one element of trustworthiness, which can be defined as the property of a system whereby it does what is required and expected of it—despite environmental disruption, human user and operator errors, and attacks by hostile parties—and that it does not do other things. Trust-

**BOX P.1**
**Statement of Task**

This project will involve a survey of the research effort in cybersecurity and trustworthiness to assess the current mix of topics, level of effort, division of labor, sources of funding, and quality; describe those research areas that merit federal funding, considering short-, medium-, and long-term emphases; and recommend the necessary level for federal funding in cybersecurity research. Technologies and approaches conventionally associated with cybersecurity and trustworthiness will be examined to identify those areas most deserving of attention in the future and to understand the research baseline. In addition, this project will also seek to identify and explore models and technologies not traditionally considered to be within cybersecurity and trustworthiness in an effort to generate ideas for revolutionary advances in cybersecurity. Structural alternatives for the oversight and allocation of funding (how to best allocate existing funds and how best to program new funds that may be made available) will be considered and the project committee will provide corresponding recommendations. Finally, the committee will offer some guidance on the shape of grant-making research programs.

Consistent with legislative language, the committee will consider:

1. Identification of the topics in cybersecurity research that deserve emphasis for the future. As discussed with congressional staff, this analysis will build on past work within CSTB [Computer Science and Telecommunications Board] and elsewhere, which has identified many important and often enduring topics.
2. The distribution of effort among cybersecurity researchers. The emphasis will be on universities, in part to address the link between the conduct of researchers and the education and training of cybersecurity experts, to ensure that there are enough researchers to perform the needed work. Comparisons between academic and industry activities will be made.
3. Identification and assessment of the gaps in technical capability for critical infrastructure network security, including security of industrial process controls.
4. The distribution, range, and stability of support programs among federal funding organizations.
5. Issues regarding research priorities, resource requirements, and options for improving coordination and efficacy in the national pursuit of cybersecurity research. Opportunities for cross-sector (and intra-sector) coordination and collaboration will be considered

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



worthiness has many dimensions, including correctness, reliability, safety, and survivability, in addition to security. Nevertheless, the charge of this report is to focus on security, and other issues are addressed only to the extent that they relate to security.

This report is not confined to technical topics alone. A number of policy issues related to cybersecurity are discussed. These policy issues provide an overarching context for understanding why greater use has not been made of cybersecurity research to date. In addition, because the report concludes that cybersecurity research should not be undertaken entirely in a domain-independent manner, the report also discusses briefly a number of problem domains to which cybersecurity research is applicable.

The committee assembled for this project included individuals with expertise in the various specialties within computer security and other aspects of trustworthiness, computer networks, systems architecture, software engineering, process control systems, human-computer interaction, and information technology research and development (R&D) programs in the federal government, academia, and industry. In addition, the committee involved individuals with experience in industrial research.

The committee met first in July 2004 and four times subsequently. It held several plenary sessions to gather input from a broad range of experts in cybersecurity. Particular areas of focus included then-current federal research activity, the state of the art in usable security, and current vendor activity related to advancing the state of cybersecurity. The committee did its work through its own expert deliberations and by soliciting input from key officials at sponsoring agencies, numerous experts at federal agencies, academic researchers, and hardware and software vendors (see Appendix C). Additional input included perspectives from professional conferences, the technical literature, and government reports studied by committee members and staff (see Appendix B).

The committee appreciates the support of its sponsoring agencies and especially the numerous inputs and responses to requests for information provided by Jaynarayan Lala and Lee Badger at the Defense Advanced Research Projects Agency (DARPA), Carl Landwehr and Karl Levitt at the National Science Foundation (NSF), Edward Roback at the National Institute of Standards and Technology (NIST), Douglas Maughan at the Department of Homeland Security (DHS), and Robert Herklotz at the Air Force Office of Scientific Research (AFOSR).

## PERSONAL NOTE FROM THE CHAIR

A large fraction of the American population now spends a great deal of time in cyberspace. We work and shop there. We are educated and entertained there. We socialize with family, friends, and strangers in cyber-

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



space. We are paid and we pay others through this medium. Millions of commercial enterprises and local, state, and federal government agencies do their business there. It has become a critical infrastructure in its own right, and it is embedded in almost all other critical infrastructures. We rely on cyberspace to help keep electricity flowing, public transportation running, and many other basic services working at levels that we have come to regard as essential elements of our society. These functions, expectations, and resulting dependencies are with us now, have been growing rapidly, and are expected to continue to grow well into the future.

The people, businesses, and governments of the rest of the world are following suit. On a per capita basis, some are even more committed to this infrastructure than the United States is. The Internet alone is now used by about a billion people and comes to ground in about 200 countries. And they are all connected to us and to one another.

It is thus very much in the public interest to have a safe and secure cyberspace. Yet cyberspace in general, and the Internet in particular, are notoriously vulnerable to a frightening and expanding range of accidents and attacks by a spectrum of hackers, criminals, terrorists, and state actors who have been empowered by unprecedented access to more people and organizations than has ever been the case with any infrastructure in history. Most of the people and organizations that increasingly depend on cyberspace are unaware of how vulnerable and defenseless they are, and all too many users and operators are poorly trained and equipped. Many learn only after suffering attacks. These people, and the nation as a whole, are paying enormous costs for relying on such an insecure infrastructure.

The Committee on Improving Cybersecurity Research in the United States was established by the National Research Council of the National Academies with the financial support of NSF, DARPA, NIST, DHS, the National Academy of Engineering, and F. Thomas and Bonnie Berger Leighton. The basic premise underlying the committee's task is that research can produce a better understanding of why cyberspace is as vulnerable as it is and that it can lead to new technologies and policies and their effective implementation to make things better.

Cybersecurity is not a topic that is new to the national agenda. Indeed, a number of earlier reports have addressed this subject from different perspectives. Many of these reports have been concerned with specific threats (e.g., terrorism), missions (e.g., critical infrastructure protection), government agencies (e.g., how they might better protect themselves), or specific sectors (e.g., banking and finance). This study tackles the problem from the perspective of protecting all legitimate users of cyberspace, including the individual citizens, small commercial concerns, and government agencies that are particularly vulnerable to harassment and injury every

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



time they use the Internet or connect to other networks. The committee strongly believes that a more generally secure cyberspace would go a long way toward protecting critical infrastructure and national security.

What would a safer and more secure cyberspace look like? To address this question, the committee has formulated a Cyberspace Bill of Rights (CBoR). It consists of 10 basic provisions that the committee believes users should have as reasonable expectations for their online safety and security. The CBoR articulated in this report is distinctly user-centric, enabling individuals to draw for themselves the contrast between that vision and their own personal cyberspace experiences.

Unfortunately, the state of cyberspace today is such that it is much easier to state these provisions than it is to achieve them. No simple research project will lead to the widespread reality of any of these provisions. Indeed, even achieving something that sounds as simple as eliminating spam will require a complex, crosscutting technical and nontechnical R&D agenda. Accordingly, this report goes on to propose a comprehensive R&D agenda and to show how that agenda would help realize the provisions of the CBoR. The report also warns that there will be no shortcuts and that realizing the CBoR vision will take a long, sustained, and determined effort. There is much to accomplish.

