All Done Except the Coding:

Implementing the International Strategy for Cyberspace

By Matthew G. Devost, Jeff Moss, Neal A. Pollard, and Robert J. Stratton III

On 16 May 2011, President Barack Obama released his International Strategy for Cyberspace,[1] which, in conjunction with cyber security legislation sent to Congress on 12 May 2011,[2] comprises this Administration's unique vision and policy for cyberspace. Implementation will be the devil in the details; the strategy is necessary, but not sufficient. This paper highlights some key decisions, balances, and actions that remain as U.S. departments and agencies craft or modify their own strategies over the next several months to align with the President's policy objectives. This paper also considers how other stakeholders—especially the private sector and other nations—regard their roles and mutual expectations.

Context

The release of the International Strategy marks two years since the Obama White House conducted its cyberspace policy review. In that time, new issues have come up, and there has been increasing need for an overarching cyberspace strategy to articulate threats and challenges, to prioritize national objectives, to provide guidance for departments and agencies developing their own strategies, and to establish expectations for all stakeholders.

The International Strategy has been introduced at a time when cyberspace issues have taken on increasing prominence. Within the United States, the President appointed Howard Schmidt as the Coordinator for White House Cybersecurity in 2009, who is responsible for reporting directly to the President. Meanwhile the Department of Defense (DoD) established U.S. Cyber Command (USCYBERCOM)—an operational command headed by the Director of the National Security Agency—as part of an articulated policy that views cyberspace as a domain of conflict, similar to land, air, sea, and space. The DoD publicly articulated its view of operations in cyberspace on 14 July 2011, when it released an unclassified version of its "Department of Defense Strategy for Operating in Cyberspace."[3] Congress has also been involved in cyber issues, producing multiple versions of comprehensive bills to address national cybersecurity, none of which have been submitted to the President for his signature.

---

[1] The White House, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (accessed 16 May 2011).
[2] The White House, http://www.whitehouse.gov/sites/default/files/fact_sheet-administration_cybersecurity_legislative_proposal.pdf (accessed 16 May 2011).
[3] Defense Department, http://www.defense.gov/news/d20110714cyber.pdf (accessed 21 August 2011).

In the private sector, leading firms in information, defense, finance, and chemical industries have increasingly suffered network attacks. Similarly, countries such as China have targeted Internet service firms, including Google, as they have delved into the international policy domain. Some attacks have been highly sophisticated, such as the targeted malware attack that was supposedly aimed at Iran's uranium enrichment processes. Wikileaks has demonstrated the other side of unsophisticated threats that arise from tactical, rather than technical, failures that can have national and international effects well beyond the military domain. Lastly, a combination of social and technical networks continues to drive change across the Middle East. All of these examples indicate how countries such as the United States, China, and Egypt will have different perspectives on what constitutes a national security threat in cyberspace.

From Policy to Implementation

The International Strategy aims to merge U.S. security, as well as economic, social, and technological values into an overarching vision that enhances prosperity, security, and openness in cyberspace. The International Strategy addresses both threats and value-laden challenges in cyberspace that range from cyber crime, intellectual property theft, and conflict, to censorship, unreasonable surveillance, repression, and disruption of networks that further political objectives. The International strategy is clear regarding the potential of conflict in cyberspace:

> The United States will respond to hostile acts in cyberspace as we would to any other threat to our country. All states possess an inherent right to self-defense, and we recognize that certain hostile acts conducted through cyberspace could compel actions under the commitments we have with our military treaty partners.[4]

Confronting these threats and challenges requires consensus and the promulgation of norms among international and private-sector partners. To this end, the International Strategy explicitly invokes the "three Ds" of implementing national security policy: diplomacy, defense, and development.[5] The emphasis that the International Strategy places on norms—even technical norms grounded in the language of standards and governance—will rely heavily on diplomacy, and particularly on State Department resources. As many observers have noted, there is a drastic imbalance in resources among agencies, as defense is significantly better resourced than diplomacy or development; this, in turn, forces the DoD to engage in non-military tasks abroad and to support civilian missions domestically.

In order to implement the International Strategy, this imbalance must be mitigated. Similarly, the United .States. must also reconcile that the State Department

---

[4] The White House, "International Strategy for Cyberspace" (May 2011), p. 14.

