ATLANTIC COUNCIL

Achieving International Cyber Stability

Franklin D. Kramer

Achieving International Cyber Stability

Franklin D. Kramer

Atlantic Council
1101 15th Street NW, 11th Floor
Washington, DC 20005

ISBN: 978-1-61977-019-5

September 2012

About the Author

The Honorable Franklin Kramer is a national security and international affairs expert and holds multiple appointments, including as a distinguished fellow, and a member of the Atlantic Council Board of Directors, and of its Strategic Advisors Group. Mr. Kramer has been a senior political appointee in two administrations, including as assistant secretary of defense for international security affairs for President Clinton, and previously as principal deputy assistant secretary of defense for international security affairs.

Foreword

Few security issues have become more prominent nor more pressing than the multiple questions surrounding cyberspace and its role in the international security arena. Cyber's well-known vulnerabilities raise fundamental national security questions in a globalized world that is now very much dependent on its Information Age capabilities.

Operational networks such as the electric grid, the military, banking and other financial institutions, and the telecommunication companies themselves are all cyber dependent. From the president down, both public and private leaders have underscored the problem of vulnerability. The media regularly describes significant intrusions in the United States and abroad.

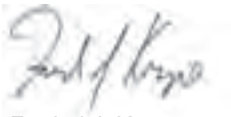
The issues are enormously complex. The cyber world was designed to facilitate reliable, prompt communication; the hardware and software were simply not developed with security in mind. Moreover, the networks and infrastructures which underlie such communications are poorly understood and in many ways interdependent. Internet Service Providers cannot operate without electricity, yet the electric grid is dependent on information from the Internet. Cyber assets are generally owned by the private sector, yet protection against a determined attack may be dependent on government action.

The difficulty is increased because cyber offensive capabilities are being developed by many nations and being sought by terrorist organizations. The consequences of a significant cyber attack against the United States, our allies, and partners have only recently begun to be analyzed. What role cyber will play in warfare or other use of force is far from clear. Whether cyber will be an escalatory factor that could tip confrontation into conflict or escalate a somewhat contained conflict into a broader exchange either geographically or in destructive power is uncertain. Intellectually, we are in a position not unlike that faced 65 years ago as we began to develop our thinking about nuclear weapons.

This report seeks to accelerate that thinking. It analyzes the issues of cyber instability—and more specifically, how to achieve international cyber stability, especially in connection with key operational networks. The report emphasizes the fundamental roles of resiliency, cooperation, and transparency in creating such stability. It proposes specific technological, regulatory, and diplomatic initiatives. It offers a way forward for the United States and like-minded nations to cooperate in the cyber arena. It proposes certain global cyber norms critical to cyber stability. It suggests that even potential nation-state adversaries may find areas of cooperation.

I am grateful to Atlantic Council Distinguished Fellow Franklin D. Kramer whose work underlies this report. The publication is a flagship effort of the Atlantic Council's International Security Program—ably led by Barry Pavel—which will soon be renamed the Brent Scowcroft Center on International Security. The report continues the invaluable work led by Jason Healey, Director of the Council's Cyber Statecraft Initiative.

We hope that this report will make an important contribution to shaping the policy debate surrounding the cyber arena by providing concrete proposals which will ensure that the reliable, trustworthy communications that are at the heart of the Information Age can be assured in the ever-developing globalized world.



Frederick Kempe

Executive Summary

The most disruptive potential cyber security concern is the capacity of information technology to generate or escalate geopolitical conflicts into open or uncontained hostilities through attacks on operational networks. Undermining critical capabilities such as the military or the electric power grid would be highly destabilizing and potentially escalatory, generating a perceived need to move a confrontation toward conflict or to escalate a contained conflict into a broader arena.

International cyber stability can, however, be achieved by generating a three-legged stool of *resilience, cooperation and transparency*. For the United States, achieving these ends will require a three-part strategy of internal action to reduce vulnerabilities focused on key operational networks; collaborative activities with close allies and partners; and transparent interaction for the creation of norms, provision of assistance, and dialogue with others, including potential adversaries, to reduce risk.

The value of cyber stability is three-fold. First, reducing vulnerabilities reduces the risk of adversary attack, since such an attack will be less able to achieve its objectives. Equally, to the extent an attack is nonetheless undertaken, the harm will be reduced. Second, by generating cooperation, it increases the prospect of successful defense. Moreover, it also creates an international geopolitical environment which can shape attitudes and thereby further reduce the likelihood of an attack in the first place. Third, by increasing transparency, it may create international norms of behavior both with respect to possible partners and potential adversaries. For the first group, it offers the prospect of information and assistance. For the potential adversaries it may create shared learning possibly leading to two conclusions: first, that there may be useful areas of collaboration—even though there is not universal agreement; and, second, that there may be good reasons to limit cyber use in order to avoid inadvertent generation of conflict and/or escalation.

In establishing cyber stability, priorities are necessary since a desire to protect everything equally is not practically implementable from either a resource or a political standpoint. Despite the fact that the Department of Homeland Security has identified eighteen critical infrastructures, not all such infrastructures equally underpin United States security or the economy. Most clearly, the military and other national security agencies need to be able to operate in a confrontation. Likewise, no activities in the United States can take place without electric power. Telecommunications and financial systems are similarly crucial. Focusing on these four key infrastructures would allow resources and tailored solutions to be generated and prioritized.

Achieving **resilience** will require a focused approach to cyber security with 1) hardware and software upgrades integrated in 2) an effective architecture combined with 3) duties on the ISPs who will 4) work with government in connection with responding to attacks and 5) be informed by greater understanding of the operations of the system under attack by use of exercises and modeling.

The first step in the establishment of resilience is undertaking a significant developmental effort for the enhancement of hardware and software capabilities. The second step will be developing and integrating the components into an operational architecture. Such an architecture will focus on what the military calls “mission assurance,” that is, the ability to do the task required, and not on maintaining the same high level of performance as would be available if the systems were not under attack.

The third element of resiliency would involve improved system visibility and greater system knowledge using the capabilities of the Internet Service Providers. While ISPs have to be engaged, they should not be asked to deal with inherently governmental functions—protection of the national critical infrastructure—without appropriate government involvement. Accordingly, there should be a combined governmental/ISP arrangement which would require the ISPs to advise the government if there were infections or other existent threats to reliability and then have the government either take or authorize the ISP to take action to help eliminate that threat.

Effective **cooperation** will require a four-part approach of establishing 1) a cooperative small group of like-minded nations including the establishment of a Cyber Stability Board, 2) utilizing agreed standards, 3) working together on operational activities, and 4) including key private sector entities in the effort.

The United States has already begun close interaction with the United Kingdom as it has with several other countries such as Canada and Australia. This cooperation should be somewhat broadened to include other key allies who have significant cyber capabilities. A potential set of additions would be France, Germany, Japan, and the Republic of Korea.

Second, common standards should be established between and among this group of like-minded countries for critical infrastructures. A Cyber Stability Board, along the lines of the financial stability board established by nations for financial issues under the Basel agreements, should be created.

