Expanding Black Sky planning efforts by public and private sector organizations in
the United States and partner nations have developed in response to a fundamental
question:

“Do the United States and other developed nations wish to be prepared to survive
extreme, Black Sky hazards?”

If the answer is “Yes,” assuring national continuity requires setting robust goals, while
challenging ourselves to develop cost effective strategies to achieve them. In EISS VIII,
infrastructure corporations and their government and NGO partners jointly took stock
of where we are, and where we need to go to achieve critical goals.
Electric Infrastructure Security Summit VIII
Summit Report

Published:
June 1, 2018

Principal Editor:
Yedidya Sinclair

Contributing Editor:
Avi Schnurr

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.
Introduction

EIS Summit VIII took place in July 2017 in the U.S. Capitol Building, Washington DC. At nearly three times the largest previous attendance, EISS VIII was the largest so far in the EISS series and convened senior leadership from government, the private sector, utilities, academia and NGOs representing 24 countries. The theme of the Summit was “Working Together to Secure Our Future:” Cross-Sector Collaboration to Achieve Robust Goals.”

Planning for Black Sky events - prolonged, sub-continent-scale power outages - by public and private sector organizations in the United States and partner nations has developed in response to these fundamental questions:

“Do the United States and other developed nations wish to be prepared to survive extreme, Black Sky hazards?” As a corollary of this question, we must further ask, “are the United States willing to invest significant effort and resources in achieving Black Sky resilience?”

If the answer to these questions is “Yes,” assuring national continuity requires setting robust goals, while challenging ourselves to develop cost-effective strategies to achieve them. In EISS VIII, infrastructure corporations and their government and NGO partners jointly took stock of where we are, and where we need to go to achieve critical goals.

The organizing principle of Summit VIII was to discuss each of the Black Sky hazards, the likely impacts that they will have on critical infrastructures, and the challenges they pose to response capabilities. Each Black Sky hazard, beginning with EMP and cyber , featured an address by a recognized subject matter expert followed by panel discussion.

Main Themes

• The critical importance of cross-sector planning
  
  As EIS Council President Avi Schnurr put it, “all infrastructures today are interconnected, so anything that shuts down any major infrastructure is going to cause everything to fail. That means infrastructures will need good, cross-sector planning to deal with the interdependencies. Without planning, there can be no restart.”

• Cross-sector emergency planning in the US has begun but falls far short of where it needs to be
  
  Former US Assistant Secretary of Defense Paul Stockton noted numerous gaps and problems in US Cross-sector disaster planning and preparedness, including lack of planning for prioritization in a Black Sky event, limited knowledge of utilities about their critical infrastructure customers, a mistaken conception of the government’s role in a major power outage and a rudimentary appreciation of the challenging homeland defense environment in which recovery from a major cyber or EMP attack would play out.

• Geo-political developments heighten the threat to critical infrastructures
  
  The alarming advances in North Korea’s nuclear weapons and missile systems were noted by several speakers. These developments render an EMP attack against US or allied infrastructure increasingly plausible. Moreover, the Russian cyber attack on Ukraine’s
power grid in December 2016 highlights the vulnerability of electrical infrastructures to a massive cyber assault.

- **Exploiting overlaps in preparation against different threats**
  As Avi Schnurr stressed, the necessary resilience measures should also be cost-effective. Former Israel National Security Adviser Ya'acov Amidror recommended, “Whenever you make preparations for one threat, ask yourself the question: how can I use this opportunity to be better prepared against other threats?”

- **Resilient communications will be essential in the recovery from a Black Sky event**
  A massive, widespread power outage would bring down the main communications networks that we rely on. Without a widely deployed, interoperable emergency communication and coordination system that does not utilize the nation’s basic telecommunications backbone, and that can operate 30-60 days without grid power, infrastructure restoration and population sustainment would not be possible. EIS Council is working to meet this critical need by developing an example of such a system, the Black Sky Emergency Coordination and Communication System (BSX). Based on the system used by the US Army in Afghanistan, key elements of BSX were planned to be demonstrated for the first time at the EPRO SECTOR Executive Committee Winter, 2017 meeting hosted at PJM Headquarters in Audubon, Pennsylvania.

- **Terrorism as a serious threat to infrastructure**
  Today there are a number of terrorist organizations with both the capacity and the motivation to carry out “mega terrorist attacks”. Such organizations recognize the potentially devastating impact of targeting critical infrastructures.

- **EMP protection exists but we are far from systematically implementing it in civilian power systems**
  Michael Rooney, Branch Chief for Nuclear Survivability at the U.S. Defense Threat Reduction Agency (DTRA,) and David Fromme, Senior EM/EMP Scientist, Scientific Applications Research Associates, presented results (some never previously published) of both DTRA and EIS Council-sponsored tests on civilian power system components against simulated EMP pulses. Many of the standard power system components failed in the test results presented, indicating serious risk in a real EMP attack. Fromme reported that, in general, control equipment was found to be much less robust under EMP testing than it needs to be. The high-power digital relays from a range of different manufacturers evinced significant EMP vulnerability. All six out of six high-power digital relays failed at some level of the tests, indicating a particular vulnerability. Battery chargers also did not perform well. The good news, Rooney and Fromme pointed out, is that mitigations for these components exist and could be implemented. Panelists stressed the importance of making these results available to utility managers and engineers. A number of speakers praised Israel as the first country to begin implementing EMP protection of its power grid.

- **US civilian infrastructure is highly vulnerable to a cyber attack**
  A massive cyber attack on infrastructure could be more costly than the worst natural disaster, according to Lloyds of London. Erez Kreiner, Former Chief of the Israel Cyber
Authority noted that cyber security of US utilities is often inadequate and stressed that utilities must protect themselves and not rely on the government to do so for them. Robert Kowalsky, Deputy Undersecretary (acting), National Protection and Programs Directorate, U.S. Department of Homeland Security, defined the role of government as “to support the owners and operators of critical infrastructure to take the steps they need to make sure the grid is secure in the face of an attack.” Several speakers asserted that good “cyber hygiene” – observance of basic, routine security practices could prevent a great many cyber attacks.

- **US response to extreme weather has improved, but the severity and frequency of events is worsening**
  
  Since Hurricanes Katrina and Sandy which caused power outages lasting weeks in some regions, many aspects of US extreme weather resilience and recovery have improved. However, the speakers pointed out that the incidence of storms causing massive damage is increasing, whether due to climate change or to greater population density in storm-prone areas such as Florida. The potential for a Black Sky event due to a concurrence of severe weather events, or in combination with a malicious threat, is thus growing.

- **The probability of a Black Sky event happening in the next decade is much higher than is generally appreciated**
  
  Lord Toby Harris showed, through some simple calculations, that such events are in fact much less rare than we think. If there are six sorts of events that might cause a catastrophic breakdown and each is estimated to be a once in a hundred year event, the chances of one of those six occurring in any particular year is 5.8%. “That means that the chance of one of them occurring by the end of the next decade is 54.3%. That is more likely than not.” Therefore, Harris concluded, “it is more than justified that we are spending these two days in this Summit, and so many of us are spending so much time working on these issues.”

- **The earth missed a Black Sky-class coronal mass ejection by two weeks in its orbit, with the major solar storm of 2012.**
  
  In 2012, a large coronal mass ejection from the sun missed the earth by just a week. Had it hit the Earth then, according to Dr. Daniel Baker, the damage to electrical systems worldwide could have been such that “we would still be picking up the pieces.” The event provided excellent and detailed data for researchers to deepen our understanding of solar weather and its potential threat to power systems.

- **Addressing Black Sky Hazards effectively requires international cooperation**
  
  Black Sky hazards cross international borders, and all infrastructure supply chains today are international. This means states will need to support one another in order to mitigate their effects and recover. Speakers praised EIS Council’s work in catalyzing international cooperation to build infrastructure resilience. Kobi Wimisberg from Israel’s Department of Defense declared, “GMD and EMP are important enough to put on the table of the leaders of the free world. This is an important topic to deal with and we have to deal with it, and better now and not later.”
Introductory Session

Introducing the Summit, Avi Schnurr, CEO of EIS Council, proposed that the motivating question for the day is “do the United States and allied countries wish to be prepared to be able to survive a hazard on this scale?” Schnurr emphasized that the consequences of answering “yes” are serious hard work and personal commitment on the part of the staff and leadership of critical infrastructures. Given the interconnected nature of infrastructure systems today, detailed, cross-sector planning and exercising is especially critical. Cross-sector resilience measures must be cost-effective.

Continuing this theme, Paul Stockton, Former U.S. Assistant Secretary of Defense noted numerous gaps and problems in US cross-sector disaster planning and preparedness, including lack of planning for prioritization in a Black Sky event, partial knowledge of utilities about their critical infrastructure customers and a mistaken conception of the government’s role in a major power outage and a rudimentary appreciation of the challenging homeland defense environment in which recovery from a major cyber or EMP attack would play.

John Heltzel, Director of Resiliency Planning for EIS Council, described how EIS Council’s EPRO projects are working to host processes that can help close the gaps in cross-sector planning through developing Black Sky sector playbooks and the Earth EX cross-sector Black Sky exercise series. Yaakov Amidror Former Head of Israel’s National Security Council, offered an Israeli perspective on how a country can exploit synergies and overlaps between the resilience measures necessary to defend against diverse threats.

Finally Bran Ferren, Co-chairman of Applied Minds, Inc. gave an overview of the BSX system – a highly resilient emergency communications platform based on the Blue Force Tracker system used by the US army, which EIS Council is developing.
Learning From the Past: Historical, civilization-scale risks in times of rapid transition

Avi Schnurr began by screening a short video “Black Sky ‘Lessons Imagined’”, which illustrated the impact of modern infrastructure interdependencies, and the consequent vulnerability of our entire interconnected utility networks. Since Black Sky events are too large to allow us the luxury of learning from experience, we must prepare for them by imagining the consequences before they occur, projecting consequences that we have not yet lived through.

Schnurr stressed that “the critical takeaway is that these are cross-sector planning responsibilities. All infrastructures today are interconnected. Anything that shuts down any major infrastructure is going to cause everything to fail. Infrastructures will need good, cross-sector planning to deal with interdependencies. Without planning, there can be no restart.” Since infrastructure interdependencies are at the root of our vulnerability to Black Sky hazards, an important part of the solution is to strengthen interconnectedness between infrastructures in their preparedness to deal with such threats.

The Fundamental Question Underlying Black Sky Planning

Given the scale and seriousness of Black Sky hazards in six categories that could lead to sub-continent-scale power shutdowns, Schnurr posited that the basic question underlying Black Sky planning is: “Do the United States and allied countries wish to be prepared to be able to survive a hazard on this scale?” along with the corollary to the question, “are the United States willing to invest significant effort and resources in achieving Black Sky resilience?” Schnurr emphasized

“...
that the consequences of answering “yes” to these questions are serious hard work and personal commitment on the part of the staff and leadership of critical infrastructures. “Business as usual is not going to be enough for this,” he cautioned. Detailed and interconnected cross-sector planning will be essential.

Overview: EIS Council’s Black Sky Initiatives

Schnurr outlined four major initiatives through which EIS Council, with the cooperation of a wide range of government, corporate and NGO leaders, is hosting a process to help address this challenge:

**EPRO Sector:** This is a systems engineering-based process where EIS Council hosts development of Black Sky plans and playbooks for each sector, with a strong emphasis on cross-sector collaboration.

**Exercising:** “No matter how good plans are, plans are useless if they’re not exercised,” Schnurr warned. As a result, EIS Council organized a unique multi-sector, international Black Sky exercise, the first in the new EARTH EX series, for August 23rd, 2017. EARTH EX was set to be the largest multi-sector, international exercise ever.

**Communications:** A Black Sky event would bring down most or all normal communications channels. Given the unprecedented complexity of interconnectivity of all resource networks today, without Black Sky-survivable, widely deployed emergency communications spanning all major corporate, government and NGO sectors, restoration of infrastructures and population sustainment would be impossible. EIS Council is therefore hosting a major emergency communications initiative called BSX, with legacy to the Blue Force Tracker system that the U.S. Army uses in Afghanistan today for communication across ~200,000 nodes and coordination points. BSX was to be demonstrated on December 12th 2017 at EIS Council’s winter EPRO Steering Committee meeting.

“**No matter how good plans are, plans are useless if they’re not exercised.**

“**We must work together with commitment, and commitment to each other, to our children, to the future of our nation and all of the 24 nations represented here.”**
Modelling and Simulation: EIS Council’s Global Infrastructure Network Optimization Model (GINOM™) initiative is designed to build the modeling and simulation effort that will be needed, hosted by an emergency communication coordination system, to convey situational awareness information and provide decision support in extreme hazard environments.

Learning from The Past

Schnurr gave a historical perspective to the current challenge, pointing out that “throughout history, shutdown of resources to a civilization has occurred again and again, and has repeatedly caused the collapse of the civilizations, right from the time where bronze weapons were replaced by iron weapons in ancient Mesopotamia.” The comparable danger today, Schnurr warned, is of “malicious or natural hazards happening at a level that cut off critical resources for too long for society to continue.”

He added that the solutions need to be not just effective, but also cost-effective, or else they will never happen. Schnurr concluded that developing and implementing the necessary planning solutions will require “working together with commitment, and commitment to each other, to our children, to the future of our nation and all of the 24 nations represented here.”
Where Are We Today? Overview of Today’s Interdependent Infrastructures and Global-Scale Risk

John Hetzel gave a brief overview of some of the main advances in EIS Council’s resilience planning over the past year.

EIS Council has been hosting development of Black Sky Playbooks, laying out key Black Sky missions, and requisite sector by sector resilience measures. Recently, this effort has expanded in the number of sectors it covers. In addition to the electric sector, the water sector, “oil and natural gas have come online, as well as the regulatory sector, state sector, NGO and volunteer sector and federal sector.” Work has also commenced on the financial sector.

All these groups are actively working on their playbooks, the next version of which will go online in August. General Hetzel urged all present to “consider yourselves partners and work with us to put these playbooks out so that everybody can take advantage of the expertise in this room.”

With input from leaders in many sector, in addition to these Playbooks the Council has developed and facilitated sector-specific EARTh EX Black Sky Simulation Exercises in several states since the beginning of 2017. Most recently, the Council facilitated exercises for the California Governor’s Cabinet and the California Office of Emergency Services, along with 200 representatives from partner organizations throughout the State.

Referring to the annual, global, multisector dimension of this series, he also strongly encouraged participants to join the international EARTh EX exercise on August 23, 2017.