Many of this report's technical R&D recommendations build on and support those of earlier reports. However, they give particular emphasis to problems that have handicapped the more extensive practice of cybersecurity in the past. Thus, the report focuses substantial attention on the very real challenges of incentives, usability, and embedding advances in cybersecurity into real-world products, practices, and services.

On behalf of the committee, I would like to thank those who took the time and trouble to contribute to our deliberations by briefing the committee. This group of individuals is listed in Appendix C. In addition, those who reviewed this report in draft form played a critical and indispensable role in helping to improve the report (see "Acknowledgment of Reviewers" on page xiii). On the Computer Science and Telecommunications Board (CSTB), Ted Schmitt's work as program officer on his first NRC project was exemplary, and Janice Sabuda provided administrative and logistical support beyond compare. Special recognition is due to Herbert S. Lin, who became the CSTB study director about halfway through the committee's lifetime, and who worked so hard to pull this report together. His tenacity, determination, and expertise were indispensable.

Seymour E. Goodman, *Chair*
Committee on Improving Cybersecurity
Research in the United States

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# Acknowledgment of Reviewers

This report has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the National Research Council's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this report:

Eric Benhamou, Benhamou Global Ventures, LLC,
Earl Boebert, Sandia National Laboratories (retired),
William R. Cheswick, AT&T Research,
David D. Clark, Massachusetts Institute of Technology,
Richard A. DeMillo, Georgia Institute of Technology,
Samuel H. Fuller, Analog Devices, Inc.,
Paul A. Karger, IBM Thomas J. Watson Research Center,
Pradeep Khosla, Carnegie Mellon University,
Butler Lampson, Microsoft Corporation,
Brian Lopez, Lawrence Livermore National Laboratory,
William Lucyshyn, University of Maryland,
Clifford Neuman, University of Southern California,
Eugene Spafford, Purdue University,



Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



Philip Venables, Goldman Sachs,
Jesse Walker, Intel Corporation, and
Jeannette M. Wing, Carnegie Mellon University.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final draft of the report before its release. The review of this report was overseen by Lewis Branscomb and Brian Snow. Appointed by the National Research Council, they were responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the authoring committee and the institution.

Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# Contents





Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html





Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html





Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html



**PART III**
**CONCLUSION**



**APPENDIXES**



Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html





Copyright © National Academy of Sciences. All rights reserved.

Toward a Safer and More Secure Cyberspace
http://www.nap.edu/catalog/11925.html

# Boxes





Copyright © National Academy of Sciences. All rights reserved.

House Armed Services Committee
Subcommittee on Terrorism, Unconventional Threats and Capabilities
"Holistic Approaches to Cybersecurity to Enable Network Centric Operations"
April 1, 2008
James Andrew Lewis
Center for Strategic and International Studies

I thank the committee for the opportunity to testify. As you know, we have seen new domains for conflict emerge in the last decade. These new domains are in space and in cyberspace. Cyberspace is in some ways the more interesting of the new domains, because the 'price of entry' is low and also because it has been an area of significant U.S. vulnerability for many years, a vulnerability that has been eagerly exploited by our opponents.

We know that networks and information technology improve performance for both businesses and for militaries when they are used to provide better information and better coordination. One study examined exercises that pitted networked F-15s against F-15 relying only on traditional voice communications, and found that networking resulted in dramatic improvements in combat effectiveness.[1] This study is indicative of the direction that future conflict is likely to take – the side with the informational advantage is more likely to win. We are only at the beginning of finding the organizational structures and tactics that will make full use of the new technologies that can provide informational advantage.

But at the same time, the use of these technologies has created serious new vulnerabilities. These vulnerabilities are the result, in part, of the newness of the technologies themselves. Our opponents have seized the opportunity created by these vulnerabilities to engage in an extensive espionage campaign against the U.S. by mapping the vulnerabilities of our networks, accessing U.S. computers through these networks, and transferring sensitive information from the U.S. to their own computers.

There is also the possibility that when an unknown intruder has accessed a U.S. computer to steal information, he or she has also left something behind. We cannot say with assurance that a network that has been penetrated has also not been infected with hidden malware that could be triggered in a crisis, disrupting data and communications. This is not the "electronic Pearl Harbor" scenario that unfortunately dominated much of the early thinking about cyber security, but the potential for disruption and at least a temporary military advantage for an opponent as a result of attacking U.S. computer networks cannot be discounted.

None of our opponents will deliberately seek conventional military conflict with the U.S. Instead, they are attracted to asymmetric attacks, which look for and exploit areas where they are strong and the U.S. is weak and unaware. To achieve asymmetric advantage, some opponents will rely on terrorism or insurgent tactics, where combatants blend with the civilian population to attack the U.S. Other opponents plan to disrupt, destroy or deceive U.S. sensors and

[1] Daniel Gonzales, John Hollywood, Gina Kingston, David Signori, "Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16," RAND, 2005

communications, to degrade our informational advantage. Their goal is to exploit vulnerabilities, places where U.S. assets are poorly defended.

Computer networks are just such a place. The nature of information technology and the internet means that in these asymmetric attacks in cyberspace, the advantage lies with the attacker. The internet was not designed to be a global network with millions of different devices all interconnected over a telecommunications backbone. The result is that there are many avenues for attack. Many different entities are exploring how to take advantage of vulnerabilities in cyberspace. These include nations, criminals, terrorist groups, political activists and perhaps even some corporations.

China and Russia are perhaps the most dangerous of our potential opponents. China has resources and is willing to spend them, and Russia has experience and skill. However, China and Russia are not the only nations interested in and capable of waging cyber warfare, nor are nation-states the only potential opponents in this new domain. The emergence of a powerful and skilled cybercrime community has serious implications for U.S. interests.

Over the last few years, cyber criminals have become technologically sophisticated and well-organized. These are not the amateurs of a few years ago. Cyber criminals have developed black markets where you can buy malware, guides to vulnerabilities, credit card numbers. There are contests among cyber criminals, to see who can be the first to hack a new system or to discover a new vulnerability. Some of these sites offer guarantees while others provide a rating system for potential buyers. It is possible to rent bot-nets, huge assemblies of hijacked computers to use in an attack, or even to hire hackers. As in any black market, an unwary buyer can end up being exploited, but a knowledgeable purchaser or one with resources and experience – and this customer base includes nations, companies, and terrorist groups - can find most of what they need for cyber attacks.

If we have underestimated the risks of cyber espionage and cyber crime, the risk of cyber terrorism is overstated. Terrorists do make extensive use of the global internet for recruitment, propaganda, fundraising, training, and for command and control. The ability of terrorist groups to use commercial communications networks has provided them with robust, flat organizations that are more difficult to defeat. It has provided them with a global presence they would not have been able to achieve twenty years ago. But this is not the equivalent of attacks with bombs or firearms, which terrorists prefer. Cyber weapons are not yet sufficiently lethal for terrorist use

To date, cyber disruption and attacks on critical infrastructure remains largely hypothetical. Cybercrime and cyber espionage are the most serious problems. Cyber-espionage is a far greater problem for national security than many recognize. Last year, the U.S. government suffered a series of breaches of its computer networks. These have been attributed to China and while attribution is always difficult when it comes to cyber attacks, we should note that senior officials in the German, French and British governmental also complained about Chinese hacking during the same time as the attacks on the U.S. occurred.

