

## 8. Physical and Cyber Security Aspects of the Blackout

### Summary

The objective of the Security Working Group (SWG) is to determine what role, if any, that a malicious cyber event may have played in causing, or contributing to, the power outage of August 14, 2003. Analysis to date provides no evidence that malicious actors are responsible for, or contributed to, the outage. The SWG acknowledges reports of al-Qaeda claims of responsibility for the power outage of August 14, 2003; however, those claims are not consistent with the SWG's findings to date. There is also no evidence, nor is there any information suggesting, that viruses and worms prevalent across the Internet at the time of the outage had any significant impact on power generation and delivery systems. SWG analysis to date has brought to light certain concerns with respect to: the possible failure of alarm software; links to control and data acquisition software; and the lack of a system or process for some operators to view adequately the status of electric systems outside their immediate control.

Further data collection and analysis will be undertaken by the SWG to test the findings detailed in this interim report and to examine more fully the cyber security aspects of the power outage. The outcome of Electric System Working Group (ESWG) root cause analysis will serve to focus this work. As the significant cyber events are identified by the ESWG, the SWG will examine them from a security perspective.

### Security Working Group: Mandate and Scope

It is widely recognized that the increased reliance on information technology (IT) by critical infrastructure sectors, including the energy sector, has increased their vulnerability to disruption via cyber means. The ability to exploit these vulnerabilities has been demonstrated in North America. The SWG was established to address the cyber-related aspects of the August 14, 2003, power outage. The SWG is made up of U.S. and

Canadian Federal, State, Provincial, and local experts in both physical and cyber security. For the purposes of its work, the SWG has defined a "malicious cyber event" as the manipulation of data, software or hardware for the purpose of deliberately disrupting the systems that control and support the generation and delivery of electric power.

The SWG is working closely with the U.S. and Canadian law enforcement, intelligence, and homeland security communities to examine the possible role of malicious actors in the power outage of August 14, 2003. A primary activity to date has been the collection and review of available intelligence that may relate to the outage.

The SWG is also collaborating with the energy industry to examine the cyber systems that control power generation and delivery operations, the physical security of cyber assets, cyber policies and procedures, and the functionality of supporting infrastructures-such as communication systems and backup power generation, which facilitate the smooth-running operation of cyber assets-to determine whether the operation of these systems was affected by malicious activity. The collection of information along these avenues of inquiry is ongoing.

The SWG is coordinating its efforts with those of the other Working Groups, and there is a significant interdependence on the work products and findings of each group. The SWG's initial focus is on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. The outcome of ESWG analysis will serve to identify key events that may have caused, or contributed to, the outage. As the significant cyber events are identified, the SWG will examine them from a security perspective. The amount of information for analysis is identified by the ESWG as pertinent to the SWG's analysis is considerable.

Examination of the physical, non-cyber infrastructure aspects of the power outage of August 14, 2003, is outside the scope of the SWG's analysis.

Nevertheless, if a breach of physical security unrelated to the cyber dimensions of the infrastructure comes to the SWG's attention during the course of the work of the Task Force, the SWG will conduct the necessary analysis.

Also outside the scope of the SWG's work is analysis of the cascading impacts of the power outage on other critical infrastructure sectors. Both the Canadian Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) and the U.S. Department of Homeland Security (DHS) are examining these issues, but not within the context of the Task Force. The SWG is closely coordinating its efforts with OCIPEP and DHS.

## Cyber Security in the Electricity Sector

The generation and delivery of electricity has been, and continues to be, a target of malicious groups and individuals intent on disrupting the electric power system. Even attacks that do not directly target the electricity sector can have disruptive effects on electricity system operations. Many malicious code attacks, by their very nature, are unbiased and tend to interfere with operations supported by vulnerable applications. One such incident occurred in January 2003, when the "Slammer" Internet worm took down monitoring computers at FirstEnergy Corporation's idled Davis-Besse nuclear plant. A subsequent report by the North American Electric Reliability Council (NERC) concluded that, although it caused no outages, the infection blocked commands that operated other power utilities. The report, "NRC Issues Information Notice on Potential of Nuclear Power Plant Network to Worm Infection," is available at web site <http://www.nrc.gov/reading-rm/doc-collections/news/2003/03-108.html>.

