ATLANTIC COUNCIL
IDEAS. INFLUENCE. IMPACT.

ISSUEBRIEF

Franklin D. Kramer

Cyber Security: An Integrated Governmental Strategy for Progress

"It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation ... It's also clear that we're not as prepared as we should be."

- President Obama, May 9, 2009

Cyber security has emerged as a critical challenge in an era defined by global interconnectedness and digital information. While there are multiple ongoing efforts that seek to enhance cyber security, an integrated governmental strategy to meet that challenge has only begun and has yet fully to take shape. All strategies demand recognition of risk and prioritization of resources, and cyber strategy will be no different.

An effective approach to creating a risk-adjusted, prioritized cyber strategy for the U.S. government would be to focus on key national security problems, provide solutions for those problems and then use that learning to help create security in the broader cyber arenas. Such a strategy would have the additional benefit of establishing an effective allocation between those efforts where government is significantly engaged in providing cyber security and the much broader area of market-generated cyber security where the private sector can provide reasonable security (although, even in this broader area, there will be value in certain kinds of appropriate governmental support).

Under a national security approach to cyber security, the cyber areas for which the government must take key responsibility are:

- ensuring that the Department of Defense (DOD) and the Intelligence Community (IC) can operate effectively while under cyber attack, including in wartime;
- ensuring through effective public-private partnerships that key critical infrastructures – electric grid, financial, telecommunications and governmental – do not suffer catastrophic failure if attacked, and can maintain/return to adequate service while under attack; and
- limiting espionage and exfiltration of national security information.

The Cyber Security Project

This issue brief is part of a broader effort of the Atlantic Council's project on Cyber Security. Led by the Council's Program on International Security, the Cyber Security initiative addresses emerging issues in the cyber security and defense realm, including international cooperation, private-public partnership in cyber security, as well as the role of international organizations including NATO in cyber defense and security. Under the umbrella of this initiative the Council hosts workshops, roundtables, working dinners and publishes occasional issue briefs. For more information, please contact the Associate Director of the Program on International Security, Magnus Nordenman, at mnordenman@acus.org.

The Council's work on cyber security is generously sponsored by SAIC.

Franklin D. Kramer is Vice Chairman of the Atlantic Council Board of Directors and is a member of the Atlantic Council Strategic Advisors Group. He served as Assistant Secretary of Defense for International Security Affairs during the Clinton Administration.

As important as the foregoing are, they do not constitute most of the cyber arena. However, with appropriate governmental support, the private sector can reduce the vulnerability of businesses and individual citizens to cyber attack across the broad spectrum so that economic, individual and social activities may make valuable use of cyber.

The Challenge: Reducing Cyber Insecurity

The National Security Strategy states, "Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation." As the statement indicates, the cyber threat is substantial. There are vulnerabilities at all levels of the cyber arena: computers themselves were designed to implement programs and manipulate data – not to provide security – and the networks were designed to transmit information, not to check its validity or safety. It is true, of course, that, while security has been an 'add-on' to cyber connectivity, numerous security capabilities have been created at the hardware, software and process levels, and have been applied by the government, private sector and individuals. The problem is that, despite some excellent capabilities and efforts, the level of security thus far achieved is not yet adequate. Indeed, perhaps the most salient characteristic of cyber is the combination of its very widespread and growing use despite the fact that there are ongoing substantial attacks, some with great success, against its users.

Cyber attacks (or their threat) can be categorized in numerous ways, but one profitable approach is to separate attacks into two categories based on attacker objectives:

- those with potential national security consequences where the aim is to undermine or have the capacity to undermine key capabilities, such as the military or the electric grid, or for espionage; and
- those with criminal objectives where the aim is to generate funds, sometime through selling or using data and sometimes through extortion.

Both national security and criminal attackers possess very advanced capabilities. The general consensus is that it should be assumed in current circumstance that advanced attackers can succeed in getting through defenses – which makes the issues of resilience and limitations on the effects of attacks quite important.

On the national security side, there have been cyber attacks in wartime (on Georgia during the conflict with Russia) and in more ambiguous circumstances (on Estonia), and there have been numerous media stories of Chinese attacks on governments (including on the United States, the United Kingdom, France, Germany and India). General Alexander, the head of Cyber Command, has publicly stated that that the Department of Defense is subject to some six million attempts per day at unauthorized intrusions, and Deputy Secretary of Defense William Lynn has said that the DOD "has not always been successful stopping intrusions" and has "experienced damaging penetrations."