Using computer break-ins for espionage has a long history. The earliest breach I know of occurred in the 1980s, when the KGB hired West German hackers to penetrate U.S. military and

research networks. There were also incidents in the 1990s involving the Departments of Energy and Defense. These incidents show that the cybersecurity problem is twenty years old, but last year we crossed a threshold in cyberattacks, with the noisy demonstrations launched against Estonia's government networks and with the massive sustained attacks – some successful – on U.S. government networks and on the networks of allied countries.

In 2007, computer networks in the Departments of Defense, State and Commerce were penetrated and had to be taken off line for repair. It is likely that other agencies suffered breaches as well. The primary intent of these attacks was to collect information. What they revealed was a remarkable unevenness in the defense of U.S. networks. Some of our government networks, usually those providing the most sensitive services – are very secure. Other networks, including some that contain information about sensitive technologies are not as secure as we would like, whether these are at the Department of Energy or State, or even the Secretary of Defense's unclassified email system, all of which have been hacked.

This series of attacks has prompted the U.S. to begin a major new initiative to improve the security of government computer systems. The Administration has reportedly issued a new, joint policy directive – National Security Policy Directive-54 and Homeland Security Policy Directive-23, which directs agencies to carry out a comprehensive federal cybersecurity initiative. Many of the initiative's elements are highly classified – some would say over-classified – But there has been public discussion of some of its elements and the Administration has said it will make more information publicly available sometime in the next few months.

We know that the initiative allocates more money and personnel to cyber security. Federal spending on cybersecurity will increase ten to twelve percent, according to press reports. The Department of Homeland Security will expand the use of its 'Einstein' system to monitor traffic in and out of Federal government networks. Einstein will be reinforced by undisclosed NSA monitoring systems as well. Building on programs initiated in the Department of Defense, the Office of Management and Budget has mandated the use of the Federal Desktop Core Configuration, a secure standardized configuration for use on all Federal Computers. OMB has also begun a "Trusted Internet Connections" initiative (TIC), which will reduce the points of connection between Federal networks and the rest of the internet from hundreds to only fifty. The U.S. is considering whether to establish new organizations to oversee cyber security efforts, and existing organizations will be strengthened. Both DOD and the Intelligence community have increased their efforts in cyberspace. The initiative has twelve separate projects to improve cyber security, including one that will look at how to improve coordination with the private sector.

These are all very positive steps, but difficult issues remain to be solved. One such issue is improving coordination with the private sector. This will be a major test for the Initiative. The U.S. has mechanisms for coordinating public and private cyber security efforts, but in some ways these are continuation of the initial programs from the 1990s, such as the FBI's National Infrastructure Protection Center (NIPC) or the Department of Commerce's Critical Infrastructure Assurance Office (CIAO). We need to rethink and improve how the government interacts, cooperates and coordinates with the private sector to assure better cyber security.

Another issue is that there is an international element to cyber security that must be addressed. These attacks on federal networks and critical infrastructure come over global networks. A national effort can provide only part of the solution. The U.S. will need to work with its allies and perhaps even with our opponents to change this. A sustained international effort could involve better cybercrime enforcement, new international norms for cyberspace, new collaborative mechanisms and, with our allies, agreed doctrine on securing networks and responding to attacks.

One advantage of better international cooperation is that it could increase the level of deterrence, at least for cyber criminals. Currently, some nations act as sanctuaries for cybercriminals. Cybercriminals who operate overseas can, with a little skill, almost eliminate the chances of being caught and prosecuted. Only international cooperation will change this.

Other forms of deterrence are less practical. It is difficult to deter by threatening counterattack if you do not know who is attacking. It is even more difficult to deter by threatening counterattack is you cannot estimate the degree of collateral damage. Attacks come over a global network to which we are all connected, and the attackers can use unsuspecting civilian computer networks, assembled into bot-nets to launch their attacks. Last year's attacks on Estonia are a good example of these problems. They are widely attributed to Russia, and in my view Russian intelligence services are almost certainly behind the attacks, yet there is no evidence to substantiate this. The attackers, a collection of cybercriminals and amateur hackers mobilized and encouraged by unknown entities used captive computers around the world, in Europe, china and in the U.S. A counterstrike against the attacking computers would have damaged innocent networks around the world. It would be a bold President who authorized counterstrikes when he or she does not know the target or the possible extent of collateral damage to friendly networks.

The attacks on Estonia highlight the problems of anonymity and attribution. The Internet is too anonymous, and too easily deceived. Identity management must be improved if cybersecurity is to be improved. This is a thorny subject, given the implications for privacy and civil liberties, but the anonymity of the internet makes it difficult to determine who is responsible for an attack or a crime, this difficulty with attribution makes it more difficult to deter attacks. Progress on measures such as HSPD-12.which will improve Federal credentials and authentication is crucial. The RealID program, although widely vilified, is also crucial for improving the quality of identity documents and procedures in the U.S. DOD has been a leader in better identity management with its Common Access Card Program

Federal organization remains a challenge. The slow pace of the rollout of the Initiative was due in part to disagreements over which agency would have the lead. The Intelligence Community has the best capabilities for cyber defense in many ways, but there are civil liberties concerns and clear links to the renewal of the Foreign Intelligence Surveillance Act (FISA) over assigning the Director of National Intelligence the lead role. There are also concerns over giving the lead in cybersecurity to a military organization, such as the U.S. Strategic Command. The Department of Homeland Security, the civilian agency with the responsibilities for cyber security, would be the logical lead but there have been questions about its competence and authority. The previous administration had a cyber 'czar,' who successfully began the immense effort required to reorient

Federal policy and to develop strategies, but a "Czar" may no longer make sense now that the Department of Homeland Security has been created.

Government organization for cybersecurity reflects a larger challenge for the U.S. In effect, we have a vertical organization trying to respond to a horizontal threat. This means we have four or five different and independent agencies each of whom are responsible for a part of the problem. There is no single agency responsible for the entire problem. Even at the White House we have two organizations – the Homeland Security Council and the National Security Council - that share responsibility for cyber security.

This sort of organizational problem is very difficult for governments to overcome. The creation of the Department of Defense in 1948 was an effort to develop collaborative and "joint" action to meet the problems of National Security. That effort was reinforced and given new impetus by the Goldwater-Nichols Act. DOD has worked for decades to achieve 'jointness.' Other agencies are far behind in achieving a collaborative, 'horizontal approach. The creation of the Department of Homeland Security can be seen as an effort to duplicate the 1948 solution for homeland security. The Intelligence Reform and Terrorist Prevention Act can also be seen as an effort to create an 'intelligence enterprise' with a powerful CEO whose remit would stretch across multiple agencies.