Third, it will be necessary to create a coordinated operational approach. One key element will be to create a network of strategic decisionmakers—including from the private sector—who could be identified in advance to deal with attacks on critical infrastructure.

A viable approach to **transparency** will have three parts: 1) the development and promulgation of norms for those who would work with the like-minded countries; 2) assistance to countries willing to be effective partners to enhance resiliency; and 3) transparent interaction involving dialogue with others, including potential adversaries, to reduce risks.

Three norms emerge for nations associated with the proposed Cyber Stability Board:

1) Governments should generate the establishment of resilient architectures in four key critical infrastructures of military, electric power, telecommunications, and finance.

2) Governments should cooperate on the creation of an international Cyber Stability Board which has standards-setting and operational capacities.

3) Governments should enter into engagements with ISPs and other key critical infrastructure and information technology entities to create resilient international cyber security architectures including in connection with the operation of the proposed Cyber Stability Board.

Expanding cyber security capabilities to other nations who are willing to participate effectively in the creation of cyber stability will also be valuable. The United States in its new defense strategy specifically looks to partnering with and/or mentoring other nation to increase their capabilities including in the global commons such as cyber.

Finally, working with countries of cyber concern such as China and Russia may be possible in particular areas. The first would be reducing the capacity of terrorists and other third parties to launch an attack on any of these countries. The second would be to generate a common understanding of the issues relating to cyber's potential role in conflict generation and conflict escalation.

Achieving International Cyber Security

New inventions often generate new problems. Information technology, the Internet, digital networks, cyberspace—whatever the preferred appellation—is no different. Cyber crime affects consumers and businesses. Cyber espionage, both of business and national security secrets, is prevalent. But potentially the most disruptive cyber concern is the capacity of information technology to generate or escalate geopolitical conflicts into open or uncontained hostilities through attacks on operational networks.

Undermining critical operational capabilities such as the military or the electric power grid dependent on cyber—and in today's Information World, most operational capabilities are cyber dependent—could generate a perceived need to move a confrontation toward conflict or to escalate a contained conflict into a broader arena. Cyber systems now are more-or-less in equilibrium. Despite some problems they are running adequately, but they are a lot like an upside-down broom being balanced with the handle in the open palm of one's hand: a small push will destroy the equilibrium.[1] The geopolitical world is, however, full of pushes—many of which are unanticipated. A more stable platform than the upside-down broom is the three-legged stool which can withstand many pushes without toppling over.

International cyber stability can be achieved by generating a three-legged stool of *resilience, cooperation and transparency*, with resilience being the fundamental component and cooperation and transparency providing supporting legs. For the United States, achieving these ends will require a three-part strategy of internal action to reduce vulnerabilities focused on key operational networks; collaborative activities with close allies and partners; and transparent interaction for the creation of norms, provision of assistance, and dialogue with others, including potential adversaries, to reduce risk.

1. Scoping the Problem

One of the fundamental questions for developing a strategy is to be clear on the problem one is attempting to solve. The strategist Clausewitz made the point this way: "The first, the supreme, the most far-reaching act of judgment that the statesman and the commander have to make is to establish … the kind of war on which they are embarking."[2]

In the context of cyberspace, however, there is a tendency not to focus on the particular problem to be resolved and instead to describe all the problems all at once—in part because the underlying technologies are the same. For example, in the United States' International Strategy for Cyberspace, the challenge posed by the adoption of networked information technology is set forth as follows:

> "These challenges come in a variety of forms. Natural disasters, accidents, or sabotage can disrupt cables, servers, and wireless networks on US soil and beyond. Technical challenges can be equally disruptive, as one country's method for blocking a website can cascade into a much larger, international network disruption. Extortion, fraud, identity theft, and child exploitation can threaten users' confidence in online commerce, social networks and even their personal safety. The theft of intellectual property threatens national competitiveness and the innovation that drives it. These challenges transcend national borders;

[1] See http://www.physicscentral.com/experiment/askaphysicist/physics-answer.cfm?uid=20080501013052

[2] Clausewitz, On War, Book One, Section 27 (Howard and Paret ed.), at p. 100.

> low costs of entry to cyberspace and the ability to establish an anonymous virtual presence can also lead to "safe havens" for criminals, with or without a state's knowledge. Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace."[3]

This listing of issues encompasses pretty much every type of cyber problem. And while that breadth has virtue in helping the nation understand the full spectrum of concerns, the downside is that it is set forth without prioritization. It is true that all stated points are important but it is likewise true that it is very hard to work all issues equally, especially given real-life resource and political constraints.

The US Department of Defense Strategy for Operating In Cyberspace is a more focused document with an emphasis on operations, but it too is quite broad, stating:

> "Potential US adversaries may seek to exploit, disrupt, deny, and degrade the networks and systems that DoD depends on for its operations. DoD is particularly concerned with three areas of potential adversarial activity: theft or exploitation of data; disruption or denial of access or service that affects the availability of networks, information, or network-enabled resources; and destructive action including corruption, manipulation, or direct activity that threatens to destroy or degrade networks or connected systems."[4]

There are very good reasons for this breadth and for including the problem of the espionage threat, but the latter is not the same problem as the attack threat to operations.

Recently, however, President Obama highlighted the criticality of operations point extremely clearly in an op-ed published in the Wall Street Journal:

> "Last month I convened an emergency meeting of my cabinet and top homeland security, intelligence and defense officials. Across the country trains had derailed, including one carrying industrial chemicals that exploded into a toxic cloud. Water treatment plants in several states had shut down, contaminating drinking water and causing Americans to fall ill.
>
> "Our nation, it appeared, was under cyber attack. Unknown hackers, perhaps a world away, had inserted malicious software into the computer networks of private-sector companies that operate most of our transportation, water and other critical infrastructure systems.
>
> "Fortunately, last month's scenario was just a simulation—an exercise to test how well federal, state and local governments and the private sector can work together in a crisis. But it was a sobering reminder that the cyber threat to our nation is one of the most serious economic and national security challenges we face. . . .
>
> "It doesn't take much to imagine the consequences of a successful cyber attack. In a future conflict, an adversary unable to match our military supremacy on the battlefield might seek to exploit our computer vulnerabilities here at home. Taking down vital banking systems could trigger a financial crisis. The lack of clean water or functioning hospitals could spark a public health emergency. And as we've seen in past blackouts, the loss of electricity can bring businesses, cities and entire regions to a standstill.
>
> "This is the future we have to avoid."[5]

It is the criticality of operations point made by the president to which this analysis is directed. Or, to put it another way, can we generate adequate international cyber stability so that a cyber attack on key operational networks will not, in and of itself, tip us into or escalate hostilities.

2. Instability and Escalation

In the real world, cyber probes, penetrations and attacks are ongoing continually. The Department of Defense has stated that its networks are "probed millions of times every day."[6] Critical infrastructure is likewise subject to intrusion. As noted above, the president has stated that "foreign governments, criminal syndicates and lone individuals are probing our financial, energy and public safety systems every day." General Keith Alexander, head of Cyber Command and the National Security Agency, has testified, "Furthermore, we believe it is only a matter of time before

[3] International Strategy for Cyberspace (May 2011) at p. 4.

