Cyber ShockWave

Simulation Report and Findings

BIPARTISAN POLICY CENTER

ABOUT THE BIPARTISAN POLICY CENTER

In 2007, former U.S. Senate Majority Leaders Howard Baker, Tom Daschle, Bob Dole, and George Mitchell formed the Bipartisan Policy Center (BPC) to develop and promote solutions that can attract the public support and political momentum to achieve real progress. Currently, the BPC focuses on health care, energy, national and homeland security, transportation, science and economic policy.

For more information, please visit our website: www.bipartisanpolicy.org.

TABLE OF CONTENTS

What Is Cyber ShockWave?

On February 16, 2010, a bipartisan group of former senior administration and national security officials participated in a simulated cyber attack on the United States—Cyber ShockWave. The simulation, which was moderated by Wolf Blitzer and broadcast as a special on CNN, provided an unprecedented look at how the government would respond to a large-scale cyber crisis affecting much of the nation.

A project of the Bipartisan Policy Center—with support and guidance from General Dynamics Advanced Information Systems, Georgetown University, PayPal, SMobile Systems, Southern Company and Symantec—Cyber ShockWave had participants play the roles of Cabinet members reacting in real time to an unfolding cyber attack and advising the President on an appropriate response.

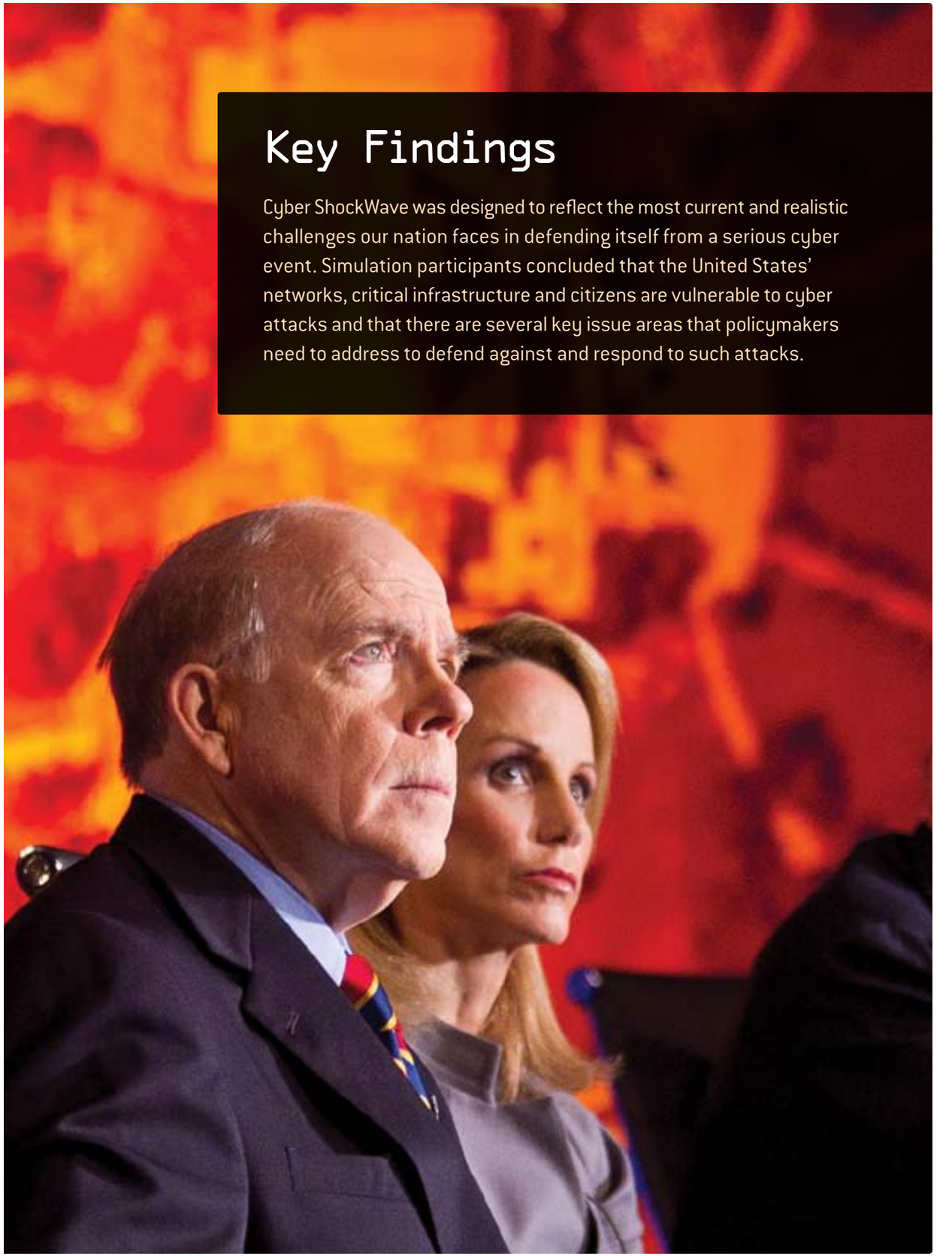
Cyber ShockWave highlighted how critical an issue cyber security has become for our nation. While protecting sensitive and personal data remains a priority, the proliferation of computers across ever-greater spheres of our personal lives and their growing role in running our critical infrastructure means a serious cyber event could have a debilitating effect on this country. Unfortunately, as Cyber ShockWave demonstrated, our current government policies are not adequate to responding to a large-scale cyber attack.