I would wish reorganization on no administration, but the structure of our government is still largely based on a template created in the 1900s. This template is inefficient in many ways. Reorganization is unavoidable, but it will take years of effort. We do not have years, however, to respond to the new security threats in cyberspace.

To be fair, this problem extends beyond government. Our conceptual framework for thinking about security has moved beyond the cold war, but not by much. My concern is that conflict in cyberspace is seen the way that airplanes were seen in 1912 – interesting toys, but not a serious security or military issue. Some, pointing to Pearl Harbor and to 911, say that we will only reshape our thinking and our organization to deal with cybersecurity after some disaster has occurred. I hope this is not the case.

Federal organization, strategy and doctrine, coordination with the private sector and allies – these and other issues remain challenges despite the progress made by the President's cybersecurity initiative. That the initiative comes in the last year of the Presidency also creates challenges. Any administration would face difficulties in making rapid progress on a new initiative after July The political realities are that the Administration has between fourteen and sixteen weeks to implement its cyber initiative. Much can be done, but much will necessarily remain unfinished.

This means that the burden of improving cybersecurity will fall on the next administration when it takes office in January of 2009. That administration, whether Democratic or Republican, will inherit a cyber security situation that is much improved. It will also inherit a cyber security initiative that is a work in progress, with a number of unfinished elements. Like any new administration, it will have to ask what should it keep or continue from this initiative, what should it change or drop, and what new steps it should take to address this increasingly serious problem for national security.

Transitions are also, as the members of the Committee well know, a moment of opportunity. The new Administration will have a degree of good will and authority. Perhaps more importantly, it will have something of a clean slate when it comes to initiatives and organization. 2009, the first year of the next administration, provides an opportunity to take the Bush Administration's cybersecurity initiative and advance it.

To help the new administration think about this opportunity, The Center for Strategic and International Studies (CSIS) established a nonpartisan commission on Cyber Security for the 44th Presidency – the administration that will take office in January 2009. CSIS is a nonpartisan, nonprofit research organization headquartered in Washington, D.C. with more than 200 staff and a large network of affiliated experts. Its focus is on security in a changing global environment. CSIS's has been conducting research, holding public events, and advising government agencies on cyber security since before 2000, and this body of work will provide the foundation for the Commission on Cyber Security for the 44th Presidency. CSIS routinely uses commissions, task forces and work groups to help it conduct analysis and develop recommendations. This approach lets us draw upon the broader communities of interest in Washington and benefit from their expertise and experience.

The goal of this effort is to look at cybersecurity as a problem for national security and develop recommendations for a comprehensive strategy to improve cyber security in federal systems and in critical infrastructure. The Commission will consider federal organization and strategy, cybersecurity norms and authorities, international issues, federal investment and acquisition policies, and it will explore ways in which the government can engage with the private sector.

The members of the commission are experts in cybersecurity with extensive government experience. In addition, CSIS intends to make the work of the Commission an inclusive process and has asked other experts and groups to participate in the development of recommendations and to make plenary presentations on substantive issues. Our first public briefing took place on March 12, in a well attended event where five widely recognized leaders in cybersecurity give their views and recommendations on how to move forward in cybersecurity. We plan to hold several more briefings in the next three months.

As part of this effort, we have created a number of working groups that will examine these issues in detail and develop specific recommendations. These groups have just begun their work. They include members of the commission and other experts, all of whom have volunteered their time for this effort. If the committee wishes, I can report back at a later stage on how their work has progressed. Our plan is for the Commission to complete its work by November 2008. The final product from the Commission will be a well-supported package of recommendations for improving cyber security that could help to guide U.S. policy in the future.

The advantage we gain from being network centric is eroded by uneven security. We will never have perfect security, but our goal, as a nation, should be to increase our ability to use network technologies to improve our military and economic performance while at the same time reduce the ability of our opponents to take advantage. Our hope is that the efforts of CSIS and the other participants in the commission can contribute in some way to this improvement.

One element of the CSIS projects is to reassess the larger strategic context for cybersecurity. This context is shaped by considerations involving national defense, law enforcement, intelligence and global economic competition. This may require a broader definition of national security. It is no surprise that one result of immense economic and technological change we are undergoing is that old assumptions about security and the policies based on those assumption do not work as well as they did in the past. The process of adjusting those policies to the new global environment is a major challenge for all governments. Each country in some way must respond to a world where the lines between government and commercial, and between domestic and foreign are blurred. This blurring makes finding solutions to cybersecurity more difficult but achieving better cyber security and greater benefit from network centric operations requires this reassessment of the strategic context.

In the 1990s, there was considerable discussion of what the international security environment would look like after the cold war and what the new threats to US security would be in that environment. Much of this speculation was wrong, not in that it misidentified the new threats, but that it gave some threats more importance than they deserved. We underestimated the threat of global terrorism. We did not prepare adequately for cyber espionage. There were a few visionaries who pointed to these problems, but in the main, they were ignored.

In the last decade, the shape and nature of the new security environment has become clearer. We face new kinds of competition and new kinds of threats. In this new environment, the ability to operate in cyberspace and to defend against the operations of others in cyberspace is a crucial task for security. The United States has begun to take the steps needed to defend and to compete effectively in cyberspace, but we have only begun and there is much to do.

I thank the Committee again and I would be happy to take any questions.

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.

## DOCUMENTS SUBMITTED FOR THE RECORD

APRIL 1, 2008

NOT FOR PUBLICATION UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

WRITTEN STATEMENT OF

LIEUTENANT GENERAL CHARLES E. CROOM, JR., U.S. AIR FORCE
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

BEFORE THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES
HOUSE ARMED SERVICES COMMITTEE

TUESDAY
01 APRIL 2008

CLEARED
For Open Publication

MAR 20 2008 6

Office of Security Review
Department of Defense

NOT FOR PUBLICATION UNTIL RELEASED BY THE
SUBCOMMITTEE ON TERRORISM, UNCONVENTIONAL THREATS AND
CAPABILITIES, HOUSE ARMED SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

08-C-0541

Good afternoon, Mr. Chairman, Congressman Thornberry, and Members of the Subcommittee. I am Lieutenant General Charlie Croom, the Director of the Defense Information Systems Agency (DISA) and the Commander of the Joint Task Force - Global Network Operations (JTF-GNO). As the Director of DISA, I report to the Honorable John Grimes, Assistant Secretary of Defense for Networks and Information Integration. As the Commander of the JTF-GNO, I report to General Kevin Chilton, Commander of the United States Strategic Command. I am pleased to appear before the Subcommittee today to discuss defense of the Department of Defense networks and the roles that DISA and the JTF-GNO play in that defense.

Information is America's greatest weapon system. In today's complicated world, there is an imperative for a global, interconnected force which demands we continue to transform the way information is managed and shared to accelerate decision-making, improve warfighting, create intelligence advantages, and optimize business processes.
It is our responsibility to ensure warfighters can operate in this world and that they have the right information at the right place and time to execute their missions.