[5] For a general description and assessment of this policy framework, see Lawrence J. Korb, "Development, Defense, and Diplomacy as a Policy Framework," Center for American Progress, http://www.americanprogress.org/issues/2009/03/korb_africom.html (accessed 19 May 2011.)

recognizes differences between domestic and foreign domains, while cyberspace does not. This is more than a question of resources: it is a question of balanced action within the U.S. government. Departments and agencies must receive clarification, directives, and prioritization as they pursue the goals and norms laid out by the President over the next several months. Furthermore, pursuing the norms of the International Strategy requires engaging all stakeholders. The U.S. government must establish more specific expectations and actionable direction for state, local, tribal, nongovernmental, and private-sector entities, as well as communities and individuals, if all of these stakeholders are to play a meaningful part in pursuing norms.[6] Finally, the White House must make hard policy trade-offs for responsibilities, resources, and investments in pursuing the International Strategy.

This final element is a fundamental question of policy and strategy. What are the trade-offs among objectives or norms that generate tension when put into practice? What are the assumptions that underlie objectives and trade-offs, and where should we strike balances to mitigate tension? What are the consequent resource implications of these balances and trade-offs? The normative nature of the International Strategy and the debate that it is sure to generate among international and private-sector partners create an opportunity to provide the guidance that departments ordinarily expect from the President on how the U.S. government will operate in cyberspace, and how it will partner with the private sector and international partners. These directives also include how department and agency priorities, resources, and actions should flow accordingly.

From Threats to Risks

Some challenges and threats outlined in the International Strategy are unique to cyberspace; others are not. For example, crime, terrorism, exploitation, and military conflict exist both in virtual networks and on real estate, but cyberspace can "boost the productivity" of legitimate and illegitimate actors alike. Framing risk in cyberspace should have a heavy economic emphasis, in terms of the deleterious economic effects of threats, as well as the negative economic effects of unwise solutions to threats, and the potential spillover of risks and costs in interdependent issue-areas. Ultimately, solutions should not be more costly or damaging than the problem. The effective implementation of the International Strategy will frame the problem and provide this risk management perspective to guide those with the responsibility to manage these risks.

Managing risk in cyberspace also means agreeing on some fundamental cyberspace assumptions and realities. If the United States suffers a societal infrastructure

---

[6] The DHS Quadrennial Homeland Security Review defines the "homeland security enterprise" as "*the Federal, State, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities who share a common national interest in the safety and security of America and the American population.*" Given the pervasive nature of modern IT networks, and the ability of individuals to rapidly form and dissolve communities of interest, this seems to the authors a reasonable list of stakeholders and levels at which policy should operate.

disruption, such as a massive power grid collapse, after some use of forensics we will likely be able to verify that we have been attacked (as opposed to an accident). For most threats, however, we should not assume that it will be apparent an attack has taken place. This is particularly true in the case of embedded malware used for stealing or corrupting information, since it can also be used for later disruption (as can most tools of espionage, cyber or otherwise). Thus, event detection can be more important than event response. Consensus around assumptions of event detection will inform where departments and agencies set priorities for actions and investments. These same assumptions will guide the government's conversation with international and private-sector partners, in building consensus for norms. Thus, the ultimate success of the International Strategy depends to some degree on articulating these assumptions, and making sure they are thoroughly considered.

Moreover, implementing and building consensus around the International Strategy should emphasize the embedded non-technical nature of the threat, ranging from insiders who are malicious, careless, or ignorant and naïve, to compromised, counterfeit, or suspicious products entering our cyber-supply chain. Similarly, responses to technical threats require a strategic, integrated, and non-technical approach. The problem of assuring reliability, integrity, and trust (in insiders, suppliers, manufacturing processes, etc.) is probably the least understood risk in cyberspace. Restoring trust and reliability is generally more expensive, time consuming, and difficult than restoring service, and involves more than mere technical patches. Mitigating threats will call for significant non-technical standards, actions, and partnerships that go beyond the traditional set of stakeholders in cybersecurity.

From Strategy to Stakeholders

The release of the International Strategy presents an opportunity to update concepts and means for identifying stakeholders in cyberspace and drawing zones of responsibility around them. In fact, it is crucial for the success of the strategy: implementing this strategy and building support for its norms will require setting, and communicating expectations among non-traditional strategic stakeholders who will drive its success. The International Strategy rightfully commented on the need for innovative incentives for the private sector to fulfill national security goals. The challenge, of course, is how to achieve this. In order to create effective incentives, the U.S. government must precisely express the roles, responsibilities, and expectations that should be placed upon the private sector, and identify how they differ from what the private sector sees for itself.