He ended by emphasizing that “we’re here to listen to you” and characterized EIS Council’s role saying, “we want to be the people that take your good ideas and make them available for everybody else, so our partnership continues to grow.”
Dr. Paul Stockton, Editor-in-Chief, EPRO Handbooks; Managing Director of SONECON; Former U.S. Assistant Secretary of Defense for Homeland Security


Dr. Paul Stockton focused his comments on four big gaps, in which, Stockton argued, “the US is utterly failing” in its cross-sector preparation for Black Sky events.

**Major gaps in US cross-sector emergency planning**

**Black Sky prioritization**

The first gap is in prioritization of assets. Stockton pointed out that “in a New Madrid earthquake, in an EMP attack on the United States, whatever the Black Sky hazard is, it will be impossible to sustain all of the water systems, all of the natural gas systems, all of the hospitals in the United States because the devastation is just going to be too big.” Therefore, we will need to prioritize the restoration of infrastructure in the way that will save the maximum number of lives. “Harsh prioritization is going to be required,” Stockton warned. “How are we going to go about doing this?”

Power utilities do have information on who their critical customers are for prioritizing restoration of service – nuclear plants, critical gas plants etc. Stockton argued that this is only the bare beginning of what is needed for informed prioritization, since the utilities only have a partial understanding of the life-saving, public safety and national security importance of their different customers.

The Department of Homeland Security’s “Section 9 List” could be an effective starting point for prioritization. This, Stockton explained, is a “secret-level list of all of the infrastructure assets in

In a New Madrid earthquake or an EMP attack on the United States, it will be impossible to sustain all of the water systems, all of the natural gas systems, all of the hospitals in the United States because the devastation is just going to be too big.
the United States that, if disrupted in a cyberattack, would lead to catastrophic damage to public health and safety, national security, and the U.S. economy.”

However, this is only a starting point. The list should not be limited to cyber but needs to be all-hazards; “We need an understanding of what are the most critical assets, regardless of the Black Sky event that occurs,” Stockton asserted.

Moreover, there needs to be a better flow of information about critical assets from the private sector to the DHS, since industry is growing and interdependencies are multiplying at such a rapid rate. Industry is understandably cautious about sharing much with the government “especially because government hasn’t always been a great protector of sensitive information by the private sector.” Stockton pointed to the food industry as one which is changing in ways that are material to Black Sky preparedness: “This is of prime concern for me in a Black Sky event because of the concentration of food distribution nodes into a handful of facilities in the United States now, and just-in-time delivery.” Given this, he quipped, “What could possibly go wrong in a Black Sky event?”

An even more serious problem is that, once such an expanded version of the Section 9 list becomes available, it needs to be shared with utilities, otherwise they will not know which assets in their service footprint are the most important for power restoration. Of course, there are good reasons why the list is classified: “We don’t want to give our adversaries a roadmap as to what to attack.” Nevertheless, Stockton urged, “let’s get clearances out to those who have a need-to-know in industry, so all of you know how to prioritize sustainment and restoration of service.”

**Private Sector Coordination**

The second gap, Stockton argued, is that we have yet to construct a mechanism to coordinate industries for Black Sky operations.

“**We need a dozen sectors and subsectors to be able to have their leadership come together in a severely disrupted environment and prioritize the coordination of operations. If we build something like that, it’ll save hundreds of thousands of lives.**
Leaders in a growing number of sectors are building Black Sky Playbooks, but the means for cross-sector operational coordination don’t yet exist. He declared, “we need a dozen sectors and subsectors to be able to have their leadership come together in a severely disrupted environment and prioritize the coordination of operations. If we build something like that, it’ll save hundreds of thousands of lives.”

Public Sector Coordination:
The third gap is in the capability of government to support restoration. “The public sector,” he declared, “is nowhere near where it needs to be in order to be able to conduct and support cross-sector operations.” Indeed, the concept of the government’s role in a major disaster is wrong. Currently the operational vision is government led. “The Emergency Support Function system is all about bringing government capabilities to bear in response to requests from governors to help save and sustain lives.” This is the opposite of what is needed, Stockton asserted. “In Black Sky events, we need the private sector building the capabilities, bringing the critical life-saving services to bear in order to prevent much larger loss of life. Responding to Black Sky events is all about industry in the lead and government in support.”

Moreover, the current conception lacks an understanding of how State Governors are to be brought into the system of coordination. This is necessary “because governors are always in the lead for the public health and safety of their citizens under the U.S. Constitution.”

Black Sky Planning for Homeland Defense
The fourth and final gap is the lack of an adequate understanding and response to the “homeland defense environment” in which the man-made Black Sky scenarios of EMP, cyber and coordinated kinetic attack would play out.

“In Black Sky events, we need the private sector building the capabilities, bringing the critical lifesaving services to bear in order to prevent much larger loss of life. Responding to Black Sky events is all about industry in the lead and government in support.”

“Adversaries are going to figure out which nodes, if taken out, would have maximum cascading effects, above all, to degrade the ability of U.S. defense installations to execute their mission-essential functions.”
Adversaries understand the US military’s deep dependence on civilian infrastructure. “They are going to analyze our own critical infrastructure interdependencies. They’re doing so now. They’re going to figure out which nodes, if taken out, would have maximum cascading effects, above all, to degrade the ability of U.S. defense installations to execute their mission-essential functions.”

Stockton also warned that information warfare will likely be a serious obstacle to restoration efforts. “Potential adversaries like Russia are going to use social media in order to plant disinformation, to confuse situational awareness, disrupt restoration operations, and incite panic amongst the American people in a way that advances the adversary’s political and military goals.”

**Coming Soon:** EPRO Handbook III will summarize recommendations to fill these gaps coming from public and private sector leaders.

Stockton concluded by noting that the EPRO Handbook III, to be published in the coming months, includes not just a diagnosis of these problems but also some recommended solutions emerging from peer-reviewed recommendations developed in coordination with leaders in both government and industry. These approaches represent a first step toward filling these gaps. And if we meet these four challenges, Stockton averred, we will not only become capable of responding effectively when a Black Sky event occurs, but also deter attacks by eliminating what is, today, a catastrophic vulnerability.

“Potential adversaries like Russia are going to use social media in order to plant disinformation, to confuse situational awareness, disrupt restoration operations, and incite panic amongst the American people in a way that advances the adversary’s political and military goals.”
Maj. Gen. (Ret.) Yaakov Amidror, Former National Security Advisor to Prime Minister of Israel; Former Head of Israel’s National Security Council

Working Together to Secure Our Future: Looking to Israel’s Experience in Coordinated Disaster Planning as a Template for Progress and Lessons Learned

A strategy for cost-effective preparation for worst-case scenarios

General Amidror raised the basic question of defining appropriate strategies to prepare against worst case scenarios. The problem, as he put it, is that “if you really take seriously the understanding that you have to be prepared for the worst-case scenarios, you must ensure the investment strategy is cost-effective.”

Israel’s relative prioritization of threats

Amidror outlined an approach that Israel has developed to address this dilemma. In the course of preparing for threats that are prioritized as high, the country has learned how, at the same time, to take measures to protect against potentially even more damaging but less common threats.

By way of example, he discussed Israel’s relative prioritization of the threat danger from missiles, cyber and EMP, each of which represent different current realities. Cyber is a threat that is already here; in the cyber realm, “we have events in which we know that we have been attacked, and we can identify the results. We know what the other side is preparing.” The cyber threat and its consequences are much better understood, a factor that is helpful in developing approaches for mitigation.

If you really take seriously the understanding that you have to be prepared for the worst-case scenarios, you need to ensure the investment strategy is cost effective.

In cyber, we have events in which we know that we have been attacked, and we can identify the results. We know what the other side is preparing.
That said, Amidror pointed out three common elements between the EMP and cyber threats, which can create synergies and overlaps in protection measures.

**Securing civil infrastructure:** “We need to think in terms of how to defend organizations that need to continue functioning, which are not exclusively state organizations.”

**Protecting machines as the primary need:** Moreover, for both EMP and cyber, the immediate challenge is to defend machines, rather than people.

**A potential advantage – Addressing a vulnerability in manmade systems:** Finally, for both of these threats, there is one built-in advantage relative to natural hazards. The systems that need to be protected have been manufactured by people, and the vulnerabilities – though massive – are more discrete and constrained than in natural hazards. Cyber and EMP both differ in this respect from earthquakes, which cause damage through disrupting natural systems that we cannot control, and whose impact, therefore, is far more difficult to bound.

Inevitably and naturally, Amidror pointed out, immediate, continuing hazards receive the lion’s share of investment. The kinetic threat of 120,000 Hezbollah and Hamas rockets receives much higher prioritization and approximately ten times more resources, than either cyber or EMP. Amidror outlined some of the protection measures: “From shelters in hospitals to safe rooms in each apartment in Israel -- at the end of the process, each apartment in Israel will have a safe room that during kinetic attacks of rockets and missiles the family can go into.” In addition, Israel spends billions of dollars on missile defense and interception systems.

Some of the measures against missiles, however, are hazard independent to some degree, and help to mitigate other threats. For example, Israel is locating some key elements of its health and financial systems underground. Although this is primarily to defend them from missiles, they will

“Whenever you make preparations for one threat, ask yourself the question: how can I use this opportunity to be better prepared against other threats?”
also be better protected against cyber and EMP. Another example of such synergy is seen in the safe rooms in Israeli houses and apartments that are part of the homefront missile defense effort; these will also provide Israeli families with much greater protection against earthquakes.

Summarising the current situation, Amidror underlined that Israel is investing all necessary resources so that in a few years the country will be very well protected against the missile threat. Israel has also initiated a new agency to defend civilian systems from cyber threats. In the EMP area, Israel is focusing first on defending the most crucial systems.

Lessons learned from Israel’s experience

Summarizing, Amidror referred to three major lessons learned from Israel’s experience.

Firstly, he stressed the importance of looking for synergistic opportunities in making investments for Black Sky protection: “Whenever you make preparations for one threat, ask yourself the question: how can I use this opportunity to be better prepared against other threats?”

Secondly, cooperation and coordination between agencies – both in advance and during a crisis -- is crucial for any effective protection and threat mitigation.

Thirdly, exercising plans is critical, and must include the highest levels of decision makers in both the public and private sectors. “If the decision makers do not take part in the exercise, at the end of the day, they don’t know what and how to decide.” This is especially true in a large scale crisis involving many sectors. In this, as in any crisis event, inevitably things will happen that were not exercised, but the more a plan has been practised, the more adaptable it will be to unforeseen contingencies.
Bran Ferren, Co-chairman, Applied Minds, Inc.; Former CEO, Disney Imagineering

Emergency Communications for a Resilient Future: The Black Sky Emergency Communication and Coordination (BSX) System and the 2017 Project Building Key Elements of a Prototype

Bran Ferren introduced his presentation of the BSX Black Sky Communication project by saying, “I’m going to talk to you about a system and a set of technologies that we all hope we never use.”

The need for a survivable emergency communications system

He defined survivable communications as systems that, no matter what happens, “will last for a very long period of time and be reliable when you need them.”

He outlined some of the ways in which ordinary communications systems are likely to fail in a major disaster. In addition to issues with loss of grid power, cell phone and satellite phone networks, even if they survive the initial event would, in any case, stop working within a day or two as system capacity is oversaturated. Communications that require ongoing electric power are dependent on emergency generators continuing to function well and to be refueled when necessary. Ferren remarked that in his experience many major organizations’ backup power systems will not work because they have never been fully tested in real-world situations.

Moreover, he warned that the interdependencies among critical infrastructures have become so complicated that we simply don’t understand them. Complex interdependencies mean that when some systems go down, they will bring others with them. “These interdependencies will not become evident until some unfortunate combination of event takes place.” Given this reality,
availability of a widely distributed, interoperable and Black Sky protected emergency communication system, independent of the national telecommunication backbones and power grid, is a fundamental requirement for restoration and eventual recovery.

Dependence on grid power, complex interdependencies and backup systems that are seldom robust for long periods of time all contribute to making our basic national communication systems brittle with respect to severe catastrophes – precisely the times when communication will be most critical. And in addition to these factors, a further risk to viable crisis communications is the deterioration in human behavior that typically occurs in a disaster. “Under these circumstances,” Ferren claimed, “you lose 20-30 points of IQ. Systems and organizations lose even more IQ. When they are rigid, well-disciplined, well-run enterprises, and the rulebook changes with no practice and no rehearsal, people react badly.”

As an example, he pointed out the common pattern whereby after a communications system goes down, people scramble to restore communications, in the process reconfiguring the system so that if it were restored it would no longer be functional. Although training and exercising can help, there is a limit to how effectively you can train for situations you have never seen. As a result, a hazard-independent, dependable emergency communication system – widely deployed and independent of our normal infrastructures and resources – is a crucial starting point for restoration and recovery in severe catastrophes.

**Specifications of a survivable communications system**

He then proceeded to outline some of the specifications of a Black Sky survivable communications and coordination system.

First, it requires reliable sensors in order to provide situational awareness. You will need to know, “if all communications, radio, television, is out, how big is the blackout if you can’t call someone
on a phone to find out? Is there water here? Is there electricity here? Is there a fire raging on some portion of the town?” Part of the solution will always be “humans sensing things and reporting to others,” and part will be “actual sensors saying “is there power up in this power line?””

Second, the user interface needs to be extremely simple and intuitive so that anyone from senior leadership to “a guy and a gal out in a truck that are going to replace a fiber repeater which has failed, or a powerline,” can use the system. One needs to be able to “flip a switch” and communicate. This requires built-in path diversity to function even when “every single communication path that you normally use is nonexistent or unreliable.”

Third, the systems needs to have long term reliability with minimal maintenance. As Ferren asked, “If you don’t use this thing for six or seven years, if it’s exercising itself, and you’ve not paid much attention to the little reports it gives you about what’s working or not, what is the likelihood it will work at the moment you need it?” The design needs built-in testing at a system level and artificial intelligence in order to ensure that the system will work when needed. Ferren emphasized the challenges in developing a system that meets all these requirement in a way that is also cost-effective, secure and scalable.

**EIS Council’s BSX communications system**

He noted that key elements of a prototype of the system would be demonstrated in December. Those system elements to be demonstrated are compatible with key BSX system features. These include “secure data transfer without the need for key exchange, and a basic iteration of the artificial intelligence necessary to do this work without requiring operator intervention, and at the same time, provide a pathway for situational awareness in these specific intervals.”

“**If all communications, radio, television, is out, how big is the blackout if you can’t call someone on a phone to find out? Is there water here? Is there electricity here? Is there a fire raging on some portion of the town?**

“**If you don’t use this thing for six or seven years, if it’s exercising itself, and you’ve not paid much attention to the little reports it gives you about what’s working or not, what is the likelihood it will work at the moment you need it?**"
Ferren emphasized that the BSX technology draws on some of the best communications ideas and technologies that other experts have developed, including very long-life batteries and power systems that can supply high energy but sit for ten years without attention or maintenance, as well as methods of modulation that are more spectrally efficient, using the spectrum in unusual ways. The ability for the devices to self-configure in a way where each device or node has an imperative to communicate are also key. All these ideas and more have helped to develop “a concept that is affordable, scalable, reliable, and for those times where – though we hope they never occur – we will need it, it’s available.”

