Department of Homeland Security

CYBER STORM II
Final Report

July 2009

Department of Homeland Security
Office of Cybersecurity and Communications
National Cyber Security Division

EXECUTIVE SUMMARY

The National Cyber Exercise: Cyber Storm II successfully executed on March 10 – 14, 2008 at player locations across the United States, as well as in international partner locations in Australia, Canada, New Zealand, and the United Kingdom. The Department of Homeland Security – National Cyber Security Division (DHS – NCSD) sponsored the exercise to improve the capabilities of the cyber incident response community, encourage the advancement of public-private partnerships within the critical infrastructure sectors, and strengthen the relationship between the federal government and its government partners at the state, local, and international levels.

The primary goal of planning and executing Cyber Storm II was to provide the arena to examine the processes, procedures, tools, and organizations of the cyber response community in response to a multi-sector coordinated attack through, and on, the global cyber infrastructure. The exercise incorporated a wide spectrum of players representing 18 federal agencies, nine states, five countries, interagency coordination bodies, and over 40 private sector companies. The coordinated cyber attacks facilitated incident response from the technical, operational, and strategic perspectives.

Cyber Storm simulated cyber attacks that were focused on critical infrastructure in the Information Technology (IT), Communications, Chemical, and Transportation (specifically Rail and Pipe) sectors and required action from foreign and domestic partners in the cyber response community. Driven by their objectives, the participants shaped the exercise scenarios to assess their response capabilities, facilitate information sharing, and refine cyber security practices. The scenarios focused on three key areas: Internet disruption, communications disruption, and control system issues. All attacks were simulated and no live networks were targeted or affected during the exercise.

This Final Report is a consolidation of findings, observations, and participant inputs gathered throughout the planning and execution phases of Cyber Storm II. It represents the informational foundation for continuing efforts to assess how those findings translate into steps that DHS and the wider player community might take to improve national cyber security in the future.

Key Achievements

Cyber Storm II served as a catalyst for both significant discovery and achievement for the cyber response community. It is important to note that this report simply recounts the proceedings and observations from the Cyber Storm II exercise. As such, it provides an informational foundation that contributes, along with other inputs, valuable data that suggest the kinds of actions that DHS and the wider player community might take to improve national cyber security in the future.

Through the exercise, the player universe:

- Made new and reinforced existing relationships within the cyber response and incident management communities that are essential to the continued development of effective codified processes and procedures in response to cyber attacks.
- Reinforced the importance of public-private partnerships in incident response and highlighted action areas that will enhance this collaboration.
- Discovered alternative means and methods of collaboration that refine cyber response capabilities.
- Informed and effected active play by senior level leadership and decision-makers from participating organizations.

- Isolated and identified specific complexities unique to cyber-related incidents and attacks. These unique attributes of cyber response highlight a fundamental paradigm shift for national level crisis response.
- Exercised information sharing capabilities across multiple boundaries.
- Identified areas and situations that will require further analysis, examination, and development to expand the Nation's cyber response capabilities.

Exercise Structure and Scenario

Cyber Storm II was a scenario-driven exercise characterized by timed simulations and injects designed to stimulate expected player actions required to meet exercise training objectives. The Cyber Storm II exercise scenario was built using adversaries with credible capabilities, both real and fictional. The exercise itself used only imaginary enemies whose political and strategic goals were enhanced or created with only one purpose in mind – to give them a plausible reason to wish to cause direct, indirect, or collateral damage to the organizations who were participating in the exercise.

The scenario was built around a series of cyber attack vectors that fell within the technical capabilities of the adversary set. Occasionally special capabilities were added to the appropriate adversary as planning proceeded in order to address specific participant objectives. Each scenario was then built using these capabilities to create the desired situations and outcomes required to meet the stakeholder objectives. The simulated attacks were sufficiently severe so that participants were required to reach beyond the resources that they control directly and to cooperate with other members of their sector, state and federal governments, as well as their partners and allies around the world. The scenario was not designed to test the technical security of systems, but to exercise the preparedness and resilience of response organizations and their abilities to coordinate their responses effectively across boundaries of jurisdiction and proprietary interest.

Cyber Storm II provided a simulated environment for participating organizations to challenge their cyber response capabilities. This no-fault, non-attribution exercise allowed participants to work out, assess, and ascertain complexities, interdependencies, and potential solutions specific to cyber-related incidents absent the pressure of real-world consequences or fault. The cross-sector nature of the cyber attacks simulated in Cyber Storm II required integrated solutions and cooperation across the cyber response community. Cross-sector attacks provided the conditions for a coordinated response leading to the development of new policies and procedures around these collaborative efforts during such attacks. The nuances of the attacks and their impacts enhanced existing relationships and forged new ones, highlighting the need for and importance of a more synthesized approach to cyber–related incidents. Furthermore, participants examined current policies and procedures at various levels across the public and private sectors, granting participants a holistic view of the interconnected nature of the cyber response community.

The cyber response community gained insight into the interdependencies between cyber activities, physical infrastructures, and economic impacts. This insight underscored the far-reaching effects of the diversity of organizational roles and responsibilities within the cyber response community. An understanding of the complexities involved in the intertwined cyber/non-cyber community can be effectively reached with clear and consistent communication with a full range of security partners, made possible by stronger organizational relationships and formal associations. The experiences, knowledge, and shared perspective gained in Cyber Storm II will have long-lasting impacts on the cyber response community, and its cohesive approach to the continually evolving challenges and complexities of the cyber domain.