Here, subsequent activity and guidance from the White House can serve two purposes. First, it can clearly articulate the U.S. government's perspective of where cyberspace issues become "governmental,", and where they should be the responsibility of the private sector. Second, it can be an instrument and a process in building trust, confidence, and cooperation between the government and private sector, as a beginning of a dialogue to draw lines of responsibilities and communicate mutual expectations. The U.S. government should use the

International Strategy as a single transparent expression of the government's intent, expectations, and priorities. Transparency is necessary, but not sufficient: the strategy process must draw lines of where government responsibility ends and private sector responsibility begins. The private sector must be actively engaged in this process. If the White House brings the private sector into the nuts and bolts of its strategy process, it will give both sides the chance to see, and test the feasibility of, each other's expectations. At the least, it will result in a process more preemptive and deliberative, and less ad hoc and reactive only to near-term failures. In the past three years, private corporations and even individuals have provided the most effective and responsive models on dealing with single threats or vulnerabilities: for example, the Conficker/Downadup Working Group, and Dan Kaminsky's effort to address critical DNS vulnerabilities. Yet the Y2K effort showed that the government can also take the initiative in models that leverage the best of both worlds: the creativity and responsiveness of the private sector, with the deliberation, resources, reach, and convening power of the U.S. government.

The strategy process is the ideal forum in which to identify critical partners as stakeholders. It is an old truism that the private sector owns between 80 and 90 percent of critical infrastructures. Reaching out to the largest publicly traded companies in any given infrastructure sector is also necessary, but not sufficient, to reach the spectrum of stakeholders who play security roles in cyberspace. The issue is complex because influential (or vulnerable) stakeholders and businesses appear rapidly, and may disappear just as quickly. Moreover, their roles in economic or national security might not be as familiar or intuitive as those of an energy or telecommunications provider. Facebook presents a good example of the challenge of defining who is a stakeholder. There is disagreement over whether Facebook and other social networks are part of the "critical infrastructure," even though Facebook has over 500 million active users and influences social issues, economic trends, and privacy in ways that are difficult to measure. Indeed, social networks have played a significant part in transforming the Middle East in 2011.

In terms of both capability and sheer ubiquitous presence, social networking media platforms like Facebook are stakeholders in cybersecurity; to consider them otherwise denies the United States both a potential source of capability and an insight into vulnerability. On the other hand, such companies highlight, in single entities, the tensions among the norms and goals of the International Strategy: prosperity, openness, stability, and privacy. Implementation of the Strategy must balance the prioritization and pursuit of norms while incorporating all stakeholders, in order to mitigate the tensions that those very stakeholders might create by virtue of their existence. Certainly, this issue will come up as U.S. diplomats engage their interlocutors in less open countries.

Prosperity, Security, and Openness: Pick Two

The International Strategy's goals of prosperity, security, and openness are interdependent. Put into practice, they may generate tension, if not mutual antagonism. This is especially true when international partners have fundamentally

different perspectives about what constitutes a national security threat in cyberspace. There remain hard decisions at the national level, about what the U.S. wants to achieve against the International Strategy's goals and norms, and at what cost to other goals. These decisions go to the heart of the priorities and trade-offs that the U.S. must set to achieve realistic and balanced security – including economic security – in cyberspace. This illustrates the complexity of a "whole of government" approach in cyberspace: there must be decisions about which instruments of national power are best positioned to achieve certain goals, and what the costs and trade-offs of those instruments will be. If all goals are equally important, none is a priority.

Cyberspace will always be an imperfect world. Attacks will happen, and despite pursuit of international norms, the United States must learn to function effectively in a cyberspace full of compromised networks, flawed systems, and vulnerable users, where risk will never reduce to zero and humans will continue to pose a primary vulnerability. Of course, we want to reduce both threats and recovery time. But resources are zero-sum and must be driven by priorities, which are based in part on assumptions, and generate expectations. In this regard there remains a gap between the International Strategy and U.S. government departments and agencies, that leaves unanswered questions of prioritization. At the departmental level, do we invest more in threat reduction and attack prevention, or in recovery and resilience? Do we seek to extend the time between failures, or to reduce the time to recovery? What kind of failures should we be prepared to accept, especially if lowering the risk is more expensive than the failure itself? How do these answers change across departments, missions, or threats?

