THE SEVENTH ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY

EISS VII | LONDON 2016

Electric Infrastructure Security Summit
Strategic Implementation

Summit Report
The EIS Summit Series is an international government, industry and NGO partnership, providing a broad framework for addressing critical infrastructure vulnerabilities. With its theme of “Strategic Implementation,” EISS VII built on this framework, as public and private sector leaders came together to advance cost effective strategies for Black Sky hazards: emerging, extreme malicious and natural hazards that could cause long duration power outages and societal infrastructure failures on unprecedented scales.

Taking place in Westminster Palace and Whitehall in London, the summit began by exploring opportunities and challenges to develop and implement collaborative strategies for lifeline infrastructure resilience and restoration addressing these extreme hazards.

The second day of the summit hosted the EPRO SECTOR Executive Committee, moving on from strategies to specific opportunities for implementation of key resilience measures and plans. With Executive Committee delegates including CEOs and senior managers from the world’s largest electricity and water utilities, government leaders and NGO executives from the U.S., the U.K., Israel and other nations, Executive Committee members discussed cross-sector planning focused on resolving critical interdependencies. Empanelled sector by sector, this meeting represented the first time senior leadership from many tightly connected sectors came together to jointly explore approaches to resolve Black Sky vulnerabilities, introduced by these interdependencies, which represent growing, unprecedented risk to national continuity for the U.S. and allied nations. Documented in developing EPRO Black Sky Playbooks, the EPRO SECTOR Executive Committee reviewed “internal” and “external” requirements defined by critical infrastructure sectors, designed to enable each sector to sustain or quickly restore critical resources and services in these extreme hazard scenarios.
Electric Infrastructure Security Summit VI
Summit Report

Published:
July 18, 2016

Principal Editors:
Yedidya Sinclair
Avi Schnurr

Contributing Editors:
Sarah Schnurr
Dr. Chris Beck

Note on text formatting: Where quotes are emphasized as “pull-quotes” in parallel with the text of the report, editing marks have been removed and slight adjustments have sometimes been made to meet the graphic requirements of the report, and to simplify reading. In all such cases, the original quote, with editing marks, may be found in the report text.
Overview

Our world and our lives have been transformed by modern, evolving, interdependent infrastructures that have brought us unprecedented capabilities. With these capabilities, however, comes a new class of risks.

“Black Sky” hazards include uniquely severe malicious and natural threats, from cyber, EMP or physical attacks on the power grid to extreme terrestrial or space weather, and recently discovered, multi-state earthquake zones. These emerging risks could cause widely distributed grid damage and long duration, subcontinent-scale power outages, with cascading failures of all lifeline infrastructures.

As in any tightly interdependent system, no major infrastructure can operate without functionality of all the others, making restoration from such hazards extremely complex. If modern nations wish to sustain national continuity in such scenarios, advance, thorough cross-sector resilience and operational planning are critical.

In EIS Summit VII, the Day One Plenary session and the Day Two EPRO SECTOR Executive Committee both provided unique opportunities to address these needs, with participation of U.K., U.S., Israeli and international government and private sector leaders in wide ranging discussions and planning. Delegates also had a unique opportunity to meet and discuss these complex matters at a gala reception and dinner, hosted in the Tate Britain Gallery.
Reception at the Tate Britain. The Summit enabled informal conversations between senior decision makers in convivial surroundings.
Executive Summary
Executive Summary

EIS Summit VII took place from July 17th-19th 2016 in London, at the Palace of Westminster and the Royal United Services Institute in Whitehall. The Summit was the largest yet held in the EISS series, convening senior leadership from government, the private sector, utilities, academia and NGOs representing multiple nations, as well as distinguished representatives from multinational organizations including NATO, the European Commission and the OECD. This Summit also featured convivial opportunities for open discussion among senior officials and decision makers, including a dinner at the Tate Britain gallery.

The overall theme of the Summit was “Strategic Implementation.” Lifeline utilities, government agencies and mass-care NGOs have begun meeting in the United States, the United Kingdom and Israel, sector by sector, to begin developing EPRO Black Sky playbooks. These playbooks set out sector-defined requirements, both internal and external, designed to enable each sector to provide those minimum Black Sky service levels, restoration priorities or support needed to enable post-hazard restoration and recovery, and to save and sustain lives. The Summit explored strategies, challenges and opportunities involved in developing and implementing these playbooks.

A number of key subthemes emerged from the discussion as critical prerequisites or objectives to advance preparations and implementation of Black Sky resilience investment measures and operational planning.

1. **Cross-Sector Planning:** Coordinated, expanding cross-sector planning, focused on extreme Black Sky hazards, is vital.

   If modern nations are to effectively survive prolonged national-scale power outages and the cascading infrastructure failures that would follow, detailed coordination is a critical prerequisite. With interdependencies among the electricity, fuel, water, health, communication, transportation and other infrastructure sectors, planning for such events can only emerge from extensive, detailed, cross-sector and multi-sector planning. Many interdependencies for such scenarios can be predicted, such as the need for electricity to pump water which in turn, used by electricity producers, and the operation of natural gas fuel pipelines and the electricity generation stations that both require and energize those pipelines. However, given the extraordinary complexity of today’s interlocked resource production and distribution systems, many will only emerge from detailed analysis.

   In this regard, former U.S. Assistant Secretary of Defense Paul Stockton declared, “Each of these individual sectors is making great progress. In comparison, we’re in the dark ages for building cross-sector resilience.”

   There is much work to be done in developing the cross-sector planning, training and working relationships that will be essential to address severe Black Sky hazards.

2. **The EPRO SECTOR Process:** EPRO SECTOR’s Executive Committee and Sector Steering Committees are proving to be unique, powerful tools to host this planning process.

   As an overarching theme, summit participants from every sector expressed a common conclusion – the EPRO SECTOR meetings, both at the individual sector level and the twice
yearly Executive Committee meetings where they come together, represent a vital new capability in addressing severe national threats. These meetings, now proceeding in the U.S., the U.K. and Israel, are driving development of both sector-by-sector and coordinated Black Sky planning. This planning is now captured in EPRO Black Sky Playbooks, as evolving, specific planning frameworks for each sector to focus their own efforts and define their external support needs.

3. **Black Sky Systems Engineering:** Systems engineering methodology provides powerful tools to host coordinated, Black Sky infrastructure planning.

Systems engineering methodologies today represent the best-in-class approaches used in aerospace and other high-tech companies to develop complex new capabilities requiring coordinated effort by diverse entities. Avi Schnurr, CEO of EIS Council succinctly summarized some of the key features of these approaches, applicable to cross-sector infrastructure planning.

“The systems engineering process begins with definition of a top-level mission that everyone involved buys into, and this mission is then used to focus development of sector-level objectives. Leaders from each sector can then define, if they are to meet those objectives, both what their sector needs to achieve if they are to meet those objectives, and what they will need from other sectors. Overall Black Sky mission requirements, sector objectives, and “internal” and “external” requirements.”

4. **Innovative Structure for EISS VII:** The highly successful, innovative format for EISS VII Day 2, the EPRO SECTOR Executive Committee, demonstrated the capability of systems engineering to frame cross-sector planning.

The Second Day of the Summit, as one of the two yearly EPRO SECTOR Executive Committee meetings, was innovatively formatted to express basic Systems Engineering methodology. Panelists from the different sectors both discussed their own sectors’ needs and goals, and responded to the other sectors’ requests and definitions of their needs. (A summary of Say Day 2 has been prepared for delegates and their organizations.)

5. **Moving on:** The EIS Summit Series has played a key role in bringing public and private sector leaders to focus on Black Sky hazards. It is time to move on to detailed planning and implementation.

Numerous speakers noted that senior decision makers now recognize the threats the danger of Black Sky hazards to critical infrastructure. As James Arbuthnot put it:

“We’re beyond the step of needing to persuade people to take this issue seriously. I think we’re now on the next step of, ‘Ok, what do we actually do about it?’”

James Arbuthnot also spoke about the diligence and imperative for action which has characterized recent decisions on addressing Black Sky-class hazards within the British Cabinet Office. Other speakers reported on high-level decisions and concrete steps taking place in the U.S. and in Israel, in both government and industry. The U.S. Congress, for example, now expects to pass the Critical Infrastructure Protection Act, which will embed Black Sky preparedness in U.S. planning and training, while the Israeli government and corporate sectors are expanding their work on critical infrastructure protection against EMP and other Black Sky hazards.
6. **Addressing Expanding Hazards:** With the threat environment worsening, Black Sky planning will need to address extreme hazard impact projections, if national continuity is to be assured.

Recent, severe terrestrial weather events have grown in impact and frequency. In 2012, a Carrington-class extreme coronal mass ejection “missed” the earth in its orbit by one week. Terrorism, empowered by social media, is rising. Cyber-attacks are becoming more frequent, aggressive and sophisticated, and in December 2015, in a world-first, the Ukrainian power grid was shut down by a cyber-attack. Iran has shown itself to be well aware of EMP as a potential weapon against more powerful adversaries, referencing the matter twenty two times in a recently translated 2010 military strategy document. As DHS Assistant Secretary Caitlin Durkovich put it, “Our adversaries understand the strategic importance of our infrastructure, whether it be the electrical sector, or the water sector.”

As these evolving conditions continue to unfold, prudent investment in resilience and operational planning must, increasingly, address the highest impact scenarios forecast for Black Sky hazards.

7. **Bringing the Public into Focus:** The resiliency of the general public is an important (and under-appreciated) aspect of Black Sky restoration and recovery.

Several speakers, especially those from Israel, stressed the pivotal importance of promoting the resilience of the general population. If the public is entirely unprepared for a Black Sky event, there is a danger of panic and a complete breakdown of civic order. Apart from the inherent evils of these phenomena, they could disrupt the restoration process, and prevent emergency personnel from repairing the grid and other key infrastructure. Taking steps to provide information to the public both as preparatory measures and after a Black Sky event could help maintain their resilience, although, as some speakers pointed out, there is a fine balance to be struck between preparation and sowing needless anxiety. Archdeacon of London, Rev. Luke Miller suggested that religious groups can play an important role here, pointing out: Faith-based organizations and related groups could potentially making the difference between “sharing the light of the last stub of candle or a fight to the death over the last tin of baked beans.”

8. **Exercises as a Critical Need:** Exercising and training, in formats suitable to the unique needs of Black Sky hazards, is of the utmost importance.

Numerous speakers stressed that training, exercises and simulations are vital for these scenarios. Moreover, it is essential that exercises simulate the severely disrupted conditions that would obtain in a Black Sky event. As Gerry Cauley, CEO and President of NERC asked, rhetorically:

“What if our computers or cyber assets are damaged or hindered? What if there’s physical equipment that’s damaged and we need to re-supply equipment?”

Such exercises must pay special attention to validating availability of adequately trained and qualified people to fulfill critical tasks, and provide a venue to exercise the unique, complex work of real time multi-sector coordination.
9. **BSX – A Template for Black Sky Emergency Communications**: A widely distributed, interoperable and self-powered emergency communications system will be critical to recovering from Black Sky events.

In a Black Sky event, our ordinary mass communications systems will fail. As one of the most common concerns expressed by all sectors building Black Sky planning, continuing, very widely distributed and interoperable communications will be crucial to any restoration or life-sustaining efforts in an extended duration, wide-area power outage. Neil Siegel and Bran Ferren summarized their research into the best available architecture for a feasible, functional and survivable communications system, assumed to require at least 100,000 widely distributed nodes. Configured to support both emergency communication and emergency coordination / situational awareness, the recommended BSX system architecture is designed to expand upon U.S. army field communications networks, which have a good track record of robustness in very challenging conditions.

10. **Taking the Lead in Black Sky Planning – The United States, the United Kingdom and Israel**: With the U.S. leading the way with multi-sector planning, the UK and Israel are moving forward in parallel, bringing unique capabilities as possible templates for use by allied nations.