[4] Department of Defense, Strategy for Operating in Cyberspace (July 2011), at p. 3.

[5] Barack Obama, Taking the Cyberattack Threat Seriously, Wall Street Journal, July 20, 2012, at p. A11

[6] Department of Defense, Strategy for Operating in Cyberspace (July 2011), at p. 3.

.

someone employs capabilities that could cause significant disruption to civilian or government networks and to our critical infrastructure here in the United States."[7] More recently, he noted that the number of probes against critical infrastructure systems has risen from nine in 2009 to 160 in 2011.[8]

Industry itself agrees. Edward Amoroso, who is the Chief Security Officer at AT&T, has stated, "The current risk of catastrophic cyber attack to national infrastructure must be viewed as extremely high, by any realistic measure."[9] Similarly, the North American Electric Reliability Council's High Impact, Low Frequency study issued in June 2010 stated "the bulk power system remains an attractive target for acts of both physical and cyber terrorism," and further concluded:

> "A highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes. . . . . [A] coordinated attack would involve an intelligent adversary with the capability to quickly bring the system outside the protection provided by current planning and operating practices. An outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods."[10]

Such attacks on military and critical infrastructure would be highly destabilizing and potentially escalatory. Joseph Nye of Harvard has noted the multiple factors, analogous to the early days of the nuclear arena, that make the cyber realm less stable, including:

> "the superiority of offense over defense, the potential use of weapons for both tactical and strategic purposes, the possibility of first and second-use scenarios, the possibility of creating automated responses when time is short, the likelihood of unintended consequences and cascading effects when a technology is new and poorly understood, and the belief that new weapons are 'equalizers' that allow smaller actors to compete directly but asymmetrically with a larger state."[11]

Nye further points out that "Even more important than these technical and political similarities is the learning experience as governments and private actors try to understand a transformative technology—and adopt strategies to cope with it."[12]

John Mallery of MIT has similarly considered multiple factors that add to the destabilizing potential of cyber.[13] He points to cyber's strategic reach; offense dominated nature; lack of strategic depth, making preemption potentially more effective; poor warning with short detection times; momentum driven actions in early stages of military conflict; and readily usable techniques and low barriers to entry including the possibility of irresponsible actions by marginal states or non-state actors. Like Nye, Mallery also notes the learning problem and the lack of shared calibrations of hostility levels arising from, among other things, the short history of cyber conflict and the limited guidance available from international law. Mallery emphasizes cross-domain responses in cyber conflict and explains how differing strategic doctrines as well as divergent perceptions and calibrations of hostile action can catalyze broader political and military conflict. Taken together, these factors make conflict generation or escalation in or via the cyber realm a significant risk that major states, like the US, China and Russia have yet to deeply analyze and incorporate into their doctrines.[14] As major actors compete for position across the new cyber terrain, they need to reflect on the consequences for systemic stability created by the collectivity of their individual actions and strategies.[15]

---

[7] Statement of General Keith B. Alexander, Commander United States Cyber Command, Before The Senate Committee On Armed Services 27 March 2012, at p.4.

[8] Cited in Washington Post, July 26, 2012, at p. A3 ("Justice trains prosecutors to counter cyberthreats").

[9] Edward G. Amoroso, Senior Vice President and Chief Security Officer, AT&T, Cyber Attacks (2011), at p. ix.

[10] NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System, at p. 26.

[11] Nye, Nuclear Lessons for Cyber Security, Strategic Studies Quarterly (Winter 2011), at p. 23.

[12] Id.

[13] John C. Mallery, "Models of Escalation and De-escalation in Cyber Conflict, presentation at *The International Information Security Research Consortium Fourth Scientific Conference*, National University of Defense Technology, Changsha, China, October 24-27, 2011.

[14] Based on presentations made by John Mallery at various workshops and discussions with the author.

[15] John C. Mallery, discussion with author, August 8, 2012. Mallery made this point in in the context of a a track 1.5 US-China dialogue organized by CSIS and CICIR in Beijing on June 13, 2012. See also the "Joint Statement from CSIS and CICIR on Sino-US Cyber Security Dialogue," June 2012. http://www.cicir.ac.cn/chinese/newsView.aspx?nid=3878

Moreover, the problem is not limited to nation state confrontation. Terrorist groups are focusing on infrastructure. "We are very vulnerable," John Carlin, the principal deputy in the Department of Justice's national security division, said in an interview. "Terrorists groups are saying publicly what they want to do – knock down the stock exchange and disrupt the electrical grid. We need to be more focused on this threat and we need to be ready."[16] As a recent news article notes, "The prospect was underscored in a chilling al-Qaeda video released recently by the Senate Homeland Security Committee. The video exhorted al-Qaeda followers to engage in 'electronic jihad' and carry out cyber attacks against Western governments and critical infrastructure."[17]

From a United States perspective, reduction of cyber instability and the prospect for escalation would be highly advantageous. The general US approach to conflict is to respond in a time and place of the United States' choosing. Instability and escalatory potential take control from the United States. While there can be no absolute defenses and confrontational situations are always highly dynamic, creating as much advantage as possible is a highly desirable US objective.

3. Cyber stability through principles of resilience, cooperation, and transparency

Security in the geopolitical world has long been sought through the creation of international stability. While obviously not always successful, techniques have included development of technological capabilities; organization of national assets including militaries but also other capacities; establishment of alliances and partnerships; and treaties including with potential adversaries. All those approaches potentially have value in the cyber realm, always with the understanding that the context of cyber, including both its ubiquity as well as its potential for change, must be included in any analysis.

The value of cyber stability through resilience, cooperation, and transparency is three-fold. First, reducing vulnerabilities reduces the risk of adversary attack, since such an attack will be less able to achieve its objectives. Equally, to the extent an attack is nonetheless undertaken, the harm will be reduced. Second, by generating cooperation, it increases the prospect of successful defense. Moreover, it also creates an international geopolitical environment which can shape attitudes and thereby further reduce the likelihood of an attack in the first place. Third, by increasing transparency, it may create international norms of behavior both with respect to possible partners and potential adversaries. For the first group, it offers the prospect of information and assistance. For the potential adversaries it may create shared learning possibly leading to two conclusions: first, that there may be useful areas of collaboration—even though there is not universal agreement; and, second, that there may be good reasons to limit cyber use in order to avoid inadvertent generation of conflict and/or escalation.

With these objectives in mind, the question becomes how actually to achieve resilience, cooperation, and transparency so as to create a greater degree of cyber stability.

A. Resilience

Two fundamental questions in discussing resiliency are why "resilience" as opposed to "protection," and if resilience, then "resiliency of what?"