Ferren concluded by affirming that this work is motivated by a sense of responsibility to future generations, saying: “I’m doing this personally for exactly one reason, and that reason is named Kira. She’s my daughter. She’s eight-years old, and we need to leave her with a world better than the one we have now.”

“I’m doing this personally for exactly one reason, and that reason is named Kira. She’s my daughter. She’s eight-years old, and we need to leave her with a world better than the one we have now.”
Session One

Malicious Black Sky Hazards

Session Chair: The Hon. Trent Franks (R-AZ),
US House of Representatives
Session Summary

In this session, subject matter experts and panelists explored the threat to critical infrastructures from terrorism, EMP and cyber attacks, surveyed the current state of mitigation measures and proposed additional steps that need to be taken to protect against these threats.

Terrorism: Professor Boaz Ganor, Founder and Executive Director, the International Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC) Herzliya, Israel.

Boaz Ganor explained that the threat of a given type of terrorism can be thought of as the product of the capability multiplied by the motivation to execute such an attack. Based on this calculus, he argued that the threat of a mega terror attack targeting critical infrastructure is real, since various groups exhibit the capability and motivation to do so.


EMP subject matter experts Michael Rooney and David Fromme reviewed data with detailed examples of where the pulses from a high altitude nuclear explosion will cause extensive damage to electrical systems. They summarized research findings (some never previously presented) from US Government’s Defense Threat Reduction Agency (DTRA) testing of different electrical systems and components subjected to a simulated EMP pulse. Some of the most recent findings became available based on cooperation between DTRA, the SARA Corporation and EIS Council. The data showed that some types of components failed, including high power relays and commercial off the shelf (COTS) devices. The high-power digital relays from a range of different manufacturers evinced significant EMP vulnerability. All six out of six high-power digital relays failed at some level of the tests, indicating a particular vulnerability. In almost all cases, the mitigation measures for the vulnerable elements are known and available, but they need to be implemented.

The industry panelists agreed with Rooney and Fromme that these findings need to be made available to utilities so that they can harden their systems. Panelists noted that awareness of EMP has advanced markedly and is at least beginning to result in practical protection measures. A number of speakers praised Israel as the first country that is taking real action to protect its power grid from EMP, in a program including consulting expertise provided by EIS Council.

Cyber: Erez Kreiner: Former Director, Israel National Cyber Authority

Erez Kreiner described the devastating potential power and reach of cyber attacks on infrastructure. He stressed that utilities must take responsibility to protect themselves from this threat; they cannot rely on government. Several of the panelists noted that “good cyber hygiene” – basic computer security habits - can go a long way to protect against cyber warfare; many successful attacks exploit elementary security lapses.
The Hon. Trent Franks (R-AZ), U.S. House of Representatives

Introduction

Congressman Franks surveyed some of EIS Council’s major milestones and achievements over the eight years since he chaired the first EISC Summit. “I think it’s fairly astonishing when you look back at the ground that we’ve covered,” Franks declared,

Franks recalled the London Summit which included an assessment by Lloyds of London of the potential financial impact of widespread long-term power outages as an important step forward. He also singled out the work done in Israel, that is beginning to protect the grid against the EMP threat. He noted that Israel is the first country in the world to be doing this and remarked that “this can be directly correlated with Avi Schnurr and the EIS Council.”

Highlighting progress in the United States, Franks discussed what he termed the “enormous legislative advances” that have been made in addressing Black Sky threats, saying, “we’ve now passed the Critical Infrastructure Protection Act, which is the first major EMP legislation in our nation’s history.” He expressed his confidence that the Act would be implemented by the new administration, averring that they are aware of and focused on threats to critical infrastructure.

Franks then turned to geopolitical developments that underscore dangers to infrastructure. On the threat from rogue regimes, he reminded the gathering that “North Korea has not only tested an ICBM, but - something that’s not talked about much - they have had a successful re-entry in May with a ballistic missile.” He also noted that Russia’s ability to use cyber warfare against an electric grid was clearly demonstrated by the attack on Ukraine’s grid in 2015

Franks concluded by expressing his deep thanks to Avi Schnurr and EIS Council for all their dedicated work in addressing the threat from Black Sky events and declared that “when there’s an event like this and we come through it, a lot will be thanks to people like you that made it possible for us to prepare for it.”
Terrorism: A New Dimension in Existential Threats to Western Nations

Prof. Boaz Ganor, Founder and Executive Director, Institute for Counter-Terrorism (ICT) at the Interdisciplinary Center (IDC), Herzliya, Israel

Terrorism as a Threat to Infrastructure

Professor Ganor addressed the issue of how terrorism poses a threat to infrastructure. As he framed the guiding question of his talk:

“How do terrorist threats actually connect to the important discussions that are being conducted here on catastrophic threats to critical infrastructure, the grid, the electricity system, EMP, and so on?”

Ganor based his answer to this question on a broader classification of different terrorist threats. Examining the scale of the terrorist entity and the type of attacks they can carry out, he set out a spectrum of levels of capability.

The “low end” of terror attacks: At one end are what are termed “lone wolf” attacks such as stabbings and car rammings carried out by individuals who have been radicalized by a terrorist organization.

Higher levels of sophistication: At higher levels of sophistication, there is organized terrorism, where groups directed by a terrorist organization initiate, plan and carry out attacks that are far more lethal than lone individuals. The Bataclan attack in Paris and the Brussels airport attacks which killed and injured hundreds of people were examples of organized terrorism.

Mega terror attacks: At the far end of the destructiveness spectrum are what Ganor termed “Mega terror attacks.” These would require the backing of a terrorism-sponsoring state and could kill many thousands of people. He pointed to four classic categories for non-conventional mega-terror attacks, often referred to as CBRN threats: Chemical, Biological, Radiological, Nuclear/EMP attacks.

“If somebody would open a bottle here with a virus, we’re definitely not going to know where it’s going to end and how it’s going to be spread. Nuclear and EMP, because of the magnitude of the attack, should also be regarded as non-limited.”

“...When we are talking about EMP and catastrophic terrorism, this is the question we need to ask ourselves: do they have the capability and do they have the motivation?”
Chemical and Radiological Attacks

Ganor classified chemical and radiological attacks as “limited.” Though potentially extremely serious, their range of impact is circumscribed. As he put it, “If somebody lets out toxic chemical material in this room, probably we’re all doomed, and maybe even the whole building. But it’s limited. We know where it starts. We know where it ends. That’s why it’s a limited non-conventional terrorist attack.”

Biological and Nuclear / EMP Attacks

Biological and nuclear/EMP attacks on the other hand should be classified as unlimited. As Ganor explained, “If somebody would open a bottle here with a virus, we’re definitely not going to know where it’s going to end and how it’s going to be spread. Nuclear and EMP, because of the magnitude of the attack, should also be regarded as non-limited.”

The threat of mega attacks: motivations times capability

Ganor pointed out that terrorist organizations today are planning mega attacks. ISIS has access to chemical weapons and “it’s only a matter of time until they will import this threat to Western countries, first of all Europe, down the road maybe -- even the United States.” Although so far terrorists have not succeeded in waging effective biological attacks, Ganor asserted that “this is the next stage of terrorism that will threaten the world.”

Ganor explained that the level of a terrorist threat is assessed as the multiple of motivation times operational capacity. “When we are talking about EMP and catastrophic terrorism, this is the question we need to ask ourselves: do they have the capability and do they have the motivation?”

Capability: Regarding capability Ganor explained that terrorists could carry out mega-terror attacks with the backing of a state.

Motivation: Turning to motivation, he identified a number of factors that could motivate terrorists to carry out a mega attack.

Repercussions of successful antiterror efforts: For example terrorists might believe that current terror methods were not working. This, combined with easy access to the means of carrying out
a mega-attack could feed motivation so that, ironically, our very success in suppressing national or transnational terror groups might inadvertently make them far more dangerous.

Sponsor Motivation: The motivation, alternatively, could come from a terror group’s state sponsor, which might tell the organization to launch an attack even if the terrorists do not have the motivation themselves, making them a surrogate that could provide such a sponsor with some sense of protection.

The Risk of a “Last Gasp” Event: Alternatively, a terrorist organization that fears it is in danger of extermination “might want to do something that will be remembered in the history books - a catastrophic terrorist attack.

Fanatic Religious Motivation: Finally a fatwa, or religious decree might be the motivation, “meaning they believe that God was telling them to do so, and that’s why they commit the attack.”

Terror Organizations Representing a Risk of Mega-Attacks: There are credible risks, today, of a mega-attack from a number of organizations. ISIS has almost all of these motivational factors. Al Qaida has proven its ability to carry out a mega attack (9/11) and Hezbollah has threatened to kill tens of thousands of Israelis by targeting Israel’s chemical storage and processing facilities.

EMP as a Terror Event: Regarding EMP, Ganor reported that his International Institute of Counter-Terrorism monitors Jihadi discourse in Arabic and has found several discussions about the potential use of EMP by terrorists, as well a Jihadist forum that provides a “cookbook” for carrying out an EMP attack. These sites also discuss IEMI attacks and the attractiveness of carrying out a terrorist attack on electricity systems.

Ganor concluded, “the real risk is when you see this combination between the motivation that is already there for many terrorist organization, and the capability which might be given to them by a sponsoring state.” In his view, that combination of capability and motivation exists, and consequently the risk of mega attacks is real and serious.
Subject Matter Expert

Electromagnetic Pulse (EMP): High Altitude (30-200km) Detonation of a Nuclear Warhead

The format for the summit plenary sessions was a discussion of each of the Black Sky hazards, their likely impacts on critical infrastructure, and the challenges they pose to response. Each hazard was introduced by a recognized subject matter expert, followed by panel discussions.

Rooney gave a short overview of DTRA’s HEMP (High-Altitude Electro-magnetic Pulse) program, and its DCI (Defense Critical Infrastructure Power) program.

A short introduction to EMP

DTRA conducts HEMP verification tests and other verification tests on operational systems and facilities in the Department of Defense, simulating and measuring the impacts of HEMP on electrical equipment. In addition, he said, “we provide expertise, tools and technology to help program offices who are fielding new equipment that must survive -- meet their survivability requirements.”

By way of background, Rooney explained that there are several types of EMP. A nuclear detonation can happen in space, in the atmosphere and near surface level. He focused his talk on HEMP, where a nuclear bomb is detonated above the atmosphere.

Rooney elaborated that “you can look at high-altitude EMP as a series of very intense, electromagnetic pulses or fields that result from a detonation of a nuclear weapon. The occurrence and characteristics of the pulse depend primarily on the weapon design, yield, height of burst, and burst location.” He continued, that the pulses range from the E1 with a
very high frequency to the E3A E3 B blasts, which are very similar to the effects of geomagnetic storms.

“Is HEMP real?” he asked, rhetorically. “I don’t think I need to explain to this audience.” Rooney briefly rehearsed the evidence from the Starfish nuclear detonation over the Pacific in 1962, which damaged electrical systems in Hawaii 800 miles away, as well as Soviet test over Kazakhstan in the same year which had similar effects. Showing a picture of Honolulu after the blast, he pointed out that some lights were still on. The EMP pulse destroyed some, but not all, electrical systems. “It depends,” he reiterated “on a lot of characteristics: the height of burst, the geographical location, the design of the weapon, the yield.”

**EMP protection of electrical systems**

Turning to EMP protection, Rooney explained that we do know how to harden facilities including airplanes and battlefield systems, using Faraday cages, terminal protection devices and other tools. However, a key challenge today is developing updated strategies and doctrine for where to use such protection. As an overarching example, he singled out the use of commercial, off-the-shelf equipment (commonly referred to as COTS) even in complex military systems, and also noted the special difficulties of protecting interconnected networks such as communications systems and power grids.

He digressed briefly to speak about MIL standards, which are military standards for equipment protection. Rooney mentioned two of these that are especially important. The first is a classified document entitled the “DOD HEMP Environment” which describes the situation and environment that would need to be protected against. The second is called MIL-STD-18-125 which details performance-based metric protection standards against the threat and is codified in handbooks of best practices on how to survive the threat.
Protecting civilian power systems from EMP; DTRA’s research and reports

Turning to protection of civilian infrastructure, especially the power grid, Rooney discussed some of the reports that DTRA has produced. He stressed the importance of giving access to this data to the utilities that need it: “It does no good for me to have this information and data in my little workspace. This information needs to get out to the power consortiums, the utilities, those groups that actually have their hands on the power grid, work with the digital relay controls, whether on the distribution or transmission side.”

“One of my objectives today is to make sure you know what is available,” Rooney continued. He referred first to a set of reports from simulations done at the Idaho National Lab on 138 Kv power lines there. He also alluded to a predictive model for source region EMP and its damaging effects on transformers and power lines. The simulation built a testing substation and injected stress waveforms into the 138 Kv transmission system to put the transformer into saturation and drive earth currents. The source region testing took place in two phases. The first was power grid component testing, i.e. radiation testing. The second involved a full, operational substation that was set up and exposed to a large quantity of photons from a HERMES machine gamma ray generator and also an EM pulse at the same time.

Many power grid components were tested in this way, including lightening arrestors, protective relays, line insulators, and also COTS IT equipment such as wireless trunk radio systems for first responders.

Summarizing the results, Rooney reported, “the good news was that the substation performed very well.” Both transformers in the substation continued to operate throughout the test. However other equipment items tested, particular those containing COTS components, experienced serious failures. Further testing planned for the near future includes intensive work on digital relays and lightning arrestors.

“\[It does no good for me to have this data in my workspace. This information needs to get out to the power consortiums, the utilities, those groups that actually have their hands on the power grid.\]
Dave Fromme continued the report, focusing in his remarks on new, recent EMP component testing, commissioned by EIS Council that included, in cooperation with DTRA existing and ongoing component testing performed by SARA at the direction of DTRA. He commented briefly on the testing methodology, saying, “the protocol that we used for these comparisons is a system-based methodology in which you look for the interfaces at which stresses occur, and you compare those stresses to the strength at that interface.” Each component is tested separately.

This method allows researchers to understand better exactly when and how a piece of equipment fails. As Fromme explained, “a lot of standards have a pass/fail criterion, and quit testing at that. That means you don’t get to see where the actual fail point comes.”

Turning to results, Fromme reported that “the high-voltage side of almost of this equipment looks really good from the point of view of the grid. There is margin for the voltage breakdowns. There’s margin on the energy breakdown.