Cyber security, both preventing attacks and preparing our government to respond to them, must be considered a national security priority.

Michael Chertoff
Former Secretary of Homeland Security

Key Findings

Cyber ShockWave was designed to reflect the most current and realistic challenges our nation faces in defending itself from a serious cyber event. Simulation participants concluded that the United States' networks, critical infrastructure and citizens are vulnerable to cyber attacks and that there are several key issue areas that policymakers need to address to defend against and respond to such attacks.



Government Organization

+ Cyber security must consist of more than protecting military, government or personal data and networks from intrusion. It is a national security issue that must address defense and preparation, response and restoration as the attack happens, and attribution afterwards.

+ The United States government—including the White House Cyber Coordinator—currently lacks clearly defined roles and responsibilities for maintaining common situational awareness of emerging critical operational developments in cyber space.

+ Our nation needs an effective decision-making framework below the cabinet level, especially between the Department of Homeland Security and Department of Defense, for coordinating the government's response to and recovery from a devastating cyber event.

+ Current policy, legal and organizational constraints drive the government to a limiting and insufficient binary response: (1) the traditional domestic-focused law enforcement approach or (2) the desire to neutralize the attack under international laws of armed conflict.

Legal Authority

+ The U.S. needs well-established legal authorities for dealing with a cyber crisis that dovetail with a broad national understanding of what constitutes a "reasonable expectation of privacy" under such circumstances.

+ Without statutory authorities for responding to and preventing cyber attacks, including the seizure or quarantine of private data, devices or networks, the President may be left with only those authorities derived from the Communications Act of 1934 (as amended by the Telecommunications Act of 1996) or the Constitution, including war powers.

+ Up to 85 percent of U.S. networks are privately owned, but there is no mechanism for government cyber defenders to effectively collaborate with the private sector to leverage their expertise, to share knowledge and situational awareness with them, or to bring their capabilities to bear during a response to a cyber attack.

International Protocols

+ There are few international norms or regulations for what can and cannot be done in cyberspace. The United States should consider whether an international legal regime governing cyberspace, parallel to those that exist for the maritime, air and land domains, would be useful.

+ A particular difficulty in formulating responses to cyber attacks is the problem of attribution—identifying the responsible parties. The United States needs mechanisms for holding entities responsible for cyber events and a declaratory cyber deterrence policy, possibly invoking the potential of kinetic retaliation.

Public Education & Awareness

+ A national educational campaign is needed to inform citizens of their role in securing U.S. cyberspace. We are all responsible for national cyber security; irresponsible individual behavior imperils the entire network.

+ Requiring updated virus and malware protection for any device attempting to connect to U.S. networks—as is already required on government networks—should be considered.

We are at a point when we're talking about "cyber attack", "cyber capabilities", and "cyber threat", in something roughly analogous to the position we faced in 1945 when we first encountered nuclear weapons and we didn't know much about them. We need to think very imaginatively, creatively, and unconventionally about how we deal with the threat.

JOHN MCLAUGHLIN, CYBER SHOCKWAVE DIRECTOR OF NATIONAL INTELLIGENCE

A Cyber Security Timeline

Though the first incidences of hacking and computer viruses occurred as early as 40 years ago, the number and severity of cyber attacks and threats has grown steadily over the last decade.

1963

The first recorded reference to hackers in the computer sense is made in MIT's student newspaper, *the tech*.

