THE 9/11 CONFERENCE

Security Solutions for the Next Ten Years

GORTON CENTER
SLADE GORTON INTERNATIONAL POLICY CENTER

The National Bureau of Asian Research is a nonprofit, nonpartisan research institution dedicated to informing and strengthening policy. NBR conducts advanced independent research on strategic, political, economic, globalization, health, and energy issues affecting U.S. relations with Asia. Drawing upon an extensive network of the world's leading specialists and leveraging the latest technology, NBR bridges the academic, business, and policy arenas. The institution disseminates its research through briefings, publications, conferences, Congressional testimony, and email forums, and by collaborating with leading institutions worldwide. NBR also provides exceptional internship opportunities to graduate and undergraduate students for the purpose of attracting and training the next generation of Asia specialists. NBR was started in 1989 with a major grant from the Henry M. Jackson Foundation.

Funding for NBR's research and publications comes from foundations, corporations, individuals, the U.S. government, and from NBR itself. NBR does not conduct proprietary or classified research. The organization undertakes contract work for government and private-sector organizations only when NBR can maintain the right to publish findings from such work.

Report authored by Michael Wussow.

Printed in the United States of America.

For further information about NBR, contact:

The National Bureau of Asian Research
1414 NE 42nd Street, Suite 300
Seattle, Washington 98105

206-632-7370 Phone
206-632-7487 Fax
nbr@nbr.org E-mail
http://www.nbr.org

THE 9/11 CONFERENCE

Security Solutions for the Next Ten Years

SEPTEMBER 9, 2011
SEATTLE, WA

The Slade Gorton International Policy Center at The National Bureau of Asian Research convened its inaugural conference focusing on September 11 and its aftermath, nearly ten years to the day of the tragic event. The "9/11 Conference: Security Solutions for the Next 10 Years" was designed to be both reflective and forward-looking in its approach. It proved to be both.

Over the course of eight hours and six sessions, former and current U.S. government officials, private sector experts, and two former members of the 9/11 Commission discussed the circumstances leading to September 11, the country's lack of preparedness on that day, and how the nation—and its systems for fighting terrorism—responded. Solutions for what needs to happen next also were discussed.

For the 125 conference attendees who gathered on Friday, September 9, 2011, at the University of Washington School of Law in Seattle, the 9/11 Conference offered perspective on how the United States responded to what **Creigh H. Agnew**, President of the Slade Gorton International Policy Center, described in her opening remarks as "a defining moment for our country."

PICTURED ABOVE: FORMER 9/11 COMMISSIONERS AND U.S. SENATORS BOB KERREY AND SLADE GORTON.

The panelists' words, at times somber but at other times lighthearted, were consistently candid. Among other insights, the conference discussed the 9/11 Commission's recommendations, the challenges the FBI has faced in adapting to its new intelligence-focused role, and the efforts of technology companies to become more aware of, and responsive to, cybersecurity threats.

After the last question was answered late in the day, the Gorton Center's namesake, former U.S. Senator **Slade Gorton**, thanked the audience and panelists. "Not only did we have every single panel on a fascinating subject," he said, "but we had every single panel with fascinating speakers from beginning to end."

> This conference focuses on perhaps the greatest failure in the post–Cold War era. It remains one of the most important and sobering issues facing our nation.
>
> —Richard Ellings,
> The National Bureau of Asian Research

BOB KERREY, SLADE GORTON, AND MIKE MCKAY.

PART I: INTELLIGENCE AND SECURITY

REFORM SUCCESSES AND FAILURES

"Early in 1998 Osama bin Laden formally declared war on the United States. For all practical purposes, we paid no attention," said former U.S. Senator Slade Gorton, addressing participants at the first session. "In the immediate aftermath of 9/11, however, President Bush decided that we were at war with al Qaeda."

Gorton said that President Bush's decision that "we were at war with al Qaeda" had important consequences and was much different from the way the United States reacted to the World Trade Center bombing in the early 1990s. The military response following September 11, he said, "contrasted with our response to the first World Trade Center bombing, which was treated purely as a law enforcement challenge, complete with Miranda warnings, lawyers, and jury trials—all successfully concluded, but with no impact on the ultimate success of the 9/11 plotters."

> Choosing war allowed a military response, covert operations, and drone searches.
>
> —Slade Gorton, former U.S. Senator and 9/11 Commissioner from Washington State

"Choosing war [after September 11]," Gorton explained, "allowed a military response, covert operations, and drone searches. The result has been the decimation of al Qaeda's leadership, including Osama himself, and the blunting of its ability to plan elaborate operations like 9/11."

Another former U.S. Senator and member of the 9/11 Commision, **Bob Kerrey**, a Democrat who represented Nebraska in the U.S. Senate, joined Gorton on the panel "Reform Successes and Failures." "I think the most important policy change is not a declaration of war," Kerrey said, explaining that on this matter he and Gorton might have "slightly different" views.

"Bush said, 'There is no sanctuary.' [President] Obama continued that policy. And as long as that's the policy of the land, I frankly don't think you need a declaration of war," said Kerrey, a former U.S. Navy SEAL.

You just call up the [Pakistanis] and say, "I've got some bad news and some good news: we penetrated your airspace last night, I know that's going to create some political problems. The good news is bin Laden is dead…He's living in your country." There is no safe place anymore for individuals like that.

—Bob Kerrey, former U.S. Senator and 9/11 Commissioner from Nebraska

Despite that difference of opinion, Kerrey said what he considers to be the United States' most important post–September 11 policy change: when the 9/11 Report was released on July 22, 2004, the 9/11 Commission had come to agree with President Bush's approach and wrote, "Calling this struggle a war accurately describes the use of American and allied armed forces to find and destroy terrorist groups and their allies in the field."

Gorton told conference participants that Kerrey, "as outspoken a person in politics as I have ever met" and who was appointed halfway through the Commission's existence, was the "key to [the Commission's] unanimity."

Successes Earned—Not Ordained

With a history of cooperation between former colleagues Gorton and Kerrey, it is not surprising that the 9/11 Conference's first panel was characterized much more by agreement than differences. The concurrence with which they spoke reflected the spirit that was ultimately—though not painlessly, according to both senators—found in the 9/11 Commission itself, a ten-member committee made up of five Republicans and five Democrats. The moderator of the panel on "Reform Successes and Failures," Founding Partner of McKay Chadwell PLLC and former U.S. Attorney **Mike McKay**, said having each party represented equally is "normally a recipe for failure," but that the 9/11 Commission was "a huge success."