On the criminal side, there is a brisk trade in criminal capabilities on the Internet. Actual losses are certainly high, including exfiltrations of intellectual property estimated in terabytes, but the unclassified data on annual losses varies by orders of magnitude from hundreds of millions to as high as an estimate of $400 billion. Finally, it is worth noting that there is not necessarily a bright line between national security and criminal objectives: the well-known attack on Google may be an exemplar of a hybrid situation.

The Proposed Strategy

As noted above, a strategic approach to cyber security would be to focus governmental efforts, first, on limiting national security consequences and, then, to use the learning from such efforts to support cyber security in the broader arena. The technical fundamentals of providing cyber security overlap between the national security and the broader cyber arenas, and thus advances in security in one arena are valuable to all. To be sure, there are important concerns in the cyber world beyond national security matters, but the focus on national security allows for a sharpened direction both of governmental resources and legislative and regulatory efforts, as well as a clarification as to what specific results are being sought.

Within the national security arena, the key requirement for an effective cyber security strategy will be to take particularized steps critical to the nature of the problem being faced. Focusing on key problem areas allows for defining achievable responses, and seeking specific

results allows for a much more programmatic, metric-driven approach.

While there are definitely overlaps among appropriate responses, not all steps taken in one national security arena are necessarily appropriate for another – and there are different levels of risk which may be acceptable among different areas. In addition, policy, legislative and regulatory steps may differ among different arenas, and focus allows for more granular analysis. Within this broad framework, the key strategic steps for national security cyber issues follow.

Department of Defense/ Intelligence Community

The DOD and IC face the issues of defending essential networks and operations and of determining how and when to use offensive capabilities.

Computer Network Defense: The DOD and IC are fully aware of the problems of cyber security and the currently available techniques of detection, protection and response. This is no small matter because for the other national security problems described below – infrastructure vulnerability and espionage – the technical solutions for security are either not available or not well understood (even to the extent they are available). Current technical capabilities are not sufficient for fully adequate cyber security, but current capabilities properly provided can significantly enhance security.[1] Knowledge, however, is not enough. The DOD's cyber assets are large, including some 7 million machines and 15,000 networks. The creation of an effective technical architecture with adequate situational awareness, resilience and interoperability will be a significant challenge. In light of the significant technical capabilities of the DOD/IC, the fundamental cyber security issues faced are less knowledge about what to do than overcoming the resource, organizational and other barriers to:

- designing, deploying and operating effective capabilities as widely as necessary;
- training against cyber attacks; and
- developing (and then deploying) better future capabilities.

A related, but different issue dealt with separately below, is integrating the use of cyber offense.

Deploying Capabilities: With respect to the first objective – DOD deployment of effective defensive capabilities – the key issues are scale and availability of resources. Historically, there has been a strong tendency within the DOD to enhance connectivity, but not to give as high a priority to integrating security into that connectivity. Network-centric warfare depends on embedded C4ISR – but that very capability has created an inherent vulnerability.[2] How quickly to provide the resources to significantly protect DOD assets, and what level of protection to provide to different groups within the DOD, is yet to be determined. But given the conclusion that the cyber threat is both widespread and advanced, it should be expected that in a significant conflict, cyber attacks will be widely used against our forces. To protect against such attacks and avoid catastrophic failure, substantial increases in cyber defenses will be necessary. A key requirement will be to establish cyber security as a critical element in the table of organization and equipment of units at all appropriate levels, including wartime missions, capabilities, organizational structures, and mission essential personnel and equipment requirements. Effecting these requirements throughout the DOD will be a very substantial task and will require highest level efforts to ensure the budgetary resource priority that cyber security should receive as compared to the many other significant demands on DOD resources.

Training: With respect to the second objective – training against cyber attacks – the problem is at once simple yet quite difficult. Generally, under current circumstances, use of cyber attack capabilities in skilled hands against a training force can be quite disruptive and undercuts achieving training objectives. The question becomes how to conduct necessary training – and also under potentially

1 An enterprise (governmental or private or even an individual) will seek to: understand the computers under its control and how they are configured and operate; ensure that communications to and from the enterprise are only between valid communicants using various identification/authentication mechanisms and rules regarding communications; provide sensors that seek to understand how/when an attack is underway (or has taken place) and to block it (using various intrusion detection/prevention devices); and limit the effects of an attack through various means including the proliferation/redundancy of computers providing the same service to the enterprise, limiting exfiltration from the enterprise, reviewing computers which may or have been attacked, or periodically changing the interface with the cyber world outside the enterprise including the use of virtual computers.

2 C4ISR abbreviates the term Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance.

realistic scenarios that would include cyber – while recognizing that, in today's wars, cyber has not yet become a significant factor with which to contend. Again, only high-level attention is likely to make progress in this arena, but as a general proposition, cyber training should be much more significantly incorporated in the training cycles. We do not want to find ourselves in the position regarding cyber that we have recently endured regarding irregular warfare in which only after years of combat has training started to catch up.