As we begin, it is useful to define two terms we use in the Defense Department and to provide some context framing my testimony. The first term is Global Information Grid, or GIG. The GIG is the globally interconnected set of information capabilities, processes, and people for identifying, collecting, processing, storing, disseminating, and managing information for the Department's three mission areas: warfighting, business, and intelligence. The GIG is supported by the network and computing infrastructure, enterprise services which enable sharing of information, and information assurance to protect and defend our ability to share information. It includes all owned and leased terrestrial and satellite communications and computing systems and services, software, data, security, and other necessary assets to ensure the Department can execute its missions. In short, it provides the end-to-end capability required for information access and distribution. DISA has a major role in providing and securing these capabilities as the joint telecommunications and information technology leader in the Department.

The second term is net-centricity. Net-centricity is the concept that generates increased combat power through information technology that joins sensors, decision-makers, and weapons systems to achieve shared awareness, increased speed of command and decision making, higher operations tempo, greater lethality, and reduced friendly fire incidents. Essentially, the concept of net-centric operations and warfare means that the United States can deploy a warfighting unit anywhere in the world, enable it to connect to the network, and enable it to pull the information it needs for its particular mission, place, and time, while still receiving timely threat information This, then, requires that the GIG be robust, agile, protected, and responsive, and indeed global as its name implies.

We envision a world in which United States military forces can deploy, connect, and operate unimpeded in a net-centric manner. It is a world with well-developed, mature standards and no seams between the sustaining base and the tactical edge. It is a world in which information, whether voice, data, and video, is converged on a mature, technology-fresh, and available Internet Protocol (IP) network. It is a world in which the past differentiation between the network and computing or data processing no longer exists since computing will be done virtually across the entire network. It is a world in which the United States military can freely exchange information routinely with coalition partners, state and local authorities, and others responsible for the security and defense of the United States. The technology employed is agile, adaptive, and capabilities-based. It uses machine-to-machine communication and wireless connectivity, allowing connection regardless of location. However, it is also a world where the security challenges are continuing to grow along with improved capabilities. And, we imagine and envision a world in which our soldiers, sailors, airmen, and marines are always equipped with state-of-the-art capabilities and services with access to protected information when and where they need it.

From my point of view, DISA provides four pillars essential to the Department's mission that enable net-centric operations and warfare.

First is the underlying telecommunications and IP network, the Defense Information Systems Network or DISN. The DISN is a global communications network that must always have bandwidth that can be configured, allocated, and managed end-to-end to meet mission demands. To augment the terrestrial portions of the network, DISA provides DoD Teleports and satellite ground stations that permit deployed warfighters using satellite communications to connect to the DISN. The Department also has many networks acquired and operated by Military Services and Defense Agencies. These networks adhere to the broad architectural and engineering guidance provided by DISA and operate under the operational command of the JTF-GNO.

As we support the network, we face two key challenges. We must continue to keep the network fresh with evolving technologies that allow greater and faster information sharing and that allow us to defend it appropriately. Additionally, we must expand it to meet changing mission and capacity demands. The establishment of the Africa Command and the growing demand for bandwidth attendant to the increased use of intelligence systems like the Predator and Reaper are two examples. Refreshing and expanding the network costs money. The Department is addressing these challenges.

The second pillar is the computing infrastructure provided by our Defense Enterprise Computing Centers or DECCs. Our professionally managed, high capacity, protected computing infrastructure is well established, and it increasingly provides highly scalable, on-demand processing just like major web services providers such as Google and Amazon. We are employing innovative, capacity-on-demand services to acquire data processing and storage as services provided by vendor partners on our data center floors. We pay only for the capacity needed. This approach has benefits of reduced time to add capacity, more efficient operation, technology currency, and reduced costs. This breakthrough in acquiring processing and storage capacity as managed services with utility-like pricing means our customers will pay only for the capacity consumed.

Third is the set of capabilities and services that enable and facilitate sharing information among systems and users. We link producers and consumers of information across all

mission areas – warfighting, business, and intelligence. This is being done through the set of core enterprise services including collaboration, discovery, content delivery, mediation, and security provided by the Net-Centric Enterprise Services (NCES) program. These are essentially the "behind-the-glass" services enabling collaboration and commerce on the Internet, but within our protected perimeter. A fundamental capability for allowing and managing information sharing provided by NCES is the service-oriented-architecture (SOA) foundation services.

Fourth are the programs enabling command and control, the Global Command and Control System (GCCS), and combat support, the Global Combat Support System (GCSS). These systems, like most others today, are tightly designed and integrated – we call them hard-wired meaning they are costly, in both time and money, to update and change. With the new Network Enabled Command Capability (NECC) program, we are acquiring a new set of joint command and control capabilities, built on the core services provided by NCES, which are loosely coupled to enable more agile, efficient information sharing for command and control. NECC uses a tailored acquisition approach to more rapidly make available a series of smaller and scalable command and control capabilities.

Additionally, DISA provides a number of special capabilities and services. The White House Communications Agency (WHCA) which is organized under DISA, provides communications for the President, Vice President, and others both on the 18-acre White House compound and when they travel. We have modernized the capabilities used to support the President over the past five years and have programmed continued modernization throughout the future year's Defense Plan. We also provide critical support to the Department through the Joint Interoperability Test Command (JITC) and the Defense Spectrum Organization. The JITC provides interoperability testing and certifications for all joint communications and information technology systems acquired by the Department. The Defense Spectrum Organization provides support to the Secretary in ensuring the Department has the radio spectrum frequency agility needed to allow us to operate globally. It also provides technical support to deploying warfighting forces to de-conflict frequency congestion and solve interference problems.

DISA is the Department's acquisition agency for joint telecommunications and information technology capabilities and services. We have a highly trained and skilled acquisition workforce, solid processes, and a solid governance and oversight structure for acquisition. We adopt innovations and processes to quickly and agilely deliver capabilities and services to close the gap between the availability of technologies and fielding them for warfighting advantage. Additionally, DISA's Defense Information Technology Contracting Organization (DITCO) is the primary acquirer of telecommunications and IT services for the DoD, and last year contracted for $3.6 billion of services.

Today, speed of delivery is often more important than a perfect solution. In DISA, we follow the precepts of "adopt-before-we buy" and "buy-before-we-create". If another organization has developed or acquired a capability or service that either fits or is close to fitting an enterprise need for which we are responsible, we adopt it. When opportunities to adopt are not available, we turn to the private sector and acquire a capability or service that either fits or is close to fitting the need. Our final choice is to create or build, and we intend to avoid development and turn to others for solutions when we can. We will pursue the "adopt-before-we-buy" and "buy-before-we create" approach as a way of getting the 80-percent quality solution in the hands of the warfighter more quickly. To help with this philosophy, we have developed relationships with industry partners for strong performance-based solutions, speed, risk balance, and mission assurance. We have taken this approach with the knowledge that acquiring information technology capabilities and services is not like buying fighter planes or naval combatants. Why? Because the rate at which IT changes requires fast and agile acquisition to keep pace with the change.