However, on the sensor side, which is the low-voltage side of a potential transformer or current transformer, you’ve got a much lower voltage signal and the wire drives from the EMP tend to be even larger ratio.”
The high-power digital relays from a range of different manufacturers evinced significant EMP vulnerability. All six out of six high-power digital relays failed at some level of the tests, indicating a particular vulnerability. That said, a mitigation/protection - MOV (Metal Oxide Varistor) protection – was identified for these components, is well known and understood and can be quite easily implemented.

Fromme reported that, in general, control equipment was found to be less robust under EMP testing than it needs to be. The high-power digital relays from a range of different manufacturers evinced significant EMP vulnerability. All six out of six high-power digital relays failed at some level of the tests, indicating a particular vulnerability, with failure levels varying from between 200-2000 Amps during pulsed current injection testing.

Battery chargers also did not perform well. They had MOV (Metal Oxide Varistor) protection already implemented, but it was deeply buried in the system and so did not function as it should have. Fromme recommended, “you’d have to move that protection outside (of the device casing) in order to improve that. But that’s straightforwardly done.”

There are not yet many results on DCS’s (Distributed Control Systems), but so far their vulnerabilities seem similar to those of relays. Fromme summarized the partial results so far, saying that relays, batteries, chargers and control electronics appear to be the components most likely to fail in an EMP attack, and which need strengthening.

This means that mitigation measures are required for the sensor and control components of the transmission substations. The positive side is that the appropriate mitigation, involving the application of metal-oxide varistor (MOV) filters is well understood and could be quite easily implemented at a reasonable cost. However, implementing the necessary mitigation measures would require a clear recognition of the seriousness of the EMP threat as well as considerable time and effort.
Panel 1 | EMP

Chair: Terry Boston: Vice-Chair, Grid Protection Alliance; Energy Security Advisor to the President of the United States; Board Member and former CEO, PJM Interconnection

Panelists: Robin Manning, Vice President for Distribution, Power Delivery and Utilization Electric Power Research Institute, Ian Grant, Senior Director for Transmission Engineering, Tennessee Valley Authority; Dr. Shlomo Wald, Former Chief Scientist, Israel Ministry of Energy and Water
Panel Discussion
Introducing the EMP panel, Terry Boston began by thanking Congressman Trent Franks and Avi Schnurr, CEO of EIS Council for their indefatigable effort and leadership to help the US and its allies prepare against the EMP threat. He noted that North Korea’s intensifying program of nuclear and missile tests underscore the importance of the subject. “The timing of the Summit is very good, as North Korea reaches new heights in ICBM tests this month,” remarked Boston, adding that an EMP attack does not require an exceptionally high level of nuclear knowledge and sophistication: “with EMP, accuracy is not that important, and you don’t have to survive re-entry.”

Turning to the history of EMP, Boston noted that we have known about the EMP effect of nuclear explosions since 1945. In 1962, US nuclear bomb test explosion over the Pacific caused the vaporization of telephone cables and fires at power plants in Hawaii over 600 miles away. In the same year, a Soviet nuclear explosion over Kazakhstan had even more powerful effects on electrical systems, causing failures on 1000 km of buried cables.

The first EMP commission in 2004, which was appointed in the aftermath of the 9/11 attacks was a turning point in the consideration of the EMP danger to civilian infrastructure. Earl Gjelde, who was Under Secretary of Energy gave a presentation which, Boston recalled, “scared the heck out of most of us.”

Boston remarked with satisfaction that over recent years, treatment of the EMP threat has at last moved from talk to initial steps toward action. Listing some of the progress achieved, he reported that “the Electric Sector Coordinating Council is up. DOE and EPRI have joined the EMP group with real funds, looking at resiliency and developing five strategy goals. There were 31 deliverables defined by DOE.

In addition, he noted that Israel has begun to take steps to harden its grid, saying “Israel is well ahead of us – they usually are.” He concluded that hardening US systems against EMP not only reduces vulnerability but also reduces the threat by serving as a deterrent to potential attackers.

In 1962, a US nuclear bomb test explosion over the Pacific caused the vaporization of telephone cables and fires at power plants in Hawaii over 600 miles away. In the same year, a Soviet nuclear explosion over Kazakhstan had even more powerful effects on electrical systems, causing failures on 1000 km of buried cables.
Robin Manning reiterated the progress that has been made in recognizing and beginning to address the EMP threat. He recalled that seven years earlier when he was first invited to an EIS Council Summit, “despite the fact that I was running one of the largest transmission systems in the United States, I hardly knew what the letters EMP stood for. There really was a knowledge gap all across the world in the electric sectors, about the impacts of EMP.” Manning acknowledged that, largely due to EIS Council’s work, the knowledge gap has been significantly filled. Most senior people in the US power industry have some understanding of the EMP threat. At the same time, he warned, immense challenges remain in preparing for EMP. Singling out one such task, he urged that “our next challenge is moving off of the grid to the homes and the hospitals and the water towers and to all the plethora of impacts that we will see out there; the millions of vulnerability points that exist around the world that have yet to be really addressed.”

Returning to Boaz Ganor’s point about terrorist motivation, he concluded that we need to convince our adversary that we have dealt effectively, not only with the broad threat to the electric grid, but also with the threat to other branches of infrastructure.

“Our next challenge is moving off of the grid to the homes and the hospitals and the water towers and to the millions of vulnerability points that exist around the world that have yet to be addressed.”
Dr. Shlomo Wald, Former Chief Scientist, Israel Ministry of Energy and Water

In his brief remarks Shlomo Wald thanked Congressman Trent Franks and Terry Boston for their appreciation of Israel moving fast to protect its electrical systems from EMP. Wald commented on this effort from his perspective as former Chief Scientist of the Israel Ministry of National Infrastructure where he was responsible for long-term national policy and technology development in the fields of: energy, water, earth and marine sciences.

He noted that Israel’s efforts still fall far short of what needs to be done. As Wald put it, “the meaning of fast is not a well determined quantity. And you know that 1,000 years is a brief moment in the eyes of God. I think to my great sorrow that even moving “fast” is too slow compared to what we need.

The program that Franks, Boston and others praised was the EPIC II project run by the Israel Electric Company and EIS Council. Wald singled out EIS Council’s role in the project, saying, “I must stress the importance of the EIS Council support in this process to the Israel Electric Company and to the Israeli regulators and authorities that are involved in the EMP threat.”

EPIC II is studying and modelling what is needed to protect the Israeli grid against EMP. The project is expected to be finished by the end of 2018, after which there are plans for experiments with prototypes and a pilot program. This is only a start on the way to implementing full protection against EMP in Israel and progress needs to be faster, Wald said.

Wald also underscored Paul Stockton’s point about the importance of understanding multi-system effects and impacts from large scale power outages.

“Fast is a relative term and Israel’s efforts in protecting against EMP still fall far short of what needs to be done.”
Ian Grant expressed reservations about any suggestion that, as far as the actual impact on the grid goes, the US is in reasonable shape to deal with an EMP event.

He contrasted EMP with earthquakes, storms and other more familiar hazards. For these “gray sky events,” he asserted, we can recognize them. We are really reasonably well-equipped to deal with them. We have people to help. We have crews coming from neighbors. We have standardized methods of restoration of damaged equipment.”

Grant then enumerated some critical differences between such events and EMP. In the case of the latter, “first, we don’t necessarily know that it’s happened. Second, we don’t know what it will do to us or to the people that we supply. And third, even if we do know it’s happened, we’re not at all sure what it has done to us. It’s not obvious, if you walk into an EMP-affected switch house, that the relays in there will work or will not.”

Moreover, communications systems that would be essential for identifying damage and restoring systems will themselves be damaged in an EMP attack. Grant noted that TVA has multiple forms of communication and is replacing its wireless system with one that’s more resilient, “based on some excellent work that the EIS Council did recently in studying communications.” He also pointed out the challenge of storing enough spares to replace transmission relays and of shielding and hardening switch houses.

Finally he described his utility’s greatest EMP-related challenge: “our generating plants are difficult to model, and we have no idea what an EMP will do to them.” Based on these reservations Grant expressed concern that there is still a great deal of work to do to make the grid resilient to EMP.
Q and A Session

Terry Boston asked about lessons for EMP preparation in light of the especially strong links between electricity and water in Israel where 60% of water use is from sea water which requires significant electricity to desalinate. Shlomo Wald added that the water market in Israel takes about 25% of total power consumption for pumping, desalination and water purification; (Israel purifies about 80% of brackish water.)

Boston asked Robin Manning what new models and tools are needed in order to use the research data about EMP wave forms to harden the grid in a cost-effective way. Manning replied that advanced modelling tools are crucial. EPRI is half way through a three year project to review the effects of EMP on the transmission grid.

The next task, addressing E1 and E2 pulses, is very challenging. He also noted the particular difficulty of “taking that information and channeling it to utilities, so that they can see it and understand it and convert it to utility language, so it becomes specifications.” Once the impacts are understood, utilities can begin to assess the right mitigation methods.

Boston also asked the panel “what makes the EMP threat so complicated? Why has it taken us so long to mobilize since we’ve known about this for 25 years? Michael Rooney responded that the main difficulties have been effectively modelling EMP and “getting the information institutionalized in the power industry.” He added that having a national power grid test bed would be very helpful.

In response to a further question from Terry Boston, “what is the government’s role in getting ready for and preparing for an EMP threat?” Manning responded that the government’s most important role is to inform; “their energy should not go so much towards forcing compliance but instead towards enabling information flow.” In particular, government should efficiently declassify information about the effects of EMP and ensure that it is sent to those in the power industry who need to see it. Shlomo Wald responded that EIS Council can and should play a crucial role in ensuring that information about the effects of EMP on electrical systems are distributed to the right players. He added that there are major gaps in our understanding of the effects of EMP on DSOs (Distribution System Operators) and TSOs (Transmission System Operators) and on renewable energy components, for example solar inverters.

David Fromme clarified, in answer to a question from Boston about how badly high power relays failed in EMP tests that the failure was permanent and required replacement of the relays.

“Boston asked: what makes the EMP threat so complicated? Why has it taken us so long to mobilize since we’ve known about this for 25 years? Michael Rooney responded that the main difficulties have been effectively modelling EMP and getting the information institutionalized in the power industry.

“Government should efficiently declassify information about the effects of EMP and ensure that it is sent to those in the power industry who need to see it.
Panel 2 | Cyber Attack

Chair: Marc Sachs, Senior Vice President & Chief Security Officer, NERC

Marc Sachs, Senior Vice President & Chief Security Officer, NERC

Introducing the panel, Marc Sachs gave a very brief sketch of the history of the cyber threat. While there is evidence that biological and chemical warfare are thousands of years old, it required the evolution of our current infrastructures for cyber to be the threat it is today. Already in the 1960s, however, futurists at the Rand Corporation were theorizing about how a hyper-connected world would afford new opportunities for aggressors. By the mid-1990s when the internet came of age, the idea that you could attack adversaries through the internet began to be discussed. The Oklahoma City bombing was a turning point, because in addition to the heavy loss of life, a number of data centers were lost in the bombing, highlighting the damage one could cause by destroying key computer systems.

The Y2K bug anxieties further focused attention on the vulnerability of globally interconnected computerized systems. Sachs underscored that cyber is a man-made problem and concluded on a hopeful note that since human beings created cyber space with all of its strengths and vulnerabilities, it is within our ability to protect them also: “We built cyberspace. We built the internet with all of its vulnerabilities."

“Human beings created cyber space with all of its strengths and vulnerabilities and it is within our ability to protect it also.”
Subject Matter Expert

Cyber Attack - Broadly Targeted at Critical Lifeline Infrastructure Sectors

Erez Kreiner shared his expertise in cyber defense, based on 25 years of working in mitigating cyber risk. He began with some statements of first principles.

The cyber threat to infrastructure

First, he declared that companies have to protect themselves; “No businessman, no CEO, no chairman can rely on governmental agencies to protect his business from cyber.”

Second, he continued “cyberattacks are a fundamental fact. They are occurring, and they will continue to occur, and they will be much faster, much harder. And it’s a great threat to any business, and especially to infrastructures.” He cited a recent report by Lloyd’s, the insurance underwriters, that the financial impact of a broad cyber attack would be greater than that of any recent natural disaster including major earthquakes and hurricanes.

Thirdly he added, for utilities and other infrastructures, cyber offense is a matter for the government but irrelevant to the private sector; only defensive abilities count. Contrary to the maxim “the best defense is offense,” in cyber, the best defense is defense. You don’t have, actually, an opponent or adversary in front of you.”

As a small country “living in a really tough neighborhood” Israel has built up considerable experience in fending off all sorts of attacks...

“...No businessman, no CEO, no chairman can rely on governmental agencies to protect his business from cyber.

“...It doesn’t matter if you put your power plant 80 meters below ground level, because cyber can reach everywhere: submarines, spaceships, bunkers with a lot of concrete surrounding them. There’s no place to hide.
on infrastructure. Based on this experience Israel has understood that power is the most important infrastructure upon which the other infrastructures depend. Consequently, he said, we must take very careful measures to defend the power system from cyber attacks.

Cyber is a uniquely powerful and dangerous weapon, he stressed. “It goes at the speed of light. It can hit 1,000 places at the same time. You don’t have a counterattack. You can hit a missile with a virus. You cannot hit a virus with a missile. It’s one way. Cybernetic weapons can defeat kinetic weapons. Kinetic weapons cannot defeat cybernetic weapons.” Moreover, Kreiner added, “It doesn’t matter if you put your power plant 80 meters below ground level, because cyber can reach everywhere: submarines, spaceships, bunkers with a lot of concrete surrounding them. There’s no place to hide.”

The last time there were foreign soldiers on U.S. soil was 200 years ago. Since then, all America’s wars have been overseas. However, “Cyber brings the war back home to American banks, to the American grid.” Moreover, with cyber attacks, it is extremely hard to identify the perpetrator; “with cyber, when you see the gun, you don’t understand who pulled the trigger. When you see the finger on the trigger, you don’t really understand to what body it is connected.”

The vulnerability of US infrastructure

The ubiquity of electronic control systems means that every new piece of hardware in the power industry creates a cyber target that must be defended. As an example, he cited a Washington DC-based power company that is renovating five substations over the next four years. Kreiner had been able to quickly find the plans online and other information that would have been useful for carrying out a cyber attack on the plants. Just the previous month, a nuclear plant in Kansas was subject to a cyber attack, along with another 12 points on the grid. “Just imagine,” Kreiner urged, “another 1,000 weak points being hit at the same time on that American grid.”

“...You can hit a missile with a virus. You cannot hit a virus with a missile: it’s one-way. Cybernetic weapons can defeat kinetic weapons. Kinetic weapons cannot defeat cybernetic weapons. Cyber goes at the speed of light. It can hit 1,000 places at the same time. You don’t have a counterattack.”