Significant Findings

This Final Report is a consolidation of findings, observations, and participant inputs developed throughout the planning and execution phases of Cyber Storm II. The exercise revealed several important findings that have far-reaching impact across all the players, beyond their support of exercise goals and objectives.

The participants agreed that exercises such as the Cyber Storm exercise series are an essential tool to observe preparedness capabilities, and for a broad range of stakeholders and participants to identify areas requiring some measure of attention.

Trends and findings that emerge from the planning and execution of Cyber Storm (and other) exercises are essential to players' and planners' abilities to identify specific processes, procedures, or operational improvements that may correlate to the findings. DHS undertakes this type of identification process, as does the broader player and planner community.

The Cyber Storm exercise series continues to grow in scale and complexity. The player and planner community grows from exercise to exercise. This, together with the fact that one finding or effect can be elicited by a variety of causes, means that seemingly similar findings will emerge out of each exercise. This pattern is desirable and to be expected. The power of these findings lies in how various players and planners initiate improvements and/or action based on how that finding impacts their particular organization.

- **Finding 1: Value of Standard Operating Procedures (SOPs) and Established Relationships.** *Preparation and effective response is significantly enhanced by established and coordinated SOPs and existing relationships in the cyber response community. These SOPs and relationships facilitate rapid information sharing among community members.*

- **Finding 2: Physical and Cyber Interdependencies.** *Cyber events have consequences outside the cyber response community, and non-cyber events can impact cyber functionality. Fully understanding this reality is critical to refining comprehensive contingency plans and response capabilities. It is necessary to continue to converge and integrate response procedures tailored for physical crises with those developed for cyber events. The unique activities related to cyber response activities must be highlighted in cyber response processes and procedures to clearly reflect the inherent differences between cyber response and traditional/physical crisis response activities.*

- **Finding 3: Importance of Reliable and Tested Crisis Communications Tools.** *Tools and related methods developed and deployed for handling crisis communications need further refinement and enhancement. To maximize tools' efficiency and effectiveness during a crisis, the cyber response community needs to examine placement of tools, the impact of tools' capabilities and limitations on response procedures, and identification and authentication protocols used with the tools.*

- **Finding 4: Clarification of Roles and Responsibilities.** *Substantial improvements since Cyber Storm I were observed in the interagency integration and coordination of cyber event response with senior leadership across interagency boundaries. Continued development and clarification of roles, responsibilities, and communication channels should further enhance our capabilities.*

- **Finding 5: Increased Non-Crisis Interaction.** *Regular, non-crisis related communications and interaction within the cyber response community through established means would solidify communications paths, strengthen relationships, and clarify organizational cyber incident response roles. Institutionalizing these pathways in non-crisis situations should solidify their role in real world response capabilities.*

- **Finding 6: Policies and Procedures Critical to Information Flow.** *The maturity and refinement of each organization's policies and procedures correlated directly to the efficiency and* *effectiveness of information flow between organizations in the exercise. Some key relationships continue to be characterized by one-way communications and unmet expectations.*

- **Finding 7: Public Affairs Influence During Large-Scale Cyber Incidents.** *An effective and organized public affairs presence has been developed since Cyber Storm I. During a cyber* event, *public affairs can be used to educate and inform the public through clear, actionable information validated by technical experts and entities such as Sector Coordinating Councils (SCCs) and sector Information Sharing and Analysis Centers (ISACs).*
- **Finding 8: Greater Familiarity with Information Sharing Processes.** *Cyber response communities understand procedures exist to enable information sharing across classification levels and proprietary boundaries. Exercise findings suggest the value of continued effort devoted to training, use of existing procedures, and familiarity with designation authorities to allow more rapid response and information flow through various mediums.*

This page intentionally left blank.

INTRODUCTION

The Department of Homeland Security – National Cyber Security Division (DHS – NCSD) established the National Cyber Exercise Program to provide DHS with the capability to plan and conduct a series of "cyber exercises to build upon previous similar terrorist attacks on the Nation's cyber infrastructure to demonstrate the impact of a cyber-based attack on critical infrastructures and to highlight the interdependencies among critical infrastructures and underscore the requirement for enhanced cross-sector cooperation." *(FY2005 Homeland Security Appropriations Act [Public Law No: 108-334])* NCSD conducted the first National Cyber Exercise, dubbed Cyber Storm, in February 2006.

The first government-led cyber security full-scale exercise of its kind, Cyber Storm I was a coordinated effort among participating federal and state governments, private sector partners, and international entities, to exercise response, coordination, and recovery mechanisms to a simulated cyber event. Cyber Storm II brought together a similarly diverse player set, including organizations who participated in Cyber Storm I and organizations new to the cyber exercise community. Returning participants contributed significantly to the goals and complexity of Cyber Storm II. New planners added fresh perspectives, points of view, and objectives to the planning and execution of the exercise, enhancing the scenarios. All planners, whether they had participated in previous cyber exercises or not, developed additional insight on the means and methods needed to improve their organization's own cyber security and response capabilities. Subject matter experts and practitioners from over 40 private sector companies and organizations, 18 Federal Departments and Agencies, nine states, and five countries were involved in Cyber Storm II's planning and execution.