Another area where we have worked hard to continue to close the gap between the availability of technologies and fielding them for warfighting advantage, is to employ risk-based testing, use right-sized information assurance (IA) certification, streamline the requirements process and speed decision making. These initiatives are risk management-

based instead of process-based, and they are required to match the pace of change of technology and deliver at near Internet speed. This means we must move away from the traditional, weapon system-based, program-centric manner in which the Department acquires today.

Now, I will turn to defense of the GIG. Fundamentally, the components of the GIG must be protected and defended to ensure they perform when needed. We must command and control the network and aggressively defend it. Yet, today's ever changing world creates many security challenges. We now have on-demand information sharing and collaboration through chat, text messaging and phones with cameras, and we rely on, in fact demand, these tools and capabilities; yet they are also vulnerable to cyber attacks and exploitation by a variety of actors. We are able to work wherever we are, given security considerations, and we see increased use of the Internet at work as routine. So, considering this highly collaborative information sharing environment, how do we defend the GIG such that it will perform the military mission when needed and still allow us to take advantage of the incredibly powerful collaboration and sharing tools and allow people to utilize the Internet?

Now, to the threats. They are on the rise and increasing in sophistication. A number of nations and groups are actively developing and refining exploitation capabilities. We have seen attempts by a variety of adversarial state actors and non-state actors to gain unauthorized access to, or otherwise degrade, our information systems and networks. Malicious penetrations and exploitations are used to steal personal, technical, and financial information and, if the actor so chooses, may be used to disrupt, degrade, or destroy information systems themselves or to prevent efficient operation of critical systems that we depend upon.

Commercial Internet security companies, who consistently monitor the Internet for deployment of malware and malicious code, have recently released their 2008 predictions of the top ten cyber security threats. The picture they present is not positive. In spite of ever-improving defenses, vulnerabilities continue to increase and are increasingly being

exploited by a variety of actors. Sophisticated website attacks that exploit browser vulnerabilities, more effective botnets, cyber espionage by resourced actors, mobile phone and Voice over Internet Protocol (VoIP) exploitation, insider attacks, identity theft, and spyware are all increasing. Thus, challenges for network defenders grow daily.

Commercially available threat reports estimate that up to one in every 600 social networking pages hosts malware. For instance, Sophos maintains that they discover one new infected web page every 14 seconds, which equates to 6,000 a day. Of these newly infected pages, approximately 83% of them are legitimate websites that have been hacked. Additionally, the number of phishing web sites continues to rise exponentially. McAfee Avert Labs saw a 784 percent increase in phishing web sites in the first quarter of 2007 alone.

Socially engineered email is increasing in sophistication and remains a particularly effective source of malware delivery. Therefore, user education in the identification of malicious email remains one of our most critical network defense tasks. One security firm noted that threats spreading via email file attachments have actually declined, as hackers and malicious code writers turn to the web to host their attacks. However, although malicious email attachments may have been reduced in percentage terms, emails containing links to malicious websites continue to pose a growing problem to computer users.

The increasing popularity of user-contributed web services and social networking sites is placing traditional web filtering and antivirus solutions at a disadvantage in the battle to maintain the integrity of the Internet. Content on many popular sites today is unregulated, user-contributed, and constantly changing. The dynamic nature of these sites facilitates the ability to embed malicious code within the legitimate web-based content with the goal of affecting larger populations. One popular networking site was attacked by an Internet worm that was designed to steal login and password information from users. The worm was so effective that when an informal scan of 150 profiles was conducted by a commercial security company, it found that almost one-third of the

profiles were infected by the worm. This is especially disturbing since the program not only captured login credentials, but also sent email embedded with malware from the compromised system to others in the user's contact list, making it self propagating.

Another increasing area of concern is the exploitation of supply chain vulnerabilities that results in infected consumer devices being sold to the general public. Through this mechanism, retail outlets are increasingly becoming unwitting distributors of spyware and malware. Devices with USB connections and the software packaged with them can contain malware that infects victims' computers and connects them into botnets.

Aware of these threats, the Department employs a multilayered strategy in operation and defense of the GIG focused on achieving maximum mission assurance by protecting secrets when necessary while sharing as broadly as possible. The strategy involves minimizing vulnerabilities, driving out anonymity in every interaction, and deploying a robust cyber attack detection and response capability. The GIG is operated as a warfighting system, with a professional NetOps force that is led by the JTF-GNO and coordinated across the entire Department. Next, I'll give a few examples of the strategic defensive layers.

A core element of our vulnerability management strategy is the employment of National Security Agency (NSA)-approved cryptography throughout the networks which carry classified information, and in the parts of the unclassified network that are more subject to eavesdropping threats, for example, most commercial satellite communication circuits. We also use commercial cryptography broadly inside the networks.

Another element is focused on ensuring that every device in the GIG is configured as securely as possible and is kept that way, and that the right people know the state of configuration of the GIG. DISA partners with the NSA, the National Institute of Standards and Technology (NIST), other federal entities, and industry to develop standard configuration descriptions and associated checklists for the technologies in the GIG. System administrators use these products to configure systems and to check the

configuration of systems. Auditors also use them to double check that systems are configured properly. As part of this work, many entities in the Department, at NIST, and in industry worked together to develop the Air Force Standard Desktop for late version Microsoft operating systems. This is being adopted DoD-wide, and has extended this year into the rest of the federal government as the Federal Desktop Core Configuration which is being mandated across the federal government by the Office of Management and Budget.

In order to ensure that the configuration of deployed equipment is updated as soon as new vulnerabilities are found, the JTF-GNO monitors government-developed and public vulnerability information. When significant vulnerabilities in important technologies are found, the JTF-GNO issues an alert to all units in DoD directing that action be taken promptly to fix the new vulnerability and directs that the status of these fixes be reported back to the JTF-GNO in a time certain. These alerts are called information assurance vulnerability alerts, or IAVAs.

DISA acts as the program manager for the Department's computer network defense oversight group called the Computer Network Defense Enterprise Solutions Steering Group (CND ESSG). The CND ESSG focuses on understanding our computer network problems and the ability of commercial and government-developed products to solve the problems. It also focuses on developing specifications for solutions and assisting in proposal evaluation. DISA holds the budget for this DoD-wide group, and performs acquisition and deployment support for products directed by the CND ESSG. They are deployed by the Military Services inside their boundaries.

Under the CND ESSG, DISA acquired antivirus tool enterprise licenses, which include "personal" firewalls and anti-spyware utilities that further harden computers. We are also deploying the Host-Based Security System (HBSS), which was the JTF-GNO's number one priority for improving the security of individual computers on both our unclassified and classified networks. HBSS will help us manage the configurations of our computers and automatically detect and block certain types of attacks while helping us to develop

the situational awareness necessary to better understand evolving threats. Deployment of HBSS to the Combatant Commanders should be complete by late spring; deployments in the Military Services will continue for several years.

