## SENIOR LEADER PERSPECTIVE: GENERAL RONALD KEYS

NSCI's Lindsay Trimble recently had the opportunity to interview General (ret.) Ronald Keys, senior advisor at the Bipartisan Policy Center and former commander of Air Combat Command, the Air Force's largest major command. After his 40-year military career, Keys now owns RK Solution Enterprises, an independent consultancy. In his role as a senior advisor to the Bipartisan Policy Center, he leads the BPC National Security Speaker Series and acts as the technical advisor to the BPC Cyber ShockWave Security simulation project series. He also advises various other Defense Department and non-Defense Department related firms on advanced technologies, marketing, strategic planning and policy development issues.
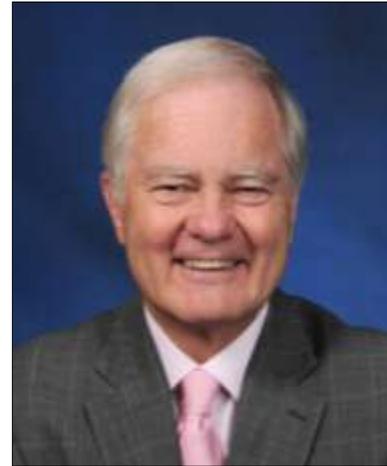
NSCI: The Bipartisan Policy Center sponsored Cyber ShockWave earlier this year to simulate a national cyber attack and test government response to such an event. In your opinion, what was the event's most important finding?

KEYS: Importantly, the role-playing simulation relied on two pillars. First, it was underpinned by a number of sponsors and contributors with "skin in the cyber game" and day-to-day experience (General Dynamics, S-Mobile, Southern Company, PayPal, Georgetown University and Symantec). Second, the role-playing involved a bipartisan group of former senior administration and national security officials with experience over a number of years. These officials included former Homeland Security Secretary Michael Chertoff; former Director of National Intelligence John Negroponte; former White House Homeland Security Adviser Fran Townsend; former Senator Bennett Johnston; former Director of the National Economic Council Stephen Friedman; former Deputy Attorney General Jamie Gorelick; former Presidential Press Secretary Joe Lockhart; former Acting CIA Director John McLaughlin; former Assistant Secretary of Policy at the Department of Homeland Security Stewart Baker; and retired Air Force General Chuck Wald.

The Cyber ShockWave simulation was not a monolithic national state attack. It was a series of cyber, environmental and natural disaster incidents that, together, cascaded upon one another and began to bring our nation's networked infrastructure and economy to its knees.

The key finding was that we simply had not thought about potential scenarios and how they might play out and so were totally unprepared to take action or, in many cases, didn't have the legal authority or policy in place (or we didn't have the consensus that we *did* have it and knew who had it!) to do what was needed. As a result, time slipped away from the participants as the situation steadily and rapidly got worse.
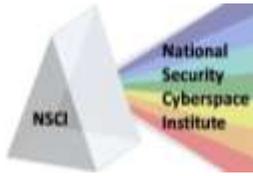
A second important finding was that the incidents didn't even need to be coordinated as one massive attack in order to be catastrophic – a combination of a hot summer, just concluded hurricane, a malware application for mobile devices, a limited domestic physical attack and an insider scheme reinforced the separate effects into a serious problem.

NSCI: Does the Bipartisan Policy Center have any follow-on activities planned?

KEYS: We have been engaged on the Hill, briefing the outcomes and making our participants available for discussions. Additionally, we have just begun a series of roundtable discussions with policymakers responsible for cyber across the government: the Federal Communications Commission, U.S. Cyber Command, State Department, Department of Justice, the Hill and other interested agencies.

Finally, due to the discussions that arose in the first ShockWave about authorities/policies and desirability of public-private partnerships, we are organizing a conference with Livermore Labs to assess the state of public-private partnership in cybersecurity and develop recommendations for how to strengthen and broaden cooperation in that area.