The White House must support a directive process that provides policy guidance to departments and agencies on prioritizing between threat reduction and prevention on one hand, and recovery and resilience on the other: what these priorities mean, and how expectations and resources should flow from them, both in the government and the private sector. This latter point will form the foundation for a new set of norms for the private sector in managing and hedging between risk and resilience, and establishing assumptions about what, and when, government resources will be available. From this guidance, departments and agencies can better build strategies, plans, and investments.

Privacy is another trade-off, since it is sometimes at odds with the goal of openness in cyberspace. The White House should take the lead in a national dialogue on privacy issues, to update public policy on private. For example, privacy invasion and risks of abuse are no longer the exclusive province of national governments. Privacy policy should also protect individuals who freely, but unknowingly, mortgage control over their personal information to a myriad of commercial third parties who have few incentives and fewer requirements to hold such information responsibly. Privacy law and policy are woefully outdated, as are many citizens' assumptions about their personal information. In this environment, lack of clear statements on privacy and data retention guidelines or expectations have caused platforms like

Facebook endless problems, and have even spawned competitors who promise better privacy.

The President should begin a dialogue that helps stakeholders to understand and begin to control the expectations and trade-offs among convenience, efficiency, privacy, and information responsibility. This will also be of immense help to diplomats and homeland security officials, as they continue to engage their foreign interlocutors in Europe as well as Asia on an issue where the U.S. stands virtually alone. However, the President alone cannot remedy privacy problems. Concurrently, Congress must modernize public policy principles in an era of e-commerce, social networking media, data mining and retention, and high premiums on information sharing.

Organization and Guidance

U.S. departments and agencies will be the primary consumers of the International Strategy, and will build on its vision in order to provide better services to the public. Consequently, many departments and agencies will develop their own strategies, plans, and capabilities for operating in cyberspace, to implement the International Strategy and pursue its goals. With this truly "whole of government" approach to cyberspace, there remain key issues that require resolution at the national level, concerning roles and responsibilities, particularly with respect to DoD and DHS, both of which have significant leading roles in securing cyberspace. Here, two substantive issues call out for White House guidance that the International Strategy does not address. The first issue is securing the global supply chain. Both DoD and DHS have roles in protecting government supply chains and logistics systems from cyber attacks. This includes awareness of risks to the cyber-supply chain: malware and counterfeit products inserted into the supply chain from malicious actors upstream, which cause unintentional failures to – or even sabotage – systems that rely on software, firmware, and hardware. It is not feasible to inspect every line of code or every processor that goes into even the most sensitive government systems. However, risk management strategies and capabilities can mitigate the risk. DHS and DoD should work in tandem, but under an overarching top-down strategy that provides guidance on common risk management approaches against this challenge.

The second issue is the question of DoD support in response to a truly national cyber-crisis. Despite the wild rhetoric surrounding "cyberwar," the material question is, what cyber events would definitively require a DoD response with its unique capabilities, what are those capabilities, when is the DoD the "lead" federal agency in response, and how does it provide its unique capabilities in support to civilian authorities, or even the private sector? Currently, the DoD has a qualitatively different level of capabilities to operate in cyberspace—offensively and defensively—than any civilian department or agency, yet there is a finite number of rather extreme scenarios in which a crisis would demand a DoD response beyond the capacity of any civilian agency. Unless a nation state is behind the attack or the attack focuses solely on defense targets, the DoD would operate in a supportive role similar to its support of civilian authorities in the event of a natural disaster. This is

one of the primary reasons behind the close integration and coordination of USCYBERCOM personnel with DHS personnel. Supporting civilian authorities in cyberspace will not be like supporting civilian authorities in real-world disasters. The government will not be able to draw a border around the disaster area, and thus will have a more difficult time gauging the extent of the damage and the unintended consequences of response measures outside the immediately affected "zone." These unintended consequences might affect privacy, movement, or economic issues of private and international actors seemingly "outside" the disaster zone. Indeed, it is not clear who has the primary legal authority below the Presidential level, to declare a "disaster" analogous to a governor in a natural disaster, and what the role of corporate leadership should be. Yet there is little policy guidance, let alone an enabling legislative framework like the Stafford Act, that provides for defense support to civilian authorities and the private sector in cyberspace. A national strategy should articulate how to expand the capabilities USCYBERCOM into a truly national resource.