This Final Report is a consolidation of findings, observations, and participant inputs gathered throughout the planning and execution phases of Cyber Storm II. As such, it is not intended as an impact analysis of the observations and findings that emerged from the planning and execution of the exercise. Rather, it is the informational foundation for continuing efforts to assess how those findings translate into steps that DHS and the wider player community might take to improve national cyber security in the future. The report establishes a baseline reference resource for stakeholders and planners in developing future exercises and refining processes and procedures that enable effective collaboration and coordinated incident response efforts. The purpose of this report is to capture attributes of existing policies, procedures, capabilities, or resources that became evident during exercise execution. Through this process, players and planners can identify factors that work well, those that require further development, elements that constitute a gap or overlap, or those things that necessarily prompt an action or effort not previously foreseen. This report also serves as a reference guide for continued enhancement of cyber incident response, a catalyst for continued cyber defense refinement, and a guide for the development and execution of future national cyber exercises among DHS and its stakeholders.

Finally, it is important to note that while this report represents these findings and direct outputs of the exercise, the collaboration that goes into planning and coordinating an exercise of this magnitude affords players and planners the significant and unique opportunity to look closely at their plans, procedures, relationships, and information sharing mechanisms as a part of the planning process. The task of planning for and executing Cyber Storm serves as an invaluable catalyst for all involved to build and refine the very same processes, procedures, relationships, and information sharing networks that are used not only in exercise play, but also in real-world cyber-incident response activities. These and other factors must be considered when characterizing the full impact of an event like the Cyber Storm exercise series.

BACKGROUND

PURPOSE

Cyber Storm II was designed to support the strategic vision of DHS, and the NCSD - a part of the National Protection and Programs Directorate's (NPPD) Office of Cyber Security and Communications (CS&C), and the *President's National Strategy to Secure Cyberspace*. This vision includes the improvement of the Nation's cyber incident response capability, the encouragement of public-private partnerships within the critical infrastructure sectors, and strengthening the ties between the Federal Government and its government partners at the state, local, and international levels.

The primary goal of planning and executing Cyber Storm II was to provide the arena to examine the processes, procedures, tools, and organizations in response to a multi-sector coordinated attack through, and on, the global cyber infrastructure. The exercise incorporated a wide spectrum of players representing federal, state, and international governments, interagency coordination bodies, and the private sector. The coordinated cyber attacks facilitated incident response from the technical, operational, and strategic perspectives.

Cyber Storm II was planned over an 18-month period in close coordination with and driven by its stakeholders and participants, whose involvement was based on their roles in the global cyber incident response community. The exercise focused on carefully tailored cyber scenarios that ultimately escalated to a level requiring a coordinated international response. The Cyber Storm II exercise focused on communications, cooperation, and coordination among the various elements of the global cyber incident response community.

SCOPE

Cyber Storm II was designed to exercise public and private sector coordination for prevention of, response to, and recovery from coordinated cyber attacks, and to assess policy issues that might either hinder or improve cyber security preparedness. Given the limits on the cyber incident response community's time and financial resources, exercise parameters focused on key stakeholder objectives and cross-sector collaboration.

Simulated cyber attacks focused on critical infrastructure in the Information Technology (IT), Communications, Chemical, and Transportation (specifically Rail and Pipe) sectors and required action from foreign and domestic partners in the cyber response community. Driven by their objectives, the participants shaped the exercise scenarios to assess their response capabilities, facilitate information sharing, and refine cyber security practices. The scenarios focused on three key areas: Internet disruption, communications disruption, and control system issues. For example, significant Internet disruption that impacted several top-level domains such as ".com," ".net," and ".gov" made Internet access difficult, especially for state participants whose websites became unreliable for information dissemination. Additionally, communications degradation caused erratic telephone service across the country, affecting players' ability to call other participants or critical services, such as 911. The scenarios in Cyber Storm II allowed a broad focus on the impacts across critical infrastructure sectors and demonstrated how information and communications technology is a cross-cutting component upon which all other sectors rely.

CYBER STORM II OBJECTIVES

DHS – NCSD, in coordination with exercise planners and stakeholders, created the following objectives for Cyber Storm II:

- Examine the capabilities of participating organizations to prepare for, protect from, and respond to the effects of cyber attacks;

- Exercise senior leadership decision making and interagency coordination of incident responses in accordance with national level policy and procedures;
- Validate information sharing relationships and communications paths for the collection and dissemination of cyber incident situational awareness, response, and recovery information; and
- Examine the means and processes to share sensitive and classified information across standard boundaries in safe and secure ways without compromising proprietary or national security interests.

PLANNING AND EXECUTION

Cyber Storm II planning occurred over an 18-month period that was marked by robust information sharing, public-private partnerships, and cross-sector coordination. A carefully executed vetting process, developed from the experiences of Cyber Storm I, regional cyber exercises, and other DHS-NCSD sponsored events, facilitated the identification of key participants and defined the exercise parameters (sectors, nations, companies, scenario depth, etc.). Measures were implemented to ensure that the participants could share information freely without the fear of compromising the proprietary knowledge of the participating organizations or the safety of the critical infrastructure. The process included a series of planning conferences, each with specific goals, building toward exercise execution. The following table summarizes the planning conferences:

Date	Conference	Purpose
December 2006	Concept Development Conference (CDC)	Establish exercise scope and objectives and implement planning group organizational structure
March 2007	Initial Planning Conference (IPC)	Finalize participant objectives, frame scenario and adversary
July 2007	Mid-term Planning Conference (MPC)	Establish primary scenario elements and assign detail scenario development tasking
December 2007	Final Planning Conference (FPC)	Report progress on scenario event details, develop comprehensive cross-sector event timeline, and define player universe, communications paths, and data collection requirements
January 2008	Final Master Scenario Event List (MSEL) Conference (FMC)	Execute dry-run of entire scenario, train field observer/controllers, finalize exercise control procedures, and establish protocol for pre-exercise (PRE-EX) period
February 2008	PRE-EX	Provide historical perspective in preparation for the exercise and encourage public-private sector engagement

Planners used the periods of time between conferences to engage in extensive interaction and collaboration with other each other. They met as individual sector working groups and also in small combined groups to refine cross-sector interactions and impacts.