Future Capabilities: The third objective – developing future capabilities – should be part of a national effort discussed below. This is critical because of the current situation in which it is generally concluded that advanced attackers have very substantial capacities to penetrate cyber defenses. While defeating all attacks always is undoubtedly too high a bar, defeating many more should be possible as should be the development of resiliency capabilities which would let the DOD operate while effectively under attack.

Computer Network Attack: Integrating the use of cyber offense via computer network attack has generated a great deal of heat and little light in the DOD. There are two major obstacles:

- conflating the considerations of use of Computer Network Attack (CNA) in wartime with potential use either in current circumstances or in gray areas where it is not clear that we are at war, and
- over-classification.

Wartime: In wartime, once the president has determined to use force, the use of CNA is generally subject to the same rules as the use of other weapons, which include the norms of necessity and proportionality. Other weapons' capabilities of some similarity have been long used in wartime – electronic warfare in particular – and the military needs to integrate CNA as appropriate in strategic, operational and tactical planning across the full spectrum of warfare including conventional and irregular. Some of this planning is already ongoing, and it will be a particular task of Cyber Command, generally in support of regional commanders. In addition, because of the speed with which cyber attacks can take place and the potential necessity in wartime for very prompt responses, there is a crucial need to develop standing rules of engagement that will allow commanders to take necessary steps to support wartime objectives. Moreover, planning and exercises are necessary to evaluate how best to use cyber, including how to calculate effects and what limits are required and/or appropriate.

Classification: Wartime planning and implementation will be significantly enhanced if classification were significantly reduced in the cyber world. The Vice Chairman of the Joint Chiefs of Staff, among many others, has eloquently and bluntly spoken to this issue. While there are good reasons to highly classify and compartment some cyber matters, there is such significant over-classification and compartmentation that planning and operational integration is overly difficult. A good deal of over-classification arises because the DOD learns threat information through the IC whose techniques are themselves highly classified and compartmented. However, cyber presents the unusual situation in which the private sector learns much (though not all) of that same information through non-classified actions (e.g., companies like Symantec, McAfee or the various Internet Service Providers such as Verizon or AT&T). A systemic effort to limit highly classified and compartmented information to the truly necessary, to allow most operational activities to be classified at the Secret level and to engage in many basic conversations at the unclassified level would significantly enhance DOD's capacity to integrate cyber. That approach is generally used in connection with electronic warfare. Its implementation will require high-level action since resolving the DOD/IC classification interface will not be simple.

Gray Areas – Less than Wartime: The most daunting intellectual challenges in cyber security concern what type and degree of responses are appropriate to a cyber attack under less than wartime circumstances. That, of course, is the situation in which the United States now finds itself. The severity of the attacks could increase without there being a decision by the President that a conflict situation had arisen and wartime-like responses are called for. In seeking to deal with such gray areas, the most appropriate approach will be for the government to develop a menu of responses – a whole of government approach – which can then be applied as determined in the particular instance to the problem at hand.

Law enforcement and forensic analysis are obviously one element of a whole of government response capability, but the more difficult issues involve responses beyond that arena. The intrusions into Google illustrate the issues. There

often will need to be coordination between the government and one or more private entities.

- A first level of response could be diplomatic at the bilateral level. In the Google case, for example, the Secretary of State has called for an investigation into the alleged intrusions by the Chinese government.
- A second level of diplomatic response would be to consider whether an international regime could be established to limit cyber attacks. There are a great many questions in this regard. For example, if the Google attacks or others reported in the media have been directed by the Chinese government, would an international regime be helpful? The Russians have proposed a regime under United Nations auspices, but Russia is thought to have been behind attacks on Estonia and Georgia and many cyber criminal gangs are said to have Russian connections – so would this be an effective regime or just a constraint on the United States? Despite these very legitimate concerns, exploration of an international approach seems warranted to determine if useful international norms might be established even if such efforts might well not end in any agreed conclusion. It may be that limits on criminal actions will turn out to be possible to agree upon even if limits on nation-state actions cannot be agreed.
- A third potential arena for response to cyber attacks would be economic. In the non-proliferation and the counter-terror areas, the use of economic sanctions is well-accepted. Adapting an economic sanctioning regime to the cyber arena would potentially be valuable, and it would add to the government's available arsenal of responses.
- At the fourth level, there is the potential use of either cyber or kinetic response. Kinetic responses are unlikely unless the President determined a conflict situation existed. However, it is worth noting that in certain cases, such as the 1989 intervention in Panama, the United States has used military force in support of what has included law enforcement issues (e.g., drug dealing). Moreover, in the counter-terrorism arena, both the Obama and the Bush Administrations, with the support of the Congress, have chosen to seek out adversaries by various means, including highly kinetic.