Stakeholders from industry, government and the NGO community are now moving forward with Black Sky coordinated planning in the UK, with some advantages related to more centralized infrastructures and resilience planning. Israel is working to expand protection of its national power grid, water utilities, gas generation facilities and other crucial infrastructure, addressing EMP as well as a wide range of Black Sky hazards. Israel’s world-class cyber expertise and long experience in preparing and exercising for “threats to the home front” also make it a unique template to address these scenarios. In combination with the EPRO SECTOR planning foundation moving forward in the U.S., all three nations now provide different, sharable best-practice approaches addressing different dimensions of Black Sky planning.
Session One
The Transition from Strategy to Implementation
The opening session set the scene for the Summit by laying out the geo-political background, reviewing progress, and establishing principal implementation challenges that became a focus for much of the Summit.

Congressman Trent Franks warned that a potential EMP attack is one of the most acute national security challenges the U.S. faces. He was optimistic that, thanks in significant part to EIS Council’s work, decision-makers now broadly recognize the seriousness of Black Sky threats and are beginning to take action. He highlighted Israel’s work in hardening its electric grid, and the milestone CIPA legislation passing through the U.S. Congress as examples of action-oriented efforts.

Avi Schnurr, CEO of EIS Council, stressed that the interconnectedness of modern critical infrastructure necessitates a high degree of inter-sector cooperation to prepare for hazards. As a result, systems engineering, the best-in-class methodology used by the hi-tech world for developing complex interdependent systems, now forms the basis for the cross-sector planning efforts hosted by the organization.

Rt. Hon. Lord James Arbuthnot, noted that, given the abrupt change in the government, the Rt. Hon. Oliver Letwin was unable to address the summit. Letwin, who had been in charge of the cabinet office until two days before the summit, had planned to address the assembled delegates when the resignation of the Prime Minister resulted in substantial changes within the U.K. government. In his place, James Arbuthnot spoke in some detail about the U.K. government’s strong and action-oriented commitment to protect the nation against the full set of Black Sky hazards, ensuring that adequate resilience investment and planning would be in place, in advance of any hazard, to ensure the continuity of the UK and the restoration of its critical infrastructures.

Dr. Paul Stockton, referring to his role as editor-in-chief of the two-volume EPRO Handbook II, spoke of critical, cross-infrastructure interdependencies. (EPRO II was released, for the first time, at the summit). Cross sector coordination and planning will be key challenges to address this class of emerging, extreme threats, he suggested. To build plans that will permit us to deal with them, “We are going to need new ways of planning and organizing as well as new capabilities,” he said. As a primary interdependency example, Dr. Stockton underlined the increasing dependence of electrical generation on natural gas pipelines in the U.S., which are themselves dependent on electricity for their operation.
Welcome and Opening Remarks: 
Lifeline Infrastructure Security

Congressman Trent Franks, U.S. Representative for Arizona’s 8th Congressional District

Congressman Franks opened the summit with warm thanks for the organizers and praise for the United Kingdom, “a firm ally of the United States and a force for good in the world that has repeatedly acted in defense of human freedom.”

“I believe that today’s discussion is one of profound implication to Western civilization,” Franks declared. The remarkable technological progress now taken for granted in modern industrial endeavors is completely dependent on electricity. “In keeping with one of humanity’s most reliable hallmarks, we now find among our greatest strengths an unsettling vulnerability.”

Turning to the EMP threat, Rep. Franks then surveyed the progress of the Critical Infrastructure Protection Act (CIPA) that he successfully piloted through the House of Representatives, and expected to pass in the Senate [The CIPA Act has now become law – ed.]. “CIPA essentially embeds EMP into our national planning scenarios,” he explained. Practical action addressing this threat is also beginning; “Israel, probably the world’s most advanced technological society… has begun to harden their grid... Looks like they’ll be the first ones to do it.”

However, the threats are gathering apace: “I believe that weaponized EMP has become the most dangerous short-term national security threat that we face. Iran marches in that direction... we were able to translate their military doctrine, which targets the grids of their opponents, especially those that were stronger and more powerful than they.”
Referring to the full set of Black Sky hazards, Rep. Franks ended by posing a crucial question for the summit: “Will the hardening of civilization’s largest machine, the electricity grid, come in time?” He asserted that with regard to the problem of critical threats to infrastructure we are at “that critical moment in the life of nearly every problem when it is big enough to be seen and still small enough to be solved.” Warning of the urgency of taking action now, he invoked Winston Churchill’s words: “Still, if you will not fight for the right when you can easily win without bloodshed, if you will not fight when your victory will be sure and not too costly, there may come a moment when you will have to fight with all the odds against you and only precarious chance of surviving. There may be a worse moment. You may have to fight when there is no hope of victory, because it is still better to perish than to live as slaves.”

Congressman Franks concluded his remarks by introducing Avi Schnurr, EIS Council CEO, praising his “constancy of purpose” as the secret of EIS Council’s success.
Avi Schnurr began his remarks by noting the high degree of interconnectedness between our critical societal resource systems, such as power, health care, water and transportation, and hence the thorough cross-sector coordination needed if adequate backup plans are to be developed to deal with prolonged subcontinent-scale power outage, with consequent global impact. He reminded the Summit of the six classic Black Sky hazards: three man-made – EMP, cyber and coordinated physical assault on key grid nodes; and three natural – severe space and terrestrial weather, and extreme regional earthquake zones.

Schnurr also highlighted recent successes in using systems engineering methodology as a template for coordinated cross-sector planning, as part of the expanding EPRO SECTOR process. Used in the aerospace and hi-tech world as a best-in-class system development approach, systems engineering may be viewed as a conceptual “toolkit.”

“Systems engineering deals with very complex problems that can only be addressed by many sectors working closely together,” he said. To address Black Sky hazards, several key elements of this toolkit are being used.

Conceptually, this process begins with definition of an overall Black Sky resilience mission that is then translated into sector-specific missions – predefined minimum service levels or restoration support priorities. Given these sector-specific missions, what “internal requirements,” Black Sky resilience measures and operational plans, will be needed from each sector? “If we’re going to accomplish this mission, addressing these extreme hazards, what does our sector need to achieve?” Finally, what will each sector need from its partners, the “external requirements” that define the resources each sector will need to mesh with their own efforts, to achieve their sector’s mission.

"When one of these events happens, we will be able to overcome it… and life will go on… But only if we here today decide and move forward in a very concrete, detail-oriented way, to continue making the progress that has already begun
“Merely doing my job will certainly not be enough in our integrated, organic, multi-sector world… what does the electric subsector need from the oil and natural gas subsector and the water sector? What do each of the utilities…need from the regulatory sector?"

However, Schnurr warned, “All of that sounds good, but it’s meaningless unless there is solid buy-in, and decision makers and leaders in each of the sectors decide this is something they need to take on.” In short, although EIS Council and its partners can help by hosting and facilitating a process, “the people who will drive it forward, who will make it work and have all of the tough decisions, are you.”

He concluded by emphasizing the responsibility that this confers: “When one of these events happens, we will be able to overcome it and move on, and life will go on… But only if we here today decide to move forward in a very concrete, detail-oriented way; to continue making the progress that has already begun.”
Lord Arbuthnot also began by warmly thanking the organizers of the event. He expressed his regret that Oliver Letwin, the former Chancellor of the Duchy of Lancaster with broad responsibilities in the Cabinet, had left his job in the recent UK government reshuffle. Letwin had been planning to speak at the summit.

Lord Arbuthnot recalled Letwin’s commitment to building infrastructure resilience in the UK and his strong grasp of the issues, noting a remarkable meeting the Chancellor held with him, Lord Toby Harris and Avi Schnurr in June. At that meeting Oliver Letwin signaled that, when dealing with the full list of Black Sky hazards that represent existential threats to the nation, probability was not a consideration. “If there were going to be the possibility of an event the consequences of which would be catastrophic, then the government needs to take action against that event, even if the likelihood of that event was low.” Arbuthnot suggested that this represented an important shift in government thinking. “The government has decided that the consequences are so serious that it does need to take account of that [i.e., low probability], and does need to act against it.”

Arbuthnot closed by remarking on the great progress infrastructure leaders and their government and NGO partners have made, with the coordination and planning processes hosted by EIS Council playing a vital role. “I think we’re beyond the step of needing to persuade people to take this issue seriously now. I think we’re now on the next step of, ok, what do we actually do about it?”

“If there were going to be the possibility of an event - the consequences of which would be catastrophic, then the government needs to take action against that event, even if the likelihood of that event was low.”
Dr. Paul Stockton, Managing Director of SONECON
Former U.S. Assistant Secretary of Defense

Lifeline Sector Interdependencies
Highlights of EPRO Handbook II

Introduction ... and Conclusion
Paul Stockton began by stating his main thesis: “Let me give you my bottom line up front. Individually, each of these individual sectors is making great progress. In comparison, we’re in the dark ages for building cross-sector resilience.” He proposed to devote his remarks first to suggesting a way of thinking systematically about cross-sector hazards, and second to focusing on two particular challenges.

Preparing for Black Sky Events Requires New Approaches
Outlining a “way of thinking about Black Sky events,” Stockton emphasized that they are quantitatively and qualitatively different from the storm and hurricane-caused outages that we have experienced. Quantitatively, the outages will be longer and broader. After Hurricane Sandy, 95% of East Coast customers had their power restored within two weeks. That would be very unlikely after a Black Sky event. Qualitatively, Black Sky Events will require entirely new plans. Stockton quoted Craig Fugate from FEMA as saying, “Do not fall into the trap of scaling up. Do not imagine that the emergency plans you had against Sandy-scale events are going to be remotely adequate for larger scale events. “We are going to need new ways of planning and organizing as well as new capabilities,” argued Stockton.

Examples of New Capabilities – and Relationships – That Need to be Developed
One of the most important capabilities needed will be emergency power generators, and extensive, prearranged plans for providing the fuel to resupply them. Most currently-installed
emergency generators will burn out long before power can be restored, in an outage lasting a month or more, and fuel distribution networks will fail. There needs to be a sharp upgrade in our ability to supply generators and fuel, and “we’re going to need harshly prioritized plans in order to ensure that the fuel gets to … the sites that are most important for saving and sustaining lives and for national security.”

However, the greatest challenge, Stockton reiterated, will be building and preparing the kind of cross-sector collaboration and relationships that will be needed to support infrastructure restoration, and save and sustain lives in these hazards. Stockton underscored the usefulness of the systems engineering approach that Avi Schnurr outlined, with definition of the minimal levels of service needed from each sector and then the internal and external requirements for reaching those levels.

**Black Sky Challenges: EMP as a Key Example**

Moving on to a typology of back sky hazard events, Stockton noted that EIS HANDBOOK I describes the direct effects of an EMP attack, and lays out cost effective strategies and options for hardening critical parts of the grid to ensure power can be restored following an EMP strike. He pointed out that some utilities in the U.S. (as well as in the UK and Israel) are already making these investments, but cost-recovery remains an issue. “Industry should always be in the lead for protection against the direct effects of Black Sky hazards, but someone’s got to pay for it… We’ve got to figure out…how we’re going to provide for cost-recovery of prudent cost-effective investments against direct effects.”

**Unique Restoration and Interdependency Challenges**

On the challenges of restoring power after a Black Sky event, Stockton noted that after, say, a cyber-attack, utilities would be less likely to lend resources for recovery to other areas than they
would after a hurricane, out of fear that they would be attacked next. He also emphasized the vital importance of “whole community preparedness.” “We’re going to need the entirety of the private sector communities, NGOs and families being prepared to take care of themselves, because the cavalry is not coming for some time.”

In addition to the direct effects of EMP, GMD and other Black Sky hazards on the power grid, the next class of impacts is cascading effects on all other lifeline infrastructures. “If you lose electrical power… that’s going to have a big effect on the water sector…the same is true of the communications and transportation sectors.” Indeed, Stockton pointed out, transport is a good example of “the electrification of everything.” All sorts of vehicles are increasingly electric-powered, and indirect impacts of an outage would affect all vehicles. The interaction of the natural gas and electricity systems is a good example of this. Natural gas is becoming the dominant fuel for electricity generation around the Western world. But the gas pumping system and the SCADA electronics that control it are dependent on electrical power. In a blackout, “because there’s less gas going to power generators, power generators aren’t going to be able to provide power to the gas transportation systems that are needed to provide for electric power generation.” It is vital to avoid such a “spiral of failure.