The Cyber Storm II exercise was conducted in March 2008. Exercise Control, located at U.S. Secret Service Headquarters in Washington, DC, served as the central coordinating body. Over 100 individuals representing key stakeholders, infrastructure sectors, states, and various subject matter experts monitored exercise play in their respective organizations from Exercise Control through regular contact with onsite observer/controllers who monitored player responses. In addition to sending scenario information to players, individuals within Exercise Control responded to requests for information, coordinated real-time scenario inputs, and supported all stakeholders to ensure objectives were met. Subject matter experts within Exercise Control simulated entities that were not represented in the player set. On the last day of the exercise, Exercise Control members and observer/controllers participated in a post-exercise discussion to identify potential findings and improvement areas. Exercise planners met during the weeks following the exercise to continue discussions on findings, observations, and outcomes.

CYBER STORM II SCENARIO OVERVIEW

In March 2008, a cadre of bad actors leveraged their collective capabilities to mount a coordinated cyber attack on a global scale. Although primary motives differed among the entities, a sophisticated network of relationships enabled the adversary to degrade Internet connectivity, disrupt industrial functions, and ultimately erode confidence in everyday communications. The adversary cultivated relationships with unaffiliated opportunistic actors. Due to their critical nature and perceived vulnerabilities, the adversary specifically targeted several critical infrastructure sectors, along with state and federal agencies, the media, and foreign nations.

The adversary was acutely aware that attacks on IT and Communications interests would not only impact those sectors but would also result in cascading conditions suffered by other targets. By generating counterfeit digital certificates, the adversary directed unknowing web users to “spoofed” websites where funds were extorted and personal information was mined. Coordinated attacks on domain name servers and telecommunications router infrastructure resulted in a distributed denial of service and unreliable telephony. Users were intermittently unable to access websites, send email, and make phone calls. Victims of the attack were forced to explore alternative methods of communication during the disruptions.

While the world experienced widespread impacts of attacks on the IT and Communications sectors, the adversary also targeted individual industries from other critical infrastructure sectors. The adversary’s intent was to cause cascading disruptions stemming from specific, focused attacks.

Meanwhile, government agencies experienced the effects of the coordinated cyber attack. At the state level, online services were infiltrated by the adversary to defraud local citizens and compromise trustworthiness. At the federal level, several agencies were impacted by communications disruptions. The Department of Defense (DoD), for example, faced severe degradation of their mobile device service and the exfiltration of sensitive information. Foreign governments around the world were victimized by similar attacks causing severe disruptions and communications challenges. As the crisis persisted, the media struggled to publish timely and accurate information.

As the events unfolded, law enforcement and intelligence agencies gathered information and responded as necessary. In coordination with the impacted private sector entities and other government agencies, law enforcement and the Intelligence Community worked to halt attacks and restore confidence in the Internet. All participating organizations relied on trusted relationships and forged new communications paths to share information and build and pass along situational awareness.

SIGNIFICANT FINDINGS

The four overarching Cyber Storm II objectives were examined through the exercise planning and execution period. A number of findings were identified through observations by participants and observer/controllers. This section provides the exercise's significant findings and supporting observations.

FINDING 1: VALUE OF STANDARD OPERATING PROCEDURES (SOPS) AND ESTABLISHED RELATIONSHIPS

Preparation and effective response is significantly enhanced by established and coordinated SOPs and existing relationships in the cyber response community. These SOPs and relationships facilitate rapid information sharing among community members.

1.1 The maturation and detail of SOPs for cyber response improved dramatically since Cyber Storm I. Cyber Storm II allowed players, both returning and new, to identify opportunities to integrate and standardize plans between organizations.

1.2 The coordinated attacks simulated during Cyber Storm II highlighted the importance of establishing relationships between organizations prior to a crisis or attack. Some participants expressed a need for greater familiarity with the roles, responsibilities, and requirements for each organization involved in incident response for the sake of context. Understanding the interconnectedness and cause/effect relationships between actions taken by each organization would help to maintain broad situational awareness and galvanize a holistic approach to cyber response.