On the first point, the record is clear: the best cyber security entities from the Department of Defense to Google have all experienced significant intrusions. While Deputy Secretary of Defense, William Lynn stated that the Department of Defense has "not always been successful in stopping intrusions. In fact, over the past several years we have experienced damaging penetrations."[18] Similarly, the Google intrusion by China led Secretary of State Hilary Clinton to go on the record with respect to the problem.[19]

The technical experts agree that, at least for now, offense beats defense and so planning must encompass that concern:

> "The notion that we can achieve 100% protection is not only unrealistic but also results in a false sense of security that puts our missions and businesses at serious risk. Consequently, we must compensate for our inability to achieve full protection by ensuring that we can accomplish our missions despite cyber attacks. The cyber defenses generally available

[16] Cited in Washington Post, July 26, 2012, at p. A3 ("Justice trains prosecutors to counter cyberthreats").

[17] Id.

[18] Remarks at Stratcom Cyber Symposium, as delivered by Deputy Secretary of Defense William J. Lynn, III, Omaha, Nebraska, Wednesday, May 26, 2010

[19] Statement on Google Operations in China, Address by Hillary Rodham Clinton, Secretary of State, Washington, DC, January 12, 2010, http://www.state.gov/secretary/rm/2010/01/135105.htm

> today help address the low-end threats against our less essential systems, but are often ineffective against most forms of cyber attacks targeting our most mission-critical systems. It is at the high end of the continuum that architecture resilience will matter most—to enable continuity of mission critical operations and support rapid reconstitution of existing or minimal essential capabilities or the deployment of alternative means of accomplishing the mission."[20]

This is not to say that there is no value in undertaking protective actions. Quite the contrary is true. As the Australian Department of Defence has stated,

"At least 85% of the targeted cyber intrusions that the Defence Signals Directorate (DSD) responded to in 2010 could have been prevented by following the first four mitigation strategies listed in our Top 35 Mitigation Strategies."[21]

Of course, "could have been prevented" is not the same as "actually were prevented." Most organizations do not have adequate protection and even for those knowledgeable as to what can be done, issues of implementation arise including personnel and other resource availability, organization, scale and cost.[22] As Edward Amoroso of AT&T points out:

"While well-known computer security techniques will certainly be useful for national infrastructure, most practical experience to date suggests that this conventional approach will not be sufficient. A primary reason is the size, scale, and scope inherent in complex national infrastructure. . . . [A]ttempts to apply existing small-scale security processes to large-scale infrastructure attacks will ultimately fail. . . As a result, a brand-new type of national infrastructure protection methodology is required—one that combines the best elements of existing computer and network security techniques with the unique and difficult challenges associated with complex, large-scale national services."[23]

In addition to the problems of scale and complexity, both as noted above and as Scott Charney of Microsoft has set forth, protection is not enough when the

"adversary is persistent (willing to work over time) and determined (firmly resolved to penetrate a particular victim). Importantly, what has become clear is that if an organization is targeted with persistence by a determined adversary, a successful penetration or major disruption is likely."[24]

Particularly with respect to key operational networks, potential adversaries do, in fact, have determination and persistence as well as high end capabilities and therefore a "successful penetration or major disruption" must be planned for.[25] Scale and complexity add to the scope of the problem. Resilience then becomes a critical approach.

On the second point—"resilience of what?" priorities are necessary since a desire to protect everything equally is not practically implementable from either a resource or a political standpoint. Despite the fact that the Department of Homeland Security has identified eighteen critical infrastructures,[26] not all such infrastructures equally underpin United States security or the economy. Most clearly, the military and other national security agencies need to be able to operate in a confrontation. Likewise, no activities in the United States can take place without electric power. Telecommunications and financial systems are similarly crucial. To be sure, others could be added,[27] but focusing on these four key infrastructures would allow resources and tailored solutions to be generated and prioritized. Such

[20] Harriet G. Goldman, "Building Secure, Resilient Architectures for Cyber Mission Assurance" (2010), at p. 1.

[21] Australia Department of Defence, Defence Signals Directorate, Top 35 Mitigation Strategies, http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm. The DSD's top four strategies are: patch applications such as PDF readers, Microsoft Office, Java, Flash Player and web browsers; patch operating system vulnerabilities; minimize the number of users with administrative privileges; and use application whitelisting to help prevent malicious software and other unapproved programs from running.

[22] For example, while according to some, "application whitelisting is . . . the most effective way to significantly reduce the impact of malware in today's environments," the same analysis also states, "Application whitelisting is not perfect. Managing the whitelist can prove difficult in large, open environments." See SANS, Application Whitelisting: Panacea or Propaganda,, http://www.sans.org/reading_room/whitepapers/application/application-whitelisting-panacea-propaganda_33599

[23] Edward G. Amoroso, Senior Vice President and Chief Security Officer, AT&T, Cyber Attacks (2011), at pp. 2-3.

[24] Scott Charney, Trustworthy Computing Next (February 28, 2012), at p. 14, http://blogs.technet.com/b/microsoft_blog/archive/2012/02/28/trustworthy-computing-next-building-trust-in-a-connected-world.aspx

[25] See Hutchins, Cloppert, Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains" ("APT actors continually demonstrate the capability to compromise systems by using advanced tools, customized malware and 'zero-day' exploits that anti-virus and patching cannot detect or mitigate.") presented at Proceedings of the 6th Annual Conference on Information Warfare and Security, March, 2011, copy at http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

[26] http://www.dhs.gov/critical-infrastructure

[27] Transportation and nuclear facilities, for example.

an effort would have three key elements: development of hardware and software for improved capabilities; integration of Internet Service Providers into an architecture utilizing such capabilities; and improved operational techniques focusing on system visibility and system knowledge.

i. Enhancing hardware/software capabilities

The development of resilience through a more effective cyber architecture begins with the enhancement of hardware and software capabilities. The cyber security problem certainly goes beyond technology, but technological improvements underlie the solution as a necessary, though not sufficient, component. Harriet Goldman of MITRE has described such a technological approach which requires using at scale capacities that are now known but not widely deployed. Goldman's analysis underscores that there are no "silver bullets," but that a combination of multiple approaches dependent on technology will be necessary. While the instant analysis is not intended to provide a technical architecture, it is important for policymakers to understand available technologies so as to combine resource, personnel, organizational and operational considerations into a coherent strategy. Goldman's description of eleven capabilities and their benefits is useful in this regard and is set forth in the box on the facing page.

But most important is Goldman's conclusion: "To reverse the asymmetric advantage of the cyber attacker and minimize the impact on our critical mission capabilities, we must be proactive in building secure and resilient systems… While it is not realistic to assume we can stop all cyber attacks or make them totally ineffective, redesigning architectures for resilience will make attacks less likely to succeed, will minimize the consequences when they do succeed, will increase adversary cost and uncertainty, and may act as a deterrent against future attacks. Improving resilience will also increase system reliability."[28]

ii. The need for resilient architectures

Goldman's analysis is not an architecture in and of itself, and the capabilities and techniques noted above will not be effective unless integrated into an architecture that can operate at scale. The first step, however, is undertaking a developmental effort that makes such capabilities available for use with the critical infrastructures described. The second step will be developing and integrating the components into an operational architecture. Such an architecture will focus on what the military calls "mission assurance," that is, the ability to do the task required, and not on maintaining the same high level of performance as would be available if the systems were not under attack. Given the differences between and among the military, electric grid, telecommunications, and financial industry, the high likelihood is that the architectures themselves will differ somewhat. There is a good deal of work being undertaken by the Department of Defense on advanced cyber security and some by the Department of Homeland Security but a very substantial, highly focused R&D program directed toward resiliency and focused on architectures as well as components should be a key element of future national security budgets.[29]

iii. Using operational techniques

Finally, as the third element of resiliency, an architectural approach based on advanced capabilities can itself be significantly improved by successful use of operational techniques—and especially improved system visibility and greater system knowledge.