This example, among others, highlights the increased vulnerability to disruption via cyber means faced by North America's critical infrastructure sectors, including the energy sector. Of specific concern to the U.S. and Canadian governments are the Supervisory Control and Data Acquisition (SCADA) systems, which contain computers and applications that perform a wide variety of functions across many industries. In electric power, SCADA includes telemetry for status and control, as well as Energy Management Systems (EMS), protective relaying, and automatic generation control. SCADA systems were

developed to maximize functionality and interoperability, with little attention given to cyber security. These systems, many of which were intended to be isolated, are now, for a variety of business and operational reasons, either directly or indirectly connected to the global Internet. For example, in some instances, there may be a need for employees to monitor SCADA systems remotely. However, connecting SCADA systems to a remotely accessible computer network can present security risks. These risks include the compromise of sensitive operating information and the threat of unauthorized access to SCADA systems' control mechanisms.

Security has always been a priority for the electricity sector in North America; however, it is a greater priority now than ever before. Electric system operators recognize that the threat environment is changing and that the risks are greater than in the past, and they have taken steps to improve their security postures. NERC's Critical Infrastructure Protection Advisory Group has been examining ways to improve both the physical and cyber security dimensions of the North American power grid. This group includes Canadian and U.S. industry experts in the areas of cyber security, physical security and operational security. The creation of a national SCADA program to improve the physical and cyber security of these control systems is now also under discussion in the United States. The Canadian Electrical Association Critical Infrastructure Working Group is examining similar measures.

## Information Collection and Analysis

In addition to analyzing information already obtained from stakeholder interviews, telephone transcripts, law enforcement and intelligence information, and other ESWG working documents, the SWG will seek to review and analyze other sources of data on the cyber operations of those companies in the United States involved in the early stages of the power outage timeline, as identified by the ESWG. Available information includes log data from routers, intrusion detection systems, firewalls, and EMS; change management logs; and physical security materials. Data are currently being collected, in collaboration with the private sector and with consideration toward its protection from further disclosure where there are proprietary or national security concerns.

The SWG is divided into six sub-teams to address the discrete components of this investigation: Cyber Analysis, Intelligence Analysis, Physical Analysis, Policies and Procedures, Supporting Infrastructure, and Root Cause Liaison. The SWG organized itself in this manner to create a holistic approach to each of the main areas of concern with regard to power grid vulnerabilities. Rather than analyze each area of concern separately, the SWG sub-team structure provides a more comprehensive framework in which to investigate whether malicious activity was a cause of the power outage of August 14, 2003. Each sub-team is staffed with Subject Matter Experts (SMEs) from government, industry, and academia to provide the analytical breadth and depth necessary to complete its objective. A detailed overview of the sub-team structure and activities, those planned and those taken, for each sub-team is provided below.

## Cyber Analysis

The Cyber Analysis sub-team is led by the CERT® Coordination Center (CERT/CC) at Carnegie Mellon University and the Royal Canadian Mounted Police (RCMP). This team is focused on analyzing and reviewing the electronic media of computer networks in which online communications take place. The sub-team is examining these networks to determine whether they were maliciously used to cause, or contribute to, the August 14 outage. It is specifically reviewing the existing cyber topology, cyber logs, and EMS logs. The team is also conducting interviews with vendors to identify known system flaws and vulnerabilities. The sub-team is collecting, processing, and synthesizing data to determine whether a malicious cyber-related attack was a direct or indirect cause of the outage.

This sub-team has taken a number of steps in recent weeks, including reviewing NERC reliability standards to gain a better understanding of the overall security posture of the electric power industry. Additionally, the sub-team participated in meetings in Baltimore on August 22 and 23, 2003. The meetings provided an opportunity for the cyber experts and the power industry experts to understand the details necessary to conduct an investigation. The cyber data retention request was produced during this meeting.