1971

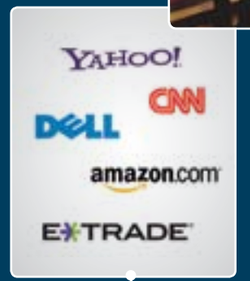
ARPANet experiences its first computer virus called the Creeper virus, written by programmer Bob Thomas. The program copied itself to the remote system where the message, "I'm the creeper, catch me if you can!" was displayed. The program Reaper was written to delete the virus.

1983

The movie "WarGames," featuring a computer intrusion into NORAD, is released.

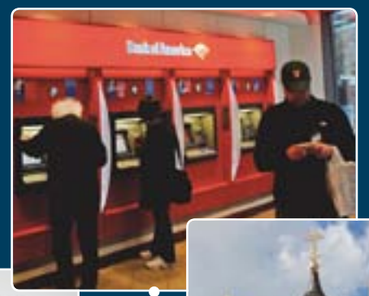
1988

The Robert Morris Worm is the first malicious worm on the Internet costing between $10-100 million in damage according to the GAO.



2000

Michael Calce (aka MafiaBoy) attacks and disables Yahoo!, Amazon, CNN, Dell, and E*TRADE. In response, the President calls for an emergency Cyber Security Summit. The estimated total loss due to the attacks was $1.2 billion.



2003

The Slammer worm brings down 75,000 servers, shutting down Bank of America ATMs, Continental Airlines' ticketing systems, and Seattle's 911 network.

2007

Russian hackers launch attacks against Estonian websites including Parliament, government ministries, banks, newspapers and broadcasters.

As Russia initiated military operations in Georgia, Russian hackers brought down almost all Georgian government websites.

Albert Gonzalez is arrested for the theft of more than 170 million credit and debit card numbers over the course of four years.

2008

2009

U.S. and South Korean government, financial and media websites are attacked, apparently by North Korea.

Attacks targeting Twitter and Facebook succeed in taking both sites offline for several hours.

2010

Chinese hackers steal data from Google and 30 other major U.S. and international companies.

Cyber Security Today

Internet connectivity has transformed how we do business, whether as individual consumers, national governments, or global companies. It has also expanded our vulnerability well beyond our physical reach, necessitating strong cooperation between connected organizations and individuals. Governments cannot secure public services without cooperation from private businesses and citizens. Businesses cannot drive a robust economy without the legal and economic incentives to make wise security investments and cooperate broadly on shared security efforts.

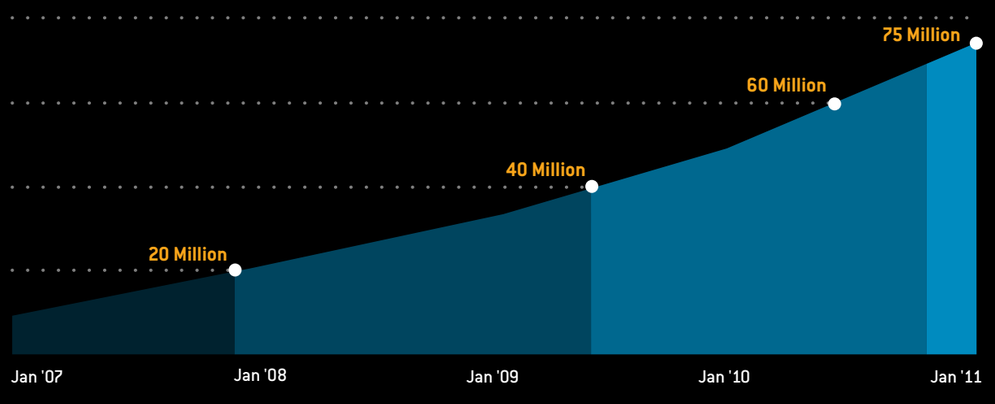
The Internet And Cyber Crime

+ The Internet has been the most quickly adopted technology of all time. It took radio 38 years to reach 50 million users. Television met the same goal in 13 years; the Internet, four years. Facebook added more than 100 million users in nine months, while Twitter added 50 million new users in a little more than three months.