This challenge will require the oil and natural gas subsector to find new ways to partner with the electric subsector, and for both to work with the regulatory sector. Stockton noted that this multi-sector planning will have to deal explicitly with the trade-off between providing more resilient generating capacity, and the requirements of environmental protection. And, as always, financial considerations cannot be ignored. Cross-sector planning will also need to find a way of incentivizing gas companies to retain more gas-fired compressors on natural gas pipelines, rather than moving toward relying exclusively on electricity-intensive electric pumps.

“Because there’s less gas going to power generators, power generators aren’t going to be able to provide power to the gas transportation systems that are needed to provide for electric power generation… A spiral of failure.

“We are going to need new ways of planning and organizing as well as new capabilities.”
Panel 1
Recent Developments in Black Sky Resilience Planning: EMP / GMD Protection Planning Update

Panel Chair: Dr. Chris Beck, Chief Scientist and Vice President for Policy, EIS Council

John Twitchell laid out the work EIS COUNCIL is doing in making extensive information on protecting the electric grid available to utility leader and staff, covering hardening key components, storing critical spares, protecting transformers and more. Robin Manning from the transmissions sector described the efforts to build resilience against Black Sky events into the everyday resilience work that the transmissions sector already does.

Dr. Shlomo Wald introduced an important and little-discussed aspect of resilience: the social dimension. He laid out a plausible scenario under which a population not prepared for an EMP attack and left without adequate information could very quickly become unruly, demoralized and revert to behaving like “urban hunter-gatherers.” In this situation, even the best technical preparations could be undermined by developing social chaos. Prior preparation and clear information could help forestall such a breakdown. Finally Dr. Seth Jonas gave an update on important developments in measuring space weather.
John Twitchell, Power Systems Engineering Lead, EIS Council


John Twitchell outlined progress being made in the early stages of EIS Council’s “EPRO EMP” Handbook. Drawing on experience coming from utility leaders in the U.S., Israel, Norway, New Zealand and other nations, the new Handbook edition will function as a supplemental publication to EPRO Handbook I’s Chapter 2, which summarized – at higher level – EMP protection strategies and approaches. This new volume will provide a detailed, peer-reviewed, volunteer EMP protection specification, with sufficient information for power utilities and power systems engineers to make and implement strategic decisions on EMP protection for a portion of their electrical system.

EPRO EMP will address EMP hardening for modern power grid systems and components, encompassing a wide range of hardware considerations. Beginning where EPRO I’s Chapter 2 left off, this special edition will begin by suggesting methodology to establish realistic protection goals, and then move on to specify approaches that can be used, where desired, for protection spanning the full range of power generation, transmission and distribution for both low and high voltage systems. Facility and hardware configuration options, maintenance and fault-finding will all be covered by the wide ranging publication, along with recommended best practices for pre-staged sparing of sensitive equipment, tooling and emergency response equipment.
Robin Manning: Vice President of Transmission, EPRI

Update on the Resiliency Steering Committee, a Joint NATF/EPRI Project

Robin Manning reported on the work of the Resiliency Steering Committee, a joint effort of the Transmission Forum and EPRI to bring together industry leaders to understand the challenges of “integrating mitigations, recovery and response to Black Sky hazards with routine resiliency.” Routine resiliency is a high priority for industry.

“We have extracted some of the real leadership in transmission in the United States. So we feel like we really have the ear of utilities in the United States in this resilience steering team.” The steering committee has already held a number of events across the U.S. to engage committee members and their companies in addressing Black Sky and other hazards. There have been workshops on cyber-security, physical security, EMP and GMD with 100-200 attendees.

The group identified a need for a more detailed, operational focus on EMP in addition to the helpful general principles that are set out in EPRO Handbook I. EPRI is establishing a project to look specifically at these principles, led by Dr. Randy Horton, formerly of Southern Company. “We’re looking at how do we characterize the threat; how do we identify the vulnerabilities of the system...What are the impacts and risks of those vulnerabilities? And then to identify...mitigations and recovery methods for those...so that utilities can make informed, risk-based decisions based on the full threat analysis.”

This is scheduled to be a three year project, but there are thirty six releases of data scheduled over the three years, the first of which is due in September 2016. By the end of 2016, the plan is to complete a full analysis of the vulnerabilities and mitigation options for large power transformers.
Dr. Shlomo Wald; European Joint Research Centre, the European Commission. Formerly, Chief Scientist, Israel Energy Ministry

Urban Hunter-Gatherers: Society During and Following an EMP Multi-System Failure

Shlomo Wald focused his talk on an aspect of Black Sky scenarios that tends to be ignored: “We forget one organic material object that is generally not discussed, and this is the social effect on the citizen.” Wald argued that this social dimension has a major effect on all of the other, physical systems important to societal resilience in extreme scenarios.

To illustrate his point, Wald described a fictitious country of 8-10 million people, about half the size of Switzerland, highly dependent on technology but not well prepared for an EMP event which would cause a widespread power outage and cascading failures of other infrastructures. He posited a nation-wide power outage caused by an EMP strike, from a terrorist-launched nuclear-missile detonating at high altitude. Wald suggested that in such a situation, without specialized planning and training, even capable citizens with military or police experience would be too preoccupied with their family’s needs to take any responsibility for the public situation.

In such a scenario, looting and vandalism would become widespread. As Wald described the situation from the perspective of a typical fictitious citizen: “In the evening, he saw vandals going down and robbing supermarkets, banks, and things like that because no policemen, no one gets there, and they took the opportunity -- all the opportunists start to make money from the situation. But close to midnight he realized that also his neighbors are part of the mob. But his neighbors are good persons. They are obedient citizens. What are they doing there?” There was a “phase transition in the society” As Wald put it, one could think of this “as a phase transition in the behavior of the society. People would become ‘hunters and gatherers.’” [In modern times] resources are in the supermarkets, the banks and
in the hands of wealthy individuals.” In the absence of any clear plan, direction or government presence, public order would continue to deteriorate.

Emergency relief in such a scenario, without specialized planning, training and resources, would also be seriously handicapped. With security forces unable to do more than maintain basic order, there would be little capability to support emergency response –sick, injured and disabled populations would be especially hard hit, with many fatalities. Although international aid would begin to arrive several days into such an event, the disrupted security environment would make it difficult to deploy and distribute. And given the levels of need, such aid might, in any case, have little impact.

In short, Wald suggested, without adequate planning, society could collapse quickly. Planning, therefore, must address not simply the technical and logistics problems of resource supplies, but must also focus strongly on social impacts which could prevent critical infrastructure restoration.

There is a solution, Wald concluded. Detailed mitigation plans to prepare, inform and care for the citizenry in such disasters must be included as an essential element of any Black Sky planning effort.

“

In the absence of a clear plan, direction or government presence, public order would continue to deteriorate. Detailed plans to prepare, inform and care for the citizens are essential for Black Sky scenarios.
National Strategy for Space Weather

Seth Jonas gave an update on the work of the Space Weather Operations, Research and Mitigation (SWORM) Task Force, as part of the White House National Science and Technology Council’s “National Strategy for Space Weather.” Their efforts were focused on reviewing the risks and impact of a severe, solar space weather event, or coronal mass ejection, on critical infrastructures.

An important development in measuring space weather was the launch of DSCOVR¹, a space weather satellite that will replace the ACE² satellite. DSCOVR will measure the magnetic parameters of any coronal mass ejection that is coming towards earth. DSCOVR will be coming on line in ten days with live streaming data that may be seen on the NOAA Space Weather Prediction Center’s website³.

Summarizing the results of their work, Jonas said the Task Force concluded there is a need for a detailed, operational focus on mitigation planning for this hazard. He ended his remarks by pointing out that this hazard provides an example of the importance of international cooperation.

“One of the goals in the Space Weather Action Plan and Strategy is International Cooperation…. it is not a single country or a single continent’s problem.”

---

¹ Deep Space Climate Observatory
² Advanced Composition Explorer
³ http://www.swpc.noaa.gov/
Session One  **Keynote Panel**

In this panel, Assistant Secretaries of the U.S. Department of Homeland Security (DHS), U.S. Department of Energy (DOE), and the U.S. Air Force (USAF) reviewed growing concerns for Black Sky hazards, and their perspectives on the road ahead. DHS Assistant Secretary Caitlin Durkovich surveyed the threat environment, focusing particularly on social media-empowered terrorism, the growing risk of serious cyber-attacks on infrastructure and the Black Sky threats of EMP and solar flares. "Our adversaries understand the strategic importance of our infrastructure," she warned. She went on to describe how DHS is working with the private sector, focusing on the National Infrastructure Protection Council, a body in which the government and utilities come together to manage risk.

DOE Assistant Secretary Patricia Hoffman distinguished between security – hardening and protection of the system, and recovery, which involves restoring the system after a Black Sky event. Since security can never be 100%, recovery must be part of any strategy. She argued that, given the unpredictable effects of Black Sky events, any protection strategy should focus on building core capacities that can dynamically and flexibly address a wide range of hazards. Key capacities include the ability to measure impacts, the ability to model their effects, the ability to harden and protect the system, and the ability to integrate new technology.

USAF Assistant Secretary Miranda Ballentine offered a range of insights and perspectives, reflecting growing concerns and new strategies being pursued by the Air Force. Assistant Secretary Ballentine discussed how fuel resilience has long been a crucial Air Force goal, now being updated for the 21st Century through, the introduction of microgrids and renewables, partnering with power utilities to enhance fuel security, and a range of other measures.
Caitlin Durkovich, Assistant Secretary for Infrastructure Protection  
U.S. Department of Homeland Security (DHS)

The Current Threat environment

Caitlin Durkovich began by citing the importance of the gathering, “if we are going to continue to make progress on these important events, it takes all of us here in this room, government and industry, to continue to work towards addressing these serious hazards.”

She then went on to outline three major elements of the current threat environment. Firstly terrorism: “there are individuals who are increasingly calling for attacks against Western interests. And they have an amazing proficiency to leverage the internet and social media to get their propaganda out,” she told the Summit delegates.

Secondly, cyber attackers are becoming increasingly sophisticated. “We need only look at what happened in the Ukraine last December, where a remote cyberattack caused an outage in the Ukrainian grid to understand the possibilities there.”

Thirdly, she pointed out, there are other malicious and natural Black Sky hazards that represent serious risk, including EMP and solar weather. “Our adversaries understand the strategic importance of our infrastructure,” Assistant Secretary Durkovich pointed out, highlighting the electric subsector and the water sector as particular concerns.

The Assistant Secretary also noted a number of areas of increasing vulnerability, including the digitalization of lifeline infrastructure sectors, the likelihood of cascading impacts due to growing cross-sector connectivity, and the greater complexity and interdependency of the supply chains that all sectors depend upon.

“We need only look at what happened in the Ukraine last December, where a remote cyberattack caused an outage in the Ukrainian grid, to understand the possibilities there.”

“Our adversaries understand the strategic importance of our infrastructure.”
Caitlin Durkovich went on to describe what the government is doing in partnership with utility owners and operators to plan and prepare for Black Sky hazards. This includes development of a Space Weather Strategy, as well as binational strategy, in partnership with Canada, focused on grid security and resilience.

DHS’s Office of Infrastructure Protection has developed “a National infrastructure Protection Plan, which is a common framework for how the public and private sectors come together to manage risk.” This has given rise to the Electric Sector Coordinating Council, working to develop coordinated strategies addressing a wide range of infrastructure subjects. An important part of this effort is mapping dependencies between sectors, “to help the providers of those essential services understand who they are servicing. So in the middle of a bad day, it can inform prioritization. “

Assistant Secretary Durkovich ended by stressing two points. Exercises, she said, are particularly critical. “The purpose of doing exercises is not to prove how great your plan is, but it is actually to identify those gaps where you have weaknesses, so you can continue to evolve it.” She went on to emphasize the need to think strategically about upgrading infrastructure so that security and resilience are built in from the beginning. In modernizing the grid, for example, it is helpful to think strategically about where to locate microgrids. She also cited the “One Water Initiative” in California as a great example of incorporating resilience planning against multiple threats into infrastructure development.