Both Gorton and Kerrey were quick to point out the challenges found during the formation of the 9/11 Commission, including that neither President Bush nor Congress wanted a commission created. They explained that although the victims' families were at first suspicious of a commission stacked with political partisans, in the end they became its biggest supporters. Gorton said that the groups representing the victims' families "deserve the credit for what Congress did far more than we do."

Investments and Information-Sharing

Gorton and Kerrey concurred that as a result of the 9/11 Commission's recommendations, the intelligence community is now much more effective than it was prior to September 11. The intelligence services have, they told conference participants, developed, although certainly not perfected, a process for sharing information both within and across agencies. Gorton said that, at $80 billion a year, the United States is investing in intelligence "twice the amount we spent ten years ago."

With the development of the National Counter-terrorism Center (NCTC), a mechanism has been created for closing the chasm separating the CIA and the FBI—thus connecting foreign and domestic intelligence-sharing. Bureaucratic silos that hampered intelligence-sharing were a significant problem before September 11. At one point during 9/11 Commission discussions, it looked doubtful that the FBI would maintain any intelligence function at all.

Additionally, Gorton and Kerrey explained, the 9/11 Commission called for the creation of a Director of National Intelligence (DNI)—a position that was created, but today is considerably weaker than originally hoped. Contributing to that weakness is the fact that the DNI does not hold budget authority over all the intelligence agencies. Gorton said, "We are doing well, but we could do better. The result is a safer America and a less effective set of terrorist organizations overseas."

Safer but More to Do

As a result of President Bush's decision that "we were at war with al Qaeda," as Gorton explained, and Congress's implementing some—but 9/11 commissioners would argue not enough—of the recommendations of the Commission, Gorton and Kerrey agreed that the United States and its citizens are safer as a result of decisions made after September 11. "Inside the United States," Gorton said, "at great cost in both dollars and personal disruption, we are clearly safer."

That does not mean, however, that the United States has gotten everything right. The one area where Americans are perhaps most reminded of September 11 and the ongoing threat of terrorism—air travel—still has a long way to go, Gorton acknowledged, calling the current process of boarding commercial aircraft "elaborate and humiliating." Although the United States has thwarted recent attacks, including those of the so-called shoe bomber and underwear bomber, "each increased elaboration in the way we go through security is a qualified but very real success for the other side." Yet he added, "Now we finally have a TSA [Transportation Security Administration] director who is at least thinking, 'Can't we do somewhat better?' I think every one of us here feels we can do a lot better."

In response to an audience question about American citizens' safety and how to interpret the government's threat warnings—specifically a warning issued on the eve of the ten-year anniversary of September 11, Kerrey said, "Wear your seatbelt, don't smoke, get a reasonable amount of sleep, do everything in moderation, and you're likely to live a long and happy life."

> Do we really deserve to be served by people like this? Are we behaving so as to deserve to be served by men and women of this quality?
>
> —Bob Kerrey, former U.S. Senator and 9/11 Commissioner from Nebraska

Rather than giving a flippant response to a serious concern, Kerrey was making the point that "America has gone back to work," and that the country has made many of the right decisions. "I think we violated civil liberties more than we should have in the early days, particularly [those of] people who are Muslim.…[But] I think we've rebalanced this thing. We're still a very open country. We're still a very free country. We still travel around about as much as we want. We ought to get up every day and feel pretty damn grateful to live in this country. Are we going to get attacked from time to time? Yes. Do we have good people protecting us right now? The answer is yes."

Recruit, Train, and Retain: Paying for the Right People

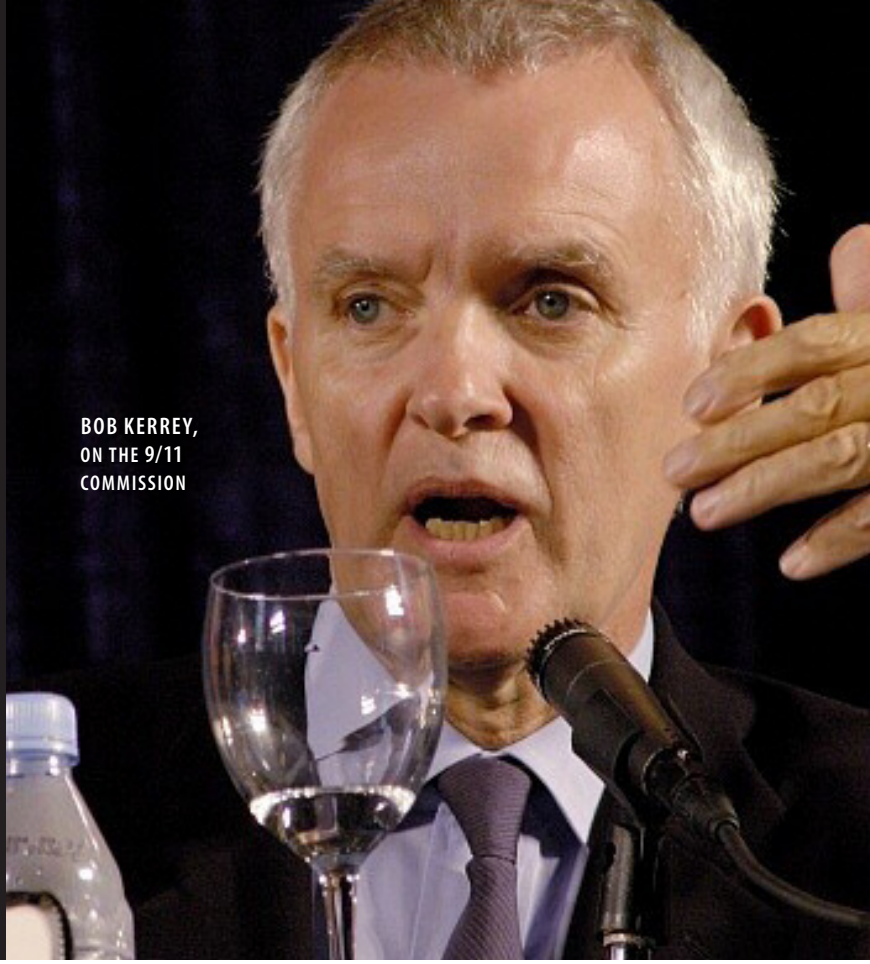
"There are three things that you have to have to get security," Kerrey said. "You have to recruit people, you have to train people, and you have to retain them—up and down the food chain, whether it's local police officers, local fire people, first responders, FBI personnel, or military personnel….[What] gives me the most confidence that we are vastly more safe and secure today is the quality of people who have come in to do that work."