Another element of our vulnerability management strategy is to drive out anonymity in all cyber transactions in the GIG. The core of this strategy is the cyber identity credential issued across the Department, the DoD public key infrastructure (the DoD PKI) as originally required by HSPD-12. Keys are issued on every DoD physical identity card (the common access card, or CAC). The JTF-GNO has directed that all workstation logons be done using these credentials instead of passwords. CAC-based PKI credentials are now used by the well over three million people to authenticate the majority of logins to DoD workstations. This has reduced our vulnerability to password problems significantly. We are now requiring more use of the credentials to digitally sign email that contains attachments or web links. This will make it harder to counterfeit DoD email or to tamper with an email.

I'd like to expand on use of configuration guidelines as a key part of our vulnerability management strategy. DISA develops guidelines called Security Technical Implementation Guides (STIGs) which are a compendium of policies, security regulations and best practices for securing an operating system, network device, or application. There are currently twenty-four STIGs. Recent additions have addressed topics such as wireless messaging, video teleconferencing, domain name system security, and access control. A primary focus in 2007 was addressing guidance for Internet Protocol (IP) Version 6. Our work on STIGs is complemented by close association in the development of configuration guides with industry, for example Microsoft and Apple, and other government agencies. We believe that close partnership among industry, DoD, and NIST will result in the acquisition and delivery of systems already configured to operate securely on our networks and avoid the labor intensive process we go through today to lock down systems prior to use.

In spite of our best efforts, our defenses will never be perfect. Clever and persistent adversaries will always be looking for holes in our defenses, even if temporary. Because of this, we deploy and operate a wide variety of commercial and government-developed attack detection and diagnosis technologies. We monitor traffic going to and from the Internet at the gateways between DoD and the Internet. DISA also monitors traffic in the network core internal to the Department. DISA and the Military Services monitor traffic that goes from the core network into bases and other enclaves. The Military Services, NSA, DISA, and the JTF-GNO have analysis cells that look at the Department's information to discover trends and find vulnerabilities which are shared among the community. DISA operates four theater NetOps centers that fall under the operational control of the JTF-GNO. These theater NetOps centers run and monitor the network infrastructure in each primary geographic theater and provide attack detection and diagnosis service in each theater.

I'd like to talk now about a few examples of other improvements we are making.

We are moving to enable greater automated configuration control and management along with associated metrics and reporting. We conform to the various standards that make up the Security Content Automation Protocol (SCAP), a set of data standards for describing things like configurations, vulnerabilities, and measurements of configuration. SCAP allows us to describe standard configurations in a machine-readable, standards-compliant way. The SCAP effort is being led by NIST with strong participation from NSA, DISA, the Director of National Intelligence (DNI), and industry.

We will move all publicly visible and partner-visible applications into what are called demilitarized zones (DMZs) at the boundary between DoD and the outside world. DMZs provide protection of web sites and services accessible from the Internet and stronger protection for databases and other data which will no longer be directly visible to those outside of the Department. All external accesses to these databases must go via servers in the DoD DMZs. We have several DMZs already, and we are building more in conjunction with the Military Services, and NSA.

Related to the DMZ effort, we are also looking at "zone" protections for selected communities of users based on the type and importance of the mission they perform. Examples of communities would include combat patrol, supply chain, or R&D. Zones would allow the communities to perform their missions in a protected manner and to isolate them from attacks from others with freer access to the Internet, in other words, segregate mission work from non-mission work. Zoning implementation will be in the network, perimeter defenses in the network, and in the operating systems of the computers in the zones. I expect we will begin this in the next year or so.

We are also modifying the structure of the DoD domain name system so that all domain name system queries from outside of DoD will be satisfied in the DoD DMZs. The distributed nature of the domain name systems today means that we must have many of these servers in the Department. This new approach will reduce the attack vulnerability of the DoD domain name system and allow us much better control over what we look like from a network perspective to the outside world. We expect this system to be deployed this year. We are also working to deploy a system that will handle domain name system queries going in the other direction, from DoD to the Internet. We will intercept all of these queries at the boundary between DoD and the Internet, and we will perform the query on behalf of the internal DoD customer, then return the result to the customer. This will allow more uniform protection from another set of attacks that depend on certain characteristics of the domain name system.

I'd like to talk now about the evolution of the classified networks. We have made efforts to further improve resistance to physical breach and to improve resistance to attacks by insiders, for example spies and saboteurs. One of the most fundamental efforts is the deployment of an improved cyber identity credentialing infrastructure on the classified networks. The so-called SIPRNET PKI is foundational both to getting stronger accountability in all interactions in the classified networks and to improving sharing by opening more information sources owing to this much stronger accountability. We

expect to begin deploying the improved SIPRNET PKI next year, and based on our experience with the unclassified PKI, I think it will take a few years to complete.

As we change the unclassified PKI to support the issuance of cyber identity credentials to more types of network hardware and software, we will also deploy this capability on the SIPRNET. This will reduce our exposure to certain kinds of attacks and it will pave the way for much broader use of the service oriented architecture enabled capabilities on classified networks.

Over the next year, we will emphasize stronger interagency operational governance of the classified networks. In addition to NetOps improvements we continue to make, we will work to improve interagency connection approval and compliance validation inspection processes to ensure we are all adhering to the same standards for connection.

One final word on interagency governance -- many of us, including vendors, are often frustrated because at least three groups of security implementation guidance exist. DoD, DNI, and NIST have each published guidance, much of which overlaps. In qualifying products, vendors must sometimes be evaluated in two or three of these overlapping sets. We have agreed to harmonize security guidance across the federal government, and to develop a uniform method of certifying that systems comply with the required controls. This should simplify things for vendors to the Department and for government employees alike, and this simplification should improve security everywhere.

Mr. Chairman, I hope I have given you a good picture of the importance of information to the Department of Defense and the imperative that we protect it diligently. In the closed door classified discussion we had with you recently, my colleagues and I described the cyber security threats the Department faces daily. Support from the Congress in this arena is critical. I ask your continued programmatic and fiscal support so that we can together work to keep the Department's networks and computers secure. Thank you, Mr. Chairman. I look forward to any questions you and your colleagues might have.

## QUESTIONS SUBMITTED BY MEMBERS POST HEARING

APRIL 1, 2008

## QUESTIONS SUBMITTED BY MR. SMITH

Mr. SMITH. Are there areas in which you believe the government is underinvested that should be enhanced (or, conversely, where there is too much investment and the areas can be deemphasized)?

Mr. KRAMER. I believe the government could usefully increase investment in four areas—people; establishment of cyber laboratories; enhanced research and development; and development and support of infrastructure protection.

People—As I stated in my testimony, "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." The federal government could support those efforts by a variety of incentives, grants, and scholarships, among other approaches.

In addition, I recommend that the Congress evaluate whether creating a "cyber corps" of high level professionals would be valuable. There are many dedicated cyber professionals already working for the government, so establishing a cyber corps should not be done without appropriate analysis—but a group that had the capacity to work across agency lines might have high value.

Cyber laboratories—As I stated in my testimony, "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. . . . 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 estalish the ability to delve deeply into key questions under government control in a way that cannot always be accomplished through the contracting process."