Cyber responses to cyber attacks (or other uses of cyber by adversaries, e.g., as a method of communication or recruiting by terrorists) could also be utilized in certain circumstances. Such responses could include possibly disabling actions taken against web sites or servers from which attacks or other actions were generated. Such responses raise a variety of questions. One frequent issue is when is the DOD empowered to take action under U.S Code Title 10 and when would a response have to be under the President's covert action powers under Title 50. Mostly, this issue concerns compliance with Congressional directives – but the ultimate decisionmaker in each instance will be the President – so the fundamental question will be when responses are justified. While the high likelihood is that any particular situation has to be determined based on the specifics of the situation, it is worth noting that under the rules of war, placing naval mines in another country's territorial seas is unlawful. Analogously, embedding potential attack capabilities or actually attacking national security structures of a country would arguably similarly authorize a cyber response if and when the President determined that would be substantively appropriate.

Distinguishing what precisely the threshold is between a wartime and less-than-wartime circumstance has gotten a great deal of attention. Often the question is put in legal terms – has an armed attack occurred under article 51 of the United Nations charter (or under article 5 of the NATO Treaty). While there are obvious legal issues, the fundamental question is a policy one. It seems extremely unlikely that any country suffering significant damage because of a deliberate cyber attack would not deem it appropriate to at least consider and perhaps take wartime-like steps – or to put it in legal terms, to determine that it had suffered an armed attack. There can be uncertainties as to how much damage would be deemed sufficient, but that calculus also is true in kinetic circumstances – and it also most probably would be affected by analysis of intent.

There are two implications from this conclusion.

- First, it will be valuable to seek to deter such a serious attack – and one step to doing that would be a declaratory policy stating the authority and capacity of the United States to respond fully to a

cyber attack of unacceptable consequence in a manner and time of its choosing.

- Second, it is also important to recognize that even if there is a cyber attack of consequence – sufficient to be deemed an armed attack under the UN charter – that United States' laws and rules must govern the United States' response – and, in particular, the relationship between the Executive Branch and the Congress. An appropriate declaratory policy, as has been used with respect to other types of potentially serious attacks, could help create a common Executive Branch-Congressional understanding.

To summarize, the development of a menu of whole of government responses and appropriate doctrinal and legal analysis to support them will be a critical element of cyber security strategy.

Key Critical Infrastructures

Cyber security varies considerably among key critical infrastructures – telecommunications, financial, governmental and electric grid. With the exception of the federal government infrastructure, the role of the government concerning key critical infrastructure is twofold:

- to help develop solutions that industry can implement, and
- to provide a framework that ensures those solutions are in fact adequately implemented.

Or, to shorthand the point, to develop effective public-private partnerships.

The major telecommunications companies which are also the key Internet Service Providers (ISPs) have a very good handle on their capabilities and vulnerabilities. As discussed below, these actors need to be integrated further into effective public-private partnerships that will enhance cyber security. Likewise, at the top of the financial industry (including the Federal Reserve, large banks and large money flows), there is also a great deal of attention to the cyber security issue, although further down the financial chain, there are significant vulnerabilities. By contrast, the federal government generally is not well-protected nor are state and local governments. Similarly, the electric grid appears highly vulnerable. Under a prioritized national security strategic approach, federal government operations and the electric grid would receive the most immediate attention, though the telecoms and the financial industry do need significant consideration.

Federal Government: For the federal government, the existence of cyber security vulnerabilities is, in significant part, a matter of priorities and resources. As noted above, the existing techniques of protection are well-known to at least some parts of the government. For example, even apart from the DOD and IC, the Department of State has developed a systematic approach that is reasonably effective and could be used by other non-DOD/IC departments to help implement cyber security. The overall responsibility for the federal government lies with the Department of Homeland Security (DHS). The needs are well-recognized by DHS, and it will be valuable for DHS, working with the DOD/IC and agencies such as State to generate architectural solutions to be adopted by other governmental agencies in order to enhance cyber security. Steps in this regard have been taken under the Comprehensive National Cybersecurity Initiative (CNCI) which discusses, among other matters, deployment of intrusion prevention systems, enhanced situational awareness and increased research and development. The recent draft National Strategy for Trusted Identities in Cyberspace is another step in this direction and there has been a recent White House memorandum requiring continuing monitoring as State has done. Making the CNCI and related efforts effective will depend in significant part on the White House and Cabinet Secretaries determining to apply appropriate levels of effort including resources. However, it will be very important for DHS, working with both the DOD and agencies like State, to go beyond continuous monitoring/intrusion detection and protection to generate architectural solutions to be adopted by governmental agencies in order to enhance cyber security. In this connection, another valuable, related action would be to adopt legislative changes to the Federal Information Security Management Act (FISMA), which currently focuses more on procedures rather than on security outcomes, and whose amendment (as has been proposed in the Lieberman-Collins Bill) would help create greater attention to security and the necessity of providing appropriate resources. None of these efforts will succeed unless cyber security becomes mandatory for governmental departments and agencies. Until now, a combination of less than sensible requirements and decisions not to allocate adequate resources have undermined efforts at cyber security. True accountability for