Members of the sub-team also participated in the NERC/Department of Energy (DOE) Fact Finding meeting held in Newark, New Jersey, on September 8, 2003. Each company involved in the outage

provided answers to a set of questions related to the outage. The meeting helped to provide a better understanding of what each company experienced before, during, and after the outage. Additionally, sub-team members participated in interviews with the control room operators from FirstEnergy on October 8 and 9, 2003, and from Cinergy on October 10, 2003. These interviews have identified several key areas for further discussion.

The Cyber Analysis sub-team continues to gain a better understanding of events on August 14, 2003. Future analysis will be driven by information received from the ESWG's Root Cause Analysis sub-team and will focus on:

- ◆ Conducting additional interviews with control room operators and IT staff from the key companies involved in the outage.
- ◆ Conducting interviews with the operators and IT staff responsible for the NERC Interchange Distribution Calculator system. Some reports indicate that this system may have been unavailable during the time of the outage.
- ◆ Conducting interviews with key vendors for the EMS.
- ◆ Analyzing the configurations of routers, firewalls, intrusion detection systems, and other network devices to get a better understanding of potential weaknesses in the control system cyber defenses.
- ◆ Analyzing logs and other information for signs of unauthorized activity.

## Intelligence Analysis

The Intelligence Analysis sub-team is led by DHS and the RCMP, which are working closely with Federal, State, and local law enforcement, intelligence, and homeland security organizations to assess whether the power outage was the result of a malicious attack. Preliminary analysis provides no evidence that malicious actors—either individuals or organizations—are responsible for, or contributed to, the power outage of August 14, 2003. Additionally, the sub-team has found no indication of deliberate physical damage to power generating stations and delivery lines on the day of the outage, and there are no reports indicating that the power outage was caused by a computer network attack.

Both U.S. and Canadian government authorities provide threat intelligence information to their respective energy sectors when appropriate. No

intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature relating to the sector, which was provided to the North American energy industry by U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack involving explosions at oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted this threat warning is not consistent with the events of the power outage; there is no indication of a kinetic event before, during, or immediately after the August 14 outage.

Despite all the above indications that no terrorist activity caused the power outage, al-Qaeda did publicly claim responsibility for its occurrence:

◆ **August 18, 2003:** Al-Hayat, an Egyptian media outlet, published excerpts from a communiqué attributed to al-Qaeda. Al Hayat claimed to have obtained the communiqué from the website of the International Islamic Media Center. The content of the communiqué asserts that the “brigades of Abu Fahes Al Masri had hit two main power plants supplying the East of the U.S., as well as major industrial cities in the U.S. and Canada, ‘its ally in the war against Islam (New York and Toronto) and their neighbors.’” Furthermore, the operation “was carried out on the orders of Osama bin Laden to hit the pillars of the U.S. economy,” as “a realization of bin Laden’s promise to offer the Iraqi people a present.” The communiqué does not specify the way in which the alleged sabotage was carried out, but it does elaborate on the alleged damage to the U.S. economy in the areas of finance, transportation, energy, and telecommunications.

Additional claims and commentary regarding the power outage appeared in various Middle Eastern media outlets:

◆ **August 26, 2003:** A conservative Iranian daily newspaper published a commentary regarding the potential of computer technology as a tool for terrorists against infrastructures dependent on computer networks—most notably, water, electric, public transportation, trade organizations, and “supranational companies” in the United States.

◆ **September 4, 2003:** An Islamist participant in a Jihadist chat room forum claimed that sleeper

cells associated with al-Qaeda used the power outage as a cover to infiltrate the United States from Canada.

These claims above, as known, are not consistent with the SWG’s findings to date. They are also not consistent with recent congressional testimony by the U.S. Federal Bureau of Investigation (FBI). Larry A. Mefford, Executive Assistant Director in charge of the FBI’s Counterterrorism and Counterintelligence programs, testified to the U.S. Congress on September 4, 2003, that, “To date, we have not discovered any evidence indicating that the outage was a result of activity by international or domestic terrorists or other criminal activity.” He also testified that, “The FBI has received no specific, credible threats to electronic power grids in the United States in the recent past and the claim of the Abu Hafs al-Masri Brigade to have caused the blackout appears to be no more than wishful thinking. We have no information confirming the actual existence of this group.” Mr. Mefford’s Statement for the Record is available at web site <http://www.fbi.gov/congress/congress03/mefford090403.htm>.