Enhanced research and development—In addition to government cyber laboratories, there would be great benefit in increasing overall research and development funding by the federal government. As I said in my testimony, "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." Accordingly, I recommend, as I said previously, "very significantly increasing RUD funding for governmental agencies; and enhancing private sector activities through direct contracts and incentives." Undertaking such actions 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.

Development and support of infrastructure protection—Cyber capabilities are vulnerable both because of security issues in the cyber arena itself and because of the vulnerability of the electrical grid. On the latter issue, the Defense Science Board has issued a recent report which underscores that vulnerability—but this is only one of very many such analyses. In my opinion, significant efforts should be undertaken to make the electrical grid less vulnerable, both from physical and cyber attack. One area of focus should be whether SCADA systems should utilize the standard Internet protocols, which make them vulnerable to numerous viruses and other forms of attack. As I stated in my testimony, "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."

More generally, whether through government laboratories, increased R&D spending or otherwise, investments in network system architectures that are less vulnerable to potential attack means and better methods of attack attribution would have high potential value.

Mr. SMITH. 2) Do you have any recommendations about how the USG should quantify the costs or economic impacts of a cyber attack?

Mr. KRAMER. The consequences of a cyber attack—depending on its nature—could include economic, governance, and social impacts. Economic impacts can be quantified in the same way other significant disruptive factors, such as hurricanes, are quantified. While cyber generally will not have physical consequences, it will have business disruption consequences, and such consequences are often calculated at both the micro and macro levels.

I understand that there are several organizations that are developing tools to estimate the costs of such attacks. While I do not have personal experience with them, they include the US Cyber Consequences Unit (a private 501(c)(3) organization), the University of Virginia Center for Risk Analysis, and the National Infrastructure Simulation and Analysis Center which operates under the direction of the Department of Homeland Security (DHS), Office of Infrastructure Protection (IP), Infrastructure Analysis and Strategy Division (IASD), and includes analytical staff at Sandia National Laboratories and Los Alamos National Laboratory in New Mexico.

It is important not to limit the analysis of the consequences of a cyber attack to the economic. The attacks in Estonia show that governmental functions can be significantly disrupted, which would be of high consequence to the American public. Similarly, societal functioning increasingly relies on cyber—for example, telephone via voice-over-IP—and cyber attacks could be highly consequential.

Mr. SMITH. 3) What sort of technology might the government be able to pursue to help enhance privacy protections without jeopardizing security?

Mr. KRAMER. The challenge is to harmonize security and privacy considerations. Unfortunately, privacy needs can come into conflict with the need for attribution of cyber attack activities. But, an appropriate balance may be reachable, particularly with technologies that are collectively referred to as "traffic flow analysis" tools. It is very important for the Congress to thoroughly analyze such issues to determine how such a balance should be struck and what protections should be required.

I do not have technical expertise, but it is my understanding that the traffic flow analysis tools do not look at packet contents, but instead focus on header information to determine the source and destinations of groups of packets. By looking for anomalies in this traffic information, sensors can detect both large-scale attacks, as well as subtle outliers that may indicate a fine-tuned attack. By subtracting nonnal, expected traffic patterns from the actual traffic on the network, such tools can highlight specific traffic flows and packets that may require more analysis. The traffic flow analysis itself is not looking at message content, as it relies on information that ISPs themselves use to route packets through their networks--though it does review some information and would still need to be under appropriate procedures. Once anomalies are identified, suitable procedures and/or court review could be established to zoom into the payload (i.e., non-header) parts of packets to discern the details of subtle, outlier attacks, while still maintaining privacy of those users whose packets are not included in the anomalous set. It is important to recognize that I am only recommending reviewing the potential of a general approach, and the specifics would need to be critically evaluated and highly important. Any such activities should be according to a framework and rules set by the Congress working in conjunction with the Executive Branch.

Mr. SMITH. 4) What sorts of actions can the government take to help create incentives for developing/adopting/deploying security technologies?

Mr. KRAMER. In addition to the research and development activities discussed above, the government can take regulatory and direct support actions and can provide incentive support related to the adoption and deployment of security technologies.

As I stated in my testimony, "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."

Based on that differentiation, "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."

I think it is important to recognize that 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."

For these reasons, it is extremely important that 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."

Mr. SMITH. 5) What lessons should we learn from the recent attacks against Estonian networks?

Mr. KRAMER. The lessons learned can be divided into the immediately derivative and longer-term:

Immediate

- Large-scale packet floods can be effective in shutting down e-commerce, electronic banking, and e-government sites for a period of 24 to 72 hours.

- Attribution can be exceedingly difficult in the cyber world.

- A distributed, world-wide cyber attack can be launched, possibly with limited or no central overt government command and control.

- Communities of defenders can work together to help respond to an attack more effectively than they can when working alone. But, such defenders often work best when they are located together geographically. That is, despite the distributed nature of cyber space, defenders at this level may need to be deployed on very short notice to arbitrary points around the world to help respond to an attack, not unlike the need for rapid-response and deployment of military forces.

Long-term

—As discussed above, certain critical networks may best be created on non-Internet protocols in order to give greater protection. Overall, the issue of building resiliency into networks needs greater consideration.

—International support needs to be established on a more formal and thorough basis. Both civilian and military partnerships need to be created and/or enhanced in order to be able to deal with such attacks.

—The problems of attribution need a much more directed analysis.

—An international regime that organizes and protects international networks need to be established.

—The policies relating to international responses to attacks should be developed.

Mr. SMITH. Are there areas in which you believe the government is underinvested that should be enhanced (or conversely, where there is too much investment and the areas can be deemphasized)?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. Do you have any recommendations about how the USG should quantify the costs or economic impacts of a cyber attack?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. What kinds of technology might the government be able to pursue to enhance privacy protections without jeopardizing security?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. What sorts of actions can the government take to help create incentives for developing/adopting/deploying security technologies?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. What lessons should we learn from the recent attacks against Estonian networks?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. How do current software practices contribute to or hinder cybersecurity efforts? Are there changes to software engineering curricula at the universities that you might recommend?

Dr. GOODMAN. [The information referred to was not available at the time of printing.]

Mr. SMITH. Are there areas in which you believe the government is underinvested that should be enhanced (or conversely, where there is too much investment and the areas can be deemphasized)?

Dr. LEWIS. [The information referred to was not available at the time of printing.]

Mr. SMITH. Do you have any recommendations about how the USG should quantify the costs or economic impacts of a cyber attack?

Dr. LEWIS. [The information referred to was not available at the time of printing.]

Mr. SMITH. What kinds of technology might the government be able to pursue to enhance privacy protections without jeopardizing security?

Dr. LEWIS. [The information referred to was not available at the time of printing.]

Mr. SMITH. What sorts of actions can the government take to help create incentives for developing/adopting/deploying security technologies?

Dr. LEWIS. [The information referred to was not available at the time of printing.]

Mr. SMITH. What lessons should we learn from the recent attacks against Estonian networks?

Dr. LEWIS. [The information referred to was not available at the time of printing.]