Very few entities have the capacity for system visibility, but the large internet service providers (ISPs) do have precisely that capability—and it should be utilized. As the ISPs themselves note, they know a great deal with respect to activities on their networks. However, though they do already undertake significant protections for their customers, the multiple vulnerabilities discussed above demonstrate that obviously there have not yet been taken enough actions so that the problem of vulnerability of operational networks has been resolved.[30]

To help achieve a better result will require ISPs to do more. However, precisely "what," "how much," and "under what circumstances" are key questions. Melissa Hathaway of Harvard's Belfer Center and former Acting Senior Director for Cyberspace, National Security Council staff, and Brown

[28] Id. at p. 18. It is also worth noting, as Goldman states, "By promoting resilience against escalating cyber attacks, we can simultaneously achieve resilience against acts of nature, loss of physical network elements, and other threats." Id.

[29] The DOD has, for example, established a "Cyber S&T Priority Steering Council Research Roadmap" http://www.acq.osd.mil/chieftechnologist/publications/docs/2011%2011%2001%20Cyber%20PSC%20Roadmap.pdf. It would be very valuable to upgrade the underlying hardware and software because their vulnerabilities flow downstream to the critical infrastructures. Scott Charney has described Mcrosoft's efforts in this regard. See Scott Charney, Trustworthy Computing Next (February 28, 2012), at p.p. 11-13, http://blogs.technet.com/b/microsoft_blog/archive/2012/02/28/trustworthy-computing-next-building-trust-in-a-connected-world.aspx

[30] The Federal Communications Commission has led efforts with the ISPs to establish and implement three voluntary best practices: 1) Anti-Bot Code of Conduct, 2) Domain Name System Best Practices, and 3) IP Route Hijacking Industry Framework. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-313159A1.pdf

Diversity and Redundancy—to "minimize the impact of technology-specific attacks."

Integrity—to "provide assurance of correctness and integrity of essential software and hardware functions and data wherever possible. . . ."

Isolation/segmentation/containment—to "partition off components of dubious pedigree from those we trust . . . [and to] reduce attacks on critical processing and data by separating them from non-critical data and processing."

Detection/monitoring—"sensors across the environment: at network segment boundaries, gateways, end systems, and servers, as well as for applications and data, not just at the perimeter as is commonly done today."

Least privilege—". . . to decouple capabilities in order to prevent ripple effects that can contaminate large portions of our systems as the result of a single attack or failure."

Non-persistence—"to set the periodicity . . . to prevent the spread or intended impact of an attack, but not so frequently that it makes the system unstable."
Distributedness and moving target defense—"By distributing critical processing and data across different hardware and physical locations, we create multiple points that attackers would have to compromise in order to defeat critical operations. . . . "

Adaptive management and response—"to measure, quantify, and set thresholds that specify acceptable levels of system."

Randomness and unpredictability—" Confusing an attacker or adding the element of surprise may possibly foil an exploit, introduce uncertainty into the results, put the attacker at risk of being detected or exposing tradecraft, or buy us time when systems are under attack."

Deception—"If we can deceive adversaries about the exact components of our system as they attempt to map out our technologies and configurations during the reconnaissance phase, we can increase the probability an exploit will fail against the actual system."[31]

University computer scientist John Savage have proposed eight rules of behavior for ISPs that relate to creating the necessary conditions to accomplish resilience on operational networks. They propose that ISPs have a:

1. Duty to provide a reliable and accessible conduit for traffic and services
2. Duty to provide authentic and authoritative routing information
3. Duty to provide authentic and authoritative naming information
4. Duty to report anonymized security incident statistics to the public
5. Duty to educate customers about threats
6. Duty to inform customers of apparent infections in their infrastructure
7. Duty to warn other ISPs of imminent danger and help in emergencies
8. Duty to avoid aiding and abetting criminal activity[32]

While there are good grounds for each of these rules, resilience would be most enhanced if there were agreement on the need to advise of infection (rules 6 and 7) and the need to provide a reliable conduit (rule 1). But while ISPs have to be engaged, it does not seem entirely sensible to put the entire burden on the ISPs since they cannot necessarily take all of the actions required to eliminate infections and ensure reliability. Neither should the ISPs be asked to deal with inherently governmental functions—protection of the national critical infrastructure—without appropriate government involvement. Accordingly, rather than ISP activity alone, there should be a combined governmental/ISP arrangement which would require the ISPs to advise the government if there were infections or other existent threats to reliability and then have the government either take or authorize the ISP to take action to help eliminate that threat.[33]

The ISP/governmental approach proposed above does not in and of itself require the software and hardware capabilities and redesigned architecture that Harriet Goldman recommends. The latter focuses on requirements

[31] Id. at pp. 9-17.

[32] Hathaway and Savage, Duties for Internet Service Providers (March 2012), at p.1.

[33] If appropriate rules can be established, the ISPs could be authorized to act in designated circumstances without the necessity of checking back with the government.

for user networks. However, the two approaches are entirely complementary—and put together would create a very significant architectural upgrade. What would be created would be an approach based on enhanced user networks complemented by ISP actions to increase reliability and government oversight and activities to improve resilience.

As part of the focus on operational techniques, a further element that would go a long way to establishing a resilient cyber architecture would be to improve knowledge of how the system actually works, particularly when being stressed by attack. There has been a great deal of conversation—and proposed legislation—about enhancing the ability to share information between and among the government and private entities. Several programs have been undertaken with that in mind including the Defense Department's cyber pilot program for defense industrial base firms.[34]

While sharing is a good approach, sharing is not the only key information requirement. Most importantly, there is all too little knowledge as to how to proceed in the event of a significant attack against critical infrastructures. The military has long undertaken modeling and exercises to add to its capacity to respond to kinetic attacks and has begun such efforts in the cyber arena. However, as President Obama's article indicates, there is a long way to go in terms of understanding the operational aspects of the critical infrastructures under attack. Expanded modeling and use of regular exercises (including red teaming to stress the system) will develop a better understanding of vulnerabilities as well as tactics, techniques and procedures needed to combat them including through the development of indications and warning to get ahead of the problem. Such modeling and exercises will include the government but also the owners/operators of the key critical infrastructures as well as the ISPs.[35]