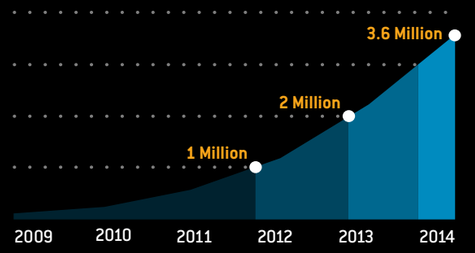
+ As a result, cyber crime has grown just as quickly. It is estimated that identity theft and other forms of online crime have replaced narcotics as the chief revenue source for organized crime, costing U.S. consumers an estimated $50 billion annually.

+ The next frontier of cyber security is defined by the convergent rise of smartphones and social networking.

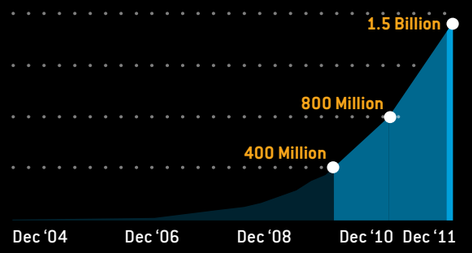
U.S. Smartphone Subscribers



Predicted Mobile Data Traffic
(Terabytes per Month)



Active Facebook Users



Government Organization

Currently, a variety of mechanisms are used to share threat activity information. Several sources of this information are freely available on the Internet or through a variety of security vendor subscriptions. The role of the U.S. government in protecting its citizens from malicious Internet activity remains unclear, although it has defined organizational roles for defending its own infrastructure. The Department of Homeland Security (DHS) has been charged with defending Federal government networks, and the U.S. Cyber Command has been charged with defense of Department of Defense networks. The National Security Agency (NSA) has the greatest capabilities of any cyber organization within the U.S. government; it plays a key supporting role for both DHS and Cyber Command.

+ By executive order, the National Cyber Security Center (NCSC) was created to coordinate operations among itself, the Office of Intelligence and Analysis in DHS, private sector partners and five other government cyber security centers: the Joint Task Force – Global Network Operations (JTF-GNO), the National Cyber Investigative – Joint Task Force (NCI-JTF), NSA Threat Operations Center (NTOC), the U.S. Computer Emergency Readiness Team (US CERT), and the Defense Cyber Crimes Center (DC3).

+ DHS also operates the National Cybersecurity and Communications Integration Center (NCCIC), which is responsible for coordinating the defense of the Federal government's networks. This is a 24-hour, DHS coordinated watch and warning center whose mission is to improve national efforts to address threats and incidents affecting the nation's critical information technology and cyber infrastructure. The US CERT is an integral part of the NCCIC. It reports on ongoing cyber threat activity through the Government Forum of Incident Response and Security Teams (GFIRST) to the Critical Infrastructure and Key Resource (CIKR) Information Sharing and Analysis Centers (ISAC), which primarily share information through their web pages.

+ The Department of Defense (DOD) announced in 2009 the creation of a Cyber Command (CYBERCOM). This new subordinate unified command is responsible primarily for protecting DOD networks. It is also responsible (to the U.S. Strategic Command) for directing DOD offensive U.S. cyber capabilities.

+ In December 2009 the President announced the appointment of a White House Cybersecurity Coordinator. This individual is on the National Security Council (NSC) staff, but also works closely with the National Economic Advisor. He is part of the policy apparatus rather than the emergency response chain. In addition, he is responsible for coordinating interagency staff work in preparation for cyber-related NSC meetings, for monitoring follow-up actions assigned by the NSC, and for periodically briefing the National Security Advisor and the President about current cyber issues.

CYBER.SHOCKWAVE

Participant Roles

On February 16, 2010, a group of ten former senior government and military officials convened to participate in a simulated National Security Council meeting. Their task: to advise the President as the nation faces a crippling cyber attack. As they enter the room, they are unaware of the details of the crisis that is about to unfold.

Michael Chertoff
National Security Adviser
Former Secretary of Homeland Security

John Negroponte
Sec. of State
Former Director of National Intelligence

Fran Townsend
Sec. of Homeland Security
Former White House Homeland Security Advisor

Stephen Friedman
Sec. of Treasury
Former Director of the National Economic Council

Chuck Wald
Sec. of Defense
Former Deputy Commander, U.S. European Command

Jamie Gorelick
Attorney General
Former Deputy Attorney General

Bennett Johnston
Sec. of Energy
Former Senator

Joe Lockhart
Counselor to the President
Former White House Press Secretary

John McLaughlin
Director of National Intelligence
Former Acting Director of Central Intelligence