Kerrey explained to conference participants that the United States has a good chance of continued success if it can keep recruiting and retaining what he called "the right people"—in the intelligence services, the military, and other government sectors. He noted, however, that the government—not the private sector—needs to be able to fund this initiative, calling it "a big government effort," and one that may become increasingly challenging since "we're converting our federal government into an ATM."

"Today, every single penny of tax dollars that goes into Washington, D.C., goes to Medicare, Medicaid, Social Security, and interest on the national debt," said Kerrey. "It doesn't go to hire anyone to protect us. It doesn't go to anybody to keep us secure….That's the biggest threat to our capacity to continue to be able to recruit, train, and retain the men and women that we're going to need to carry out all of these policies to keep us as safe as possible."

I am unwilling to pay the price to get the risk to zero.…It costs too much in freedom, it costs too much in dollars, it costs too much in lives. None of us is going to get out of this deal alive. If we want a free and open society, if we want a vibrant economy, we have to accept some kind of risk. You get that risk to zero, and we're all in straitjackets. We're going to feel safe as heck, but we can't do anything.

—Bob Kerrey, former U.S. Senator and 9/11 Commissioner from Nebraska



BOB KERREY, ON THE 9/11 COMMISSION

Risks of Complacency and Weak Oversight

Kerrey and Gorton said that under the circumstances, many of the steps taken to fight the war on terrorism and to secure Americans have been successful so far, even if they have not all been implemented as completely as they should have been.

In addition to the impact of the country's budget woes on its ability to fight terrorism in the future, among Kerrey's biggest concerns is the fact that the intelligence oversight committees in Congress are still very weak. He stated that the 9/11 Commission had to be created because Congress was unable to conduct a credible investigation of the September 11 attacks, and that "the families [of the victims] did not trust the analysis done by the intelligence committees."

"The oversight is exceptionally weak," Kerrey said. "It doesn't permit you to get to a point where you have confidence that we're spending the right amount of money on the right things….I think we're going to continue to be vulnerable to not being able to answer the question 'Are we doing enough of the right things?' until those committees are strengthened."

Gorton said that as more and more time passes without a terrorist attack on U.S. soil or against Americans directly, the country and its leaders risk becoming complacent and forgetting about the threat.

"While in many respects, the response of the United States has been effective and measured," Gorton said, "we are in a struggle, a struggle with another civilization that is not going to be over soon. In my view, perhaps our greatest enemy is complacency. The longer our administrations are successful in preventing terrorist attacks here in the United States, the more restless we will be with what goes on in every airport whenever we decide to take a plane. The more resistance there will be, and the more temptation there will be for presidents to concentrate on other matters. So the paradox is, the more successful we are, the more difficult it will be to continue that success."

REFORMS IN THE FBI

One of the questions thoroughly examined by 9/11 Commission members was what role the FBI should have in the intelligence community. A decision was made to better develop the FBI's intelligence capabilities, requiring dramatic changes at the Bureau. In the view of **Tracy Reinhold**, Assistant Director of the FBI's Directorate of Intelligence, there could not have been a wiser course—and it is one that his organization has embraced wholeheartedly.

"I will tell you that this is not the FBI that I joined 21 years ago," Reinhold said. "I would venture to say that it is a better organization than it was, and that is reflective in the tenure of our employees. Over 40% of our employees have come on board since September 11… I will stack our intelligence apparatus against any intelligence apparatus in the U.S. government."

From Case-centric to Intelligence-led

Reinhold, who started his FBI career working in violent crime—"where you needed to make your bones"—spoke candidly of his own transition from working as a violent crimes supervisor in Las Vegas before the September 11 attacks, to his rapid transition leading the Bureau's Directorate of Intelligence, the largest division at FBI headquarters. "I arrived… knowing very little about the utilization of intelligence in law enforcement," he said. "But from that period forward, we learned what we needed to do."

Reinhold explained to conference participants that in the immediate aftermath of September 11, the FBI "kind of messed up…in that we abdicated the responsibility to develop an intelligence program." The FBI had brought in analysts from other parts of the intelligence community to establish an intelligence program within the Bureau. In retrospect, Reinhold said that move was a mistake because even though the intelligence professionals were "wickedly smart," they didn't understand the FBI's mission and how an intelligence-gathering function could best support it.

The FBI has since changed from an organization that before September 11 had only about 80 intelligence analysts to one that today has more than three thousand, said Reinhold. For an organization that for its first 90 years of existence was "case-centric," transitioning to an "intelligence-led, threat-focused" entity required changing both minds and culture.

"One of the biggest challenges in the FBI in transforming the organization was speaking in terms that resonated with the intended audience," Reinhold remarked. "So, if I am a violent crime agent in a field office, and somebody comes up to me in 2006 and says, 'I need to know about your collection posture,' I guarantee he's going to stand up straight. He has no idea what that means. What we're talking about here is, if I want to know what your capability to collect against a certain threat is, that is your collection posture."

Reinhold said that at first, the FBI did not acknowledge the "fundamental cultural shift" that it had undergone, which "sort of denigrated" the role of special agents. He said that it was imperative—and remains so—to make sure agents understand their vital role in the intelligence function. "The intelligence cycle begins with collection, and it ends with action," he explained, and the special agent does both. "The success of the FBI's intelligence program is based on one thing, and one thing only, and that is the integration of intelligence and operations."

Reinhold explained that of all the intelligence programs in the United States government post–September 11, "the FBI has probably changed the most, and probably the fastest." He noted that the *Harvard Business Review* wrote about the FBI's transformation and referred to the bureau's changes as "the most significant transformation in the shortest period of time in the history of government."

> I can tell you right now that no organization in the U.S. government has changed more since September 11 than the FBI.
>
> —Tracy Reinhold, FBI

Intelligence is all about relationships—it's about demystifying the process and providing a valuable service to an entity. And I can tell you that in the last several years in particular, we have made monumental strides in that respect.