Observations:

- Exercise players changed their respective organizational alert levels over the course of the exercise in response to scenario injects and player actions. While these responses were generally in accordance with an established SOP, they highlighted the disconnectedness between the alert systems and the lack of general understanding of the range, meaning, and implications of alert levels to external organizations. In many cases, the announcement of changes in alert level failed to fully communicate meaningful information to the broader cyber response community, even those familiar with the organization's SOPs.
  - While some of the SOPs established a process for changing alert levels, some participants that were external to the organization noted that they often required more context to fully understand the significance of the alert level change. Participants noted that further clarification on how the alert systems aligned to one another might reduce confusion regarding the various alert levels (e.g., United States Computer Emergency Readiness Team's [US-CERT's] Severity Level 4, DHS Homeland Security Advisory System [HSAS] threat level Orange [high], IT Information Sharing and Analysis Center's [IT-ISAC's] AlertCon 2, and DoD's Information Operations Condition [INFOCON] 3).   Clarifying the alignment of alert systems could enhance an incident responders' ability to communicate the significance of alert levels to decision-makers.
  - Having an understanding of the significance and requirements of each individual alert level would greatly enhance situational awareness among response partners and improve the effectiveness and efficiency of their preparedness and response strategies.
- Exercise participants universally commented on the direct correlation between established relationships and successful incident management practices. Formal relationships allowed exercise participants to leverage the knowledge, capabilities, and resources of known and recognized

response partners to prepare for and mitigate the effects of cyber attacks. Informal relationships also provided an avenue for troubleshooting and resolving the cyber incidents with the group's collective information and knowledge.

FINDING 2: PHYSICAL AND CYBER INTERDEPENDENCIES

Cyber events have consequences outside the cyber response community and non-cyber events can impact cyber functionality. Fully acknowledging this reality is critical to refining comprehensive contingency plans and response capabilities. It is necessary to continue to converge and integrate response procedures tailored for physical crises and those developed for cyber events. The unique activities related to cyber response activities must be highlighted in cyber response processes and procedures to clearly reflect the inherent differences between cyber response and traditional physical/crisis response activities.

2.1 In the event of any complex cyber incident, cyber-specific response actions must be coordinated across the critical infrastructure protection community. Due to the longer history and accumulated depth of experience with physical threats, some incident response SOPs triggered by cyber threats tended to be oriented toward the mitigation of and response to physical threats. These mitigation techniques often include increased physical security measures that may or may not be relevant during a cyber incident. More tailored and coordinated security response measures are needed to address actions and considerations that are unique to cyber incidents.

2.2 Procedures for escalating incidents to higher authorities and standards for establishing heightened alert levels tend to use concepts and methods appropriate for single-location, physical events with locally measurable physical impacts. The conditions that trigger physical emergency response activities are clearly defined. Cyber parallels to these triggering conditions are not clearly understood outside of the cyber response community.

2.2.1 Elements of a cyber attack are not always easily discernable until viewed in relation to other factors. Whereas physical response procedures are often driven by discrete and quantifiable "events", the incremental and distributed nature of the cyber threat landscape must be reflected in cyber incident response plans and procedures

2.3 Physical and cyber attacks are rarely mutually exclusive. Physical attacks impact cyber infrastructure and cyber disruptions can have severe physical consequences. An "all hazards" approach to incident response could strengthen preparedness and mitigation efforts.

Observations:

- Changes to HSAS threat levels trigger the implementation of specific protective measures based on the targeted sector or sub-sector. Many of these protective measures were seen as being geared towards physical security, and not as focused on the advancement of cyber security. Developing additional cyber-specific guidance that correlates to relevant physical security controls could enhance the incident response as well as reinforce the interconnectedness of the concepts and required implementation.
- Prior to Cyber Storm II, some exercise participants had not exercised responding to a coordinated cyber attack. Through exercise play, these organizations increased their awareness of the correlation between physical and cyber events and identified knowledge gaps. As an example, the potential cyber consequences of seemingly physical events, such as laptop theft, helped these organizations gain a better understanding of the interdependencies between cyber and non-cyber events.

- Some private sector partners experienced reluctance to activate contingency plans as a response to cyber attacks. These plans are often geared toward physical events and do not encompass a more inclusive incident response framework. Some private sector partners use a joint response team incorporating physical and cyber security experts, which could serve as a valid model in the future.

FINDING 3: IMPORTANCE OF RELIABLE AND TESTED CRISIS COMMUNICATIONS TOOLS

Tools and related methods developed and deployed for handling crisis communications need further refinement and enhancement. To maximize tools' efficiency and effectiveness during a crisis, the cyber response community needs to examine placement of tools, the impact of tools' capabilities and limitations on response procedures, and identification and authentication protocols used with the tools.

3.1 The effective use of crisis communications and collaboration tools depends heavily on the location of, access to, and familiarity of users with these tools. Various tools are available to the critical infrastructure protection and response community. However, many players lacked the fundamental knowledge to access and use the tools. Increased awareness of the location of these devices, distribution of the access cards, and key operational procedures could enhance the tools' effectiveness for the cyber response community.

3.2 The scenario in Cyber Storm II highlighted the likely confusion during a serious cyber attack that can erode trust and confidence in both conventional and alternative communication paths. In a crisis environment, players discussed the need to embed effective communication tools with trustworthy validation mechanisms. To address this issue, organizations discussed exploring authentication protocols for primary and back-up communication methods that could promote trust and mitigate the spread of misinformation.

<u>Observations:</u>

- Participants identified limitations related to specific tools available to the critical infrastructure community. Some participants realized that the tools were placed in inconvenient locations that limited responders' access to them. Others noted that they were not familiar enough with the operational processes needed to use the tools. Many organizations are reevaluating their tools to address the limitations and issues discovered during the planning process and exercise execution.
- Participants recognized a need to establish additional security protocols for communication prior to a crisis situation. Mechanisms to authenticate information sources and verify reports and alerts could help ensure trusted communication and relationships during a crisis.
- The varied success of communication methods across the player spectrum highlighted the opportunity for public and private sector dialogue on available systems and tools. Further exploration of current government crisis communication capabilities and technologies already employed by private industry could enhance the viability and depth of alternative communication protocols. Standardization of communication methods within the response community could alleviate confusion as to which method should be used in a crisis and facilitate the development of crisis communication best practices in the cyber response community.