meeting appropriate mandatory performance requirements is necessary, and there should be no doubt that, at the end of the day, improved security will require such additional resources.

In addition to the steps noted, there are two important issues affecting cyber security for the federal government which go beyond priorities and resources.

- The first is how to establish DHS as an effective agency in the cyber security arena.
- The second is to determine, as the government interfaces both with individuals and also economic entities, how protection of civil liberties, privacy and proprietary information should be ensured – and how should that should be balanced against, or (more optimistically) integrated with, effective cyber security.

On the first question of DHS development, at the simplest level there is the issue of providing adequate resources – and most particularly well-trained people. DHS will need a sufficient cadre of personnel to be an effective agency in the cyber security arena. However, it may not be easy for DHS to quickly obtain the number of highly qualified cyber security personnel that would be desirable, and a policy of assignments from other agencies would supplement DHS capabilities. Creating an overall "jointness" approach between at least the DOD/IC and DHS also would reduce future frictions on the inevitable issues of which agency will have which capacities.

There are, and likely will continue to be, important questions of whether there should exist multiple capabilities (some would say "redundant" capabilities) when resources are scarce, especially since creating multiple centers may add to complexity which may reduce effectiveness. To maximize use of available resources, the CNCI (and other recent decisions) provides for the DOD/IC to support the rest of the government through the Department of Homeland Security. That relationship is still maturing, as is generally acknowledged (there are different views – the negative often only expressed privately – as to how well it is developing). The issue of situational awareness particularly raises concerns for some, both with questions as to the appropriateness and/or legality of the DOD/IC engaging in cyber activity within the United States even when in support of the DHS, or – for some – whether or not DHS should undertake surveillance as is planned with the so-called "Einstein" intrusion detection and protection systems with respect to the governmental cyber security domain (.gov). Given, however, the very substantial cyber threats, the indivisibility of cyber across national boundaries, and the information and capabilities needed to meet the challenge, including the necessity of situational awareness to protect governmental networks, the best solution will be to have a domestic agency undertake domestic activities although receiving appropriate support from the DOD/IC and to establish both significant civil liberty/privacy standards to be followed in cyber activities and a robust oversight approach, which would encompass not only the Executive Branch but also including engaging both the Congress and the courts (the latter through the Foreign Intelligence Surveillance Act court). A good deal of work has taken place in these areas, but clearly structured arrangements will remain invaluable.

Most particularly, there needs to be open discussion of the civil liberties/privacy standards noted above, including clarity on ar least two questions:

- First, when/how does an entity seeking to interface with the government have to provide identification/ authentication.
- Second, in order to protect the functioning of government and government networks, whether, how, and how much will government review non-government communications.

Each of these questions is getting consideration today, but there is a highly important political component to them – and, therefore, a strong case to be made to be as open as possible with the public and for engaging with the Congress either informally or formally – as part of the decision mechanism. As a general proposition, it seems sensible for the government to be able to authenticate identity when it is providing a service or a benefit. This is the approach being followed in the recently released draft National Strategy for Trusted Identities in Cyberspace.

Electric Grid: The vulnerability of the electric grid has received a good deal of attention (including, for among other reasons, the publication in China of papers on how to disrupt the U.S. grid). As noted above, this is an arena in which the infrastructure is largely in private hands, and effective solutions will depend on effective public-private partnerships. On the research and development (R&D) side, the Department of Energy (DOE) has taken various steps including the provision of grant moneys for R&D, and certain

of the DOE labs are likewise working on the vulnerability issue. The industry also has taken some first steps through the North American Electric Reliability Corporation (NERC), which recently issued its report on "High-Impact, Low Frequency Event Risk to the North American Bulk Power System" that includes a useful discussion of cyber security and the grid.