—Tracy Reinhold, FBI

TRACY REINHOLD

Communicating Intelligence

Reinhold said that there are five operational divisions or investigative disciplines in the FBI: counterterrorism, counterintelligence, cyber, weapons of mass destruction, and criminal. His job is to ensure "that all [the divisions] talk to each other and that they're all hunting the most significant threat."

In the post–September 11 world, ensuring intelligence-sharing has not only become imperative, but also a part of the FBI's culture. "The intelligence program from the FBI's perspective drives all five investigative disciplines. We have just as much responsibility to utilize intelligence in addressing our criminal threats as we do with our terrorism threats," Reinhold emphasized.

The FBI has 56 field offices and 71 overseas legal attaché offices, all of which work together, both to collect information and to mitigate risks. Sharing information across the Bureau and with other partners at the local, state, federal, and sometimes international levels is "crucially important because of the pace of the threat," Reinhold said. He explained that someone can be in Abbottabad, Pakistan, and just 24 hours later "actuate a threat in New York."

Reinhold explained that the FBI has placed intelligence analysts in field offices whose responsibility is to assess threats "cross-programmatically" instead of "stove-piping the issue." That cross-programmatic assessment, along with the FBI's cooperation and intelligence-sharing with other federal agencies is key to collecting intelligence and mitigating threats, he emphasized.

The FBI's mission is to protect the American people. Everything else is how we do it. It's that simple.

—Tracy Reinhold, FBI

"Our focus is on the domestic United States," Reinhold reminded the audience. "Our threats don't always emanate from inside the United States. So if we're not seamlessly connected with the organizations in the U.S. government that are primarily focused on [threats] … outside the continental United States, then we're going to miss that threat environment."

Reinhold closed by reiterating how far the FBI has come in adding to its own capabilities and contributing to the intelligence capabilities of the U.S. government as a whole. "Our job is to mitigate threat," he said. "Our analysis is used so that we have a better understanding of that threat.…Intelligence is all about relationships—it's about demystifying the process and providing a valuable service to an entity. I can tell you in that the last several years in particular, we have made monumental strides in that respect."

PAUL NICHOLAS, CHERI MCGUIRE, AND GORDON MATLOCK.

PART II: THREATS OF TODAY

CYBERSECURITY

The war on terrorism often brings to mind al Qaeda, Osama bin Laden, and other nefarious groups and characters. But for many technology professionals, such as those from Symantec, Microsoft, and the University of Washington, other threats come to mind as well. For individuals like Cheri McGuire, Paul Nicholas, and Mark Haselkorn, cybersecurity is a high stakes game, with consequences for their enterprises, their customers, and their country. This is the lens through which they view the threat of terrorism.

Changing Threats

The threat landscape has changed dramatically in the ten years since September 11, stated **Cheri McGuire**, Vice President of Global Government Affairs and Cybersecurity Policy at Symantec Corporation. "Ten years ago, we talked about script kiddies predominantly," she said, "teenagers in their basement, hacking away. Today we talk about nation-states, organized hacker criminal syndicates, and hactivists—groups like Anonymous and WikiLeaks. These are all new types of threats on the horizon, and I don't think we yet have a good handle on how to address all of them. We're also looking at targeted attacks now—much more targeted attacks…against consumers and enterprises."

Paul Nicholas, Director of Global Security, Strategy, and Diplomacy at Microsoft, said that the United States will change dramatically the way it thinks about the concept of "cyber" in the coming years. "There are four fundamental things that are going to change cybersecurity as we know it, and greatly alter the risk profiles that we started building the day the twin towers fell. And those four elements are people, devices, data, and the cloud."

Both McGuire and Nicholas said that the increase in the number of people online and the interconnectedness of networks and devices present opportunities for businesses but also challenges for cybersecurity. "In 2001, when 9/11 happened, there were about 250–300 million people on the Internet, and we had about 500 million cell phones in the world," Nicholas said. "Today, we have two billion people on the Internet, and we have about five billion cell phones."

In the panel moderated by **Gordon Matlock**, Senior Policy Advisor at the Pacific Northwest National

Oftentimes countries that have emergent economies have high piracy rates and poor security rates. So they tend to become platforms where people can attack the computer through things called botnets, where software gets maliciously installed in a very surreptitious manner. The user doesn't even know they're infected. But they become a platform that can be used to attack other things.

—Paul Nicholas, Microsoft

Laboratory (PNNL), the panelists shared that the world of cybersecurity has changed dramatically in the last decade in terms of threats and the need to counter them. As new platforms and technologies are developed and put into use, cybersecurity will become even more challenging.

Nicholas observed: "It took us about ten years to get to two billion people," he said. "Now we're going to add another billion in four years." Those new users will be predominantly from countries with emerging economies, such as Brazil, Russia, India, China, and Indonesia, where users on average are in their early twenties. By contrast, the average age of users in the United States is 37. "That's good for business. That's good for communication. That has tremendous benefits economically," Nicholas explained. "But it also creates new risks."

Symantec's "2011 Norton Cybercrime Report," released in September 2011, estimates that cybercrime costs consumers billions of dollars per year. Its annual "Internet Security Threat Report" does not offer good news either. McGuire told conference participants that the report found "more than 286 million unique variations of malicious software or malware," which she said was "an increase of 19% over 2009."

As the threat landscape has grown more complex, so too has public policy awareness of cybercrime, panelists noted. Although they pointed to some successes, the response is not yet sufficient.

"We've seen an increased focus in the public policy arena," McGuire stated. "In 2009 President Obama said that cyber was a national and economic security imperative. President Bush released the National Strategy to Secure Cyberspace in 2003 and the Comprehensive National Cybersecurity Initiative—the CNCI—in 2008 to try to focus on government.…We've seen new agencies stand up with new responsibilities: DHS, DNI, and Cyber Command. We've also seen new policies released: Homeland Security Presidential Directive 7 that focused on critical infrastructure protection…the National Strategy for Trusted Identities in Cyberspace, and the International Cyberspace Policy."

Securing the Cyber Landscape

The third member of the cybersecurity panel, **Mark Haselkorn**, highlighted a point that he believes is critical to understanding what cybersecurity is and how policymakers should consider it. Dr. Haselkorn is a Professor and Director of the Pacific Rim Visualization and Analytics Center at the University of Washington.

The cost of global cybercrime is approximately $114 billion a year. That's just in what is actually taken from consumers. But in addition to that, the value of lost time due to the recovery and the impact on their lives is an additional $274 billion a year. [That's a cost of] $388 billion a year, just on the consumer side…not taking into account what's happening on the enterprise side.