FINDING 4: CLARIFICATION OF ROLES AND RESPONSIBILITIES

Substantial improvements since Cyber Storm I were observed in the interagency integration and coordination of cyber event response with senior leadership across interagency boundaries. Continued development and clarification of roles, responsibilities, and communication channels should further enhance our capabilities.

4.1 The relationship and responsibilities of Sector Coordinating Councils (SCCs), ISACs, the US-CERT, and the National Cyber Response Coordination Group (NCRCG), and the Crisis Action Team (CAT) were interpreted differently and resulted in varying expectations across the spectrum of play. While significant improvements in information flow were observed when compared to previous interactions, participants generally agreed that recurrent clarifications about roles and responsibilities, as well as the appropriate entry points to share information based on these roles and responsibilities, should continue. Once roles and responsibilities are clearly understood, organizations can articulate those responsibilities in existing and new SOPs. DHS can help to facilitate the dialogue among these coordinating organizations to enhance their cooperation during a cyber event.

4.2 National level policies and procedures for crisis response and critical infrastructure protection require clarification with respect to cyber events. Communications between senior leadership that normally would work smoothly in the face of a physical disaster were hampered by the scarcity of cyber concepts, use of cyber jargon, and ambiguities in critical infrastructure response doctrine.

Observations:

- The NCRCG and the CAT have distinct roles in the cyber response community as defined by their respective SOPs, but these roles were unclear to many exercise participants. NCRCG served as a strategic advisory body to the CAT, the operational lead for government-led incident response. While the operational lead role was clear at the strategic level, responsibilities for specific operational tasks were vague at times. This ambiguity resulted in some confusion among entities that interact with these organizations.
- US-CERT, as the operational cyber lead at the national level, provided technical subject matter expertise to the NCRCG and the CAT, intended to help the CAT articulate the cyber issues to senior leadership. Some exercise partners, including those from the private sector, noted that the NCRCG could have leveraged private sector IT experts, via US-CERT, for additional technical insights. The NCRCG could have then provided that information to the CAT adding perspective on impact assessments and response requirements.

FINDING 5: INCREASED NON-CRISIS INTERACTION

More frequent, non-crisis related communications and interaction within the cyber response community through established means would solidify communications paths, strengthen relationships, and clarify organizational cyber incident response roles. Institutionalizing these pathways in non-crisis situations should solidify their role in real world response capabilities.

5.1 Many exercise participants developed stronger relationships with incident response partners and counterparts as they interacted during the Cyber Storm II lifecycle. The planning and execution phases provided insights to the roles and responsibilities of various organizations in a crisis response situation and allowed participants to leverage the capabilities and expertise of other organizations.

5.2 Building on the experience gained from Cyber Storm I, other cyber exercises, and intervening real-world events, the interaction and coordination between the public and private sector in a cyber crisis have continued to improve significantly. These relationships would continue to benefit from joint public-private coordination activities such as integrating and harmonizing response plans; refining appropriate security measures associated with threats and attacks; and cross-training and joint-training of personnel to enhance understanding and synchronize expectations. Cyber Storm II also highlighted specific relationships, such as between the NCRCG and private sector partners, that should be explored and leveraged to improve cyber preparedness.

<u>Observations:</u>

- The planning process gave private companies an opportunity to gain working exposure to DHS policies and procedures as well as develop a better understanding of their implications for public–private sector interactions. This knowledge helped participants adapt to response needs and capabilities of both the government and industry during exercise play, resulting in stronger collaboration as the players responded to cyber attacks.
- Participants noted the need for enhanced understanding of the roles and responsibilities of the agencies with which they interacted, especially in those areas that involved unfamiliar activities. For example, in areas where state government and the private sector participants found themselves interacting with federal law enforcement, a better understanding of the jurisdiction and objectives of each law enforcement group would have streamlined interactions and improved information sharing.

FINDING 6: POLICIES AND PROCEDURES CRITICAL TO INFORMATION FLOW

The maturity and refinement of each organization's policies and procedures correlated directly to the efficiency and effectiveness of information flow between organizations in the exercise. Some key relationships continue to be characterized by one-way communications and unmet expectations.

6.1 The participants relied on the sector-specific ISACs and the US-CERT as focal points for sharing and requesting information. Participants noted that the ISACs are at various maturation levels and continue to fully develop their operational capabilities by learning from real world incidents and exercises. Increased attention to analysis prior to sharing information coupled with adequate staffing to ensure information is shared in a timely fashion could enhance situational awareness and facilitate a common operating picture. This learning process strengthens relationships through time and experience.

6.2 Participants have become more familiar with the roles and interactions among some ISACs and SCCs. Frequent conference calls between participating ISACs and their constituents, as well as daily ISAC-to-ISAC calls, were central to the crisis response. Some sectors do not have an ISAC, but they have organizations, including their SCC, that perform similar functions. Participants acknowledged that these organizations could benefit from increased interaction with the other sectors' ISACs and SCCs.