Current assessments suggest that there are terrorists and other malicious actors who have the capability to conduct a malicious cyber attack with potential to disrupt the energy infrastructure. Although such an attack cannot be ruled out entirely, an examination of available information and intelligence does not support any claims of a deliberate attack against the energy infrastructure on, or leading up to, August 14, 2003. The few instances of physical damage that occurred on power delivery lines were the result of natural acts and not of sabotage. No intelligence reports before, during, or after the power outage indicate any specific terrorist plans or operations against the energy infrastructure. No incident reports detail suspicious activity near the power generation plants or delivery lines in question.

## Physical Analysis

The Physical Analysis sub-team is led by the U.S. Secret Service and the RCMP. These organizations have particular expertise in physical security assessments in the energy sector. The sub-team is focusing on issues related to how the cyber-related facilities of the energy sector companies are secured, including the physical integrity of data centers and control rooms, along with security procedures and policies used to limit access to sensitive areas. Focusing on the facilities identified as having a causal relationship to the outage,

the sub-team is seeking to determine whether the physical integrity of the cyber facilities was breached, either externally or by an insider, before or during the outage; and if so, whether such a breach caused or contributed to the power outage. Although the sub-team has analyzed information provided to both the EWG and the Nuclear Working Group (NWG), the Physical Analysis sub-team is also reviewing information resulting from recent face-to-face meetings with energy sector personnel and site visits to energy sector facilities, to determine the physical integrity of the cyber infrastructure.

The sub-team has compiled a list of questions covering location, accessibility, cameras, alarms, locks, and fire protection and water systems as they apply to computer server rooms. Based on discussions of these questions during its interviews, the sub-team is in the process of ascertaining whether the physical integrity of the cyber infrastructure was breached. Additionally, the sub-team is examining access and control measures used to allow entry into command and control facilities and the integrity of remote facilities.

The sub-team is also concentrating on mechanisms used by the companies to report unusual incidents within server rooms, command and control rooms, and remote facilities. The sub-team is also addressing the possibility of an insider attack on the cyber infrastructure.

## **Policies and Procedures**

The Policies and Procedures sub-team is led by DHS and OCIPEP, which have personnel with strong backgrounds in the fields of electric delivery operations, automated control systems (including SCADA and EMS), and information security. The sub-team is focused on examining the overall policies and procedures that may or may not have been in place during the events leading up to and during the August 14 power outage. The team is examining policies that are centrally related to the cyber systems of the companies identified in the early stages of the power outage. Of specific interest are policies and procedures regarding the upgrade and maintenance (to include system patching) of the command and control (C2) systems, including SCADA and EMS. Also of interest are the procedures for contingency operations and restoration of systems in the event of a computer system failure or a cyber event, such as an active hack or the discovery of malicious code. The group is conducting further interviews

and is continuing its analysis to build solid conclusions about the policies and procedures relating to the outage.

## **Supporting Infrastructure**

The Supporting Infrastructure sub-team is led by a DHS expert with experience assessing supporting infrastructure elements such as water cooling for computer systems, backup power systems, heating, ventilation and air conditioning (HVAC), and supporting telecommunications networks. OCIPEP is the Canadian co-lead for this effort. The sub-team is analyzing the integrity of the supporting infrastructure and its role, if any, in the August 14 power outage, and whether the supporting infrastructure was performing at a satisfactory level before and during the outage. In addition, the team is contacting vendors to determine whether there were maintenance issues that may have affected operations during or before the outage.