—Cheri McGuire, Symantec Corporation

> We tend to focus on what we understand and feel we can control. External threats are better understood, and therefore we focus on them more. That doesn't mean they're not also critical, it just means it's harder to focus on the systemic threats because we don't understand them as well.
>
> —Dr. Mark Haselkorn, University of Washington

There are "two flavors of threats" in the cybersecurity world, according to Haselkorn. The external threat is something like a terrorist attack—it originates outside an organization or country. The internal threat is sometimes more difficult to see because it happens "between functional nodes" in an organization or entity and "is much more an interdependency management" matter. "In one the goal is to deter, in the other the goal is to coordinate," he explained.

Haselkorn noted that internal threats often are not given as much attention. "They're under-addressed, in part," he explained, "because they're not understood. Systemic complexities run a huge gamut, from an individual person doing their job to mission threats involving multiple agencies and systems."

Just as Senator Kerrey and Assistant Director Reinhold spoke of finding the right people for the job—and training and retaining them—Haselkorn said that the way to address systemic vulnerabilities while maintaining security against external threats is to place "the right people…and the way they work at the center."

Though the panelists indicated that there is still a long way to go, they believe that public-private collaboration offers hope for tackling current and future cyber challenges. Public-private partnerships done well need to have three goals, McGuire explained. Those goals are governance (managing the risk), protection (improving resiliency), and visibility (collaboration and coordination). She cited the development of a national cyberexercise program, the U.S. Department of Homeland Security's Cyber Storm program, as an example of a successful public-private partnership approach.

Nicholas encouraged the development of a "shared threat model" that would help the public and private sectors analyze threats collaboratively. One of the challenges, he said, is that the "things the government is interested in are incredibly small compared to the bulk of the risk management that the private sector deals with."

"I would posit that there is no solving the problem," McGuire told participants. "We can only mitigate the risk. We can buy down the risk. But there's no single silver bullet to solve the issue."

DOMESTIC PREPAREDNESS

One theme that emerged from the conference's panel on domestic preparedness, moderated by **Steve Stein**, Director of PNNL's Northwest Regional Technology Center for Homeland Security, was the idea that securing America's national security involves nearly every layer of society—from the federal to the local governments, from elite military units to local firefighters, from those paid to fight terrorism to citizens involved in nearly every walk of life. The panelists referred to this as a "whole of government approach." They also spoke of how the United States, especially in the last ten years, has refined its medical surge capacity and its ability to quickly assemble and deploy first responders and others to disaster areas.

> A key outcome that we saw from these Cyber Storm exercises was that we were able to identify weaknesses or gaps between industry and government and how we actually shared information.
>
> —Cheri McGuire, Symantec Corporation

One system predates another, but the gears haven't been meshed together.

—Dave McIntyre, Jr., TriWest Healthcare Alliance

KENNETH MURPHY, DAVE MCINTYRE, JR., AND MAJOR GENERAL TIM LOWENBERG.

The Federal Emergency Management Agency (FEMA) is the federal agency charged with responding to disasters such as Hurricane Katrina. FEMA's Region X administrator, **Kenneth Murphy**, said that in the aftermath of September 11 the agency now spends a lot of time on terrorism planning. "I think the money that has been spent since the terrorist attacks of 9/11 has made significant differences, whether it's terrorism or natural disasters."

Murphy cited the response to the tornado that devastated Joplin, Missouri, as an example of how the investments that communities have made in search and rescue equipment since September 11 have paid off. "We immediately mobilized urban search and rescue teams—a few around the country. [Because of] the money they had invested…they had enough search and rescue assets that were within minutes, if not an hour of Joplin, and they could immediately get to Joplin and help the people who were under the debris."

Surge Capacity

"Terrorism becomes very unique and hard," said Murphy. "You can see a hurricane coming; terrorism, you can't." Despite the difficulties in planning for terrorist attacks, he explained that the United States has an enviable capacity, exemplified by having "surged 3,000-plus people in tactically deployed places" for Hurricane Irene in fall 2011.

Medical personnel are obviously needed after any disaster, whether manmade or natural. One panel member, **Dave McIntyre, Jr.**, President and CEO of TriWest Healthcare Alliance, explained that the infrastructure available for surging medical services is robust and its participants dedicated. One important question the United States should address when it comes to surge capacity, according to McIntyre, is how to coordinate systems that, in some cases, duplicate functions.

He said that TriWest Healthcare Alliance has a network of 175,000 providers in 21 states that provides care for servicemen and women and their families, along with military retirees. "We get paid by the taxpayer to build out this amazing network," he said.

"Our job is to build the networks—the healthcare networks—and make them available to deliver services that can't otherwise be delivered," McIntyre said. "The second thing we're paid to do is to make sure that if there is a national disaster, as very narrowly defined by the federal government, …that we make that network

You can see a hurricane coming; terrorism, you can't.

—Kenneth Murphy, FEMA

available to the federal government for the purpose of backing up the VA [U.S. Department of Veterans Affairs] and backing up the Department of Defense."

He explained that there is also another system in place to respond to national disasters—the National Disaster Medical System (NDMS). The NDMS, McIntyre said, is the "second piece that sits in existence, side by side with [the networks that TriWest helps create]," and which "predates the very product that we're required to deliver for the federal government on behalf of the taxpayers." He indicated that the NDMS is designed to be the United States' "emergency response mechanism."

According to McIntyre, creating and maintaining a NDMS that can be an "emergency response mechanism," requires that there be "a bunch of folks out there who get paid and spend their time to think about, 'What network do you have to have in place in the private sector to respond to a disaster?'" He said, they "go out and develop all of those relationships—the very same [ones] that [he] got paid by the taxpayer to develop for the Defense Department."

McIntyre emphasized that, overall, the system works well. But it nonetheless could likely be improved and save taxpayer money through better coordination and elimination of redundant processes. He cited the federal government's role in coordinating the evacuation of active duty military personnel and their families from Japan following the earthquake in March 2011 as an example where emergency response systems and the various components involved in providing care to military personnel and their families worked well together.