6.3 Unanticipated concerns and sensitivities impact cyber response activities. While conducting response activities during the exercise, one private sector entity appeared uncertain about legal aspects of information sharing. The entity's uncertainty resulted in some delay and circumspection in providing the information. The entity's uncertainty created an impediment to efficient collaboration during the exercise. The incident exposed the need for organizations to proactively work with their legal counsel to obtain guidance and instruction on the laws and regulations applicable to information sharing.

<u>Observations:</u>

- While many organizations participating in both Cyber Storm exercises have demonstrated increased cyber response capabilities since 2006, Cyber Storm II illuminated additional areas for improvement. One participant group noted that some key internal teams required additional staff resources to respond to the time sensitive crisis situation. The exercise helped them identify specific areas that could benefit from additional personnel. Adjusting the staffing model was seen as a way to potentially alleviate some information flow issues that they experienced as well as to enable them to better meet the expectations of the cyber response community.

- Despite improvements in information flow, some perceptions persist that 1) organizations that share information receive little feedback on how their information is used and 2) the information flow is largely unidirectional. Clarity in the processes and procedures surrounding the government coordination bodies may be beneficial to organizations that rely on them.
- The civilian CERTs of Australia, Canada, New Zealand, UK, and U.S. were able to share important information during the exercise over their designated collaboration tool. The collaboration tool was created in response to information sharing issues identified in Cyber Storm I, and their procedures were updated to include guidelines for portal use. The maturation of these procedures significantly enhanced the countries' collective situational awareness in the exercise.
- Scenario play during Cyber Storm II highlighted the impact that unanticipated concerns and uncertainty about ramifications of response actions can have on the effectiveness of critical information sharing during a crisis. One private company identified a solution to a prevalent cyber attack in the exercise, but then expressed uncertainty about legal aspects surrounding information sharing. The company ultimately shared the solution verbally. However, the lack of familiarity with the legal protections available for information sharing potentially delayed the distribution of the solution.

FINDING 7: PUBLIC AFFAIRS INFLUENCE DURING LARGE-SCALE CYBER ATTACKS

An effective and organized public affairs presence has developed since Cyber Storm I. During a cyber event, public affairs can be used to educate, inform, and direct the public through clear, actionable information validated by technical experts and entities such as Sector Coordinating Councils (SCCs) and sector Information Sharing and Analysis Centers (ISACs).

7.1 The media can serve as a source to distribute concise and accurate information about a cyber attack in order to provide situational awareness and avoid misinformation and inappropriate actions that might result. Publicly released information developed in collaboration among public affairs professionals, appropriate technical specialists, and subject matter experts can be used to accurately communicate the implications of a cyber attack.

7.2 Incorporating cyber messages into crisis communications plans and materials provides a foundation for initiating a public affairs response to a cyber attack. This cyber messaging can provide technical background on the physical manifestations of a cyber attack as well as provide actionable information.

Observations:

- Both public and private sector public affairs players leveraged and enhanced relationships with technical experts during the exercise. In some cases, technical experts were integrated into the public affairs team to provide context for public affairs outreach. Other players noted that technical experts reviewed their publicly released materials prior to distribution. Expert reviews were critical as some press releases were inadvertently edited for perceived clarity, yet the edits changed the technical meaning of the information. This technical expertise was crucial in understanding and communicating the impact of the cyber attack.
- Players noted that developing public affairs materials (message guides, press releases, Frequently Asked Questions, etc.) in preparation for the exercise helped sharpen and articulate their organizational cyber security posture. Several players used the exercise platform for players to exercise their crisis communications plans, in some cases globally, to understand how their existing

materials can be applied to a cyber attack.

FINDING 8: GREATER FAMILIARITY WITH INFORMATION SHARING PROCESSES

Cyber response communities understand procedures exist to enable information sharing across classification levels and proprietary boundaries. Exercise findings suggest the value of continued effort devoted to training, use of existing procedures, and familiarity with designation authorities to allow more rapid response and information flow through various mediums.

8.1 Time-sensitive, critical information was successfully disseminated throughout the cyber watch, warning, and response community in multiple scenarios. Exercise participants shared information across various boundaries and through specific communities of interest utilizing standard communication pathways.

8.2 The upward information flow from the private sector to the federal law enforcement and intelligence communities proved to be more challenging despite some success with the downward information flow from the federal communities to the private sector. Cyber incident responders still need greater clarity on the mechanics of the two-way communication paths between public and private sectors so that those processes can be included in private sector partners' policies and procedures when appropriate.

8.3 The law enforcement and intelligence communities, the state governments, and the private sector conducted extensive crisis watch, warning, and response actions. However, the need for continued coordination was noted by players to ensure a balance between the short-term goals (e.g., addressing the immediate crisis, reconstituting business processes with minimal disruption) and the long-term goals (e.g., establishing attribution, apprehending the perpetrators, gathering information on potential threats).

Observations:

- International military and intelligence communities shared classified information with their U.S. counterparts regarding the report of a potential physical attack with significant cyber consequences. This threat tested players' abilities to share information across multiple boundaries and at multiple classification levels. Players were able to identify the necessary procedures to disseminate the information from the intelligence community to the critical infrastructure operators without compromising national security. This scenario also highlighted the need for more frequent training and increased awareness of declassification procedures and requirements to ensure actions that are more expedient during a crisis.
- While the Cyber Storm II adversaries' activities were largely criminal acts, private sector players often focused on an incident's direct effect on their business rather than realizing the need to report the crime to law enforcement officials and to treat the situation and any related "evidence" accordingly. Short term prioritization of system reconstitution and business continuity is understandable, especially since the players did not always realize that the incidents could be a part of broader criminal activity and that they might be in possession of information and/or evidence that could further a criminal investigation. As the exercise played out and situational awareness improved, private sector partners recognized the need to consider engaging law enforcement earlier in the incident response process. Organizations also observed the need to develop relationships between law enforcement and private companies to increase understanding of their respective roles and responsibilities as well as facilitate reporting and information sharing.
- Cyber Storm II scenarios enabled national and international level law enforcement and intelligence data to be synthesized for use at the state level. Participating state fusion centers used the synthesized information to reduce or mitigate impending threats to state and local communities.