“...The last time there were foreign soldiers on U.S. soil was 200 years ago. Since then, all America’s wars have been overseas. Cyber brings the war back home to American banks, to the American grid.”
Elements of cyber protection

Protection requires more than just technology and regulations. Kreiner recalled that when he was a cyber regulator in Israel, he made the role into one of coordinating between the private and government sector, providing new technologies, methodologies and guidance to companies about how to set up the best protection systems. Above all, protection needs companies to be nimble and flexible. The cyber threat landscape is changing rapidly so the ability to react rapidly and sometimes proactively is critical. It is important to remember, he said that “with cyber, the opponent needs to touch your systems many times before they launch the attack. So this is the time where you can catch him, where you can find him.”

He warned that whereas the 9/11 attacks had been technically possible for some 50 years before they took place, he was certain that it will not be as long as 50 years before the technical possibility of a catastrophic cyber attack is realized in practice. Concluding on a hopeful note, he noted that cyber was created by human minds, meaning, he pointed out, it can be mitigated by human minds.

“With cyber, the opponent needs to touch your systems many times before they launch the attack. So this is the time where you can catch him, where you can find him.”
Panel Discussion
Robert Kolasky, Deputy Undersecretary (Acting), National Protection & Programs Directorate, U.S. Department of Homeland Security

Bob Kolasky from the Department of Homeland Security echoed Erez Kreiner’s assessment of the urgency of the cyber threat. He added that adversaries and potential adversaries are taking actions indicating that critical infrastructures would be a target for attack in a geopolitical conflict.

DHS endorses public-private partnerships as the best vehicle for protecting key infrastructure. “The role of government,” he proposed is “to support the owners and operators of critical infrastructure to take the steps they need to make sure the grid is secure in the face of an attack.” A key element of this supporting role is to ensure that information and intelligence are made available to the utilities.

Kolasky noted that the President’s recently signed Executive Order 13800, on protecting critical infrastructure “directs us to do as much and as fast as possible to get any information, resources government has to support infrastructure, to make sure our tools are available.”

The order also directed DHS to work with the Department of Energy to study any potential gaps in the electric system that could be exploited by a cyber attack. The 90 day study is nearing completion and will make recommendations to the administration on how to fill the key gaps. Kolasky noted that the gap analysis relies largely on the work of people in the room.

The other major task for DHS mandated by the Executive Order is to deepen the Department’s relationship with the nation’s most critical infrastructure companies on critical facilities lists where a failure could potentially cause catastrophe. In this area, Kolasky reported that DHS is “focusing on strengthening our ability to share information, both at a classified level and then at a real-time level.”

He added, “we really have to be the translator of a lot of what’s going on across the federal government, things that are happening in the intelligence community, DOD, and the research community.”
Tamara Lance spoke from her perspective as a practitioner and as an owner/operator about risk mitigation and resiliency.

Drawing on her 15 years of experience in information technology, focusing on data security for energy utilities, she began her brief remarks by discussing how to mitigate some of the risks to utility owner/operators involved in sharing information for the purpose of protecting infrastructure.

She noted that, while working in the electricity and gas utility sector, she uses the types of security best practices that one would find in the financial sector or in a critical manufacturing industry. These include relying on different data centers and having diversified and resilient telecommunications.

Lance added that “one of the beautiful things about working in natural gas is that it’s about physics for us. So as long as we have pressurization from upstream in our pipelines, we are still able to provide service to our customers.” She recalled that after Hurricane Katrina, although telecommunications and the power grid were badly damaged, gas suppliers were still able to supply downstream customers.

“I am in the oil and gas utility segment, however, I use the same best practices from a corporate network that you would find in the financial sector or a critical manufacturing industry.

“One of the beautiful things about working in natural gas is that it’s about physics for us. So as long as we have pressurization from upstream in our pipelines, we are still able to provide service to our customers.”
Lt. Gen. Mark Bowman, U.S. Army (retired), former Director, Command, Control, Communications and Computers (C4)/Cyber, Chief Information Officer, Joint Staff, J6/CIO

Mark Bowman opened by emphasizing that a large proportion of cyber attacks can be avoided by the consistent practice of good security habits. He quoted Robert Johnston, the President and CEO of Adlumin. Bowman who said, “There’s never been a sophisticated cyberattack.” While not discounting the possibility that adversaries certainly could mount sophisticated cyber attacks, Bowman added that, in his experience, “they tend to be pretty simple. It basically comes down to cyber hygiene.”

He recalled how in the Defense Department, computer networks were at first designed to be as easy as possible for staff to use. However “easy makes it easy for the bad guys as well.” So security was tightened and “patches” were issued to cover weak points in the system. Later an endpoint management tool Tanium, was also added.

Bowman left his audience in no doubt as to the seriousness of a major cyber attack on infrastructure. He warned that “if we have an attack on our electrical grid, and it shuts part of our nation down for any extended period of time, we’re going to have chaos at a level we have never seen in our lifetimes in this country. It’s an indisputable fact. And it will severely affect Department of Defense as well, because we’re all in this together. So we need to work together to ensure that our networks are absolutely as tight as we can make them.”

“If we have an attack on our electrical grid, and it shuts part of our nation down for any extended period of time, we’re going to have chaos at a level we have never seen in our lifetimes in this country. It’s an indisputable fact. And it will severely affect Department of Defense as well, because we’re all in this together. So we need to work together to ensure that our networks are absolutely as tight as we can make them.”
Nick Santillo from American Water gave a perspective on cyber security from the perspective of the water and waste water industries. He noted the critical importance of these infrastructures. If they fail for more than a day or two then large numbers of people are likely to try and move to somewhere that has functioning water systems.

Santillo argued that, contrary to what some think, water utilities are highly interconnected via the internet and industry networks. This makes cyber security critical. The National American Water Works Association is addressing this area by developing a holistic, risk-based approach and an operations-focused, cyber protection guideline document for utilities.

“Partnerships is the other key area,” Santillo stressed. “We cannot do it alone.” Some of the key partnerships are with industry organizations and with the DHS for information sharing on threats. Exercising plans is also essential for preparedness. The sector is now moving from primarily internal exercises to cross-sector exercises with the electric, gas, chemicals and transportation sectors, recognizing the deep interdependencies between water and these other areas.

“Water utilities are highly interconnected via the internet and industry networks. This makes cyber security critical. The National American Water Works Association is addressing this area by developing a holistic, risk-based approach and an operations-focused cyber protection guideline document for utilities.
Q and A Session

In the Q and A session, Marc Sachs asked Erez Kreiner whether one should model the cyber threat as coming from a particular country, such as Russia, or from a particular technology. Kreiner cautioned against binding oneself to any particular paradigm either of adversary or technology. The paradigms in cyber are changing all the time; “this is an open-ended arena.” Moreover, he warned, it is very hard to identify the adversary with any confidence: “it’s very easy to put some Cyrillic letters inside a program, and you will say: I have found some traces of the attackers over there. But there’s no attacker. It is foggy.” Instead, he recommended careful research into how one’s organization is perceived on the internet by any potential aggressor: “Just go there to the darknet, go to social media. Understand how your organization is being looked at from the other side. Are they talking about attacking your organization? Are you being exposed? Is somebody trading privileged information and passwords from your power plant over there in the darknet? This is something that organizations can do.”

In response to a question about the most useful information sharing that the water utilities do, Nick Santillo remarked that discussion with other utilities is very valuable, particularly after one of them has been attacked and they share operational information; “where after the fact, they were able to say “here’s what we saw. Here’s what we did.”

Marc Sachs posed a question about the metrics for cyber protection, asking, “can I stand in front of somebody and say I am more secure today than I was yesterday, and here’s how I prove it?” Tamara Lance responded that indeed there are KPIs (Key Performance indicators) that industry uses to determine risk mitigation. However, some of the greatest risks are “unknown unknowns” where there is no agreed mitigation practice. “She explained, “It’s just like physical defense, and you have to continue to change your playbook for everything that comes up. It is a moving target.”

In conclusion, Bob Kolasky noted that one of the important roles of DHS is looking at the gaps between current preparedness and possible, realistic threats. This understanding has emerged from working with EIS Council. DHS published the “National Cyber Incident Response Plan” last year and it needs to be taken further.

Nick Santillo remarked that discussion with other utilities is very valuable, particularly after one of the them has been attacked and they share operational information; where after the fact, they were able to say here’s what we saw. Here’s what we did.

Bob Kolasky noted that one of the important roles of DHS is looking at the gaps between current preparedness and possible, realistic threats. This understanding has emerged from working with EIS Council. DHS published the “National Cyber Incident Response Plan” last year and it needs to be taken further.
Session Two

Natural Black Sky Hazards

Chair: Lord Toby Harris, Co-chair, EIS Summit
Series’ Member, House of Lords, UK
Session Summary

Natural Black Sky hazards – severe terrestrial weather, severe space weather and earthquakes - can wreak disastrous damage and cause a Black Sky level power outage. This session presented expert perspectives on the potential impacts of these hazards, surveyed the progress that utilities are making to mitigate against the threats and laid out the considerable work that remains to be done.

The United States suffers from more extreme weather than any other country, according to Dr. Louis Uccellini of the National Weather Service. He surveyed the impacts of major recent hurricanes including Katrina and Sandy, which caused weeks long power outages in such regions. He presented the NWS’s “Weather-ready Nation initiative and argued that through partnering with utilities, the National Weather Service can enable power suppliers to plan proactively for the recovery from severe weather events.

Panelists noted that extreme weather events are getting worse, whether because of climate change, or because of population increases in vulnerable areas; some hurricane-exposed parts of Florida have many times more people living there than 50 years ago.

The United States has markedly improved its resilience and recovery in the face of extreme weather since Hurricane Katrina in 2005 but infrastructures are severely tested by increasingly frequent and destructive storms.

Severe space weather, especially coronal mass ejections from the sun can cause Geomagnetic Disturbances leading to serious disruption to power systems, similar to the effects of the E3 pulse from EMP. Dr. Daniel Baker described the current state of space weather research. He focused on the massive CME that occurred in 2012, from which scientists were able to derive enormously useful observations and data. That solar flare missed the earth by about a week. Otherwise, Baker said, “We would still be picking up the pieces.”

Baker noted that “The operational space weather community has long sought some definition of what would be a realistic worst-case or plausible worst-case scenario. I believe again that the July 2012 case fits that bill pretty well.” Panelists also discussed approaches to educating the public about space weather.

Dr. Thomas Pratt presented an overview of the earthquake threat to the U.S. Contrary to what many think, “earthquakes are not just a California problem,” he observed. A major seismic event in the New Madrid Seismic Zone in the center of the US could be at least as devastating as one on the better known San Andreas fault. Moreover, geological structures in the eastern US are such that earthquakes would be felt over a wider area than in the West. The high density of oil and gas pipelines in the New Madrid zone is an additional source of danger.

Pratt stressed that we cannot predict earthquakes. At best, after a quake has begun we can give 30-60 seconds warning before it reaches peak intensity. Panelists discussed what guidance to give to the public about how much emergency water to keep at home in case of an earthquake. Danny Lacker from the Jerusalem Water Authority described the earthquake detection devices in place in Israeli reservoirs and schools.
Lord Toby Harris introduced the Natural Black Sky Hazards section of the program by briefly surveying EIS Council’s work in the UK, “to try and bring forward some of the ideas that have already been worked on in the United States.”

Harris joked that while it is true of the UK, that as Henry Higgins said, “In Hertford, Hereford, and Hampshire, hurricanes hardly ever happen,” Britain has suffered extreme weather events in recent years. For example, on the 5th of December 2015, Storm Desmond led to the river Lune flooding. “That was described as a once-in-a-hundred-years’ event,” remarked Harris. “It’s funny how these things are always described as a once-in-a-hundred-years’ event.”

**Cascading impacts on infrastructure of Storm Desmond**

Harris went on to detail the disastrous consequences of the flood: “It swamped an electrical substation in the city of Lancaster in the northwest of England. More than 60,000 homes and businesses and at least 100,000 people were left without electricity for four days. ATM machines went out of action. Garages were unable to dispense fuel as their pumps needed electricity to operate. Traffic lights stopped working. Train stations had to close. Text messaging, digital radio, and the internet ceased to be available. 75 emergency generators had to be brought to Lancaster from as far away as the southwest of England, and over from Northern Ireland in order to regain electric supplies.”

Harris noted that since the flood affected a localized area, manageable in size, importing generators was possible. “In a much larger area with a much bigger population, such arrangements would not have worked.”

“Schools will close. Hospitals will cease to function unless they have an emergency generator which is working. And communications would not operate. How long will major supermarkets remain open? In 2004, our security service, MI5, famously reported that the United Kingdom was four meals away from anarchy. It doesn't take much imagining what the implications are for civil order are of there not being food supplies, there being no communications, and it not being possible to access your bank accounts.”
The cascading impacts from this relatively contained incident highlighted the interconnected nature of critical infrastructure. In a larger outage, the impacts would be much worse, Harris warned. “Schools will close. Hospitals will cease to function unless they have an emergency generator which is working. And communications would not operate. Domestic refrigerators and freezers will stop. So will those in small retailers. How long will major supermarkets remain open? In 2004, our security service, MI5, famously reported that the United Kingdom was four meals away from anarchy. It doesn’t take much imagining what the implications are for civil order are of there not being food supplies, there being no communications, and it not being possible to access your bank accounts.”

**Catastrophic events are more probable than we think**

Harris ended by showing how, through some simple calculations, that such events are in fact much less rare then we think. If the Lancaster flood was really a “once in a hundred years” event and there are six sorts of events that might cause a catastrophic breakdown the chances of one of those six occurring in any particular year is 5.8%. “That means that the chance of one of them occurring by the end of the next decade is 54.3%. That is more likely than not.” Therefore, Harris concluded, “I think it is more than justified that we are spending these two days in this summit, and so many of us are spending so much time working on these issues.”

“If there are six sorts of events that might cause a catastrophic breakdown and each is a ’once in a hundred years event’ the chances of one of them occurring in any given year is 5.8%.
Keynote

Expanding Civil Infrastructure Interdependence: 
An Unprecedented Problem, with Efforts Just Beginning Internationally to Analyze the Problem

Prof. Brian Collins: Professor of Engineering Policy at University College London; Director of the International Centre for Infrastructure Futures (ICIF); Former special advisor to the House of Lords Science and Technology Committee; Chief Scientific Advisor (CSA) to the British Government (Transport, Business Innovation, and Skills)

Professor Collins opened the session with a keynote address discussing problems of infrastructure interdependency. He began with a story from when he served as Director of Technology at GCHQ, (the UK equivalent of the NSA) illustrating the nature of critical interdependencies. GCHQ was the UK signals intelligence center and housed three quarters of a billion pounds worth of computing equipment, much of it purpose built and virtually irreplaceable.