> One of the basic changes that has evolved just in the past two years, to set the stage for the coming decade, is how we are attempting as a whole of government to address the CBRN threat.
>
> —Tim Lowenberg, Adjutant General for the state of Washington

> In preparing for the growing threats and addressing those threats in the next decade, we have to engage the whole of society, and in particular, the whole of government—not just the federal government.
>
> —Tim Lowenberg, Adjutant General for the state of Washington

"We all came together [to help military personnel and their families]," he said, "to figure out…to plan, 'How is it that we would actually meet their needs?'" He explained that they "tested" how it would work after the Japan earthquake and found that it was successful. McIntyre indicated that more should probably be done to integrate response systems that are funded by taxpayers.

"The bottom line," he said, "is that sometimes, we don't step back…and say, 'What's the new requirement?' or 'What programs got built, and how did they get layered in?'" Despite the impressive medical surge capacity that the United States has, McIntyre argued that it could be made better: "One system predates another, but the gears haven't been meshed together."

The Whole of Government Approach

Long before the 9/11 Commission issued its recommendations, the Hart-Rudman Commission warned Congress that the United States was far behind—and needed exponential improvements—in planning for a terrorist attack on U.S. soil. That report was released on February 15, 2001, less than seven months before the attacks of September 11.

The Hart-Rudman Commission advocated a "whole of government approach," said **Major General Tim Lowenberg**, Adjutant General for the state of Washington. "They were aware of…the active engagement of state and local governments in preparing for this approaching transnational terrorist threat that pre-dated the attacks of 9/11."

Think about what you can do personally; think about what you can do in your neighborhood, your community, your county, parish, borough, wherever you may live, your state, tribal nations. Do you have relationships with the private sector or the government? And think how we're going to do this—the whole of community—FEMA embraces the whole nation. It's really a whole of global effort to convince everybody what we must do to deal with terrorism and natural disasters.

—Kenneth Murphy, FEMA


KENNETH MURPHY

Lowenberg said that after September 11, the state of Washington had "a two-year running head start on identifying what we needed to do," because, as early as October 1999, a group of elected and other state officials had been meeting to think about, and plan for, the possibility of a terrorist attack. After September 11, when asked to share with the federal government and other states what "gaps needed to be identified," officials were prepared and highlighted the lack of interoperable communications, information-sharing and intelligence fusion, and medical surge capacity, or as Lowenberg explained, "a lack of medical surge capacity to meet the needs of the new threat environment."

"We have not yet, in this country, experienced an actionable event, an attack that is predicated on a conscious, chemical, biological, radiological, or nuclear [CBRN] attack," Lowenberg explained. "But we know that…[CBRN] threat agents are available to individuals, not just nation-states.…One of the basic changes that has evolved just in the past two years, to set the stage for the coming decade, is how we are attempting as a whole of government to address the CBRN threat."

Collaboration and Change

By fall 2012, thanks to sustained efforts often initiated at the state level by the adjutant general, among other response capabilities, the United States will have a "designated homeland response force in the National Guard…within a 250-mile driving radius of more than 85% of the American population."

Communication across different levels of government may be improving. Lowenberg explained that a council of governors has been created to help facilitate dialogue between state and federal authorities with regard to planning and the national response framework. "We're focusing in that joint action plan on interoperable communications and a common operating picture—that's a whole of government approach that's inclusive of all of the federal and state agencies and local agencies that engage domestically."

Another positive development, according to the panelists, has been presidential policy directives addressing domestic preparedness.

"One came out this year that's very important," noted Murphy. "It's on national preparedness….I think it's important because it really talks about every citizen in the United States….We will do much better and survive much better—whether its terrorism or natural disaster—if everybody participates in this process."

HARRY SCHNEIDER, JR.; MICHAEL O'NEIL; JOHN MCKAY; AND KELLYE TESTY.

PART III: COUNTERING THE THREATS

LEGAL CHALLENGES TO SECURITY, DEFENSE, AND INTELLIGENCE

"One of the things that the law is often tasked with doing is making really hard choices between competing values," said **Kellye Testy**, Dean of the University of Washington School of Law, as she introduced the panel on "Legal Challenges." "I don't think there is any area like this one that really brings those challenges forward so acutely—trying to both preserve the security of our nation, [and] at the same time the freedoms and the rights and liberties of all of our citizens….So this has tested us in many ways like nothing else."

The panel consisted of three experts: one an attorney who successfully challenged the legality of military commissions to try detainees at Guantanamo Bay, another who served as the general counsel of the CIA, and a former U.S. attorney. Each approached the issue of legal challenges differently, and their respective experiences were reflected in their individual comments about the legal issues in security, defense, and intelligence.

Intelligence—An Insider's View

There are probably few people better prepared to offer informed commentary on the impact that September 11 and the 9/11 Commission had within the intelligence community than the former general counsel of the CIA.

Michael O'Neil, who had that role and is now a partner at K&L Gates LLP, shared with participants his views on the landscape that the 9/11 Commission was assessing when it made its recommendations, as well as on some of those recommendations as they relate to the world of intelligence.

"What the report said was that we needed as a nation a unity of effort that wasn't there, and that accountability and organization were not what they should be—that the responsibility and accountability were diffuse within the intelligence community," O'Neil said. He listed the solutions that the 9/11 Commission wanted, such as a National Counterterrorism Center (NCTC), a Director of National Intelligence (DNI), better intelligence-sharing, improved congressional oversight, and changes at the FBI to focus on domestic intelligence collection.

Of the changes he discussed, O'Neil deemed only the creation of the NCTC "an extraordinary success." He explained that intelligence-sharing has improved

The U.S. Supreme Court has looked at the role of the executive, and to some extent the role of the Congress…and has reined in—in certain key places—claims of power and authority by the president and by the Congress, beginning with President Bush's decision to stand up Guantanamo as a detention facility and to indicate that this was going to occur outside the reach of the federal courts.

—John McKay,
Seattle University School of Law

to some extent, but that the DNI role has not been implemented as first envisioned.

"When you originate intelligence in our system, you have ORCON, you have originator control," O'Neil said. Today there is much more intelligence-sharing. "That's good," he told the audience, "but some of those same ORCON controls are still there, and the most sensitive information remains tightly controlled."

O'Neil does not support the 9/11 Commission's opinion that a joint congressional intelligence committee should be created. Having also served as the chief counsel of the U.S. House of Representative's Intelligence Committee for twelve years, his view is that two committees are better than one. "I didn't think it was terrible to have small defense appropriations subcommittees also looking at the same things we did," he said. He offered the example of the Foreign Intelligence Surveillance Act (FISA) to explain and support his reasoning.