“The purpose of doing exercises is not to prove how great your plan is, but to identify gaps, where you have weaknesses, so you can continue to evolve it.”
Key Capabilities for Security and Resilience

Assistant Secretary Patricia Hoffman began by clarifying some terms in order to sharpen an understanding of the Energy Department’s goals. She proposed that the twin goals could be summarized as security and resilience. As she put it: “Security is comprised of hardening protection of the system. Resilience incorporates the ability to recover. We know we can’t be 100% secure. We can’t gold plate the system. Our cost infrastructure won’t support it, so we have to recognize both components.”

Assistant Secretary Hoffman argued that since the threat events of concern are unpredictable and it is uncertain how they would play out, the main priority must be to develop capabilities that can be flexibly applied to a wide range of scenarios.

The first critical capability is the ability to measure. One needs sensors and other tools to measure the impact of events. The Space Weather strategy is developing such tools for measuring solar flare activity, and similar developments are occurring in the cyber field.

Next is the ability to model, to help make predictions. “We want to be able to say what the extent is to which some action is going to cause a cascading failure, and to characterize that impact from a technology and from a system and a system-of-systems point of view.”

Another crucial capability is system hardening, directed toward the most effective security investments. An emerging dimension of this

“Security is comprised of hardening protection of the system. Resilience incorporates the ability to recover. We know we can’t be 100% secure. We can’t gold plate the system. Our cost infrastructure won’t support it, so we have to recognize both components.”

“...We want to be able to say what the extent is to which some action is going to cause a cascading failure, and to characterize that impact from a technology and from a system and a system-of-systems point of view.”
challenge is integration of new technology and architecture into our systems. On the resiliency side, the key capability is to have a recovery plan and an effective restoration process.

Hoffman noted that over recent years the U.S. has placed much more emphasis on system security, with cyber-security becoming a particular area of focus. EMP and GMD protection are still in the strategy development phase. By way of conclusion, Hoffman noted the importance of the U.S. Department of Energy’s quadrennial energy review. The review includes an examination of resilience-related issues, such as development of a strategic transformer reserve and an analysis of the risks to transformers.

“the main priority must be to develop capabilities that can be flexibly applied to a wide range of scenarios.”
Miranda Ballentine described how the Air Force addresses energy resilience. Fuel and electricity security are critical to the Air Force’s ability to carry out its missions throughout the world.

“The Air Force has thought about energy resilience,” Ballentine explained, “although I would say we’ve done it in a fairly nineteenth century way. We’ve had a tool kit in our left hand of technologies, which primarily consisted of diesel generator backup, and in our right hand we’ve had a tool of financial mechanisms to buy these…we’re right now looking to update and bring into the 21st century both of those tool kits.”

Ballentine listed three pillars of this strategy. First, protect and defend the infrastructure that the Air Force owns and operates. The Air Force has many industrial control systems and these need to be hardened against EMP and other threats. The USAF is also building many more smart microgrids that are much more resilient to grid disruption.

Second, “Be resilient.” Ballentine noted the recent establishment of an Air Force Office of Energy Assurance, “whose mission will be to bring together resilient, cost-effective, cleaner sources of power.” In addition, the Air Force has created a “Resilient Energy Demonstration Initiative” – key bases that are building smart microgrids.

The third pillar is rapidly deploying game-changing technologies. Congress has allocated funds to an Air Force Research Laboratory project called the Advance Power Technology Office, which takes market-ready technologies and accelerates their deployment by testing them in real world situations.

“We’ve had a tool kit in our left hand of technologies, primarily diesel generators for backup, and in our right hand we’ve had a tool of financial mechanisms. We’re looking to update and bring into the 21st century both of those tool kits.
In the technology area, Ballentine also stressed the importance of protecting USAF industrial control systems against all threats including EMP. “we need to make sure that those industrial control systems are not only protected themselves from disruption of electricity but also are protected so that they’re not back doors into our other secure systems that manage our mission. Likewise, there needs to be lots of hardening efforts around EMP.”
In a wide-ranging talk, NATO Deputy Assistant Secretary General Dr. Jamie Shea encouraged the audience to rethink concepts of risk, and what it is they are trying to protect against. Drawing on examples from NATO strategy and operations over the past twenty years, he illustrated how attacking a problem in a creative way may yield much-improved results in terms of effectiveness and efficiency. As an example, he spoke of the enormous leverage that can come from choking off terrorists’ sources of funds, rather than fighting them on the ground.

Dr. Shea also emphasized the radical nature of the threat from cyber, noting that “Cyber is the first thing that more or less connects everything together at once. It’s also the first time...when anybody can attack anything from anywhere at any time. It has completely obliterated neutrality or any other kind of physical boundary.”
The Deputy Assistant NATO Secretary General focused his talk on probing our concepts of resilience and risk. Referring to hard-earned experience, as the primary focus of his remarks, he pointed out that creativity, and addressing risks in less obvious, indirect ways can be enormously powerful. By rethinking risk and what it is we are trying to protect against, we can often arrive at better and more cost-effective ways of defending ourselves.

**Anticipation and Strategic Awareness are Key to Resilience**

Dr. Shea urged the audience to think of resilience not just as “bounce-back-ability,” the capacity to “quickly get your systems up and running again, limit the damage and the disruption,” but also as “anticipating, strategic awareness and having a better sense of what’s coming at you; and when.” As the British historian, Thomas Carlyle said about the French Revolution, no one predicted the revolution, but after the event, everyone understood that it was inevitable. The same was true of 9/11. “A lot was out there. We simply didn’t know what we were looking for.”

Mapping vulnerabilities is also a very important aspect of resilience. The internet makes this much harder. NATO has invested enormous efforts in the cyber realm to identify and secure all private and public networks.

**A Key Strategy: Looking for Creative, Cost Effective Solutions**

It is also critical, Dr. Shea explained, to have a clear understanding of what type of risk you want to cover, and the most efficient way of doing so. He related how a few years ago NATO was spending 8 billion Euros a year on counter-piracy operations in the Gulf of Aden, until they realized that placing armed guards on ships was equally effective, and far cheaper.

In this regard, Dr. Shea warned against situations where a problem has become so commonplace...
that doing more of the same becomes ineffective and new thinking is required. He gave, as an example, the devastating, ISIS truck attack in Nice, which 10,000 French soldiers on the streets failed to prevent. Efforts to prevent Islamist radicalization in prisons or on the internet might well be more effective than more troops. “One has to look, when the old paradigm is not working, and therefore you’re getting less and less return on more and more spending on the old methods.”

**Paying Attention to the Evolution in Risk is Critical: The Blurring of Internal vs External Threats**

Dr. Shea noted how threats today have both internal and external dimensions that are increasingly fused. This helps explain why many feel that Russia today is a more dangerous threat than the Soviet Union ever was: “Russia is inside our systems. It owns infrastructure. It controls banks...It has the ability to conduct hybrid warfare on our increasingly sophisticated systems,” he said. “Our vulnerabilities internally make the degree of external power massively more dangerous than it would be if we were simply talking about straightforward tank-to-tank battles.” A similar point holds true for ISIS and other Jihadist groups. This means that resilience and the ability to maintain internal social cohesion in the face of attacks are vital. NATO just declared resilience to be the third area of its military strategy.

**Cyber as a Paradigm Changing Threat**

Dr. Shea then made some observations about the radical nature of the threat in the cyber realm and some of NATO’s challenges in addressing it. “Cyber increasingly controls space, land, and air. So cyber is the first thing that more or less connects everything together at once. It’s also the first time...when anybody can attack anything from anywhere at any time. It has completely obliterated neutrality or any other kind of

“As a symptom of the blurring of external vs internal threats, NATO just declared resilience to be the third area of its military strategy.

“Our vulnerabilities internally make the degree of external power massively more dangerous than it would be if we were simply talking about tank-to-tank battles. Resilience and the ability to maintain internal social cohesion in the face of attacks are vital.
physical boundary… NATO has 200 serious cyber incidents on its systems every month.”

It is also particularly hard to measure cyber resilience or cyber risk. Whereas with conventional weaponry one could go and inspect physical equipment procured, it is much more challenging to assess whether investments made in cyber are effective. “You go to a lot of people who say, yeah, we are in great shape because last year I doubled my cyber defense budget. I feel a lot more secure. What did you buy? I have no idea. Does it work? I have not the foggiest idea.” Another issue is that cyber requires the involvement of industry. Often industry does not understand the special needs of governmental organizations and government does not understand what industry could provide.

**Black Sky Resilience Will Require Creative Solutions**

Shea ended with a warning that success, in addressing Black Sky hazards, will demand creative, original and cost effective solutions that are unlikely to be limited to the most obvious approaches. He concluded, “For every problem, there is a very expensive, very long term, very complicated and ultimately dumb solution. But there is often a much easier, faster, more effective and cheaper solution, if you’re just smart enough to go and find it.”

“Cyber increasingly controls space, land, and air. So cyber is the first thing that more or less connects everything together at once. It’s also the first time… when anybody can attack anything from anywhere at any time. It has completely obliterated neutrality or any other kind of physical boundary.
Panel 2: Primary Challenges and Opportunities in Developing and Implementing Black Sky Playbooks

In this session utility executives and regulators from the United Kingdom and the United States discussed some of the key issues in developing Black Sky Playbooks. Some common themes ran through the remarks of many speakers.

Speaking of the unique challenges posed by prolonged, widespread power outages, many panelists spoke of the value of an all-hazard approach to emergency preparedness, and the critical need for focused, intelligent resilience investment to ensure utilities are robust. Panelists also referred to the valuable role regulation can have in encouraging resilience, but there was agreement that, when it comes to extreme events, regulatory standards are inadequate – the focus for Black Sky hazards needs to be on best practices.

Interdependencies among critical infrastructures were also highlighted as an issue that is particularly crucial to addressing Black Sky hazards. Panelists were uniform in their support for Black Sky playbooks as a vital tool to lay out the comprehensive, cross-sector coordinated planning that will be needed to address interdependencies for these extreme scenarios. Panelists also called out the playbooks’ utility in laying out and planning for tools that will be needed across all sectors, like Black Sky-compatible emergency communications.

Panelists also referred to the role of Black Sky playbooks in helping define the key elements needed for Black Sky exercises. The importance of international collaboration and shared learning was also emphasized.

Among the differences that emerged between the U.K. and U.S. was the far more concentrated nature of infrastructure and utility ownership in the UK compared to the much more diffuse system in the U.S. In the U.K., this centralized ownership pattern, combined with strong government regulation of utilities has helped provide for more coordinated and systematic development of detailed emergency planning for conventional hazards, at least within individual sectors, across the power and water industries.
Government
Sector
Best Practice Resiliency Planning

Joe McClelland began by pointing out that, though Black Sky events may have diverse causes, including EMP, cyber, earthquake, extreme weather, it is helpful to consider them from a common perspective. One overarching concern, when addressing extreme events that go beyond the normal realm of regulation, is “promoting the implementation of best practices to protect the critical infrastructure facilities that matter most.”

Black Sky events will require different planning, procurement, and operations from those conducted to guide the routine course of business. “By definition, black sky events are extreme and must be met with preparation that exceeds routine regulatory requirements that are established to provide foundational practices for application across all the sectors.”

Defining best practice for such situations comes down to answering five questions, according to McClelland.

**Five questions, key to driving best practice resilience development**

1. **Why is the action necessary?** “To get buy-in from the utility industry you’ve got to answer that question.”
2. **What is the best practice for each hazard scenario?** Determining the best practice that should be employed to protect against this situation is essential to ensuring reliable resilience.
3. **“Where do you want me to take this action?”** There are some 55,000 transmission nodes in the U.S. transmissions system. It will not be feasible to implement best practices at all of them.

“By definition, Black Sky events are extreme and must be met with preparation that exceeds routine regulatory requirements that are established to provide foundational practices for application across all the sectors. Promoting best practices to protect critical infrastructure is key.”