Stewart Baker
Cyber Coordinator
Former National Security Agency General Counsel; DHS Assistant Secretary for Policy

SIMULATION DEVELOPMENT

Contributors & Experts

In addition to the invaluable contributions of our Cyber ShockWave Cabinet members, experts in the fields of national and cyber security were consulted to develop the scenarios used in the simulation and, in some cases, to brief the Cabinet during the simulation. The BPC extends its special thanks to the following individuals for their contributions:

Gen. Michael Hayden
Former Director of the CIA;
Former Director of the NSA;
Principal, Chertoff Group

Gen. Ronald Keys
Senior Advisor, Bipartisan Policy Center

Michael Barrett
Chief Internet Security Officer, PayPal

Larry Castro
Managing Director, Chertoff Group

Shane Eaker
Senior Security Analyst, Southern Company

Catherine Lotrionte
Associate Director, Institute for International Law and Politics, Georgetown University

Daniel Hoffman
Chief Technology Officer, SMobile Systems

Timothy Roxey
Manager, Critical Infrastructure Protection, North American Electric Reliability Corporation

Matthew Stern
Senior Cyberspace Operations Advisor, General Dynamics Advanced Information Systems

PARTNERS

The BPC is grateful to the following partners for providing their expertise, guidance, time and support to Cyber ShockWave.

SEGMENT 1 // JULY 2010

"March Madness"

A major telecommunications outage has occurred in the U.S. and elsewhere.
As the scenario opens, over 20 million smart and cell phone users have no service and this number is growing rapidly. The outage is traced to a BOTNET attack that uses smartphones infected by "March Madness" malware to send a Red Army video to everyone on the owner's contact list, including social networking sites. The process is then repeated with everyone on the recipients' contact lists. Preliminary analysis connects the BOTNET attack to an IP address in Irkutsk, Russia.

News networks report growing smartphone outages across the country. The outages appear to be linked to a viral video being sent to smartphone and social network users. The video shows soldiers marching across Moscow's Red Square. Initial reports suggest that as many as 20 million Americans are already without cell phone service.

The US CERT traces the attack to a large smartphone BOTNET—a network of remotely controlled, infected devices—that is distributing the video to everyone in the host phone's contact list, including social networking sites. The BOTNET, in turn, is traced to "March Madness," a popular smartphone application.

"March Madness" was a known piece of malware that had been used to perpetrate massive financial fraud earlier in the year. Taking advantage of the expanded use of smartphones and the lack of security they possess, an unknown individual or group had created and distributed a free NCAA March Madness Basketball bracket application for iPhone, Blackberry, Microsoft Windows Mobile, Android, and Symbian smartphones, which proved to be extremely popular.

Unbeknownst to the end users, the application also included spyware components capable of logging every keystroke typed on the device and intercepting e-mail and SMS messages. This information was used to funnel millions of dollars directly to overseas bank accounts or was sold on the black market to other criminal and hacker groups around the world.

The security breach had been recently tracked to the March Madness smartphone application and a security patch was made available to all users. Unfortunately, two weeks after the security patch was announced, less than half of the smartphone users in the U.S. had downloaded it. Just as the FBI was closing in on identifying the perpetrators of the original financial fraud, the March Madness application was used to launch this massive BOTNET attack. US CERT was not able to determine whether the BOTNET was controlled by the original malware authors or was being exploited by a third-party.

THE BOTTOM LINE

Cyber attacks can target critical infrastructure, not just sensitive data. The U.S. government is currently unprepared to deal with such an attack. Effectively responding to a large-scale cyber crisis will require having well-defined roles, responsibilities and legal authorities for government agencies.

The NSC is tasked with determining and advising the President on: (a) how much worse the situation will get and what can be done to recover as quickly as possible; (b) who did this and why; (c) what the President's short-term response options are; (d) what can be done to keep the situation from happening again; and (e) what can the President do to reassure the American people?

The advisors begin by debating what legal authorities the President might have to curtail the impact of the attack—including seizing control of private telecommunications networks or quarantining individuals phones. While there is disagreement about what the government is actually empowered to do, and whether the President can act robustly in the name of public safety, all the advisors agree on the need for swift and decisive action.

As they continue their deliberations, the advisors learn that the telecommunications outage is spreading. It has affected some 30 million users and is plaguing not only smartphones and internet access, but is also resulting in landline congestion as users move to that medium. Moreover, recent evidence suggests that the last known server to host the BOTNET is located in Irkutsk, Russia. This information leads Congressional leaders to demand retribution against the country.