Despite this, concerns remain high. Two critical questions are:

- what techniques, including architectures, are necessary to protect the power grid, and
- how can/should such capabilities be deployed in a way that provides adequate protection taking account of both risk requirements and business considerations?

There are techniques that potentially can provide additional cyber security for the power grid. Thus far, however, there are no generally accepted architectural and/or specific capabilities solutions. A much more significant effort would seem to be warranted, especially since there is widespread agreement that the grid is vulnerable, there are media reports that the grid has been penetrated, there are (as noted above) apparent research efforts in China (and perhaps elsewhere) on how to take the grid down and the desire to transition to the "smart grid" likely will increase vulnerabilities unless cyber security is built in from the beginning. Government can, of course, not do this alone; there needs to be a significant public-private partnership. To date, that partnership has not been built. In part, this is because of the industry's understandable concern about how a requirement for cyber security will affect its economics – and also its clear requirements for reliability and safety.

In broad terms, then, this electric grid issue, like ones noted above, depends on priorities and resources. There is an important additional reason why the grid deserves high-level attention: the DOD cannot function without electricity. While there is considerable focus in the DOD at this time on that vulnerability, and many efforts toward off-grid power solutions, very significant vulnerability currently exists and will continue to exist for a long time. Further, even if the DOD made its own facilities relatively immune to grid disruption, the Pentagon depends heavily on other civilian infrastructures that themselves rely on electricity, the most obvious being telecommunications, but also all elements of transportation and logistics.

The foregoing then raises important issues of legislation and regulation. The electric power industry is, of course, significantly regulated in certain ways concerning rates and connections. However, there is no federal legislation specifically concerning cyber security over the electric grid (although the federal government does have certain authorities over the electrical transmission systems). Inasmuch as the vulnerability of the electric grid presents a national security vulnerability of high consequence, there appears to be a strong case for legislation and regulation that would set a fully integrated framework to deal with this problem. Just as the safety requirements for cars and the environmental requirements limiting water and air pollution have greatly improved the national posture, legislation and regulation that created an effective requirement for cyber security for critical infrastructure like the electric grid would meet an important national need.

While there is a strong case for regulation, two important considerations need to be taken into account.

- First, enhancing cyber security will require costs of some consequence to the industry. Any legislation should take account of that fact and allow for an appropriate return; otherwise, the effort to enhance cyber security would face widespread resistance.
- Additionally, a second important factor is the quickly changing nature of the cyber sector. Cyber looks very different today than it looked only ten years ago, and there are good reasons to believe that it will significantly change again in ten years. Any regulatory scheme that is not flexible enough to take account of such changes would either be a failure or else leave the United States with a cyber industry that would fall behind those of other countries.

So, while legislation and regulation potentially have an important place, the injunction "first, do no harm" is key.

The considerations that inform the discussions of electric grid and government vulnerabilities also relate to the telecommunications and financial industries. Without trying to repeat the analysis, the key effort would be to enhance and expand existing government-industry interactions to ensure effective combined private-public cyber security actions. This would include progress on such key issues as effective cyber architectures; sharing of information

International Security Program

The Program on International Security shapes and influences the debate on international security by facilitating dialogue through critical analysis and policy-relevant programming on the greatest security challenges facing the United States and the transatlantic community. The Program on International Security builds on its extensive network of experts and practitioners in North America and Europe to inform policy and to introduce ideas into the public debate. The Program influences policy and shapes ideas by publishing task force reports and analytical issue briefs, providing a public speaking platform for leaders in international security, briefing policymakers and national security leaders in private strategy sessions and hosting working groups to tackle the most complex challenges in international security. For more information, contact Vice President and Director of the Program on International Security Damon Wilson (dwilson@acus.org) or Associate Director Magnus Nordenman (mnordenman@acus.org).

on threats, vulnerabilities and responses; and combined research and development. Legislation and regulation that requires effective protection would also seem appropriate so long as it takes into account the structures and needs of the industry including the need to allow for innovation, competition, and effective flexible approaches (the Lieberman-Collins bill, noted above, takes this general approach).

Espionage and Exfiltration

Government and industry suffer significantly from espionage and exfiltration by national security and business adversaries. As noted, there are public estimates from government officials that the losses are measured in terabytes. The problems arise from a combination of failure to deploy existing capabilities, failure to follow security procedures and adversary capabilities that can defeat deployed security measures.

At the national security level, there is a good deal of attention to this problem in appropriate government agencies and among firms significantly connected to the DOD and/or IC. There are capabilities which can be deployed today that can be worthwhile. This again raises the issue of priorities and resources and risk-adjusted analysis. That analysis needs to be undertaken. But, as with the discussion above of critical infrastructure, it needs to include not only government, but also the private sector.