Joseph McClelland, Director, Office of Energy Infrastructure Security, Federal Energy Regulatory Commission (FERC)
4. “When do you want me to do this? Is this urgent? Is it something that can wait for a year?”

5. “How am I going to pay for this expense? Who’s going to provide for cost recovery?”

McClelland pointed out that his Directorate in FERC, the Office of Energy Infrastructure Security, has a unique role, intended to help utilities by providing expertise and information on threats which can help inform decision making by industry executives. He summarized this role as comprising four main areas of activity:

**Utility support roles of FERC’s Office of Energy Infrastructure Security**

- Working with government intelligence agencies to identify current threats
  - Informing utilities, by conducting briefings with the facility owners and operators to explain the threats
  - Assessing utility system resilience to key threats, in conjunction with partners at DOE and DHS
  - Offering recommendations to address the vulnerabilities that are identified.

“FERC has determined that it is important to employ both a traditional and a collaborative approach,” he said, concluding. “These programs better enable us to work together to address these threats pro-actively and reactively to prevent - very important to prevent black sky events, and also to limit the events so that recovery can occur. Attacks and vulnerabilities do not respect traditional regulatory processes or jurisdictional boundaries.”
Electric Subsector
Terry Boston, CEO Emeritus, PJM Interconnection

Being Strong in a World Where Things Go Wrong

Terry Boston opened by remarking that he had titled his talk, “Being Strong in a World Where Things Go Wrong.” He noted that the recent mass-casualty terrorist attack caused by a truck ramming in Nice, France underlined the challenging and unpredictable nature of the times we live in.

Boston spoke at some length about the many surprising, unusual hazards he has faced in his career, making the point that we need to ensure we have a robust, resilient grid that can deal with a full set of severe hazards. As one example, he pointed out that power grid configuration changes, and increased redundancy can greatly contribute to its resilience. “The best way to protect a critical substation is to not have any. To have alternate feeds, to have a redundant, robust system. In China, they don’t talk about the smart grid. They talk about the smart strong grid.”

In that regard, he offered his thanks and appreciation for the work done by Joe McClelland and the FERC OEIS Office. “Let me commend Joe and what he’s done on providing the resources to be a robust, reliable, and resilient grid,” he said.

As examples of the full set of hazards, Boston stressed the importance of strengthening the grid against threats of severe terrestrial and space weather, pointing out that – on the “terrestrial” side of that subject, changing climatology seem to be confronting the power industry with increasing, unpredictable challenges. He also referred to the recent cyber-attack that caused a power outage in the Ukraine, and expressed concern about possibility of a major earthquake on the New York Seismic Fault Zone.

“The best way to protect a critical substation is to not have any. To have alternate feeds, to have a redundant, robust system. In China, they don’t talk about the smart grid. They talk about the smart strong grid.”

“In Hurricane Sandy the internet was a good way to communicate. During Katrina, the internet was completely shattered. It took us three days to get communication on wheels, COWs in place so we could talk to the crews.”
Madrid fault in U.S. Midwestern states, with impacts likely to go far beyond that seismic zone.

Boston emphasized how the playbooks are key to the overall Black Sky planning process. “We’ve talked a lot about the playbooks, and today and tomorrow we’re going to talk a lot about coordination between the playbooks, like communication, like potable water, and electricity. Each of the events we learn a lot about and one of the things we learned in hurricane Sandy was the internet was a good way to communicate with all the customers. During Katrina, the internet was completely shuttered. And we could not use it. As a matter of fact, it took us three days to get communication on wheels, COWs in place so we could talk to the crews.”

He focused, in addition, on the role of the playbooks as a stimulus and a tool for developing and then practicing disaster preparedness scenarios, explaining, “Black Sky playbooks… are increasing the opportunities for us to perform drills, and do it for real and build that back into the learning process.”

Boston thanked EIS Council for their unique, new exercise material, referring to EIS Council’s facilitated Black Sky Exercise initiative, and especially the video simulation it provides, as a vital tool. “[EIS Council] put together two videos to say what it’s like to have a plan and not have a plan. He used real actors, which surprised even me, in that video. We showed it at the great halls of Congress in the U.S. at last year’s meeting.”

Terry Boston closed by framing his advice on training with a quote from Vince Lombardy, a famous college football coach. “Practice does not make perfect. Perfect practice makes perfect.” Practicing plans, refining and developing the plans, then feeding back experience from exercises into those plans leads is crucial for the learning and improvement that are needed to address extreme hazards scenarios.

“EIS Council’s Black Sky Exercise video shows what it’s like to have a plan and not have a plan. We showed it at the great halls of Congress in the U.S. at last year’s meeting.”
Scott Aaronson, Managing Director, Cyber and Infrastructure Policy, Edison Electric Institute (EEI)

Public-Private Partnerships for Addressing Black Sky

Scott Aaronson spoke from his perspective at EEI, a trade association for United States shareholder-owned utilities, and also as secretary of the Electricity Subsector Coordinating Council (ESCC). He began by describing the main areas of the ESCC’s work.

Working with government, the ESCC Council can provide opportunities to improve situational awareness, to be better informed about threats so that informed actions can be taken.

Second, information sharing: helping foster the exchange of ideas and information so that CEOs can make the right decisions, at the right times, and improving tools for information exchange at the operator level.

The third area is working across sectors. Aaronson stressed the profound interdependencies between sectors: “If we don’t have water, we can’t generate steam or cool our systems. If we don’t have telecom, we can’t operate.” He underlined the importance of building relationships with other sectors before a disaster, “so that we’re not exchanging business cards on the tarmac.”

There is an essential, symbiotic relationship between government and industry in emergency planning, Aaronson explained. The private sector owns between 88-92% of critical US infrastructure. While industry may be good at running systems, it does not have, for example, intelligence gathering abilities, an army or a law-enforcement mandate. These are crucial government capabilities and prerogatives that will need to work in concert with industry in a disaster situation.

Aaronson pointed to the government’s regulatory role. It not, however, the end of the story. “There is a regulatory responsibility and a regulatory role in protecting critical infrastructure. But it can’t stop there. If you believe that standards in and of themselves are the answer, it’s actually worse than being secure; you’re complacent.

“If we don’t have water, we can’t generate steam or cool our systems. If we don’t have telecom, we can’t operate.”
Challenges in developing a Black Start Playbook for the UK

National Grid is the primary power transmission and distribution company in the U.K. It plays a critical role in enabling all U.K. infrastructure to function. Over the years it has evolved black start planning, which would be used to restart the grid in the event of a full grid power outage. Pullen described four fundamental challenges that National Grid has faced in developing a playbook to lay out these plans for “black starting” the U.K. grid.

The first and biggest challenge is the changing energy landscape in the UK, with the emergence of the low-carbon economy and the consequent shift in the generation mix. The UK’s black start playbook has relied on traditional sources of generation, particularly coal and nuclear. With nuclear plants reaching the end of their operating lives and many coal plants on a trajectory to close over the coming years, it is not clear how the emergency startup capacity will be replaced.

Secondly, the very rapid growth of small-scale renewables in the UK, together with domestic solar, smart grids and smart homes is both an opportunity and a challenge. These sources could potentially provide a lot of help in a Black Start, but much work is needed to understand how they could be connected and controlled as part of the broader power system.

The third factor, involves the commercial challenges of incorporating resilience. “Securing a viable pricing structure that gives large-scale generators the proper incentives to build a black start capability is incredibly difficult,” Pullen warned. Winning consumer acceptance of the costs of

“What is the price people are prepared to pay for an insurance policy for very low-probability events?

“Securing a viable pricing structure that gives large-scale generators the proper incentives to build a black start capability is incredibly difficult.”
resilience investments is another dimension of this challenge: “What is the price people are prepared to pay for an insurance policy for very low-probability events?”

The fourth challenge is deep interdependencies, particularly in the telecoms and communications space. As an example, a primary interdependency concern is the “secondary” telecom systems, needed to communicate with the workforce. “The secondary telecom systems,” he said, is an important concern. In particular, “the reliance on consumerized telecoms, such as mobile phones to make sure you can connect with your workforce. What happens if those systems aren’t available, and you still need the human beings to get to sites to do the things that need to be done to get the grid reconnected?”

Pullen also spoke of the importance of international cooperation. National Grid has some operations in the U.S., and so it is involved with EPRI’s (Electric Power Research Institute) work on EMP and is examining how the results may be implementable in the UK. Also, since “the British have an absolute obsession with weather,” the U.K. is closely connected to the international cooperation around space weather.

“An important interdependency example: The reliance on mobile phones to connect with your workforce. What happens if those systems aren’t available, and you need human beings to get the grid reconnected?”
Water Sector
Playbooks for the US Water Sector

Playbooks for the water sector need to take into account that, unlike in the U.K., the water industry in the U.S. is highly decentralized. There are 52,000 community water systems in the United States. If you add in wastewater, truck stops, amusement parks, and so on, there are around 152,000 water organizations. Most of these are municipally operated which presents issues of governance that are very distinct from those in private companies. “They’re not publicly traded, so that creates a different issue in the sense of governance and establishing issues of priority,” he said. “Those will be some things we would need to work through for something of a Black Sky scenario.”

For Black Sky scenarios, the electricity – water interdependency is crucial, he pointed out. While water utilities make the best use they can of gravity, “power is our major great limiting factor in recovering a water system. Having that coordination between the water utility and the power company is something we’re trying to develop and evolve on.”

Morley also made a key, general observation. A critical resilience issue for water systems in the U.S. is the aging infrastructure, and the expense and complexity in replacing it. “On the drinking water side alone, from an aging infrastructure perspective, [we will need] on the order of one trillion dollars between now and 2035 for just distribution and transmission.”

The majority of those systems are municipally operated. That creates an issue for governance and who actually sets priority. Those will be some things we need to work through for a Black Sky scenario.

Power is our major limiting factor in recovering a water system. Having that coordination between the water utility and the power company is something we’re trying to develop.
Budgetary issues are key for resilience investment, pointing to the need for cost effective measures, and regulatory buy-in. Small organizations have small budgets to invest in security and resilience.

In closing, Morley noted how Hurricane Katrina was a pivotal event for resilience planning in the water sector. It catalyzed a shift towards an all-hazard approach to emergency planning and also led to the creation of “a relatively robust mutual aid network” among water utilities. However, that in itself raises the concern that resilience investment, in the water industry as elsewhere, tends to be exclusively episodic.

“In the 1940s water utilities spent a lot of time talking about mutual aid and assistance. But … we didn’t talk about it again until after hurricane Katrina,” he said. “But that points to the challenge here of episodic attention. We’re really good at … saying this is really important after something like Sandy.” This episodic approach, he suggested, will need to be overcome to build resilience for Black Sky hazards.

Summarizing, he emphasized the importance of the summit, and the presence of many interdependent sectors. “Working together and being involved in this conversation I think is really important.”

“In the 1940s water utilities talked about mutual aid and assistance. But we didn’t talk about it again until after Hurricane Katrina. We're really good at saying this is really important, after something happens, like Superstorm Sandy.
Emergency Planning in the UK water sector

Falsey described some of the resilience planning at Yorkshire Water. The water industry in the UK is competitive but also highly regulated. “We have to justify our investment to customers and regulators… Companies receive instructions from the government on resilience.” Falsey explained.

The U.K. water industry also has well-practiced mechanisms for sharing resources in an emergency, for example pumps, personnel, vehicles, power. Falsey noted how impressive it is “that commercial organizations work so hard to assist each other, rather than exploit their weaknesses for gain.”

There are extensive plans and exercises that are regularly rehearsed to prepare for emergency situations, including power outages. “[There has been] a focus on building flexibility for local short-lived problems. A number of critical assets have standby generation for 72 hours,” he said. However, policy for such standby generators varies. “Some companies have 100% fixed standby; on large sites, some half of that; on smaller sites, it could be 20%, and some companies have limited numbers of movable generators that they own, or they have framework agreements. However, frameworks give no guarantees.”

These emergency power limitations make power restoration to water companies critically important. “Some power companies may concentrate on getting as many customers back on in urban areas as a priority. A water company may count as one customer, and our assets usually are important assets, are usually in rural areas.”