The Director of National Intelligence is quick to point out that attributing the identity of cyber attacker can be extremely difficult. Though the BOTNET may have been traced to a Russian server, it might merely be a routing point, and not the origin of the attack. Nor is there any way to prove the involvement of the Russian government.

Acknowledging these difficulties, the group decides that attribution and aggressive response actions must come second to managing the unfolding crisis at home. As the financial, aviation and other sectors become affected by the lack of communications, the Attorney General is urged to find any ground on which to give the President legal authorities to act. She points out that in times of extreme stress, the President can choose to act without regard to the law and seek to explain his actions to Congress later.

Further discussion is cut off by breaking news of power outages along the East Coast.

SEGMENT 2 // JULY 2010

"Lights Out"

The ongoing cyber attack brings down SecureTrade—a computer-based, electricity trading platform for the Eastern Interconnection. Coupled with several other factors already stressing the power grid, this causes blackouts across the East Coast, sparks public panic, shuts down financial markets, and complicates ongoing recovery efforts.

As the NSC reconvenes, news reports are already estimating that well over 10 million customers have lost power in the Eastern two-thirds of the country. In addition, simultaneous explosions have been reported at electric substations in Mississippi and Tennessee. The electric grid was already stressed by a persistent heat wave and by damage caused by an unusually strong hurricane that struck the Gulf Coast, several days earlier, knocking out a key corridor for transporting both natural gas and refined petroleum products to the center of the country.

The Department of Energy's Office of Electricity Restoration reports that the outages are due to a cyber attack on the electronic trading platform called SecureTrade, which is used for wholesale trading of electricity. As a result, some transmission utilities have disconnected from SecureTrade and reverted to manual trading of electricity, which cannot keep up with real-time fluctuations in demand. In addition, power generators in the Southeast and Midwest are having difficulty bringing peaking generation units on-line in a timely fashion, due to continuing shortages of natural gas supplies.

SecureTrade, the nexus that connects the transmission grids, is the most vulnerable point in the electric grid. It uses an "on-demand" patching process for updating virus definitions. Initial reports suggest that this process was exploited to bring the system down, thereby crippling wholesale trading of electricity, causing trading to quickly revert to manual and essentially bringing operations to a standstill. Being unable to trade wholesale electricity means that some load-serving entities were unable to serve their customers, and were forced to begin selective load shedding.

> This is a dynamic problem. We're going to live with this for as many years as we can foresee. There also seems to be a surprising amount of uniformity in taking very aggressive, vigorous action; but, I think also a sense that it would be important very quickly thereafter to get public buy-in to it.
>
> **MICHAEL CHERTOFF, CYBER SHOCKWAVE NATIONAL SECURITY ADVISOR**

With the telecommunications outage continuing to spread and many parts of the country now without power, financial markets shut down and panic begins to set in. Political pressure mounts as Congressional leaders urge the President to take sweeping action, including enacting new security regulations. The Secretary of Treasury warns that any number of trading platforms including the New York Stock and the Mercantile Exchanges, could be vulnerable to similar attacks, imperiling the economy even further.

The advisors all reiterate that the greatest danger to the President is not doing enough, rather than doing too much. They all endorse strong measures, including calling out the National Guard and advising the President to invoke war-time authorities. Given the severity of the crisis, the Secretary of Homeland Security notes that the situation has effectively morphed from homeland security to homeland defense, requiring active participation of the military. The advisors agree on the need for cooperation with the private sector, which controls 85 percent of U.S. critical infrastructure, and ultimately decide that the President might have to use his Article II Constitutional powers to nationalize utilities and call out the National Guard.

CONCLUSION

The cyber threat to our national security is real. The U.S. government needs updated policies, legal authorities and operational capabilities to respond to cyber attacks, whether it means defending our networks from intrusion by hackers or securing critical infrastructure. These measures, however, need to be balanced against considerations of privacy, free commerce, and constitutional authority. A national discussion on how to secure our nation's cyberspace and balance these competing concerns is of vital importance. Cyber ShockWave has been the first step in this process. The Bipartisan Policy Center is committed to facilitating dialogue and consensus on this pressing national security issue.

BIPARTISAN POLICY CENTER

1225 I Street NW, Suite 1000, Washington, D.C. 20005
Tel: 202.204.2400 · www.bipartisanpolicy.org

Design by MSDS · MS-DS.com