As the Google matter shows, however, even capable companies with extensively deployed cyber security measures are vulnerable. Current capabilities can only go so far. As noted above, generally an advanced attacker will be able to negate currently available defenses. The fundamental question that espionage/exfiltration raises, therefore, is whether an enhanced cyber security capability can be created. Or, to put it another way, how valuable would a significant R&D program be? If it would seem to be valuable, how should it be undertaken, including what should the division of labor be between government and the private sector (including how the government should appropriately leverage private investment)?

There are, of course, many existing efforts. Some exist under DOD and IC auspices, including efforts by the Defense Advanced Research Projects Agency (DARPA). Others are at DHS, which has developed a cyber security R&D program, and at DOE which has focused on the electric grid. The National Academy of Sciences also implements a program, and there are substantial resources from the private sector, some in response to the government programs and some independent R&D.

A much enhanced R&D program nonetheless would be highly valuable to improve cyber security. Such a program could likely profitably be divided among the government (which could do more pure research than in the private sector, could focus on particular types of applications and could help guide private research) and the private and academic sectors (which could benefit from increased government support, but which also will undertake research on their own in order to meet market demands).

The key considerations are to have an integrated view of federal cyber security R&D and to ensure that appropriate amounts are being spent on developing particular solutions. Such an R&D program should have three parts.

- The first would focus on protection – can advanced techniques such as virtualization, dynamic addressing and moving targets, and tailored trustworthy spaces be developed to create much enhanced cyber security?

- The second would assume, as seems entirely likely, that security will not be perfect and will therefore focus on resilience – how to operate a system effectively even though security has been breached.
- A third key element would be to develop a systematic approach to measuring security. One element of this would be to greatly enhance the area of modeling and simulations to test the results of both attacks and defenses. Work is ongoing in this arena now, but it would be valuable to substantially enhance these efforts.

In addition to specific R&D approaches, one important, long-term approach to enhanced R&D would be to greatly expand education and training for cyber professionals. A significantly increased governmental education/ scholarship program would be very valuable. Another consideration would be whether and how to take advantage of the increasing number of cyber professionals being trained worldwide.

Reducing the Vulnerability of the Private Sector and Individual Citizen

The recommendations thus far have been to prioritize governmental efforts toward cyber security problems that have potential national security consequences. Such prioritization, as discussed, will allow for focused use of resources and a particularized approach to problem solving which should allow for greater granularity and likelihood of solution.

Such an approach does not mean that the larger cyber arena will be devoid of improvements for enhanced cyber security.

- First, much of the capabilities created for protecting cyber are, and will continue to be, provided by the private sector.
- Second, to the extent that the government develops techniques, architectures or processes, those generally can be equally utilized on the non-governmental side. Therefore, advances created or undertaken for government can be transferred to the private sector. Of course, whether that will be done involves both classification, bureaucratic and legitimate security issues. There always will be concerns that sharing information provides a blueprint for getting around the protective action. Nonetheless, a policy of generally considering transferring advances from the public sector to the private sector could be a critical tool in the overall development of cyber security. While there will be some matters which will need to be kept classified and/or limited in circulation, that should not mean that no useful transfers would be possible. There already is good dialogue between the government and key elements of the cyber security industry, and this approach is consistent with the draft National Strategy for Trusted Identities in Cyberspace and other governmental efforts.
- Third, the private sector may have certain advantages over the government, particularly at the network level. Networks are run by ISPs and the ISPs in broad terms have the capacity to know a good deal of what is on their networks. ISPs and other security providers likewise have the capability to remove or limit malware or other cyber security vulnerabilities and attack vectors. The ISPs and other security providers must take into account their relationships with their customers, and there are legislative limits on the degree of information-sharing ISPs and other security providers can do which limit the effectiveness of their technical capabilities. Engaging the ISPs and other potential private sector providers will be important to the overall cyber security effort; few non-specialized entities or individuals have the capacity to provide effective security and a widespread professional industry will be invaluable.

Two legislative changes would potentially make security provided by ISPs (or other private entity) significantly more effective.

- The first would be to provide authority to allow for information-sharing and also a mechanism that would allow the sharing without compromising proprietary and/or personal information. A possible approach in this regard would be to create an independent entity which would undertake the information transfer.
- The second legislative change would be to consider a legislative structure that would limit private liability if (and when) there was a security breach when a private entity like an ISP had undertaken to provide cyber security for its customers. The

fundamental issue would be whether such an action would enhance the development of an effective cyber security industry or whether limiting liability would potentially make high standards less likely to be achieved. One important element would be only to provide protection if designated standards had been met (which would require defining standards, currently a quite difficult task). If it were determined that such an approach would be valuable, consideration could be given to a variety of techniques, including government insurance or a cap on liability or some combination of these and perhaps other techniques as well.