This White House coordinator should work with DoD, DHS, and other key stakeholders to articulate situations in which a military response would be necessary, when it would be in support of civilian authorities (perhaps even specifically which agencies), and what operational command and accountability lines different agencies should follow. Additionally, the White House should update its legislative package sent to Congress to call out where the legislative framework and consequent authorities are insufficient to enable DoD to come to the aid of civilian agencies. Given such a response would likely cross international borders quickly, the International Strategy can be a useful device to extend U.S. defense in cyberspace beyond our borders, in the spirit of support to both civilian authorities, the private sector, and international partners, when their own vulnerabilities pose a hazard to the United States.

Interagency Effectiveness and Coordination

No one likes having homework graded. Yet, measuring departmental and agency progress against national objectives is necessary to track improvements and to ensure that the "whole of government" effort is well tuned and making the nation safe and prosperous. To implement the International Strategy, the White House should produce a roadmap and general benchmarks against which departments, agencies, and other stakeholders can measure whether activities, resources, and investments are progressing and consistent with priority activities established in the Strategy. Strategic-level benchmarks will address strategic effectiveness at an enterprise level, beyond simple technology acquisition and will reduce dependencies on technical remediation or meaningless compliance thresholds (e.g., agencies being graded on how many firewall or anti-virus licenses they buy). Moreover, any strategy will be a snapshot in time; as strategy iterations mature, national leadership will be able to identify what works and which national activities are moving the private sector or international community toward consensus around norms.

Perhaps the greatest utility for the International Strategy is its use as a tool for the White House Coordinator. This is most apparent at the nexus of national security, economic development, and trade policy. Coordination is critical among the Cybersecurity Coordinator, the National Security Staff, the National Economic Council, and the U.S. Trade Representative. Presidential direction from the International Strategy can enhance coordination by providing the Coordinator with a tool to assist the departments and agencies, by presenting them with values, goals, and top-level guidance. Indeed, as the Coordinator can articulate the cyber aspects of what the U.S. government is prepared to do to defend U.S. businesses on the world trade stage, he can serve a primary role as proponent of America's competitiveness in cyberspace.

This is where practical tensions arise and require White House coordination, not only among prosperity, security, and openness, but among policies for cyberspace, economic development, national security, and trade. For example, does the World Trade Organization framework offer adequate protection against obvious intellectual property theft and unfair competition today, and how can U.S. trade policy compensate? What are the economic and national security considerations and trade-offs? What can the national security community offer the trade community in protecting IP while pursuing commerce in the globalized marketplace? Are we finally at the point where our intelligence community has something to offer, such as defensive advice or due diligence, to American corporations?

These questions present difficult choices, and future policies will require careful and transparent deliberation, balance, and coordination among stakeholders and regulatory regimes. Unintended policy interactions and consequences can weaken America's overall cybersecurity posture as well as economic strength. For example, tight encryption export controls can adversely affected the ability of business and financial sectors to protect their information. Economic policies intended for intellectual property protection can impact security research, as has been the case with the Digital Millennium Copyright Act and anti-circumvention/reverse engineering prohibitions. Cost-of-entry of software patents has driven some innovators out of Silicon Valley and into overseas innovation hubs. To the extent that we add risk or cost to private sector cybersecurity research and development, we are likely to drive capabilities and markets overseas.

The White House Coordinator for Cybersecurity will not solve these problems, but can provide the process and discipline to translate the International Strategy into actionable guidance and priorities across cyberspace norms as well as U.S. security, economic development, and trade goals. Furthermore, the Coordinator can ensure that the aggregate efforts of the United States reflect the best possible trade-offs while building international consensus around norms, while ensuring government actions are coordinated, integrated, and prioritized to maximize the nation's economic and national security.

Congress

Congress must act to update public policy and legislation on both substantive (privacy) and administrative (authorities) issues. This is beyond the authority of the President, and it highlights another element of the complexity of this issue. There is a myriad of committees and subcommittees with jurisdiction over DHS, DoD, and the Intelligence Community, in addition to economic activities, diplomacy, development, law enforcement, science and technology, commerce, etc. In the President's own legislative package presented to Congress on 12 May 2011, Obama noted that the last Congressional session introduced approximately fifty cyber-related bills, including some comprehensive ones. As broadly as the President's vision covers cyberspace, it is the vast number of Congressional committees that might claim jurisdiction over the matter.