Working in conjunction with Federal Bureau of Investigation (FBI) field offices, the fusion centers and state police successfully facilitated information sharing with multiple state governments and across law enforcement jurisdictions.

CONCLUSIONS

Cyber Storm II was a catalyst for significant examination of processes and procedures for the cyber incident response community. An objectives-based, stakeholder-driven scenario caused players to evaluate their response capabilities in a different light yet in a safe environment, providing substantial value to their organizations. While exercise planners identified various strengths and weaknesses within their respective organizations, analyzing trends across the full player spectrum yielded a collective set of findings that highlight the progress made through participating in cyber-dedicated exercises, evaluating real world events, and increasing cyber security awareness. These findings also highlight potential areas for improvement to increase overall cyber security preparedness. DHS-NCSD uses these findings to then assess the implications and impacts from its perspective as a leader in the cyber response community to identify steps that can be taken to address them and make improvements in its own operations. DHS also engages other exercise participants to encourage them to undertake a similar analysis and follow-on actions.

PARTICIPATING ORGANIZATIONS

Central Intelligence Agency

Chemical Sector

- American Chemistry Council
- 12 Companies

Commonwealth of Pennsylvania

Commonwealth of Virginia

Department of Commerce

- National Telecommunications & Information Administration

Department of Defense

- Asst Secretary of Defense/Networks and Information Integration
- Defense Information Systems Agency/Joint Interoperability Test Command
- Defense Intelligence Agency
- Joint Staff
- Joint Task Force – Global Network Operations
- Marine Corps Network Operations and Security Command
- U.S. Northern Command
- U.S. Strategic Command
- U.S. Transportation Command

Department of Energy

- Office of the Chief Information Officer
- Los Alamos National Laboratory
- Pacific Northwest National Laboratory

Department of Health and Human Services

Department of Homeland Security

- Customs and Border Protection
  - Security Operations Center
- National Protection and Programs Directorate
  - Office of Cyber Security and Communications
    - Nation Cyber Security Division/US-CERT
    - National Communications System
  - Office of Infrastructure Protection
    - National Infrastructure Coordinating Center
    - Partnership Outreach Division
    - Chemical & Nuclear Preparedness & Protection Division
- Office of Intelligence and Analysis
  - Homeland Infrastructure Threat and Risk Analysis Center
- Office of Operations Coordination
  - DHS Crisis Action Team
  - National Operations Center
- Office of Public Affairs
- Transportation Security Administration
  - Transportation Sector Network Management
    - Exercise Evaluation Branch
    - Freight Rail
    - Pipeline Security
    - IT Security
- U.S. Secret Service

Department of Justice

- Computer Crime and Intellectual Property Section
- Federal Bureau of Investigation/Cyber Division

Department of State

- Bureau of Diplomatic Security

Department of Transportation

- Federal Aviation Administration
- Pipeline and Hazardous Materials Safety Administration

Director for National Intelligence

- Intelligence Community Incident Response Center

ISACs

- Communications ISAC
- Electricity Sector ISAC
- Financial Services ISAC
- IT-ISAC
- Multi-State ISAC
- Public Transportation ISAC
- Research and Education Networking ISAC
- Surface Transportation ISAC
- Water ISAC

IT Sector

- Sector Coordinating Council
- 15 Companies

Interagency

- NCRCG

International Lead Participants

- Canada – Public Safety Canada
- United Kingdom – Centre for the Protection of National Infrastructure
- Australia – Attorney-General's Department
- New Zealand – Centre for Critical Infrastructure Protection

National Security Agency

State of California

State of Colorado

State of Delaware

State of Illinois

State of Michigan

State of North Carolina

State of Texas

Tennessee Valley Authority

Transportation Sector

- 2 Pipeline Companies
- 3 Railroad Companies

ACRONYMS AND ABBREVIATIONS

Acronym/Abbreviation	Full Text
CAT	Crisis Action Team
CDC	Concept Development Conference
CERT	Computer Emergency Response Team
DHS	Department of Homeland Security
DHS/NCSD	Department of Homeland Security/National Cyber Security Division
DNS	Domain Name Service
DoD	Department of Defense
FBI	Federal Bureau of Investigation
FMC	Final MSEL Planning Conference
FOUO	For Official Use Only
FPC	Final Planning Conference
HSAS	Homeland Security Advisory System
HSPD	Homeland Security Presidential Directive
INFOCON	Information Operations Condition
IPC	Initial Planning Conference
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MPC	Midterm Planning Conference
MSEL	Master Scenario Event List
NCRCG	National Cyber Response Coordination Group
OMB	Office of Management and Budget
PRE-EX	Pre-Exercise
SCC	Sector Coordinating Council
SOP	Standard Operating Procedure
U.S.	United States
UK	United Kingdom
US-CERT	United States Computer Emergency Readiness Team