Finally, government focus on national security issues, as recommended herein, does not mean government abandonment of other efforts – in particular law enforcement. The FBI and other agencies will continue to have important roles in maintaining cyber security.

The Conclusion

A governmental strategy for cyber security of focusing on critical national security issues, but developing through them valuable benefits for the entire cyber sector will allow the appropriate prioritization and allocation of resources necessary to make progress. The strategy itself will still require programmatic actions, including the development of key building block efforts – including technology, governmental and business processes and governance, and human resources. With appropriate effort, very significant progress can be made – and, with that, cyber's trustworthy use substantially enhanced.

The views expressed do not necessarily represent the views of the Atlantic Council.

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN,
INTERNATIONAL
ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

CHAIRMAN EMERITUS
*Henry E. Catto

VICE CHAIRS
*Richard Edelman
*Brian C. McK. Henderson
*Franklin D. Kramer
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURERS
*Ronald M. Freeman
*John D. Macomber

SECRETARY
*Walter B. Slocombe

DIRECTORS
*Robert J. Abernethy
Timothy D. Adams
Carol C. Adelman
Michael A. Almond
*Michael Ansari
*David D. Aufhauser
Nancy Kassebaum Baker
Donald K. Bandler
Lisa B. Barry
Thomas L. Blair
Susan M. Blaustein
*Julia Chang Bloch
Harold Brown
Dan W. Burns
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
Sarah C. Carey
Michael P.C. Carns
*Daniel W. Christman
Wesley K. Clark
Curtis M. Coward
John Craddock
*Ralph D. Crosby, Jr.
Thomas M. Culligan
W. Bowman Cutter
Brian D. Dailey
Kenneth W. Dam
Robert E. Diamond, Jr.
Paula Dobriansky
Lacey Neuhaus Dorn
Conrado Dornier
Stanley Ebner
Eric S. Edelman
Thomas J. Edelman
Stuart E. Eizenstat
Robert F. Ellsworth
Julie Finley
Lawrence P. Fisher, II
Lucy Reilly Fitch
Barbara Hackman Franklin
*Chas W. Freeman
*John L. Fugh
Carlton W. Fulford
Jacques S. Gansler
*Robert Gelbard
Richard L. Gelfond
*Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
C. Boyden Gray
Marc Grossman
Stephen J. Hadley
Ian Hague
Harry Harding
Rita E. Hauser
Marten H.A. van Heuven
Richard C. Holbrooke
Mary L. Howell
Benjamin Huberman
*Robert E. Hunter
Robert L. Hutchings
Mansoor Ijaz
William Inglee
Wolfgang Ischinger
Robert Jeffrey
*A. Elizabeth Jones
Francis J. Kelly
L. Kevin Kelly
*James V. Kimsey
*Roger Kirk
Henry A. Kissinger
Philip Lader
Anthony Lake
Muslim Lakhani
Robert G. Liberatore
Henrik Liljegren
*Jan M. Lodal
Izzat Majeed
Wendy W. Makins
William E. Mayer
Barry R. McCaffrey
James P. McCarthy
Eric D.K. Melby
Jack N. Merritt
Franklin C. Miller
*Judith A. Miller
Alexander V. Mirtchev
*George E. Moose
William A. Nitze
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ana Palacio
Torkel L. Patterson
William J. Perry
*Thomas R. Pickering
Andrew Prozes
Arnold L. Punaro
Joseph W. Ralston
Norman W. Ray
Teresa M. Ressel
Joseph E. Robert, Jr.
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Marjorie M. Scardino
William O. Schmieder
John P. Schmitz
Jill A. Schuker
Matthew R. Simmons
Kiron K. Skinner
*Helmut Sonnenfeldt
Richard J.A. Steele
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
Peter J. Tanous
Peter Thomas
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Carl E. Vuono
Charles F. Wald
Jay Walker
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Dov S. Zakheim
Anthony C. Zinni

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Frank C. Carlucci, III
Warren Christopher
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS
Lucy Wilson Benson
Daniel J. Callahan, III
Geraldine S. Kunstadter
Steven Muller
Stanley R. Resor
William Y. Smith
Ronald P. Verdicchio
Togo D. West, Jr.

* members of the Executive Committee

Board list current as of April 22, 2010

The Atlantic Council of the United States is a non-partisan organization that promotes constructive U.S. leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

1101 15th Street, NW, Washington, DC 20005 (202) 463-7226

www.acus.org