Besides more standby generation, he also pointed out, critical assets needed for continued operation in a prolonged outage will include chemicals, and staff with the right skills.

“It is impressive to note that commercial organizations work so hard to assist each other, rather than exploit their weaknesses for gain.”

Martin Falsey, Physical and Electronic Security Manager, Yorkshire Water
Session 1 Concluding Remarks

Congressman Trent Franks, U.S. House of Representatives

Congressman Franks first looked back on the evolution in Black Sky hazard awareness and efforts, reviewing progress in six years of Electric Infrastructure Security summits. He recalled how hard it was, years ago, for people to understand the gravity of the concern and, by contrast, today’s strong bi-partisan understanding of the issue and support for taking action. As an example Rep. Franks cited the Critical Infrastructure Act, which has passed in the House of Representatives and would, Franks cautiously predicted, soon be approved by the Senate.

He noted that EIS Council’s EPRO Black Sky Exercise has been particularly helpful in helping decision makers to understand the gravity of severe hazards, enabling people to absorb the implications of a massive, prolonged power outage. Franks recalled the first, facilitated Black Sky Exercise, which took place as part of EISS VI in the U.S. Capitol Building in Washington D.C. “About half an hour into that, we saw people who were previously pretty skeptical, all of a sudden begin to realize what kind of danger there would be if a significant part of the grid were damaged.” As the exercise forced them to begin thinking through their own response options, it quickly became apparent that cascading failures, “a ripple effect” from the outage, would disrupt nearly all options. They then realized it “made what they were going to do impossible or very difficult.”

Franks ended by encouraging the audience to recognize the urgency of the work, invoking Ronald Reagan’s words:

"'You and I have a rendezvous with destiny...If we do fail, at least let our children and our children's children say of us that we justified our brief moment here. We did all that could be done.' -- Rep. Franks, quoting President Ronald Reagan"
Session Two:
Black Sky Recovery Planning and Implementation
Session Chair

The Rt. Hon. Lord James Arbuthnot

This session surveyed some of the key components of a Black Sky recovery. Among the subjects covered were several of particular importance to ensuring national continuity through a Black Sky event:

- The technical complexity of executing black start (restart of power grid segments without using power from outside the disabled grid segment)

- The critical importance of extensive, well-maintained, regionally deployed emergency generators designed for continuous operation and for Black Sky-compatibility. This is connected to the need for assured, continued production and distribution of diesel fuel for critical, prioritized facilities, preplanned for these scenarios.

- The vital significance of having sufficient, trained power engineering teams available, with pre-planned and pre-certified supplemental technical support labor to find and repair power grid damage, and region-by-region restoration and restart.

In going through these subjects, a number of important points were highlighted.

Avi Schnurr, chairing the session, reviewed emerging ideas for changes that could utilize nuclear power stations as a key asset during restoration operations, rather than a significant liability and drain on diesel fuel production and distribution, and technical support resources.

Gerry Cauley, the CEO of NERC4 stressed the importance of training and exercises, and especially the critical significance of designing training exercises that incorporate the highly disrupted reality that technicians and engineers would face. “What if our computers or cyber assets are damaged or hindered? What if there is physical equipment that is damaged, and we need to re-supply equipment?” he asked. “What if fuel supplies, transportation, those kinds of things are no longer available?”

Finally, Dr. Fernando Maymi, Deputy Director of the U.S. Army Cyber Institute at West Point, strongly emphasized that the overall infrastructure restoration process after a Black Sky event will require far more than technical and engineering expertise. Planning is needed, he pointed out, to provide for the extensive coordination and management that will be essential to enable many teams from multiple sectors with diverse backgrounds to work effectively together in highly disrupted environments.

4 North American Electric Reliability Corporation

“How can we begin thinking more about nuclear power as a black start cranking path asset, rather than struggling to answer the question: ‘How on Earth are we going to provide adequate diesel to keep such systems cool when they are shut down?’
Introducing the panel, Avi Schnurr reviewed some of the main areas where resilience investments and coordinated planning for restoration support are essential in preparing for Black Sky hazards. The planning and investment needed fall into three main areas.

The first, foundational level is the “black start” system – the regionally distributed grid elements designed to restart segments of the power grid when an outage is so widespread that “outside” power is not available to kickstart the system. The procedures for black start are well-thought out and robust, but they can only be implemented if four preconditions are met.

**Preconditions for grid “black start”**

- **First:** The black start system components themselves have built-in protection against Black Sky hazards, and – at least for some units – are “fuel secure:” they have adequate collocated or solid connectivity to large scale fuel supplies so generating stations can operate for weeks, even if “just in time” natural gas pipeline deliveries are disrupted.

- **Second:** Emergency power is a key requirement to initiate these “black start” units. Emergency generators are typically available at black start facilities, but it is important they are designed to survive the full set of Black Sky hazards. Diesel fuel for these emergency generators – adequate to support both a “safe shutdown” and for system restart – must either be onsite, or provided for by a preplanned, multi-sector efforts to ensure diesel fuel delivery in these disrupted scenarios.

- **Third:** Key personnel represent a critical requirement. High-power relay engineers, for example, who would be critical to troubleshoot and activate black start hardware after an extreme event, are in short supply at the best of times.

Avi Schnurr then went on to detail a number of initiatives that EIS Council is hosting, designed to help address these areas.

Since those emergency generators available today are resourced to address only conventional, local or regional hazards, there are simply not enough in the world to deal with such an event. The “National Emergency Power Council” Initiative develops some ideas and recommendations on
joint business and government approaches to address this shortfall. This will require, in particular, provisions for broad, multi-sector coordination – both pre-event and during restoration – that does not currently exist. In consultation with government and business leaders, work is beginning to suggest approaches to address this need in a new SCSR Initiative, as a key element of next year’s planned EPRO HANDBOOK III publication.

Another effort – the BLACK SKY / BLACK START PROTECTION (BSPI) INITIATIVE, is designed to consider operational changes that could potentially utilize nuclear power plants as can an asset, rather than a liability, in a Black Sky situation. “How can we begin thinking more about nuclear power as a black start cranking path asset, rather than struggling to answer the question: ‘How on Earth are we going to provide adequate diesel to keep such systems cool when they are shut down?’”

In the key personnel area, the Certified Power Recovery (CPRTM) Initiative is hosting cross-sector discussions on opportunities for preplanning, and pre-certifying, auxiliary tech support personnel. This effort is exploring development of a possible new talent reserve that would far exceed today’s limited consultant support resources, bringing in volunteer cyber and IT professionals and aerospace engineers, who, with a few days a year of training at local power companies, could become a source for a vital supplemental capability in restoration following extreme events.
Gerry Cauley, CEO and President North American Electric Reliability Corporation (NERC)

Black Start Planning for the US Electric Sector

Gerry Cauley spoke about the current state of the electric subsector's black start and power restoration capability, and some of the challenges going forward. Summarizing these subjects, he made five key points.

Black start challenges
Black start is difficult. "It is highly complicated and technical," Cauley emphasized. "It’s really a very complicated technical engineering feat to do a recovery.” Most system restarts are not black start events, because it is extremely rare for a very large segment of the grid to crash – there is usually some accessible, nearby operating portion of the grid to build upon. But in an actual black start recovery, “you basically have to disconnect everything, start your black start generators and start connecting lines one thing at a time.” You have to carefully watch the frequency and voltage to ensure they do not exceed the systems protection limits. “You could very easily topple the dominoes and have to go back to ground zero. It could take days…”

There is a role for restoration standards and requirements
Secondly, there is a role for standards and requirements because they set minimum expectations. “In North America, all transmission operators, grid operators are required to have restoration plans that have been validated through testing.”

Exercises, practice and training are vital
Thirdly, “We need to back this up with exercise and practice and training. Because they’re rarely deployed, we need to be able to have that capability to practice and make sure that it works.”

“ It’s really a very complicated technical engineering feat to do a recovery.

“ What if our computers or cyber assets are damaged or hindered? What if there’s physical equipment that's damaged and we need to re-supply equipment? What if fuel supplies or transportation … are no longer available?
Cauley recalled how gratifying it is to observe first hand black start drills and exercises at utilities including PJM, ERCOT, Southeast Region CERC, the Florida Grid, Alberta, and San Diego. NERC and FERC have done a joint study on black start restoration plans.

**Expanding training and exercises to include preparation for Black Sky events**

Cauley’s fourth point, which he framed as a challenge to industry, is that it’s important to include Black Sky restoration in training efforts, recognizing that there may be major disruptors to plans in a real Black Sky event. There could be civil disorder and riots. “What if our computers or cyber assets are damaged or hindered? What if there’s physical equipment that’s damaged and we need to re-supply equipment? ... What if fuel supplies, transportation, those kinds of things are no longer available? And what if telecommunications are not available?” Therefore, Cauley stressed, black start plans should be implementable in a resilient and self-reliant way, compatible with the needs for Black Sky events. This will mean planning for adequate backup personnel, fuel supply and emergency communications planning, designed to minimize dependence on external support as much as possible.

“It is important that new wind and solar resources have voltage control and ride-through capability and frequency responsiveness, so that they can help recover the system in a time of need, rather than be a burden.”

**Renewables and other new power resources must be built into black start planning**

The fifth point was that as new resources, especially renewables, are added to the grid, it is important to maintain robust generators that can start independently and can also flexibly manage the voltage and frequency of a portion of the grid. It is important “that new wind and solar resources have voltage control and ride-through capability and frequency responsiveness, so that they can help recover the system in a time of need, rather than be a burden.”
Emergency Power, Fuel and Consumables for Black Sky Scenarios

Peter Navesky focused on the issue of temporary emergency power, another of the key components of a Black Sky recovery. “Does this mean the cavalry is coming over the hill? Well, it may be the cavalry, but they’re on Shetland ponies,” he quipped.

In an emergency, the Army Corps of Engineers will install FEMA inventory generators, typically less than one megawatt at sites that the state and local authorities deem critical. “Right now, FEMA’s current inventory of generators is only about 800. And that’s between the four Continental United States distribution centers,” Navesky explained. This number is sufficient for storms and hurricanes, but falls far short of what would be needed in a Black Sky event.

Moreover, “Most of the FEMA inventory is about a minimum of 10 to 20 years old. They’re analog type units.” The inventory is being modernized to be digitally controlled. However, they are not being hardened in any way, so there is a serious question about whether they would work after an EMP or GMD event.

Navesky also mentioned, a federal program to equip diesel electric buses to be sources of emergency power generation.

Although also quite limited in availability, FEMA units may be supplemented by commercial units rented through the Defense Logistics Agency, which also hires fuel distribution contractors to supply bulk fuel to FEMA in support of a disaster. FEMA generators require refueling about once every 24 hours – a serious challenge in a Black Sky event that will require special planning.

“Does this mean the cavalry is coming over the hill? Well, it may be the cavalry, but they’re on Shetland ponies. Right now, FEMA’s current inventory of generators is only about 800. And that’s between the four Continental United States distribution centers. This number falls far short of need for a Black Sky event.
Dr. Fernando Maymi, Deputy Director, U.S. Army Cyber Institute at West Point

The Need for a Technical Labor Surge Capacity: A Cybersecurity Example

The U.S. army is increasingly concerned about a major cyber-attack, Dr. Maymi reported. “There’s really very little probability that our adversaries are going to land tanks on the shores of the Hudson River and invade New York City, or drop paratroopers in the plains around the city... But there is a very high probability that a sophisticated and determined adversary is going to use cyberspace to inflict some significant damage on us for strategic reasons.”

As part of an Army priority to examine cyber-protection for urban mega-cities, the Army Cyber Institute partnered with EIS Council and Carnegie Mellon University to run a “cyber mutual assistance workshop bringing together government, academia, and the power sector to discuss what cyber mutual assistance would look like.” Dr Maymi reported on some of the findings of the workshop.