"We all learned after the 9/11 Commission…that the president had authorized a series of intelligence programs that were outside the limits of FISA," O'Neil said. "Most people, including the authorizing committee that wrote the language in the statute, thought [that FISA] was the exclusive means by which electronic surveillance was going to be conducted inside the United States. As the story unfolded, we learned that this was all based on a legal opinion written by one person in the Office of Legal Counsel at the Department of Justice, [and] not reviewed by anybody else in the department, including the attorney general."

O'Neil went on to say that the opinion was "flawed," and that "everybody agreed afterwards that it was based on mistakes in facts." As a result of this episode, he said, the statute was rewritten and Congress "has rebalanced."

"Secrecy can be our enemy here," O'Neil said. "I think we had…flawed legal analysis and operations that I think Congress would've approved—maybe not very quickly, but they would've approved in the end. This wasn't the way to get to the right solution, by keeping it all a secret from everybody and then having it dragged through the press and through the process to improve it."

We've got more intelligence-sharing. There's a lot more intelligence. That's good. But some of those same ORCON [originator controlled] controls are still there, and the most sensitive information remains tightly controlled.

—Michael O'Neil, K&L Gates LLP

The Role of the Courts

"The question I would raise is whether military commissions were, and remain, the preferred way to prosecute those charged with crimes against the United States arising out of terrorist acts," said **Harry Schneider, Jr.**, a partner at the Seattle-based law firm Perkins Coie. "I don't pretend to be an expert; I don't pretend that it's an easy question to answer." Schneider was on the legal team that successfully defended Salim Hamdan, the only Guantanamo detainee who has been tried to a verdict.

In the years since September 11, as enemy combatants have been detained at Guantanamo, the United States has been embroiled in a debate about the proper role of the courts there and in other places. This issue has brought to the surface questions about the executive branch and the separation of powers.

"The U.S. Supreme Court has looked at the role of the executive branch, and to some extent the role of the Congress here [at Guantanamo]," Seattle University law professor and former U.S. attorney **John McKay** said. The court has "reined in—in certain key places—claims of power and authority by the president and by Congress, beginning with President Bush's decision to stand up Guantanamo as a detention facility and to indicate that this was going to occur outside the reach of the federal courts."

McKay said that the initial government position was that such decisions were the "purview of the executive branch." However, the court "very clearly weighed in and said…the scheme and structure of Guantanamo being a place of detention by the United States military does not mean that the U.S. Constitution…[or] basic human rights don't apply." The court thus ruled that "the executive branch, even acting under the authority of the Congress, has gone too far."

> In retrospect, I think what happened was we were looking for a more predictable outcome. We were looking for a more predictable result in a more predictable manner. And the question I would raise is, since when has the American system of justice been about predictable outcomes? What it's about is a predictable process, despite the outcome.
>
> —Harry Schneider, Jr., Perkins Coie LLP

Hamdan: One Case, Many Lessons

Salim Hamdan was Osama bin Laden's driver. His arrest, detention, and eventual U.S. Supreme Court case had "nothing to do with Hamdan's guilt or innocence," said Schneider. "It has nothing to do with terrorism. It has to do with presidential authority and the separation of powers, and whether the president—any president—can design a court of his own making without congressional approval and authorization." The case also concerned "whether that court can adopt procedures which are at odds with the Uniform Code of Military Justice, a revered—and deservedly so—body of law, and whether those procedures can confound and betray the Geneva Conventions."

Schneider explained that Hamdan was the first person tried under the Military Commissions Act of 2006. "The result of the Supreme Court case," he explained, "was that the court found that the president did not have the authority…to implement the court that he chose to implement, that the decision not to honor the Uniform Code of Military Justice, absent a legitimate explanation, was lacking, and that Geneva should apply."

The military jury acquitted Hamdan of conspiracy after a four-week trial. "The sentence the military jury gave him was four months," Schneider told conference participants. "Four months in addition to time served. I think there's an interesting lesson in that outcome. Despite the surprisingly successful outcome for the person we represented, I'm not an advocate of the military commissions. I think we are better off to try these people in federal court or in a military court marshal proceeding where the Uniform Code of Military Justice would apply in full."

McKay added that the debate about legal questions will not end any time soon. He pointed to an executive order that President Obama signed in March 2011 that has the effect of allowing continued detention without trial at Guantanamo Bay.

"We got there because we painted our way right into a corner," McKay said. "In response to the courts intervention…the Military Commissions Act of 2009 essentially extended many of the same sort of procedures to military commissions that exist in Article III courts. That means people like Khalid

JOHN MCKAY, KELLYE TESTY, AND MICHAEL O'NEIL.

Sheikh Mohammed can't be tried before a military commission. The reason is, a military commission is likely to throw out the indictment and it's going to throw it out because we tortured [him]. And no federal judge, I think no one really, wants to see this risked by a military court under a military commission—the risk that they would reach exactly the same result because we've now changed the rules in the military commissions to look so much like federal courts. We are not going to get the kind of conviction that I think President Obama unwisely said was guaranteed for some of these individuals. He and Attorney General Holder both indicated that we're going to convict Khalid Sheikh Mohammed and others."

Schneider said that he understands why the legal questions have become so muddied but thinks the American justice system can do much better. The explanation for the way the U.S. has approached prosecuting detainees was that the people who made decisions had "legitimate, compelling" reasons. "In retrospect, I think what happened was we were looking for a more predictable outcome. We were looking for a more predictable result in a more predictable manner," Schneider explained. "The question I would raise is, since when has the American system of justice been about predictable outcomes? What it's about is a predictable process, despite the outcome."

The former attorney for Hamdan added that while U.S. federal courts are "up to the task," there is too much "opportunity for abuse" when the executive and judicial branches are not clearly separated. "The genius of our system has been that separation of powers and that independence of our federal judiciary."

KENT PATTON

After 9/11, a lot of very smart people at the State Department, within NGOs and academia sat down and said, "What happened here?" The president sat with his advisors and said, "What happened?" One of the key elements of everyone's consultations within the international community within the United States was, "We obviously have a problem in the Middle East."

—Kent Patton, Patton & Associates

DEMOCRATIC DEVELOPMENTS IN THE MIDDLE EAST

"The Middle East and North Africa are in the throes of revolutionary change as we speak," observed **Kent Patton**, partner at Patton & Associates and a former deputy assistant secretary of state for Near Eastern affairs at the U.S. Department of State. "These changes are good for the United States; they're good for our allies," he explained. "They will provide greater stability and greater freedom for the people of the region." Patton was the first speaker at the conference's final session, "Democratic Developments in the Middle East."