NSCI: How do you think the image of cybersecurity and its importance has changed for national leaders since Cyber ShockWave and other efforts to demonstrate the reality and severity of the cyber threat?
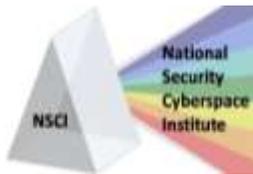
KEYS: I think we are slowly making progress. It will be critical to moving the issue ahead that we have all the stakeholders at the table – government, commercial, consumers, privacy and civil liberty advocates, and legal experts. This is not just about the technical aspects of cyber. This is very much understanding what could happen and agreeing on what we want to do about it – before we are in the crisis and systems start going down.

NSCI: What do you see as the most significant benefits and challenges regarding the recent stand-up of U.S. Cyber Command?

KEYS: I moderated a panel at this year's AFCEA DC Cyber Symposium on just that. It started with a short clip from the BPC's Cyber ShockWave concerning attribution and military options and then segued into a discussion about CYBERCOM's role. I think the consensus was that the significant benefit at this point is in the integration of all of the .mil networks under one master. That goes a long way to building a common operational picture, ensuring standards and sharing capabilities across DoD.

The challenge remaining is what exactly and when exactly does CYBERCOM do something as a matter of agreement and law *beyond* the .mil networks? There is much discussion, many conspiracy theories, privacy concerns, proprietary concerns and simple capacity concerns that need to be hashed out now – not in the middle of a crisis as Cyber ShockWave showed.

NSCI: Many security experts have said the United States is not prepared for major cyber attacks. How do we move from talking about the problem to taking action?

110 Royal Aberdeen ● Smithfield, VA 23430 ● ph. (757) 871-3578

CyberPro   *National Security Cyberspace Institute*   **P a g e | 2**

KEYS: In most of the fora that I have been involved in, there seems to be a real lack of someone in charge – not just a nametag, but someone with budget authority, legal authority and clout. Cyber is a very diffuse, if you will, domain; legal, intelligence, commercial, personal and more threads run through it. As a result, each one of those tribes look at the problem differently, understand the problem differently and want differing rules, regulation and freedom.

I wrote an article in the run-up to ShockWave entitled, "Battlespace, Marketplace or Playground... Solving the Cyber Riddle," and posited the answer was, "All three." Until we are prepared to "govern" this "ungoverned space," we are a long way from having any cohesive plan to deter the deterrable; defend against what can't be deterred; repair what we will have to repair; and operate through the effects. That's a long answer, but it boils down to who can say, "Do it," and make it stick. That has to be step one.

NSCI: What do you feel are the most pressing cyber-related issues we need to tackle?

KEYS: I think there are three: 1) Establishing a common operational picture – who's on my net, are they authorized on my net and are they authorized to do "that" on my net; 2) Establishing within that COP the ability to readily share situation awareness – stripped of sources and methods, stripped of identification and proprietary/competitive advantage concerns – what is happening or what is about to happen; and 3) Establishing the list of public, private and personal responsibilities when it comes to operating in the cyber domain. I really do think there is too much focus on the individual technology widgets that purport to be a silver bullet, vice the policy of how and when we would be allowed or should do certain things.

NSCI: In your opinion, what is the most effective way for public-private partnerships to work?

KEYS: Well I think there are a number of public-private partnerships that are working now. They tend to be issue or technology specific, but I think they are all underpinned with trust – trust that competitive information will not be lost, trust that relationships are guarded appropriately, trust that intelligence information will be carefully handled, trust that the relationships are a two-way partnership. All of that becomes harder to ensure as the circles of trust get bigger. Additionally, the partnerships need to be at a deep enough level that actions can actually be taken in time. Briefing a chairman or CEO might feel good, and make you feel you have a PPP, but not much may actually flow into the day-to-day operations where it needs to.

NSCI: Is there anything else you'd like to add?

KEYS: Just keep looking for the Bipartisan Policy Center Cyber ShockWave II near the end of the year. It will focus on the public-private partnership issue and we think it will be even more illuminating than our first one.