The sub-team is focusing specifically on the following key issues in visits to each of the designated electrical entities:

- ◆ Carrier/provider/vendor for the supporting infrastructure services and/or systems at select company facilities
- ◆ Loss of service before and/or after the power outage
- ◆ Conduct of maintenance activities before and/or after the power outage
- ◆ Conduct of installation activities before and/or after the power outage
- ◆ Conduct of testing activities before and/or after the power outage
- ◆ Conduct of exercises before and/or after the power outage
- ◆ Existence of a monitoring process (log, checklist, etc.) to document the status of supporting infrastructure services.

## **Root Cause Analysis**

The SWG Root Cause Liaison sub-team (SWG/RC) has been following the work of the ESWG to identify potential root causes of the power outage. As these root cause elements are identified, the sub-team will assess with the ESWG any potential linkages to physical and/or cyber malfeasance.

The root cause analysis work of the ESWG is still in progress; however, the initial analysis has

found no causal link between the power outage and malicious activity, whether physical or cyber initiated. Root cause analysis for an event like the August 14 power outage involves a detailed process to develop a hierarchy of actions and events that suggest causal factors. The process includes: development of a detailed timeline of the events, examination of actions related to the events, and an assessment of factors that initiated or exacerbated the events. An assessment of the impact of physical security as a contributor to the power outage is conditional upon discovery of information suggesting that a malicious physical act initiated or exacerbated the power outage. There are no such indications thus far, and no further assessment by the SWG in this area is indicated.

## Cyber Timeline

The following sequence of events was derived from discussions with representatives of FirstEnergy and the Midwest Independent Transmission System Operator (MISO). All times are approximate and will need to be confirmed by an analysis of company log data.

- ◆ The first significant cyber-related event of August 14, 2003, occurred at 12:40 EDT at the MISO. At this time, a MISO EMS engineer purposely disabled the automatic periodic trigger on the State Estimator (SE) application, which allows MISO to determine the real-time state of the power system for its region. Disabling of the automatic periodic trigger, a program feature that causes the SE to run automatically every 5 minutes, is a necessary operating procedure when resolving a mismatched solution produced by the SE. The EMS engineer determined that the mismatch in the SE solution was due to the SE model depicting Cinergy's Bloomington-Denois Creek 230-kV line as being in service, when it had actually been out of service since 12:12 EDT.
- ◆ At 13:00 EDT, after making the appropriate changes to the SE model and manually triggering the SE, the MISO EMS engineer achieved two valid solutions.
- ◆ At 13:30 EDT, the MISO EMS engineer went to lunch. He forgot to re-engage the automatic periodic trigger.
- ◆ At 14:14 EDT, FirstEnergy's "Alarm and Event Processing Routine" (AEPR)-a key software program that gives operators visual and audible indications of events occurring on their portion of the grid-began to malfunction. FirstEnergy system operators were unaware that the software was not functioning properly. This software did not become functional again until much later that evening.
- ◆ At 14:40 EDT, an Ops engineer discovered that the SE was not solving. He went to notify an EMS engineer.
- ◆ At 14:41 EDT, FirstEnergy's server running the AEPR software failed to the backup server. Control room staff remained unaware that the AEPR software was not functioning properly.
- ◆ At 14:44 EDT, an MISO EMS engineer, after being alerted by the Ops engineer, reactivated the automatic periodic trigger and, for speed, manually triggered the program. The SE program again showed a mismatch.
- ◆ At 14:54 EDT, FirstEnergy's backup server failed. AEPR continued to malfunction. The Area Control Error (ACE) calculations and Strip Charting routines malfunctioned, and the dispatcher user interface slowed significantly.
- ◆ At 15:00 EDT, FirstEnergy used its emergency backup system to control the system and make ACE calculations. ACE calculations and control systems continued to run on the emergency backup system until roughly 15:08 EDT, when the primary server was restored.
- ◆ At 15:05 EDT, FirstEnergy's Harding-Chamberlin 345-kV line tripped and locked out. FE system operators did not receive notification from the AEPR software, which continued to malfunction, unbeknownst to the FE system operators.
- ◆ At 15:08 EDT, using data obtained at roughly 15:04 EDT (it takes about 5 minutes for the SE to provide a result), the MISO EMS engineer concluded that the SE mismatched due to a line outage. His experience allowed him to isolate the outage to the Stuart-Atlanta 345-kV line (which tripped about an hour earlier, at 14:02 EDT). He took the Stuart-Atlanta line out of service in the SE model and got a valid solution.
- ◆ Also at 15:08 EDT, the FirstEnergy primary server was restored. ACE calculations and control systems were now running on the primary server. AEPR continued to malfunction, unbeknownst to the FirstEnergy system operators.
- ◆ At 15:09 EDT, the MISO EMS engineer went to the control room to tell the operators that he thought the Stuart-Atlanta line was out of service. Control room operators referred to their