The workshop identified 52 specific skill sets that would be necessary to be part of a mutual assistance effort. 30 of those map directly to IT (Information Technology) skills that the army has been tracking through the cyber workforce development programs run by DHS. A further 10 dealt with OT (Operational Technology). But 12, to Dr. Maymi’s surprise, dealt with leadership and management: “Who’s going to lead extended teams from multiple organizations where government is working side-by-side with industry?” he asked. “Who has experience doing this sort of integration work? How are we going to do command and control?”

In addition, he said, there is an acute need for people whom he termed “translators,” that is to say, “people who can relate to the acquisition world, to the contracting world to get assets very,
very quickly that may not be in abbreviated timelines -- people who can translate between OT and IT…"

The Army’s cyber mission forces have “Cyber Protection Teams… who have the responsibility, when requested by the private sector and State governments, to go in and assist in recovery efforts.” But the ability of these forces to accomplish such missions has barely been tested. Moreover, there is little understanding of how local, state and federal government would interact in dealing with a cyberattack crisis, and very few exercises have attempted to model this. Furthermore, “there’s very little evidence of any exercise being done that integrates both the technical component and the leadership component, meaning they force the technical folks to not do things that they want to do because they make no business sense.”

In addition, Maymi found, there is a more general problem in addressing leadership issues for Black Sky events. In typical exercises, he said, “You weren’t coordinating the efforts between the financial sector and the power sector and the healthcare sector.” This became apparent in the workshop itself. The cyber defense workshop brought together different sectors, public and private in the New York area. To their surprise, cyber professionals from these different areas had never met each other. None had participated in such an exercise before.

Dr. Maymi concluded with the observation that there is a need for much more training and cross-sector cooperation, if we are to be prepared for a large scale, multi-sector cyberattack that will likely occur at some point.

“Who’s going to lead extended teams from multiple organizations where government is working side-by-side with industry? Who has experience doing this sort of integration work? How are we going to do command and control?”
**Overview**

In this extended talk, Neil Siegel summarized the Black Sky emergency communication and coordination architecture study that he, Bran Ferren and the Applied Minds, Inc. team developed for EIS COUNCIL. Leaders from all the sectors involved in the hosted Black Sky planning process have broadly agreed that without a widely distributed, interoperable, robust emergency communication and coordination system that could function with no external power for more than a month, infrastructure restoration and saving and sustaining lives in such extreme scenarios would be, essentially, impossible.

Summarizing the “social architecture” of the system – its concept of operations – Siegel pointed out that, to meet the needs for a subcontinent-scale, long duration outage, an emergency communication system would need to support at least 100,000 nodes in the U.S. Based on extensive trade studies, the team selected a technical configuration that addresses the unique needs for these extreme hazard scenarios. The BSX architecture calls for radio-based operation, using substantial robust vanadium redox flow battery modules, capable of hosting voice communication and some data transfer. The system is designed to closely resemble the U.S. Army’s Digital Battle Communication System, with additional features required for Black Sky scenarios. The Army system, also designed by the Siegel / Ferren / Applied Minds team, has now been successfully used in three battle theatres.
Note: Dr. Siegel summarized the results of the BSX architecture study for the summit delegates, focusing his remarks on the communications portion of the overall system architecture. Key aspects of the system’s “coordination” design were addressed (and summarized in this report) later, by Bran Ferren. Commissioned by EIS Council and undertaken jointly by Neil Siegel, Bran Ferren and Applied Minds, Inc., the study will be the subject of an extensive and expanded review as part of the upcoming EPROM Handbook III, now scheduled for publication at EIS Summit VIII, summer, 2017.

BSX Top Level Requirements

The top level mission requirements for BSX are applicable, in concept, to any emergency communication system intended to be Black Sky-compatible and nationally deployed. They call for a highly interoperable, very widely distributed emergency communications system designed to survive and be viable in Black Sky scenarios. To achieve this, the system must provide for adequate voice and data communication, as well as flexible routing to allow for the multi-sector connectivity needed to support infrastructure restoration and save and sustain lives when the nation’s existing communication backbone is inoperative.

To meet these needs, the system is designed to utilize very cost effective nodes that can be deployed at nearly all utilities, at key fuel / water / food / pharmaceutical / hospital / transportation / security facilities and suppliers, at state and federal agencies and with many other stakeholders. The architecture is configured to be easily adaptable for interoperability with government agency or corporate-based communication systems, where they are both available and operational in these disrupted, extended duration scenarios.
Provenance of BSX Requirements

The background to the study is the fact that our extraordinarily fast, cheap (per user) and pervasive communications systems, carried by electrical or fiber optic cables, microwave transmission, internet, satellite, or cellular systems are not expected to remain continuously operational in subcontinent-scale power outages lasting weeks to months, caused by EMP, cyber, earthquake or some other Black Sky hazard. As Siegell put it, “unfortunately, every study that I’ve seen that looks at these really serious black sky events, whether caused by EMP or some of these other causes, basically says when the power goes down for more than a few hours, all these communications systems also go down.” In fact these systems did fail, sooner than most people expected, in far smaller disasters such as Hurricanes Andrew, Katrina and Sandy.

Based on input from each of the sectors involved in EIS Council’s EPRO SECTOR coordination initiative, a Black Sky exercise was developed, simulating two very different scenarios. In one, with no provision for any comprehensive communication system, coordination among restoration teams and other essential sectors was extraordinarily difficult, a key contributor to the disastrous consequences projected for that scenario. In the other, a widely distributed, solid emergency communication system was instrumental in allowing all sectors to coordinate both restoration support and lifesaving operations. This result, coupled with the extensive feedback sectors provided from these facilitated exercises, provided the basis for system’s top level requirements.

“...unfortunately, every study that I’ve seen that looks at these really serious black sky events, whether caused by EMP or some of these other causes, basically says when the power goes down for more than a few hours, all these communications systems also go down.”

Note that, in Superstorm Sandy, New York’s emergency communication system remained continuously operational when all normal communication systems failed. That system was designed and built by the same team responsible for the BSX study.
Detailed Requirements and Concept Design

- Social Architecture

Siegel first presented the “social architecture” of the system: “Who uses this thing? Where do they use it? What do they use it for? Who do they talk to? How often do they need to talk to those people?” Siegel estimated that the required system would need to provide around 100,000 nodes in the U.S.

Given this system size, the economics of current telecommunications systems that serve hundreds of millions do not scale down to 100,000. Replicating some reduced version of the nation’s telecommunications backbone would, therefore, be unaffordable, by a very large factor. This mandated a very different technical design. “The system is going to provide a more modest data rate than what we have gotten used to, but it’s still going to provide more information than human beings can assimilate.” A lot of this will be voice communication, but the system will also provide a capability to communicate statistical data sharing.

In the next phase of development of the BSX system architecture study, this capability will be used to support situational awareness so coordinators and decision makers will have visibility into real time status, as well as infrastructure interdependency model hosting to provide for decision support. It also can support public messaging, anticipated to be particularly useful if, and when, personal vehicles or other devices eventually have provisions for long-duration operation of at least basic emergency message readout. Finally, the system is designed to be flexible and adaptable, as a Black Sky scenario is inherently unpredictable.

- Technical Architecture

Siegel next moved on to the “technical architecture.” In developing the technical aspects of a system’s concept design, key questions include, for example, “What does this thing look
like? What’s the design? What kind of devices? How do we power it? How do we train the people? And of course, reliability, long storage life, feasible economics at the modest scale of deployment...” Siegel proposed to walk the audience through some of the key steps in implementing these system requirements with the selected concept design.

Transmission – To transmit information, the system will use radios, using two different frequencies. One would operate for low data rate transmission over long ranges, and one using a higher frequency would provide higher data rates at intermediate ranges.

Power Supply – Nodes must operate without external power for 30-60 days, far more than the 8-10 hours of backup power that cell phone towers are typically supposed to have. Diesel generators are not the solution – if they are stored for years they won’t work when needed, the fuel will have gone bad and they will break down after a few weeks of continual use. The power source must, therefore, utilize batteries, of a type and design that can still work well after 20-30 years of storage, supplemented, where appropriate, by solar panels. Vanadium Redox flow batteries were selected to meet this need.

Storage and Portability – The radios and batteries can be stored at fixed strategic locations such as power plants, substations, water plants or suppliers’ facilities, and are also portable enough to be mounted on trucks to operate on the move, as emergency staff inspect power lines and manage traffic, for example. Trucks may also be used to recharge the batteries, where appropriate.

Network Reliability – Clearly the system needs to be specified for high reliability. The design achieves network reliability through provisions for flexibly routing communications through many..."
different, available paths, so that if one or more are down the message can still get through. The system chooses the best path automatically.

Frequency Selection – Careful consideration was given to frequency selection. “We have to use this in normal times for rehearsal and practice,” Siegel pointed out. In addition, at any time, including in an emergency, there will be many different users competing for frequency use.

Legacy from Existing System Configurations – This system does not end up looking much like today’s VoIP or cell phone systems. However it does in large part resemble the U.S. Army Digital Battlefield System, which the BSX team designed, and which has operated successfully for over 15 years in three theaters of war. A similar system, also designed by the BSX team, was in use in New York during Superstorm Sandy and was one of the few systems that kept working. This “legacy value” is important in building confidence in the viability, and reliability, of the design.

EMP and Cyber Protection – Siegel elaborated on protection of the system against EMP and cyber-attack, responding to a question. Building system components to be intrinsically EMP protected would increase the cost. Instead, the approach selected is storage of key components in Faraday Enclosures or, for small units, Faraday bags. Given the architecture, cyber protection, he pointed out, can make use of some unique features of the design and planned system utilization.

Siegel , emphasized that a similar tested had been tried and tested in an emergency: “We built the emergency communications system in the city of New York. During Sandy, it was the only thing after about hour four that still worked. It operated continuously through the whole multiple weeks… So there’s actually some data points that says this is an appropriate design for this scale and this reliability system.”
Panel 2
Key Considerations for Black Sky Recovery Operations – National and International Challenges and Opportunities

Panel Chair: Brig. Gen. (Ret.) John Heltzel, Director, Resilience Planning; EIS Council

This session covered a range of operational areas and perspectives. Bran Ferren presented the essentials of what a functional situational awareness and decision support system for a Black Sky event would need to look like. He stressed that such a system needs to be simple and resilient so that it can operate under conditions where there will inevitably be numerous technical and human failings, and to compensate for them. “At times of disaster, people behave badly and imperfectly, and they lose dozens of points of IQ,” he counselled.

Officials from the European Commission and the OECD\(^6\) offered perspectives on how their international organizations can offer member states support, both in preparing for and responding to emergencies. James Kish from FEMA stressed, like other speakers, the paramount importance of training and exercising. He also acknowledged the difficulty for companies and government agencies in investing adequate time to address severe scenarios, when “we all have day jobs.” Building scope into both public and private sector organizations for addressing these catastrophic scenarios will, he pointed out, be essential. He also highlighted training for Black Sky hazards as a key enabler, noting that after the training, a program for implementing lessons learned is always essential.

Yechiel Kuperstein from Israel’s National Emergency Management Authority emphasized the critical importance Israel places on fostering public resilience; this is a precondition for recovery workers from all sectors to be able to function. He also discussed Israel’s remarkable efforts in stockpiling food, water, fuel and medical supplies for emergencies. Finally, Paul Stockton brought the discussion back to recovery, stressing the goal to “build back stronger” after a disaster. He recommended that this be included, as a priority, along with other elements of planning for Black Sky hazards now moving forward.

\(^{6}\) Organization for Economic Co-operation and Development
Bran Ferren, Co-Founder, Co-Chairman and Chief Creative Officer, Applied Minds, Inc.

BSX™ Communication and Coordination System:
Key Architecture Considerations for a Black Sky-Compatible National Recovery Coordination System

Note: As noted earlier, Neil Siegel, Bran Ferren and Applied Minds, Inc., are developing the architecture of a Black Sky Emergency Communication and Coordination System (BSX) for EIS Council. This presentation, reviewing the “coordination” aspects of BSX, follows the earlier presentation by Neil Siegel, which reviewed the communication-related features of the system.