Such efforts are highly important since, to be most effective, the government's authority would need to extend to taking active defense steps to disrupt or disable attackers operating on critical infrastructure and ISP networks. This would need to be done in a way that did not adversely affect the reliability and safety of those networks. But with such a tripartite approach, resilience would be significantly enhanced.

iv. Priorities

While the capabilities and requirements noted above analytically would apply to all cyber activities, a more focused approach would be to start with the four key critical infrastructures of the military, electric grid, telecommunications and financial both because of their importance and because of their ability to build the type of framework as suggested above. The military has the competency and resources to undertake the hardware and software and architectural changes suggested. While the electric grid is composed of some 3200 operators much of the grid is run by a much smaller group who have the capacity to provide system wide efforts. Moreover, the grid is already heavily regulated and the operators have begun to create cyber security standards. The ISPs are the telecommunications companies and the so-called Tier 1 companies (e.g., Verizon, AT&T) are already heavily regulated and have the capacity to operate at scale. Their rate structures, as is also true of the electric power companies, can allow for recovery of costs to enhance cyber security. The financial industry, at least at the large company level and with respect to significant monetary flows (as opposed to retail activities), is heavily engaged in cyber security to protect their business model.

In short, a focused approach to cyber security with 1) hardware and software upgrades integrated in 2) an effective architecture combined with 3) duties on the ISPs who will 4) work with government and the critical infrastructure providers in connection with responding to attacks and 5) informed by greater understanding of the operations of the system under attack by use of exercises and modeling would very significantly upgrade cyber security for critical operational networks.

B. Cooperation

Cyber is inherently international, but multiple elements are subject to national sovereignty. While the electrons move quickly over international networks, the networks themselves including the means of transmission, the routers and servers, the data storage centers and the users' computers all are within some sovereign realm. Those sovereign entities

[34] See News Release, DOD Announces the Expansion of Defense Industrial Base (DIB) Voluntary Cybersecurity Information Sharing Activities (May 11, 2012), http://www.defense.gov/releases/release.aspx?releaseid=15266

[35] There will be a cost component to the private sector participants and this should be covered, perhaps by including the amounts in the DOD or DHS budgets for reimbursements.

can join together to create more effective international cyber stability. Security would be significantly enhanced by a four-part approach of establishing 1) a cooperative small group of like-minded nations, 2) utilizing agreed standards, 3) working together on operational activities, and 4) including key private sector entities in the effort.

Cyber is inherently a complex environment and it becomes more complex the more entities are involved in decisionmaking. For example, the recommendation above to focus on only a few critical infrastructures derives in part from the value of limiting the complexity of the political and bureaucratic environment. That is equally true—perhaps truer—in determining how to go about international cooperation. To accomplish certain of the goals noted above, it will be necessary to start with a small group of like-minded nations.

To put in context the small group of like-minded nations approach recommended here, this is not to suggest that broader multilateral efforts be ignored. Rather, it is important to recognize that there are already a multitude of cooperative efforts begun in the cyber arena that operate at a broad multi-participant level. The US International Strategy for Cyberspace notes:

> "An increasing number of international organizations are taking up cybersecurity and other cyberspace issues, and the United States continues to promote this important work, building cyberspace into their range of work to meet the needs of their varied memberships. We have worked to include relevant cyberspace issues on the agenda at the Organization of American States (OAS), the Association of Southeast Asian Nations (ASEAN) Regional Forum (ARF), the Asia-Pacific Economic Cooperation Organization (APEC), the Organization for Cooperation and Security in Europe (OSCE), the African Union (AU), the Organization for Economic Cooperation and Development (OECD), the Group of Eight (G-8), the European Union (EU), the United Nations (U.N.), and the Council of Europe, and to ensure that work is supported by an effective institutional framework. The United States will continue, in these and other fora, to consolidate regional and international consensus on key cyberspace activities, including norms."[36]

All these activities are potentially worthwhile, but to make significant progress, focusing on a small group of like-minded entities will reduce the complexity and potential for political disagreement while allowing constructive dialogue on difficult questions of resilience and regulation. It is much more likely that, for example, the United States and the United Kingdom which have years of cooperative effort will be able to agree on actions in cyber than will be true between the United States and China—especially inasmuch as China has been identified by the United States as a source of significant cyber instability through its espionage and other cyber activities.[37]

In point of fact, the United States has already begun close cooperation with the United Kingdom as it has with several other countries such as Canada and Australia. This cooperation could be enhanced in four ways. First, it could be somewhat broadened to include other key allies who have significant cyber capabilities. A potential set of additions would be France, Germany, Japan, and the Republic of Korea.

Second, common standards should be established between and among this group of like-minded countries for critical infrastructures. A Cyber Stability Board, along the lines of the financial stability board established by nations for financial issues under the Basel agreements, could be created. It should be recognized that effective cooperation along these lines will require changes in domestic legislation and regulation. As has previously been written:

> "However, to go beyond current efforts and achieve adequate resilience will require coordinated regulation by … countries far beyond current approaches. It should be clearly recognized that the required legislative and regulatory authorities do not exist for the most part. And, beyond the authorities themselves, no concept of operations has been developed that meets both security needs and private sector requirements. All of this means that a new approach to cyber security will be necessary, one that is much more inclusive and require a combination of military, civilian governmental and private industry actions… Establishing the framework for such a coordinated cyber approach is a critical step . . . and effective implementation will require continued high level attention. This will not be an easy task, but there are instances—for example the Basel accords in the financial arena—

[36] International Strategy for Cyberspace (May 2011) at p.18.

[37] Office of the National Counterintelligence Executive, "Foreign Spies Stealing US Secrets in Cyberspace," Report to Congress (2011).

> where such agreements have been created that affect both governmental and private operations. Such a step—call it the creation of an international Cyber Security Board—needs to be undertaken in the cyber arena also."[38]

Third, it will not be enough simply to create standards under a Cyber Stability Board. In addition, it will be necessary to create a coordinated operational approach. For example, one of the fundamental areas of cooperation that efforts by like-minded nations could significantly improve is the enhanced operationalization of self-defense efforts. These would include sharing data, analysis and tools concerning threats and remediations as well as undertaking combined operations. By way of example, a number of well-publicized cooperative efforts have been undertaken to reduce the threat from botnets. For example, Microsoft has worked with United States authorities and others to take down the Rustock botnet,[39] and the FireEye firm worked with multiple entities to take down the Grum botnet.[40] Botnets, however, are hardly the only threat to critical infrastructures. Cooperative action by like-minded nations will significantly enhance resilience efforts.

The fourth points can be drawn from these examples above. The involvement of private entities is at a minimum very valuable and often indispensable. Such involvement, however, is not something that can be done with existing institutions working as they have done until now. For example, the North Atlantic Treaty Organization is a very fine institution but it does not deal with electric power or telecommunications. The European Union does not include the United States and it has only limited authority over cyber activities and even less over the military. Neither organization is able to organize in any major way private entities to meet operational cyber challenges. An operational entity that combines all these capabilities will be necessary to meet challenges that cut across existing bureaucratic lines. That entity will have to include in its operational approach key private sector entities. One key element will be to create a network of strategic decisionmakers—including from the private sector—who could be identified in advance to deal with attacks on critical infrastructure. There is no virtue in having an ad hoc approach to such a significant problem, and organized procedures would be of great value.