Collins was instructed to ensure that the center was guaranteed to be operational 24/7 without fail. In the course of scanning the local surroundings to make sure he hadn’t missed anything, he noticed a concrete rampart on top of a nearby hill. Upon enquiring, he was informed that this was the Severn Trench reservoir, containing 500,000 gallons of water. Collins recalled, “we immediately said so if someone breaches the wall of that reservoir, we’ve lost our data center, right? So we physically moved the reservoir. In other words, we built another one and drained that one. That for me was where I started to realize that interdependency was a really critical issue.”

He proceeded to touch upon some key issues of infrastructure interdependency and resilience based on his experience helping develop the UK National Infrastructure Plan, and lately convening a multi-university program to research infrastructure.

“City governance starts to become a very important issue for the wellbeing of the population were any of these incidents or natural disasters that we’re talking about to hit.
Scale and infrastructure interdependency

The first issue is one of scale; “what’s the right scale at which to do your analysis of interdependency?” Collins argued that one needs to keep different scales in mind at the same time. In the example of the reservoir, a local piece of water infrastructure interacted in an unexpected way with an intelligence infrastructure facility of major international importance.

The importance of city governance for building population resilience

Collins identified large cities as places where the local level interacts constantly with the national and international. Today, more than 50% of the world’s population lives in cities. Consequently, Collins argued, “city governance starts to become a very important issue for the wellbeing of the population were any of these incidents or natural disasters that we’re talking about to hit.” He reported on data showing that a quarter of a million people is about the largest scale on which people feel able to identify with a community.

Collins posed the question of whether this would be the right level at which to design, build, and operate resilient infrastructure. Research on good city governance in the UK shows that “while there’s no one-size-fits all, there might be principles that are transferrable from one community to another” and this appears to have much to do with scale.

He stressed that we need to ask, “what is the role of city leaders in organizing ourselves to be capable and resilient, and understanding the interdependency and the high-density spaces we live in? That’s what cities are, high-density spaces that deliver huge economic advantages, but they also deliver huge vulnerabilities.” Moreover we must ensure that city leaders have enough delegated authority to deliver the required resilience.

“Cities are, high-density spaces that deliver huge economic advantages, but they also deliver huge vulnerabilities. What is the role of city leaders in organizing ourselves to be capable and resilient, and understanding the interdependency and the high-density spaces we live in?”

“Collins emphasized the importance of balancing the use of sophisticated analytical tools with intelligent interpretation of well-known information, saying, Sometimes we’re sadly lacking in the use of common sense in applying what we already know.”
Collins moved on to speak about governance as it relates to flexibility of decision-making processes and culture. He suggested that the protection of critical infrastructure against major threats is moving from the stage of “convening a group of people who are like-minded about a problem” to the point “where you’re beginning to direct people to do the right thing because a lot of work has been done to show what the right things to be done are.”

The dynamics of policy and cultural change

The dynamics of change processes in communities vary. Some change quickly and easily while others are resistant. Collins noted that regulatory and legislative frameworks tend to take the most time to adapt. The dynamics of the change of governance sometimes work in perverse ways around investments in resilience “which aren’t going to help the industry’s profitability in the short term, though it may help their sustainability in the long term. We need to ensure that resilience investments are made early enough in infrastructure projects to avoid the much larger costs of failures later in the cycle.

Utilizing aerospace-class systems analysis to analyze infrastructure resilience

He proceeded to discuss some of the technology and modeling requirements for systems resilience. “System of systems” thinking, long familiar in aerospace, intelligence and defense is now entering the infrastructure field. Resilience in handling and transmitting data and metadata for communications is an important research area. Similarly, we need to consider resilience of the financial system and automated payment mechanisms, without which an advanced society will have great difficulty functioning. Collins referred to some promising applications of topology and network theory to understanding complex infrastructure interdependencies which show how “the way in which you lay out your network affects its vulnerability to area and point attacks or point events, which may be natural.”

Collins added that although modelling of multi-sector activity is very difficult, the development of super computing capacity begins to make it possible. He reported that the cross university infrastructure program has just invested 18 million pounds in developing the capacity to model cross-sector infrastructure so as to understand the nature and strength of the interactions.
While appreciating the contribution of mathematical and algorithmic analysis, he cautioned that “we’re sadly lacking in the use of common sense in applying what we already know.” Referring to an earlier speaker who mentioned artificial intelligence, Collins responded “I want to see a bit more application of intelligence first.”

**Cyber hygiene and personal hygiene**

Collins ended with some advice about cyber which he described as primarily a problem of hygiene, not dissimilar to personal hygiene. “We all in this room, look after our personal hygiene because we live in a shared space, especially in a high-density space. We would all get really uncomfortable if we knew that we were the one that made the space we were in not nice for everyone else to live in, for all sorts of reasons. So we don’t infect each other, we don’t upset each other. Yet, somehow once we’re in the virtual space, we allow all sorts of things to happen, which infect everybody. And it rebounds back on us.”

It is essential to educate employees in good cyber hygiene – putting in place very basic checks and safeguards against infection. This is the most cost-effective approach: “it costs you a hell of a lot less to deal with things if you’ve done as much protection as you can right in the first place.”

“We all in this room, look after our personal hygiene because we live in a shared space, especially in a high-density space. Yet, somehow once we’re in the virtual space, we allow all sorts of things to happen, which infect everybody. And it rebounds back on us.”
Panel 1 | Extreme Terrestrial Weather

Chair: Nick Santillo: Vice President, Internal Audit and Chief Security Officer, American Water

Panelists, Tom Galloway, President and CEO, North American Transmission Forum, Steve Bieber, Chief, Urban Watershed Programs and Homeland Security, Metropolitan Washington Council of Governors; Michael J. Gaffney, Senior Director, Gas Distribution Field Construction, Public Service Electric and Gas (PSE&G); Bill Chiu, Bill Chiu: Director of Engineering - Transmission and Distribution Engineering, Southern California Edison
Dr. Louis Uccellini, Director, National Weather Service, U.S. NOAA

Subject Matter Expert
Extreme Terrestrial Weather

Dr. Uccellini gave a presentation surveying the United States’ increasing vulnerability to extreme weather events and an update on its state of preparedness. He asserted that “the US probably has the the worst severe weather in the world,” including the prolonged drought in the western third of the country as well as floods, storms, hurricanes and tornadoes. (The fall of 2017 proved Dr. Uccellini to be, unfortunately, right. The exceptionally destructive hurricane season included Hurricanes Maria, Irma and Harvey, as well as the first (bounded Black Sky event in history – in Puerto Rico. (Ed.) The gravity of the threat is widely recognized. At the most recent Davos Economic Forum, business leaders consistently ranked extreme weather as one of the most serious dangers that we face.

Extreme weather in the United States since 2005

Uccellini began by noting the frequency of the “derecho” weather phenomena. These are long-lived, rapidly moving lines of intense thunderstorms which can travel at over 60 miles per hour. They affect a wide area of the US, especially in the summer. Derechos regularly cause local power outages by bringing down trees and electric pylons. The incidence of Derechos is increasing, though Uccellini suggested that part of this rise may be due to increased awareness and reporting by weather enthusiasts.

Turning to tropical storms, noted that Hurricane Katrina in 2005 did damage mostly through surge flooding rather than winds. Katrina was one of the most destructive US hurricanes ever, causing at least 1245 deaths and $108 billion of damage. Uccellini then described a number of
the exceptional storms that hit the U.S. in 2011 and 2012. Hurricane Irene caused major damage in the North East of the country, particularly on the Western side of the storm's track. Irene was the biggest storm to hit Long Island since 1985, causing power outages for around half a million customer; it took eight days to fully restore service.

Hurricane Sandy, which struck in 2012 was even more destructive. New York City received the full force of the storm and Long Island was buffeted by 30 hours of sustained tropical force winds. Sandy brought down many transmission lines and caused outages for 1.2 million customers.

“Building a Weather Ready Nation”

Uccellini went on to introduce a new strategic plan for the National Weather Service entitled “Building a Weather Ready Nation.” He explained, “The idea of becoming weather ready is about building community resilience in the face of increasing vulnerability.” Uccellini elaborated on the reasons for increased vulnerability to extreme weather: “whether it’s climate change or not, there are more people living in vulnerable areas: tornado alley, fire-prone areas, along the coast older people living along the coast, so it takes longer to evacuate and longer to prepare.”

Uccellini referred to the process of connecting warnings to storms, which he called “Impact-Based Decision Support Services”. He emphasized the importance of the National Weather Service being more fully integrated in emergency operations centers and emergency exercising. He warned, “if we’re not there practicing with them, we don’t know how to map the uncertainty or certainty of a forecast on to their key decision points.”
Weather forecasting and proactive emergency planning

If it is properly involved in emergency planning, “the National Weather Service can transform the emergency management community from one that reacts to events, to one that proactively prepares, and stays ahead.” This was achieved in Hurricane Matthew where three types of emergency response were required to the surge along the coasts and winds and heavy rainfall inland.

Uccellini recalled, “for inland flooding, we had fast-rescue teams that were being pre-positioned in North Carolina and South Carolina days in advance based on the forecasts. I saw the trucks coming down from New Jersey on the parkways and interstates here, heading down two and three days in advance. FEMA was organizing infrastructure response from west to east for Florida almost a week in advance for Matthew. This did not happen during Katrina.” This integration of weather forecasting with emergency response represents real progress and learning since 2005.

Uccellini cited advice from Craig Fugate, the former head of FEMA: “Prepare for the worst; hope for the best. But if you don’t prepare for the worst, there’s no way you can get ahead of it.”

Uccellini stressed that the “Building a Weather Ready Nation” strategic initiative is founded on partnerships. The recently passed Weather Act mandates government to government partnerships, and private sector, utility and NGO members are also joining in large numbers; currently 6000 different organizations are affiliated, acting as ambassadors for the program. As Uccellini explained, “these ambassadors have become force multipliers, not only during the event itself, but more importantly, during all the safety campaigns that are organized by organizations like FEMA.”

Partnerships enable the National Weather Service to go beyond forecasting warnings: “we have to understand your needs. We have to make sure that our forecasts and warnings actually meet your needs in terms of key decision points and risk preferences.” He ended by urging the utility representatives present to grasp the opportunity of partnering with the National Weather Service and join the “Building a Weather Ready Nation” initiative.

“

The National Weather Service can transform the emergency management community from one that reacts to events, to one that proactively prepares, and stays ahead.
Panel Discussion
Chairing the panel discussion, Nick Santillo raised the question of how to communicate with the public about extreme weather events. He questioned whether talking about once in 100 year events helps public understanding, when in reality extreme weather happens very much more frequently than that.

Santillo pointed out that with infrastructure now much more developed in places exposed to extreme weather, a comparable event will cause much more damage now than it did in the past. For example, he pointed out that in Broward County, Florida a hurricane zone, the population has increased by 8000% since the 1930’s. “That’s more people, more infrastructure. So when that hurricane does blow through Florida, there’s more stuff to break and get rebuilt.”

Communication with the public is critical during and after an extreme weather event. Building on Louis Uccellini’s presentation, Santillo posed the question of how utilities use weather forecasting information to prepare their systems and the expectations of the public. The issue of expectations is vital for the water industry where there are huge public health implications to the delivery of water and waste water services.

Santillo suggested that managing expectations is challenging in an era of social media and instant messaging where communication is instant, but restoration is not: “infrastructure doesn’t get put back in a tweet,” as he put it.

A final issue that Santillo raised for the panel’s consideration is the gap between the data that is shared with the public and the operational-level data that the utility uses to make decisions.
Steve Bieber began with warm praise for the National Weather Service, saying, “there has never been a time I can think of when we’ve asked for help from the Weather Service and they said no. Their forecasting tools are invaluable.”

Bieber referred to Paul Stockton’s comments about emergency coordination and prioritization. To give an indication of how complex that can be for an urban water utility, he explained that “in the Metro Washington region, we have 16 different wastewater collection systems and 18 major wastewater plants. They own and operate about 16,000 miles of pipe. On the drinking water side there’s 13 separate drinking water suppliers, and 27 distributors of the water.”

He added that the water sector faces the challenge of aging infrastructure in dealing with extreme weather, noting that in Washington DC the average age of the pipes is 79 years and many date back to the time of the Civil War. “So you’re balancing the cost of maintaining, operating, or replacing that infrastructure with investments to mitigate against other threats like severe weather.” Many hundreds of millions of dollars of investment are needed in water infrastructure just to meet population growth and demand, let alone investments to mitigate against particular threats.

Finally, Bieber spoke about the extent of cross-sector interdependencies; DC Water is the largest user of power in the District of Columbia. One facility, Blue Plains requires 25 MW hours of power per day.

“In the Metro Washington region, we have 16 different wastewater collection systems and 18 major wastewater plants. They own and operate about 16,000 miles of pipe. On the drinking water side there’s 13 separate drinking water suppliers, and 27 distributors of the water.

“The water sector faces the challenge of aging infrastructure in dealing with extreme weather. As Bieber put it, You’re balancing the cost of maintaining, operating, or replacing that infrastructure with investments to mitigate against other threats like severe weather.
Tom Galloway declared that “the electric industry is very acutely aware of the issue with severe weather. It’s how we live and breathe.” NERC’s Reliability Issues Steering Committee has designated severe weather as one of the top nine priorities for the electric industry and has put together a multi-year action plan that places a focus on cross-sector dependency. Moreover, Galloway noted, “NERC’s Severity Reliability Index has identified severe weather as the most impactful issue on the grid over the last several years.”

One important initiative in this area has been the establishment of the NRE, National Response Event. Galloway explained that this is “a governance structure to help share mutual assistance and support across the entire nation for a large-scale, severe weather event.”

Recent examples of major utilities making major investments in resilience include the work by Con Edison in New York. Galloway described how “in the wake of Sandy they implemented a lot of improvements, including elevating a lot of their important control systems, changing out control cabling with fiber optics, and going to synchrophase modular transformers that are adaptable in a lot of locations.”

In addition, he praised the work done by Florida Power & Light who have invested around two billion dollars since 2006 in system resiliency after a series of storms in 2004 and 2005.

Galloway noted, “with Hurricane Matthew, [in Florida – ed.] they were able to restore 99% of their 1.2 million customers out within two days, and attributed that to a lot of improved system hardening.”

Similarly, Entergy is another forum member that has invested in system hardening, including “underground cabling where it was appropriate, changing elevations on key devices, and consolidating control centers from six down to two, and relocating those off the hurricane path.”