In his opening remarks, panel moderator **Reşat Kasaba**, Director of the Jackson School of International Studies at the University of Washington, said, "Within less than a year…three of the most entrenched autocrats in the region are gone now, and at least two others in Yemen and Syria are in very shaky situations." Deciphering the causes and potential implications for the change occurring in the region was the purpose of the conference's final panel. As participants learned, it turns out that interpretations, though similar, also vary.

Causes of Change

"With regard to progress that we've seen recently in the Middle East," said **Jennifer Butte-Dahl**, "I'd offer three points: First, I think that this progress that we're seeing is both in spite of U.S. efforts, as well as because of them….The second point is that our counterterrorism goals and our democracy freedom agenda—that is, human rights agenda goals—have almost always been in concert in principle, but very discordant in practice. And [third], I believe that a whole of government approach is critical for addressing these national security challenges, but that doesn't mean it's not hard or that it always works." Butte-Dahl was formerly a senior advisor to the deputy secretary of state for management and resources and also to the U.S. envoy for Middle East peace in the U.S. Department of State.

Butte-Dahl said that the United States' efforts to achieve the country's goals in the Middle East have become more complex because of the challenge of managing the image conveyed, on the one hand, through arm sales in the region and, on the other hand, by a public diplomacy emphasis on democratic reform. She cited Saudi Arabia, Tunisia, and Egypt as examples

of countries with which the United States has partnered during the Iraq War, but in which it also hopes to see democratic reforms.

"So in a sense," Butte-Dahl explained, "we're simultaneously training democracy advocates in these countries and, in parallel, spending a massive amount of time justifying large arm sales to these countries' governments, which…sends a very mixed message to the civil society groups that we're trying to work with."

Another panelist, **Jamie Nelson**, a former senior advisor for Near Eastern Affairs at the U.S. Department of State, said he believes that although the United States cannot claim full responsibility for the changes that are happening in the region, the changes can partly be attributed to the freedom agenda and related democracy development efforts.

"The freedom agenda is kind of a loose term that we've used in the democracy development world for a while," Nelson said. "It's basically the idea that the United States, through a form of extended soft power—and this was begun under the Reagan administration with the National Endowment for Democracy—could extend its power through supporting emerging democracies as a way of fighting the Cold War without military tools."

For Patton, the changes that have occurred in the Middle East can be attributed in part to five developments: the United Nations–sponsored Arab Human Development Report; an end to the notion of Arab exceptionalism; U.S. outreach to citizens of the region; a desire among Arab communities to not have al Qaeda–type violence in their own neighborhoods; and the development and use of tools, such as social media, that have empowered individuals in the region.

> As we look forward, I think that a whole of government approach is critical, but we should always have our eyes wide open to the fact that national security objectives are not always perfectly in sync. There's always going to be a juggling and a prioritization of key objectives.
>
> —Jennifer Butte-Dahl, Artistry Global

> We see now that the U.S. government links defense, development, and democracy as three parts of an integral, strategic, U.S. view of foreign policy. And we didn't use to do that.
>
> —Jamie Nelson, williamsworks

Patton observed, "After 9/11, a lot of very smart people at the State Department [and] within NGOs and academia sat down and said, 'What happened here?' The president sat with his advisors and said, 'What happened?' One of the key elements of everyone's consultations within the international community within the United States was, 'We obviously have a problem in the Middle East.'"

The Arab Human Development Report was the product of a group of Arab intellectuals asking similar questions under the auspices of the United Nations. Patton explained that they "came together and said, 'What is wrong with our community?'…'What's going on?' And they came out with some very strong recommendations about the deficits in the region and some of the drivers for the dissatisfaction…[such as] lack of freedom, lack of freedom for women, lack of good education systems, [and] corrupt economic systems." "The empowering of the individual within that culture," Patton said, "is a cultural change that is going to take a long time to see its final effects, but, again, is going to be a good, positive development in the region."

Going Forward

Butte-Dahl, Nelson, and Patton generally agreed that the changes taking place in the Middle East are positive, not only for those countries but for the United States as well. Not surprisingly, however, none of them said the path will be easy.

"At the end of the day, the U.S. [has] been working with democracy advocates in these countries for years," remarked Butte-Dahl. "I think the U.S. played a role in kind of urging some of those activities we've seen.…As we look forward, I think that a 'whole of government' approach is critical, but we should always have our eyes wide open to the fact that national security objectives are not always perfectly in sync. There's always going to be a juggling and a prioritization of key objectives."

Patton said that he is hopeful that change will continue to occur in the region and is "less concerned about making people like U.S. policies," provided that the United States "has moral clarity about its own mission in the world." That mission "isn't always perfect but is better than most countries in the world." He concluded, "Terrorism will be beat at the ballot box in the Middle East and North Africa. It won't be beat by armies or by intelligence agencies."

> Terrorism will be beat at the ballot box in the Middle East and North Africa. It won't be beat by armies or by intelligence agencies.
>
> —Kent Patton, Patton & Associates

The Slade Gorton International Policy Center honors the living legacy of Senator Gorton's values and significant contributions to Washington State and the nation by sponsoring world-class policy research and inspiring the next generation of leaders. The Center was founded in January 2010 by a group of colleagues, friends, family, and former Gorton staffers who wanted to establish a premier policy research center to honor over six decades of Senator Gorton's extensive political career and service to Washington State and our nation. The Center is a core, permanent program of the National Bureau of Asian Research (NBR) with three focus areas: policy research, fellowship and internship programs, and the Gorton History Program.

GORTON CENTER
SLADE GORTON INTERNATIONAL POLICY CENTER

INTELLIGENCE AND SECURITY • THREATS OF TODAY • COUNTERING THE THREATS

NBR THE NATIONAL BUREAU of ASIAN RESEARCH

Seattle and Washington, D.C.

1414 NE 42ND STREET, SUITE 300
SEATTLE, WASHINGTON 98105 USA
PHONE 206-632-7370, FAX 206-632-7487

1301 PENNSYLVANIA AVENUE NW, SUITE 305
WASHINGTON, D.C. 20004 USA
PHONE 202-347-9767, FAX 202-347-9766

NBR@NBR.ORG, WWW.NBR.ORG