Bran Ferren discussed what a coordination network for a Black Sky event might look like. “A ‘command-and-control’ network is a thing… whose job it is to use artificial intelligence and other techniques to manage the flow of communications and understand the status of the network,” Ferren explained. “Let’s just say the lights here went out. The phones are out, the radios are out, the television is out. Well, is half the country a smoldering crater or is everything just fine and someone with a backhoe cut a cable in front of the building? It’s very hard to know… So the first part of a system like this is to provide visualization of what’s there. What is the network status? Is it up? Is it running? Is it operating?”

Ideally, such a system is integrally connected to a communications network, and is also used to manage communications. There are three relevant classes of communications: people to people, machines-to-machines, and then hybrids of people and machines talking together.

“Let’s just say the lights here went out. The phones are out, the radios are out, the television is out. Well, is half the country a smoldering crater or is everything just fine and someone with a backhoe cut a cable in front of the building?

“Tomorrow, what we do is start designing a network that gives you the lowest baseline of survivable communications.
“A machine talking to a person could be a generator reporting its load, its status, its condition, its operating health. People-to-people might be saying ‘okay, now.’ And at the same time machine-to-machine is background status, which keeps that visualization picture up, which shows you what nodes are up and operating. You want to keep the network busy, reliable, and active,” Ferren stressed. It’s also important to keep these systems simple: “The more technically complex these systems become, the more vulnerable they are to compromise and attack”. Ferren emphasized the urgency of establishing a simple, working system. “The question is what do we do tomorrow? And tomorrow, what we do is start designing a network that gives you the lowest baseline of survivable communications with a command-and-control network that takes that network and all of the other available networks and provides you with those three basic classes of service.”

The system also needs to be able to “heal itself,” that is to operate under conditions where there will inevitably be numerous technical and human failings and to compensate for them: The “social architecture” needs to take into account that, “At times of disaster, people behave badly and imperfectly, and they lose dozens of points of IQ. So you need systems that are simple and that are able to work with people under extreme stress, worried about their family.” The technical architecture needs to be to be “sufficiently robust, resilient, and reliable so that if attacked it can rebound. If subject to a cyberattack, it is sufficiently resilient that parts of it will fail and collapse, but you may still have push-to-talk capability left,” Finally there is the operational architecture, that is, “the playbook, rehearsals, and mission scenarios and planning we’ve all decided that we think we’re going to do in conclusion, Ferren reiterated that a system needs to be self-healing and adaptive.

“At times of disaster, people behave badly and imperfectly, and they lose dozens of points of IQ. So you need systems that are simple and that are able to work with people under extreme stress, worried about their family.

“The technical architecture needs to be to be sufficiently robust, resilient, and reliable so that if attacked it can rebound.
Ian Clark, Humanitarian Aid and Civil Protection Office European Commission

European Commission: Highlights of Existing Civil Protection Plans and Future Considerations for Severe, Wide-Area Power Outages

Ian Clark outlined some of the ways in which the European Commission manages disaster relief cooperation across the European Union (EU). The EU acts to support national disaster relief efforts. “The EU role is essentially to match the needs of the country with offers which come from other EU countries’ in-kind offers. These could be pumping stations, forest fire airplanes, medical teams, or mobile generators,” he explained.

In the newer area of preventing and preparing for disasters, EU counties have agreed to share national risk assessments which cover all hazards, particularly in the area of resilient infrastructure. Countries have also agreed to cooperate and share information on risk-management capabilities.

A tool which has been recently introduced learned from the Organization for Economic Cooperation and Development (OECD) is a peer review of disaster management capabilities in countries, whereby they invite experts from other countries to provide recommendations on how they can approve policy and operations. The European Commission is also cooperating internationally, for example, with FEMA in the United States on space weather warnings.

“The EU role is essentially to match the needs of the country with offers which come from other EU countries’ in-kind offers. These could be pumping stations, forest fire airplanes, medical teams, or mobile generators.”
Jack Radisch, Project Manager, High Risk Level Forum Organization for Economic Cooperation and Development (OECD)

Key Considerations for International Organizations in Black Sky Recovery

Jack Radisch reported that of 35 OECD countries, 16 have a critical infrastructure protection program. He discussed a number of lessons and observations from his involvement in peer reviews of disaster preparedness on behalf of the OECD.

Reviewing the massive 2011 earthquake and Tsunami in Japan which led to the Fukushima Nuclear Plan disaster, Radisch asserted that this was initially comparable to a Black Sky event. “There was a communication blackout. There was no electricity in the affected areas. There was very little information that could go in or come out.” Although Japan has the reputation of being one of the best prepared nations in the world for civil contingencies, they were not prepared for an event of this magnitude.

Radisch painted the picture: “So people are out of their homes, they’re in the cold, they have no electricity. They have no communication. They have very little food, and they don’t know when or where they’re going to get help.” When he had asked why Japan’s emergency mobile communications units, which he saw deployed on the hilltops, were not used, the answer was that there was no fuel for them.

Radisch concluded that, as hazards become more severe, Japan’s experience shows us that cross-sector coordination is critical. “Japan is very well prepared in many cases. However, they have a culture of being very siloed in their operations across ministries… you don’t see a real complexity in the resilience building that takes into account these very ‘wicked’ situations.”
James Kish, Former Assistant Administrator for Response
U.S. Federal Emergency Management Agency

Key Considerations for Federal Roles in Black Sky Recovery

James Kish surveyed some of the challenges and opportunities associated with Black Sky events from the point of view of FEMA, the agency in charge of emergency management for the federal government.

The first, obvious challenge is that a Black Sky event “exceeds by at least an order of magnitude the types of planning that we’ve undertaken,” he said. “The notion of a total blackout pushes us beyond what we have traditionally been prepared to deal with.”

A further challenge is the degree to which the efforts of many different agencies would need to be integrated together in responding to such a widespread, long duration, catastrophic event. Kish emphasized, “We need to train more. We need to exercise more.” Moreover, the “bandwidth” that organizations have to devote to preparations for extraordinary events has been limited. “The problem is, we all have day jobs. Every organization here has a budget cycle that’s built for the status quo.” Building scope into both public and private sector organizations for addressing these catastrophic scenarios will, ultimately, be essential.

Kish pointed to training as an essential part of addressing new threat categories like “Black Sky.” This will, he said, include a unique challenge: How thoroughly can one test elaborate contingency plans for events whose consequences are difficult to imagine? However, while the learning that can come from exercises for new hazard classes could be vital, Kish cautioned about the capacity of relevant organizations to manage such a process well. “Honest, critical, effective assessment” is essential, he pointed out. Also, he said, extracting and understanding “the distillation of tasks
that must be managed, and improvements that must be made is an inherent weakness of the organizations I’ve been part of.”

Moving to opportunities, Kish described how FEMA has developed a “cycle of improvement for doctrine, training and exercises.” FEMA has identified a standard methodology for planning that is used at both national and regional levels. This planning calls for increasing integration of the “whole community” into emergency planning. Overall, Kish concluded, high-profile disasters like Sandy have brought greater focus on emergency management from the top levels of political leadership in the federal government.

“The problem is, we all have day jobs. Every organization here has a budget cycle that’s built for the status quo.

“This planning calls for increasing integration of the whole community
Yechiel Kuperstein, Consultant, Israel National Emergency Management Authority

Israel’s Emergency Management Approach to Severe National Disaster Scenarios

Yechiel Kuperstein described the Israel National Emergency Management Authority’s unique approach to disaster response. He traced the evolution of the country’s emergency response bodies from a civil defense organization in the 1948 war of independence, through the Economic Emergency Committee designed to deal with the economic fallout of war. This evolved significantly, most recently following the Second Lebanon War of 2006, where Israeli civilians were intensively targeted by Hezbollah, making the distinction between civilian and military response increasingly unhelpful. Today, NEMA is part of the Ministry of Defense. It has developed in numerous iterations to respond to diverse threats.

The primary functions and critical sectors for disaster management

Israel defines five main functions of disaster management:

- Lifesaving
- Resilience of the community and persons - Enabling people to continue with their daily routines
- Information
- Civil defense
- Resilience of the economy.

The most critical sectors for supporting restoration and saving and sustaining lives, he said, are power, emergency fuel, communications, natural gas and public resilience: “If one of them is going to break down or crack, all the rest of them are going to need to support.”
The crucial importance of building an attitude and capability for public resilience

Kuperstein noted the special importance of public resilience as a precondition for resilience in other areas: “In most cases we look at public resilience as the objective. We want to create public resilience. But it’s also the one that generates all the others. You need public resilience to bring manpower into the power stations, and you need people in place to support communications or whatever else is needed to restore civil functions.”

The three key requirements for societal and economic resilience

Societal and economic resilience, Kuperstein explained, rests on three key requirements.

- **Emergency Supplies:** The first is stockpiles of emergency supplies: “And I’m sure someone is going to ask, ‘stockpiles, who’s paying?’ Yes, the government is paying, ... they range from food to fuel, medical supplies and even animal food. Because you will need milk and eggs, so you have to pay for it.”

- **Utilities:** The second component is utilities. NEMA coordinates the flow of vehicles, machinery and manpower necessary to keep the key utilities running.

- **Private sector corporations:** The third component is the private sector, which under Israel’s emergency authorities can be compelled by law to continue functioning, to provide key necessities. Of course, this also requires preplanning to ensure that there is adequate cross-sector coordination so such corporations will have the resources they need to continue operating.

“... In most cases we look at public resilience as the objective. But it’s also the one that generates all the others. You need public resilience to bring manpower into the power stations, and you need people in place to support communications or whatever else is needed to restore civil functions.”
Paul Stockton noted that little of the discussion in the panel had been about recovery. He defined the difference between response, restoration and recovery thus: “Response includes immediate lifesaving, life sustaining, keeping people alive, making sure water systems are working,” he said. “Restoration means restoration of power and other key services.” Recovery, Stockton declared, is best captured by FEMA’s phrase, “build back stronger.” Recovery challenges us: “How do we rebuild the grid, water and wastewater systems and other critical infrastructure in ways that make them inherently more resilient than the legacy systems that we have and that we continuously modernize?”

Stockton argued that it is critical to develop recovery plans, not just response plans, and integrate them into the playbook system. This is firstly because, “In the midst of a Black Sky event, when you’re saving and sustaining lives, that’s a terrible time to think about how to re-architect the grid. Ain’t going to happen. The urgent is going to drive out the important.” Secondly, he explained, it is important because, in the midst of restoration and recovery, we need to know what our restoration goals are.

How do we rebuild the grid, water, wastewater and other critical infrastructure in ways that make them inherently more resilient than the legacy systems that we have and that we continuously modernize?

In the midst of a Black Sky event, when you’re saving and sustaining lives, that’s a terrible time to think about how to re-architect the grid. The urgent is going to drive out the important.
Session Chair: The Rt. Hon. Lord James Arbuthnot

Plenary Session Concluding Comments

Lord Arbuthnot summarized his impressions of key, recurring themes from the day’s discussions. “One of these days,” he asserted, “there will be an event. Every day when we build more smart cities we increase our efficiency, and we also increase our vulnerabilities. If it is an attack, it will be multi-pronged. And because of our interdependencies and because of cascade effects, the consequences will start serious and get worse.”

Among some optimistic developments that Arbuthnot hailed were that government actions in Israel, the U.S. and the U.K. – either completed or in progress – are increasingly mandating infrastructure protection against a broad range of threats. Lord Arbuthnot concluded by noting some of the outstanding challenges and opportunities that were highlighted by the day’s speakers.

Key challenges and opportunities highlighted by Lord Arbuthnot

- On cost recovery: “We need to put in place a good system of cost recovery for Black Sky resilience investments.
- On self-healing design: “We need to make the systems that we introduce self-healing.”
- On creative hardening: “The way to deal with critical electricity substations is not to have them.”
- On building cross-sector coordination: “Don’t form relationships on the tarmac.” The critical cross-sector collaborative relationships need to be built and nurtured before a crisis hits.
- On training: Exercising and training are crucial.
- On Recovery: We must aim to build back stronger; “We don’t want to bounce back, we want to bounce forward.”
EIS Summit (EISS) is hosted as a government / NGO partnership. EISS NGO Hosts:

www.eiscouncil.org

www.henryjacksonsociety.org