Summing up, Galloway noted that “there’s a lot of good information sharing around severe weather that’s going on in the transmission forum and outside,” in addition to the sustained increase in resilience investment by many forum members.

“The electric industry is very acutely aware of the issue with severe weather. It’s how we live and breathe.
Michael Gaffney recalled the extremely challenging restoration work that he assisted with after Hurricane Sandy as a Director of PSE&G in New Jersey: “over 90% of our electric customers were without power. We lost 14 switching stations. I think 58 substations went underwater, due to the surge, not to flooding, and we had 51 transmission lines out. Our electric system was pretty much done.”

The gas transmission side of the utility lost 26 M&R (Metering and Regulation) stations. This is very serious because these stations regulate the flow of gas, which otherwise needs to be operated manually. 42,000 of the gas customers lost service and reported that they had no heat or hot water.

Since 2012, PSE&G has spent close to a billion dollars on making its systems more resilient.

**Over 90% of our electric customers were without power. We lost 14 switching stations. I think 58 substations went underwater, due to the surge, not to flooding, and we had 51 transmission lines out. Our electric system was pretty much done.**
Bill Chiu began by remarking that contrary to many people’s impression of California as enjoying year-round pleasant sunshine, “we have more than our share of catastrophic events, and particularly weather-related, whether it be rain storm, gale-force winds, wild fire, seismic activities, you name it.” SCE has worked on building its resilience to severe weather in recent years after a wind storm devastated the distribution network in part of SCE’s service area in 2011. Among the lessons learned from that event were improving the design criteria to strengthen SCE’s 1.5 million power poles.

In addition, Chiu stressed, “I can’t emphasize enough the importance of having a rigorous and robust response system. As a result of that lesson, we now have a fairly robust, rotating team providing 24/7 coverage in case of any type of event.” The system is working well. As a recent example, Chiu recalled, “earlier this year we had some torrential rain that hit the west coast. Within 24 hours in advance of the rain we had already mobilized our incident management team and were working with the local community to coordinate potential restoration efforts.”

“I can’t emphasize enough the importance of having a rigorous and robust response system. As a result of that lesson, (from a wind storm in 2011) we now have a fairly robust, rotating team 24/7 coverage in case of any type of event.”
Q and A Session

Louis Uccellini expanded on some of the communications challenges of the “Weather Ready Nation” policy. For example, there has been a large growth in Florida’s population: “More than 30% of today’s population did not experience hurricanes. They weren’t there in 2004, 2005,” he explained. Moreover, “they have older people living along the coast, so it takes longer to evacuate. They actually start a process seven, six, five days before the event.” He also noted the importance of communicating accurate weather data post event, during the recovery activities. Insurance companies, for example, want to know whether it was wind or water that caused the damage.

Mike Gaffney added that the states have made a lot of progress with centralizing communication between emergency services prior to a big storm. Usual practice now is to hold a conference call 72 hours before the event to coordinate plans.

Steve Bieber commented that coordinating and prioritizing the restoration of key facilities has improved in his region, saying, “I think we do a better job of communicating and coordinating critical facilities to get back online, whether it’s a water treatment plant or an acute-care hospital, so that the electric company, the emergency manager, the water utility, everybody is at the EOC working together on a common list of priorities.”

Bill Chiu noted that now utilities have operational plans tailored for specific weather events, so when a particular event is known to be approaching, “we can take that plan off the shelf and be ready to execute right away.”

“More than 30% of today’s (Florida) population did not experience hurricanes. They weren’t there in 2004, 2005.”
Panel 2 | Extreme Space Weather Panel

Chair: Dr. Daniel Baker: director of the Laboratory for Atmospheric and Space Physics, University of Colorado; Chair of NASA/NAS Study on Societal Impacts of Space Weather

Panelists, Bill Hackett, Director, Connecticut Department of Emergency Management; Michael Bryson, Vice President of Operations, PJ Interconnection; Charley English, National Emergency Management Liaison, American Red Cross.
As the subject matter expert on extreme space weather, Daniel Baker surveyed how extreme space weather can impact human societies. As he put it, “we live in the outer atmosphere of an active magnetic star, the sun. Coronal mass ejections, (CMEs), powerful blasts of energy from the sun can interact with the earth’s protective magnetic envelope, the magnetosphere and cause significant problems for many technological systems.” These CMEs can create currents that couple into long conductors such as pipelines and the electric power grid, causing significant damage.

CMEs also affect the ionosphere, causing disruption of high-frequency radio communications (which airlines use.) They can also interfere with GPS communications, which are essential today for precision agriculture, navigation at sea and a host of other uses.

A solar flare can affect the ionosphere within eight minutes of being ejected from the sun. The longer duration effects from coronal mass ejections that can severely impact power systems may take between 12 hours and a few days to travel from the sun to the earth.

Baker noted that “electric power in turn affects the ability to pump oil and gas, to provide water, to deal with sewage, to have communication, government services. We as a society are making ourselves more and more vulnerable to these interconnectedness issues every day.” As Baker put it, “We are making ourselves more tightly networked. We are in a global cyber-electric cocoon.”
In assessing the risk of a severe space weather event, Baker assessed that “while we shouldn’t be unduly alarmist about this, we should be duly alarmist. The possibilities of severe long-lasting effects are certainly there.” The economic effects on critical infrastructures, including perishable food, medication, water, wastewater, fuel supply, transportation, could reach many billions of dollars.

The 2012 solar storm

Turning to the sun’s solar activity cycle, Baker showed data indicating that the peaks of the sunspot cycle have been declining in intensity since 1990. Nevertheless, in 2012, the sun still produced a very powerful CME event emitting a strong blast of high-energy charged particles. Thanks to observations from spacecraft we have excellent data about the magnetic fields and speed of flow unleashed by the 2012 solar storm. This CME was comparable to the famous Carrington event of 1859, which impacted the Earth affecting the telegraph and other basic electrical systems operating at the time.

The 2012 solar storm narrowly missed the Earth. Had it occurred a week early, the Earth would have been hit by its largest solar storm ever, probably larger than the Carrington event. Baker observed that “if the had earth been there at that time, or had it occurred a week earlier, we’d probably still be picking up the pieces from this storm.”

Advancing a national space weather strategy

Baker contended that great progress has been made on developing a national space weather strategy and a national action plans and that much of the credit for this is due to the Office of Science and

“While we shouldn’t be unduly alarmist about this, we should be duly alarmist. The possibilities of severe, long-lasting effects of space weather are certainly there.”

“The 2012 solar storm narrowly missed the Earth. Had it occurred a week early, the Earth would have been hit by its largest solar storm ever, probably larger than the 1859 Carrington event which impacted the Earth affecting the telegraph and other basic electrical systems operating at the time. We’d probably still be picking up the pieces from this storm.”
Technology Policy. He declared that “part of the National Action Plan is to establish better benchmarks about how severe space weather can really get. I contend that the event of five years ago is a very good candidate for that.” It turns out that just a few days before the Summit, another severe space missed the Earth by only a week and a half. “The question, is how long can the earth go on dodging these bullets?” Baker asked.

Among the encouraging advances in space weather preparedness, Baker noted that “improving assessment modeling and prediction of the effects on critical infrastructure is also underway.”

Baker added that EMP can be considered as a kind of anthropogenic space weather. He cited a recent article in Space Science Review showing that the large nuclear tests of 1962 which gave us a lot of our data about EMP effects, also released high energy electrons which “killed a dozen spacecraft.” With around 1400 active spacecraft orbiting Earth today, the effects would be far worse. Summarizing the main point of his talk, Baker said, “the operational space weather community has long sought some definition of what would be a realistic worst-case or plausible worst-case scenario. I believe that the July 2012 case fits that bill pretty well. It’s a perfect experiment, if you will.”

“
Update on FERC Order 779: Space Weather

Michael Bardee’s presentation described recent federal regulations addressing space weather. He explained that the Federal Energy Regulatory Commission (FERC) designated the North American Electric Reliability Corporation (NERC) as the responsible body for electric reliability about a decade ago with the mandate to propose standards to FERC and to enforce them.

NERC has been focused on space weather for about five years and has so far proposed two standards on this issue. The first of these concerned operational procedures to follow in the face of an imminent GMD event. The second dealt with assessing system vulnerabilities with regard to GMD and making any upgrades necessary to mitigate them.

The first standard, known as EOP-10 was approved in 2014, becoming effective in April 2015. It contained three essential requirements as Bardee described them: “One applies to reliability coordinators, which are the utilities with the largest regional footprint. They are required to have operational plans for their areas to implement during and right before a GMD event. They also are required to disseminate forecasted and current space weather information. And the last requirement is that transmission operators must implement procedures to prepare for these events.”

For the second standard, NERC proposed TPL-07, where TPL stands for Transmission Planning. Bardee explained that “they based it on a benchmark event for GMD, a 100-year event. Based on the science available at that time, NERC estimated the 100-year event as one that would produce a GMD leading to a geoelectric field of 8 volts per kilometer. And that would be adjusted for latitude and also for ground conductivity.” Utilities would be required to perform vulnerability assessments every five years, and to mitigate against
harm to reliability revealed by these assessments. TPL-07 was approved in September 2016. The next vulnerability assessments are due to be done in 2022.

NERC is working on some modifications to the standard which it expects to submit in May 2018. These include more refined latitude scaling, which refers to the scaling that reduces the expected effects of GMD as you move further South. Another area of work is improved Earth conductivity modelling taking into account, for example, coastal effects where GMD could have a greater effect on infrastructure because of the conductivity of water. Also, NERC is assessing whether the assumed criterion of 75 amps per phase for assessing transformers’ resilience to GMD is correct.

Bardee also touched on the issue of US Geological Survey observatories that provide magnetometer data that is useful to utilities for protecting against GMD. Those stations are in danger of being cut from the Federal Budget. Congress is now deciding whether to maintain this budget item.

In conclusion, Bardee affirmed that utilities are implementing the current standards and NERC’s research plan is progressing towards finalizing the proposed standard modifications.

“NERC is working on some modifications to the TPL-07 standard which it expects to submit in May 2018. These include more refined latitude scaling, which refers to the scaling that reduces the expected effects of GMD as you move further South.”
Panel Discussion
Charley English began by noting that he represents the American Red Cross (ARC). The ARC is one of 62 organizations that are part of the national group Voluntary Organizations Active in Disaster (VOAD). “These organizations are relied upon very heavily by government and our citizenry to respond and provide that human interface with the disaster survivors in an event,” he observed.

English emphasized that although the nation relies heavily on these organizations for disaster relief in emergencies, their members are all volunteers; “we can’t compel our membership to respond, even though many will run to. But we cannot force those folks.”

What the organizations can do, however, is to train the large numbers of willing volunteers so that they are available to respond in an emergency. “We have found that among the American people, there’s an outpouring of volunteers,” he declared.

“ These 62 organizations that are part of the national group Voluntary Organizations Active in Disaster (VOAD) are relied upon very heavily by government and our citizenry to respond and provide that human interface with the disaster survivors in an event.
Michael Bryson, Vice President of Operations, PJM Interconnection

Michael Bryson, hailed the big advances in awareness of space weather that have taken place over the past few years. He noted that it has begun to enter popular culture telling the summit, “I asked my son this morning, “Do you know what space weather is?” And he said, “Yes. In the first Fantastic Four movie, it’s the thing that turned the Fantastic Four into the Fantastic Four.” I said, “Actually, I guess you really do know what it is.”

Bryson especially praised the greater awareness of space weather among state commissions; “They ask the right questions when we do emergency management exercises or we do Black Sky exercises,” he noted.

He described how PJM has developed a resilience roadmap for space weather, based on the EOP (Emergency Operations) and TPL (Transmission Planning) standards that Mike Bardee discussed, under the headings “Prepare, Operate, and Recover.”

“Prepare” includes system planning, “so the TPL standards are really important to that,” Bryson emphasized. In addition, “prepare” covers “making sure that we’re building things into the infrastructure to help be ready for that. It also includes developing plans. It includes the exercises and drills that are very important. The EOP standards help us with how do we operate through near-term. When we start getting the NOAA (National Oceanic and Atmospheric Administration) alerts, we take a look at those.”

“Recover” refers to system restoration. “We have very robust plans for system restoration,” he declared. “After what we call a normal blackout, we have a plan that we think will recover the system in a couple of days. A GMD event will require us to develop and implement a recovery plan on steroids.”

“After what we call a normal blackout, we have a plan that we think will recover the system in a couple of days. A GMD event will require us to develop and implement a recovery plan on steroids.”
Hackett began by noting that the United States has an “all-hazards” approach to emergency management planning and preparedness. Each state has its own emergency operation plan, under the federal National Response Framework.

Elaborating on the structure in his state of Connecticut, Hackett explained, “we operate under our state response framework, which outlines roles, responsibilities, and procedures, including the interaction between state and local governments and the private sector. Each municipality or county also has an emergency operations plan, since every incident begins and ends locally.” This is also the case for a space weather event. “The symptoms from a space weather event will need to be dealt with in each community that is affected.”

The unified standard for response in the United States is the National Incident Management System, or NIMS. “A key component of NIMS is the concept of Emergency Support Functions, or ESFs, which bring together subject-matter experts from different levels of government and different disciplines to collaborate and solve problems.

During a space weather event, state ESFs would be activated to address restoration and other related recovery activities. Hackett noted that “one ESF that I would like to highlight is ESF 15, External Affairs, with a focus on life safety communications. “The public needs to be continually reminded to make their own preparations in order to be self-sustaining.”

With space weather there is an additional need for good communications, because the event is unfamiliar to people. As Hackett put it, “Over the years, people have become more aware of the effects of hurricanes, tornados, floods, and fires. But the idea of a solar flare or a geomagnetic storm is less understood and very likely to generate fear and panic, especially if it is long term. The people we serve, including our first responders, will be looking to us for factual information.”
Q and A Session

Charlie English noted that in a space weather event “the nightmare scenario is not being able to communicate with our workers to get them mobilized to the scene. That cascades into the consequences of not being able to provide those critical resources that folks will need if they’re out of electricity, out of food and not able to store food or shelter in place.”

Mike Bardee added that his nightmare would be that “a lot of big equipment on the grid gets damaged in a way that it can’t be put back online quickly. In which case, you’re talking weeks or longer before you can get the grid fully back up into operation.”

Michael Bryson suggested that a worst case would be having multiple things happen at once. “If during a massive GMD storm you also had a cyberattack or a terrestrial storm. You would be trying to figure out what is causing the problem that you’re trying to fix, and restore the system at the same time.”

Bill Hackett agreed with Charlie English that communications would be the biggest challenge. “Situational awareness, a common operating picture of what’s happening in the world, what’s happening in our nation, and what’s going to happen down the road is very important, to establish that communication base to protect our citizens.”