The key here is a much increased set of actions in terms of scope. While nations have long focused on classic kinetic efforts in terms of national security, there is no such analogue in terms of cyber security. Partly, this is because significant cyber threats are only relatively recently phenomena. Partly, this is because cyber crosses over from classic military to what are generally considered civilian activities. And, partly, this is because civilian entities such as Microsoft and FireEye as well as the operators of critical infrastructures need to be involved in the efforts as opposed to governmental entities. All this requires a different approach to international security than has heretofore been the case. Stovepiping military from civilian and public from private is a certain way to ensure failure. Building new institutions to enhance cooperation will be required.

C. Transparency

The third element of an international strategy for cyber stability will be to enhance resilience and cooperation through transparency. That effort will itself have three parts: 1) the development and promulgation of norms for those who would work with the like-minded countries; 2) assistance to countries willing to be effective partners to enhance resiliency; and 3) dialogue with others, including potential adversaries, to reduce risks.

The development of global norms for cyber security is an ongoing effort, given impetus by the 2011 London and following conferences. For the most part, the effort has as yet resulted in very general propositions to be put forth as norms. However, the recommendations set forth above allow for a more specific set of norms that can be adopted as guides for countries seeking to improve cyber security. In particular, if the discussion herein is followed, three norms emerge for at least the group of like-minded nations associated with the proposed Cyber Stability Board:

1) Governments should generate the establishment of resilient architectures in four key critical infrastructures of military, electric power, telecommunications, and finance through

—development of hardware and software

—use of private sector capacity for visibility

[38] Kramer, Transatlantic Nations and Global Security: Pivoting and Partnerships (March 2012), at p.11.

[39] http://www.pcmag.com/article2/0,2817,2382203,00.asp

[40] http://www.fireeye.com/news-events/press-releases/read/fireeye-takes-down-grum-botnet

—increased knowledge regarding escalation potential via modeling and exercises

2) Governments should cooperate on the creation of an international Cyber Stability Board which has standards setting and operational capacities

3) Governments should enter into engagements with ISPs and other key critical infrastructure and information technology entities to create resilient international cyber security architectures including in connection with the operation of the proposed Cyber Stability Board.

These norms focus on the stability for critical infrastructures and there are, to be sure, other issues such as espionage and crime. However, the norms suggested are very important because of the benefit their implementation can provide to critical infrastructures. They provide a basis for actually working together, as opposed to simply having conversations, and they also suggest the second important element of transparency.

While, as the discussion in this paper emphasizes, it is important to start with—and to have at the core of the cyber stability effort—a small group of like-minded nations, it is also important to recognize that stability will be enhanced as more entities are engaged. This is simply an example of the well-known networking effect, often discussed in the cyber arena under the particulars of Metcalfe's Law.[41] It therefore will be valuable for the like-minded nations to expand their cyber security capabilities to other nations who are willing to participate effectively in the creation of cyber stability. While some have called for a "duty to assist," it is not necessary to go that far to recognize the self-interest factor which nations have long recognized in the national security arena. The United States, for example, in its new defense strategy specifically looks to partnering with and/or mentoring other nations to increase their capabilities including in the global commons such as cyber:

"Building partnership capacity elsewhere in the world also remains important for sharing the costs and responsibilities of global leadership. . . . America, working in conjunction with allies and partners around the world, will seek to protect freedom of access throughout the global commons . . . . Both state and non-state actors possess the capability and intent to conduct cyber espionage and, potentially, cyber attacks on the United States, with possible severe effects on both our military operations and our homeland. . . . The United States will continue to lead global efforts with capable allies and partners to assure access to and use of the global commons."[42]

But a key element of expanding cooperation will be the necessary transparency so that other entities feel that their interests are appropriately taken account of in undertaking cooperation. This will involve the development of trust both with respect to creation of standards and agreement on operational approaches. The proposed founding nations for the Cyber Stability Board—United States, United Kingdom, Australia, Canada, France, Germany, Japan, and the Republic of Korea—have developed real relations of trust through alliances and activities over many years. Others will need time to come to the same conclusions.

Transparency will also be important to bring standards and operational approaches to relevant multilateral organizations including, for example, NATO and the European Union. The politics and limitations of each of those organizations argue against their being a place to develop the standards and operational approaches recommended for the Cyber Stability Board itself. However, successful actions by the Cyber Stability Board can be of high relevance to the members of NATO and the EU.

Finally, transparency can be of importance to nations that present challenges which will make cooperation more difficult. As noted above, China and Russia have been identified by the United States as very significant centers of cyber espionage.[43] Further, China and the United States have very complicated relations over Taiwan and increasingly over the South China Sea. Russia continues to list NATO as its top security concern and cites the NATO missile defense plan as a significant area of contention. In these circumstances, with each of China and Russia having an element of military competition with the United States, the question is whether there could nonetheless be any constructive arrangements concerning cyber dependent critical infrastructures.

Despite these real differences, there are two areas of engagement that would be of value. The first would be reducing the capacity of terrorists and other third parties to launch an attack on any of these countries. The second

[41] Metcalfe's law states that the value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). See http://en.wikipedia.org/wiki/Metcalfe's_law

[42] Sustaining US Global Leadership: Priorities for the 21st Century, at p. 11.

[43] Office of the National Counterintelligence Executive,"Foreign Spies Stealing US Secrets in Cyberspace," Report to Congress (2011).

would be to generate a common understanding of the issues relating to cyber's potential role in conflict generation and conflict escalation.

As an opening point, it is worth noting that there is certainly no inevitability of military confrontation or conflict between the United States and either China or Russia. As has been noted by many, each of those countries has multiple positive involvements with the United States especially in the arenas of international trade and economics and even in some areas on the military side—China in the counter-piracy efforts off the coast of Africa, Russia in supporting logistics for Afghanistan through its territory. To be sure, there are also differences—both as noted above and also especially in the governing systems and the degree of democracy and individual rights. However, a common arena has been dealing with the problem of terrorists. Since September 11, both China and Russia have provided certain types of useful assistance to the United States and cooperation in particular areas continues.[44]

Keeping terrorists from having significant cyber capabilities is a common interest of each of the United States and China and Russia. Any such capabilities could be used against any of the three countries, all of whom have consequential terrorist concerns. As noted above, terrorists are seeking cyber capabilities. A good approach to transparency would be to work toward and/or expand intelligence sharing on the issue. Likely, this would best be done on a calibrated bilateral basis. The focus might be on cyber criminal networks which have significant cyber capabilities and which potentially could provide those capabilities to terrorists. It is entirely possible that there will be differences in the success of this approach as between China and Russia, but it is a general direction which might be utilized. Over time such transparency might even allow for combined actions, though that probably will take some significant time.