Congress should be as bold as the White House and streamline how it exerts oversight on different aspects of cyberspace. Congress should reform its oversight, both structurally and substantively, to better address the spectrum of challenges in cyberspace. While there will be no single Committee in either House with plenary and sole jurisdiction over cyberspace, a good start would be to reform oversight and organization over those departments and issues that have significant responsibilities or implications in cyberspace, especially in homeland security, intelligence, and foreign relations and trade.

This will come to a head if there is a significant incident. In responding to every modern crisis thus far, the United States has acted consistently in one respect: it forms a commission. This will likely be the case in response to a catastrophic cyber event. In that case, such a commission would likely be needed just to manage effectively the number of queries from the lawmakers on committees with jurisdiction. Here, the authors see this type of commission as sharing the unfortunate lament of the Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism: "One consequence of Congress's failure to adapt to the evolving nature of national security threats is the outsourcing of national security oversight to external commissions like this one."[7]

Conclusion

The International Strategy for Cyberspace gives the United States a solid vision for norms of behavior to make cyberspace prosperous, secure, and open. Now the government needs a plan for implementation. Despite the clarity of the President's vision, different agencies will have differing interpretations of strategies, authorities, and priorities. Interagency coordination—a primary challenge in cybersecurity—fails without implementation and accountability. Departments and agencies will be responsible for engaging international partners and can use different sets of incentives to build consensus with their counterparts. The private sector is also a critical partner, but cannot be expected to respond to the same

[7] Senator Bob Graham et al, *World At Risk: The Report of the Commission on the Prevention of WMD Proliferation and Terrorism* (2008), p. 90.

incentives as government agencies or international partners. Implementation is key to reconciling these potential points of divergence and tension. Furthermore, this Strategy should be considered a snapshot of a point in time: it should be updated regularly, given the enormous, dynamic, and uncertain rate of change in technologies, threats, opportunities, and progress toward the Strategy's vision.

President Obama announced in his 2011 State of the Union Address that he intends to meet this generation's "Sputnik" moment with a policy of massive investment in research, development, and innovation that "we haven't seen since the height of the Space Race," referring to the Soviet Union's surprise launch of their Sputnik satellite. As in the Space Race, the U.S. President has tied economic progress, technological innovation, and national security to an implied set of national priorities, in response to an external economic and political threat. Now we are in a race for innovation in cyberspace. As President Obama said, "after investing in better research and education, we didn't just surpass the Soviets; we unleashed a wave of innovation that created new industries and millions of new jobs."

Unlike in the Sputnik era, however, the costs and barriers of stealing our innovations are significantly lower than the costs of that innovation. Genius flows from networks, but our ability to network has always outpaced our ability to protect the network. The priority of the President's policy should be to create security around our genius, to ensure that we realize the full extent of return on investment, and to position the country against whichever competitors provoke a Sputnik moment, by whatever means they choose to compete with us.

Matthew G. Devost is President & CEO of FusionX, LLC, a cybersecurity consultancy. Additionally, Mr. Devost has been an Adjunct Professor at Georgetown University since 2002, where he teaches a graduate course on Information Warfare and security, and is a Founding Director of the Cyberconflict Studies Association. Mr. Devost co-founded the Terrorism Research Center, Inc. (TRC) in 1996, where he served as President and CEO until November 2008.

Jeff Moss has been a hacker for over 20 years. He is currently Vice President and Chief Security Officer of the Internet Corporation on Assigned Names and Numbers (ICANN). He is also the Founder and Director of Black Hat and DEF-CON Computer Hacker Conferences. He currently serves as a member of the U.S. Department of Homeland Security Advisory Council, and is a member of the Council on Foreign Relations.

Neal A. Pollard is a Director at PricewaterhouseCoopers. He is also Adjunct Senior Fellow for Cyber Policy at the Federation of American Scientists, and Adjunct Professor at Georgetown University. Previously, he was a senior officer in the Office of the Director of National Intelligence, International Affairs Fellow of the Council on Foreign Relations, and General Counsel and Board Director of the Terrorism Research Center, a corporation he co-founded in 1996.

Robert J. Stratton III is an independent consultant specializing in multinational network security. Previously, he was Director of Government Research at Symantec Research Labs, co-founder and Chief Technology Officer at StackSafe, the first Director of Technology Assessment at In-Q-Tel, co-founder and Chief Technologist at Security Design International, and founder of the security organization at UUNET, one of the first tier 1 Internet service providers.