“Outage Scheduler” and informed the EMS engineer that their data showed the Stuart-Atlanta line was “up” and that the EMS engineer should depict the line as in service in the SE model. At 15:17 EDT, the EMS engineer ran the SE with the Stuart-Atlanta line “live.” The model again mismatched.

- ◆ At 15:29 EDT, the MISO EMS Engineer asked MISO operators to call the PJM Interconnect to determine the status of the Stuart-Atlanta line. MISO was informed that the Stuart-Atlanta line had tripped at 14:02 EDT. The EMS engineer adjusted the model, which by that time had been updated with the 15:05 EDT Harding-Chamberlin 345-kV line trip, and came up with a valid solution.
- ◆ At 15:32 EDT, FirstEnergy’s Hanna-Juniper 345-kV line tripped and locked out. The AEPR continued to malfunction.
- ◆ At 15:41 EDT, the lights flickered at FirstEnergy’s control facility, because the facility had lost grid power and switched over to its emergency power supply.
- ◆ At 15:42 EDT, a FirstEnergy dispatcher realized that the AEPR was not working and informed technical support staff of the problem.

## Findings to Date

The SWG has developed the following findings via analysis of collected data and discussions with energy companies and entities identified by the ESWG as pertinent to the SWG’s analysis. SWG analysis to date provides no evidence that malicious actors—either individuals or organizations—are responsible for, or contributed to, the power outage of August 14, 2003. The SWG continues to coordinate closely with the other Task Force Working Groups and members of the U.S. and Canadian law enforcement and DHS/OCIPEP communities to collect and analyze data to test this preliminary finding.

No intelligence reports before, during, or after the power outage indicated any specific terrorist plans or operations against the energy infrastructure. There was, however, threat information of a general nature related to the sector, which was provided to the North American energy industry by

U.S. and Canadian government agencies in late July 2003. This information indicated that al-Qaeda might attempt to carry out a physical attack against oil production facilities, power plants, or nuclear plants on the U.S. East Coast during the summer of 2003. The type of physical attack described in the intelligence that prompted the threat information was not consistent with the events of the power outage.

Although there were a number of worms and viruses impacting the Internet and Internet-connected systems and networks in North America before and during the outage, the SWG’s preliminary analysis provides no indication that worm/virus activity had a significant effect on the power generation and delivery systems. Further SWG analysis will test this finding.

SWG analysis to date suggests that failure of a software program—not linked to malicious activity—may have contributed significantly to the power outage of August 14, 2003. Specifically, key personnel may not have been aware of the need to take preventive measures at critical times, because an alarm system was malfunctioning. The SWG continues to work closely with the operators of the affected system to determine the nature and scope of the failure, and whether similar software failures could create future system vulnerabilities. The SWG is in the process of engaging system vendors and operators to determine whether any technical or process-related modifications should be implemented to improve system performance in the future.

The existence of both internal and external links from SCADA systems to other systems introduced vulnerabilities. At this time, however, preliminary analysis of information derived from interviews with operators provides no evidence indicating exploitation of these vulnerabilities before or during the outage. Future SWG work will provide greater insight into this issue.

Analysis of information derived from interviews with operators suggests that, in some cases, visibility into the operations of surrounding areas was lacking. Some companies appear to have had only a limited understanding of the status of the electric systems outside their immediate control. This may have been, in part, the result of a failure to use modern dynamic mapping and data sharing systems. Future SWG work will clarify this issue.