A second level of transparency with potential adversaries would be to increase dialogue and mechanisms to support dialogue on the issues of cyber attacks. The United States has made some good strides in this regard thought there is still far to go. Among other efforts, there are effective non-official dialogues,[45] and the US and Russia have instituted a cyber hot line. Dialogue takes time to be effective, but it is a valuable way to understand others, and should be continued. Some of the key issues include matters of the relevance of the laws of armed conflict (LOAC); what rules, if any, apply if that LOAC threshold level has not been reached; what are the factors leading to escalation either before or during conflict; and what would be the elements of an effective risk reduction approach. To put these questions on the table is not to suggest that they are easily resolved nor that they will necessarily affect other problems such as espionage. But they could be the basis of a continued dialogue with benefits for international cyber security.

4. Conclusion

International cyber stability can be achieved by generating a three-legged stool: of *resilience, cooperation and transparency*—resilience being the fundamental component with cooperation and transparency providing supporting legs for the stool.

Achieving **resilience** will require a focused approach to cyber security with 1) hardware and software upgrades integrated in 2) an effective architecture combined with 3) duties on the ISPs who will 4) work with government in connection with responding to attacks and 5) informed by greater understanding of the operations of the system under attack by use of exercises and modeling would very significantly upgrade cyber security for critical operational networks.

Effective **cooperation** will require a four-part approach of establishing 1) a cooperative small group of like-minded nations including the establishment of a Cyber Stability Board, 2) utilizing agreed standards, 3) working together on operational activities, and 4) including key private sector entities in the effort.

A viable approach to **transparency** will have three parts: 1) the development and promulgation of norms for those who would work with the like-minded countries; 2) assistance to countries willing to be effective partners to enhance resiliency; and 3) transparent interaction for the creation of norms, provision of assistance, and dialogue with others, including potential adversaries, to reduce risks.

Taken together, these actions would significantly enhance international cyber stability and thereby fundamentally improve international security.

[44] See, for example, the State Department's "Country Reports on Terrorism" for 2011 and 2010.

[45] See the "Joint Statement from CSIS and CICIR on Sino-US Cyber Security Dialogue," June 2012. http://www.cicir.ac.cn/chinese/newsView.aspx?nid=3878

The Atlantic Council's Board of Directors

CHAIRMAN
*Chuck Hagel

CHAIRMAN, INTERNATIONAL ADVISORY BOARD
Brent Scowcroft

PRESIDENT AND CEO
*Frederick Kempe

VICE CHAIRS
*Robert J. Abernethy
*Richard Edelman
*C. Boyden Gray
*Richard L. Lawson
*Virginia A. Mulberger
*W. DeVier Pierson

TREASURER
*Brian C. McK. Henderson

SECRETARY
*Walter B. Slocombe

DIRECTORS
Odeh Aburdene
Timothy D. Adams
*Michael Ansari
Richard L. Armitage
Adrienne Arsht
*David D. Aufhauser
*Ziad Baba
Elizabeth F. Bagley
Ralph Bahna
Sheila Bair
Lisa B. Barry
*Thomas L. Blair
Julia Chang Bloch
Francis Bouchard
R. Nicholas Burns
*Richard R. Burt
Michael Calvey
James E. Cartwright
Daniel W. Christman
Wesley K. Clark
John Craddock
David W. Craig
Tom Craren
*Ralph D. Crosby, Jr.
Thomas M. Culligan
Gregory R. Dahlberg
Brian D. Dailey
*Paula Dobriansky
Markus Dohle
Lacey Neuhaus Dorn
Conrado Dornier
Patrick J. Durkin
Thomas J. Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Dan-Åke Enstedt
Julie Finley
Lawrence P. Fisher, II
Michele Flournoy
*Ronald M. Freeman
*Robert Gelbard
Richard L. Gelfond
Edmund P. Giambastiani, Jr.
*Sherri W. Goodman
John A. Gordon
*Stephen J. Hadley
Mikael Hagström
Ian Hague
Frank Haun
Rita E. Hauser
Michael V. Hayden
Annette Heuser
Marten H.A. van Heuven
*Mary L. Howell
Robert E. Hunter
Robert L. Hutchings
Wolfgang Ischinger
Deborah James
Robert Jeffrey
*James L. Jones, Jr.
George A. Joulwan
Stephen R. Kappes
Francis J. Kelly
Zalmay Khalilzad
Robert M. Kimmitt
Roger Kirk
Henry A. Kissinger
Franklin D. Kramer
Philip Lader
David Levy
Henrik Liljegren
*Jan M. Lodal
*George Lund
*John D. Macomber
Izzat Majeed
Wendy W. Makins
Mian Mansha
William E. Mayer
Eric D.K. Melby
Franklin C. Miller
*Judith A. Miller
*Alexander V. Mirtchev
Obie Moore
*George E. Moose
Georgette Mosbacher
Bruce Mosler
Sean O'Keefe
Hilda Ochoa-Brillembourg
Philip A. Odeen
Ahmet Oren
Ana Palacio
Torkel L. Patterson
*Thomas R. Pickering
*Andrew Prozes
Arnold L. Punaro
Kirk A. Radke
Joseph W. Ralston
Teresa M. Ressel
Jeffrey A. Rosen
Charles O. Rossotti
Stanley Roth
Michael L. Ryan
Harry Sachinis
William O. Schmieder
John P. Schmitz
Kiron K. Skinner
Anne-Marie Slaughter
Alan Spence
John M. Spratt, Jr.
Richard J.A. Steele
James B. Steinberg
Philip Stephenson
*Paula Stern
John Studzinski
William H. Taft, IV
John S. Tanner
Peter J. Tanous
*Ellen O. Tauscher
Paul Twomey
Henry G. Ulrich, III
Enzo Viscusi
Charles F. Wald
Jay Walker
Michael Walsh
Mark R. Warner
J. Robinson West
John C. Whitehead
David A. Wilson
Maciej Witucki
R. James Woolsey
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
David C. Acheson
Madeleine K. Albright
James A. Baker, III
Harold Brown
Frank C. Carlucci, III
Robert M. Gates
Michael G. Mullen
William J. Perry
Colin L. Powell
Condoleezza Rice
Edward L. Rowny
James R. Schlesinger
George P. Shultz
John Warner
William H. Webster

LIFETIME DIRECTORS
Carol Adelman
Lucy Wilson Benson
Daniel J. Callahan, III
Kenneth W. Dam
Stanley Ebner
Barbara H. Franklin
Chaz Freeman
Carlton W. Fulford, Jr.
Geraldine S. Kunstadter
James P. McCarthy
Jack N. Merritt
Steven Muller
William Y. Smith
Helmut Sonnenfeldt
Ronald P. Verdicchio
Carl E. Vuono
Togo D. West, Jr.

**Executive Committee*
List as of September 14, 2012

Atlantic Council
1101 15th Street NW, 11th Floor
Washington, DC 20005

Address Services Requested

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting the global challenges of the 21st century.

1101 15th St. NW • 11th Floor • Washington, DC 20005 • 202-463-7226 • acus.org