In response to a question by Daniel Baker about how much warning utilities would need to prepare for extreme space weather, panelists praised the information coming from NOAA that gives a few days notice. Bill Hackett argued that the reliability and accuracy of the information is at least as important as the lead time it gives and that he would want to have space predictions reliably marked as “high probability, moderate probability etc.”. 

Regarding the importance of accurate information, Daniel Baker recalled that when there had been a large solar event a few years earlier, “a French woman read about it and then went and spoke to her emergency preparedness people in France and asked what should she do if a large solar storm were coming. They said it would be the worst thing that could happen to humanity. She should buy a large chocolate cake, eat it, and wait for the world to end.” In light of this story, Baker stressed the importance of education the public in a measured and restrained way about the threat of space weather. Charlie English opined that for educating the general public, an all-hazards approach works best: “You just have to be ready when stuff goes wrong, regardless of the cause.”

Winding up the panel, Daniel Baker said, “I’m immensely impressed that government agencies, the Congress, the community are all trying to work together responsibly place space weather into a proper all-hazards context.” He also thanked EIS Council for its important contribution to this work.
Panel 3 | Earthquakes

Randy Garrett, Director, Disaster Relief, Arkansas Baptist State Convention

Panel: Xavier Irias: Director of Engineering and Construction, East Bay Municipal Utility District (EBMUD); Danny Lacker: Head of Water Security and Emergency Division, Israel Water Authority, Bridgette Bourge: Senior Principal, Legislative Affairs, National Rural Electric Cooperatives Association; William Parker: Joint Planning Officer, Georgia Army National Guard; Former Current Operations Chief 201st RSG, FEMA Region IV Homeland Response Force
Dr. **Thomas Pratt**, Research Geophysicist, U.S. Geological Survey (USGS)

**Subject Matter Expert**

**Earthquakes**

Dr. Thomas Pratt surveyed the basic nature and causes of earthquakes, discussed the most seismically vulnerable areas of the U.S. and touched on the state of earthquake prediction and warning systems.

An earthquake, he explained, is a rupture in the ground, where tectonic plates are forced apart, leading to shaking and often to horizontal movement of land. A lot of earthquakes don’t break the surface; the rupture remains underground.

Earthquakes are usually caused by the earth’s tectonic plates moving along their faultlines. However, he added, there’s another category of earthquakes that’s very relevant to the United States. That’s the stable continental interior earthquakes, where you’re in the middle of a plate, so in theory you shouldn’t have earthquakes because there’s nothing moving around in there."

**Earthquakes in the United States since 1700**

Pratt presented a list of the 15 largest earthquakes to have hit the continental United States since 1700. He pointed out that “they’re not all in California. Earthquakes are not just a California problem.” While two thirds of the largest earthquakes were centered on the West Coast, the rest were in the New Madrid or Charleston, South Carolina areas. The last major earthquake under a U.S. city was the San Francisco quake of 1906.

Surveying the main earthquake centers of the U.S. Pratt pointed to the San Andreas Fault part of the Cascadia subduction zone, the Rocky Mountain area, the St. Lawrence Valley, the New Madrid seismic zone and the Charleston seismic zone.

"Earthquakes are not just a California problem."

"You can take the same size earthquake, you put it in the two sides of the country, you’re going to get much greater damage in the Eastern U.S."
He also pointed out that the areas affected by earthquake zones are much larger in the eastern U.S. than in the west. Pratt explained that "In the eastern U.S., you’ve got really old, really hard rocks that have been around for a billion years or so. They transmit energy really well. When you look at the western U.S., you’ve got young, fresh rock. It’s broken up. It doesn’t transmit energy very well."

The implication is that "you can take the same size earthquake, you put it in the two sides of the country, you’re going to get much greater damage in the eastern U.S." Moreover, since infrastructure in the East is, unlike in California, not built to withstand earthquakes, the potential for damage in the East is all the greater.

**Making earthquakes worse through induced seismicity**

In addition to natural occurring seismic activity, Pratt explained that we are making the problem worse by inducing seismicity in a number of ways. One cause is loading from reservoirs, which can place more stress on a fault. Another is the injection of high pressure fluids into the earth’s crust as part of the oil and gas exploration process. This forces faults open and is leading to many more earthquakes, especially in Texas and Oklahoma where the bulk of oil and gas activities are located. Whereas for decades, Oklahoma had on average 1.5 earthquakes of magnitude 3 and above, since 2013 the numbers of such quakes have been in the hundreds. Moreover, Pratt warned, “we don’t know what the largest earthquake that we can induce is. It could be much larger than the 5.8, which is the largest one we’ve induced so far.”

Describing how an earthquake does damage, Pratt said that although “when you think about an earthquake, you think about a fault ripping through a city, tearing everything up, the much more...”
widespread damage is from the strong ground shaking.” Shallow earth deposits and formations of soft rock can have a huge effect on ground-shaking by increasing the amplitude of vibrations. There are a lot of cities in the US including Washington DC that are sitting on shallow rock formations. This geological feature would significantly strengthen the impact of earthquakes that could potentially strike these cities. Pratt demonstrated this effect with videos of computer simulations of earthquakes affecting cities including Washington DC, Los Angeles, Santa Clara, Lancaster and Seattle. He also showed how a major earthquake along the Seattle fault would also cause a tsunami that would flood the port and industrial area of Seattle.

An additional animation visualized a 7.3 magnitude earthquake in the New Madrid seismic zone that would cause strong shaking for 200km in each direction. Pratt acknowledged that “these earthquakes in the continental interior are a real mystery. We don’t really understand why they’re happening.” One of the unanswered questions that Pratt referenced is “whether the seismicity is stable in these continental interiors or whether it jumps around. Will the next earthquake again be in New Madrid Seismic Zone or is it going to be in Nebraska? We don’t know the answer to that.”

Pratt also showed maps overlaying oil and gas pipelines and electric power lines with seismic activity zones, showing that there is a high concentration of pipelines and powerlines around the New Madrid zone. There is also, he noted, a high concentration of hydo plants near the California and Oregon seismic zones, pointing to potential vulnerabilities.

**The state of earthquake prediction**

Pratt concluded with some comments on earthquake prediction and early warning. He acknowledged that “we have no way right now of predicting when the next earthquake is going to occur. Occasionally, we get some foreshocks, and we might be able to see one coming, but that’s very unusual.” Earthquake early warning then is not prediction, but identification of the beginning

“... When we identify it and say this is growing into a large earthquake, we can send a warning to cities 50 or 100 kilometers away and give you 15, 20 seconds’ warning, maybe up to a minute warning for a very large earthquake.
of an earthquake: “When we identify it and say this is growing into a large earthquake, we can send a warning to cities 50 or 100 kilometers away and give you 15, 20 seconds’ warning, maybe up to a minute warning for a very large earthquake.”

Prediction is, however, possible for aftershocks: “When there is an earthquake, we can tell you the chances of aftershocks of different size going out for a few weeks to months after that.” Looking at the history of earthquakes on a fault can generate a hazard or forecast map with percentage probabilities of of earthquakes at different places on a fault, but such forecasts are not very reliable.
Panel Discussion
Introducing the panel, Randy Garrett began with some remarks about his work on disaster relief for Arkansas Baptist State Convention, particular as it relates to earthquakes. Arkansas is within the range of the New Madrid fault and so Garrett’s organization participates in regional and state exercises that simulate a major earthquake.

It emerged from the exercises that large bridges in the area may not be usable after an earthquake. In response, Garrett described how ABSC is working with the U.S. airforce “taking our mobile mass kitchens and we’re deciding which ones we can put in a container. And we can drop these into those areas that are affected. If we can’t drive them in, we’ll drop them in, as well as the food supply.”

Another challenge that came out of the exercises is the high level of centralization in U.S. food supplies. As Garrett explained “one of the main distribution points for the New Madrid fault is Memphis, Tennessee. So when Memphis is in trouble, we lose the bridge structures we have in a major earthquake, what are we going to do?”

Communication and coordination will also be critical challenges. Garrett asserted, “there’s no way in the world we can do anything to help the public unless we have the coordination, both with the government and non-government entities.” Exercises are often based on assumptions that “that cell tower is out there and it will work forever,” and that if cell phones fail, people can use their sat. phones. However, Garrett cautioned, based on his experience of working at AT&T that in certain disasters both cell and satellite phones could be inoperable. “That’s a very acute problem that I know EIS Council is looking at,” he said.

Finally Garrett warned that if people cannot get their basic needs, there is a danger of mob violence breaking out. “There are three things we need to survive: food, water and shelter. When people do not have food or water, they band together and they attack the resource where they can get it. We learned this in Katrina. We saw it again in Sandy.” Given this experience, there will be an essential role for the National Guard to protect the NGOs’ relief work in future disasters.
Irias discussed the Loma Prieta earthquake in the San Francisco area on October 17th 1989, a quake of 6.9 magnitude, which killed 63 people. This event shaped subsequent resilience work in the California water industry where Irias has worked since.

As he described the impact on future work, “In the immediate aftermath of the Loma Prieta quake we did a systematic evaluation of the whole water system. 100-something tanks, 126 pumping plants, 26 dams, 4,000 miles of pipe, just a huge system. And we figured out money is not infinite, so what can we reasonably do? We talked to the rate payers and came up with different packages.”

After discussions with the 1.4 million people served by the water utility, Arias recalled, “we ended up spending about 300 million dollars, 201 million on a major package and then another 100 million on miscellaneous projects. That’s a substantial investment for each person.”

Arias learned “one big lesson” from the incident: “If we communicate the risks well, people are pretty supportive of mitigating those risks, at least if an event has just happened.” The challenge is that as time goes on, the risk increases, if only because of the rise in population in the at-risk areas.

For example, today there may be a far large population living downstream from a vulnerable dam than was there when the dam was built. Public perception of the risk, however, decreases as the time since the large major earthquake elapses.

Irias concluded that even though the Loma Prieta quake was relatively small, the water system restoration work was severely disrupted because “transportation was essentially broken. The Bay Bridge was down. The freeway was collapsed.” If and when “the big one” hits, the situation would be far worse.

---

**Xavier Irias**, Director of Engineering and Construction, East Bay Municipal Utility District (EBMUD)
Danny Lacker, Head of Water Security and Emergency Division, Israel Water Authority

Danny Lacker outlined some of the Israel Water Authority’s preparations for an earthquake hitting Jerusalem. He assessed that in a major quake, “production and transit lines won’t be damaged severely, due to a lot of redundancy in production and transit. Distribution lines inside the city will be heavily damaged.” This leads to the conclusion that the IWA will have to cut off water supply to the population in the city. Although Jerusalem has large water reserves in reservoirs, water would not be able to be transported through the damaged pipelines.

An immediate challenge will be to close down the reservoirs so as to conserve their water supplies. Lacker reported, “we are testing earthquake alerts, to see what can you do within 15 seconds of an alert,” and mentioned commercial detectors that can give you up to 30 seconds notice of an earthquake. Many schools in Israel also have these detectors.

Lacker emphasized that “public trust and public peace are very dependent on the extent to which people feel the authorities are taking care of them, and one of the major areas of care is water.” To ensure that water reaches people, the Water Authority is preparing for water distribution throughout the city in tankers. However, this will take lot of human resources which are likely to be lacking after an earthquake.

Lacker quipped that “hopefully gravity will still work after an earthquake,” and so there are designated pipelines from the reservoirs to the streets just below it to supply some of the population.

For additional water supply, Lacker noted that “the Israel Water Authority had contracted out with the major bottling companies in the state to buy all the bottled water in the event of an earthquake.” The IWA had also arranged to work with the supermarkets’ production, transit and distribution systems to bring water to the people.

“Public trust and public peace are very dependent on the extent to which people feel the authorities are taking care of them, and one of the major areas of care is water.”
Bridgette Bourge, Senior Principal, Legislative Affairs, National Rural Electric Cooperatives Association

Bridgette Bourge outlined the main types of suppliers in the electric sector and the mutual assistance agreements that are in place between them. There are three kinds of supplier structure: investor-owned utilities, municipal-owned utilities and electric cooperatives. The last of these serving, some 37 million customers throughout the country, are not-for-profit, private, independent and consumer-owned.

These different types of suppliers tend to have mutual assistance agreements in place. Recently, many cyber assistance agreements have been established so that the larger companies, with greater resources and expertise will come to the aid of the smaller entities.

Physical assistance agreements have been in place for decades. As Bourge explained how they work, “basically it says utilities will come and help each other out. So for example, if a cooperative in a state has an suffers a terrible storm, or a minor earthquake, that individual cooperative will reach out to their state organization who will help them find their spare components, and other help when and how they need it.”

“If the other cooperatives don’t have what they need, then they’ll reach out to the rest of the sector and to other states to see who does. There are plans, and lists of who has what type of spare equipment, so that we can get access to it quickly.”

In a major earthquake, however, it would not be just counties but whole states that were impacted. Mutual assistance agreements between states would then come into operation. Moreover, the DOE would activate ESF Function 12, which gives it the power to coordinate energy infrastructure. Hopefully, she stressed, all this work will be based on prior coordination between counties, states and utilities.

“If the other cooperatives don’t have what they need, then they’ll reach out to the rest of the sector and to other states to see who does. There are plans, and lists of who has what type of spare equipment, so that we can get access to it quickly.”
Parker spoke briefly about his work with FEMA Region IV on rewriting the response plan for a catastrophic earthquake in the New Madrid seismic zone.

His particular role was ensuring that the federal, state and local authorities are aware of the capabilities that the National Guard has and where its resources are located.

Some of the Georgia National guard's assets include engineering assets such as route clearance, bridging, and firefighting, logistics in the form of bulk fuel, “and of course, just moving food and water from point A to point B.”

Security assets include infantry units. The Guard also has the capacity to purify 14,000 gallons of water a day, and to evacuate 225 walking wounded and 75 non-ambulatory wounded per hour as well as search and extraction, medical, and fatality search and recovery teams.
Q and A Session

In response to a question about his point that soft ground amplifies earthquake shaking, Thomas Pratt clarified that for large buildings such as hospitals a site specific survey mandates what earthquake proofing is necessary.

Asked about the relative importance of water and waste water after an earthquake, Xavier Irias answered that they are both crucial, with water marginally more so. Danny Lacker added that in Jerusalem, “the major wastewater plant is generated by the gas that is produced in the wastewater purification process. So it has its own power source and it is not dependent on the electricity grid”

In answer to a question from Randy Garrett about how much water citizens are recommended to have for emergencies, Danny Lacker said “the recommendation for civilians is to have a few bottles of water - about two liters half a gallon per person per day at home for times of emergency. It is complicated for us as a utility to advertise this, because it suggests that we are not trustworthy in times of emergency. This store is for use until the Water Authority can start to distribute water.”

Xavier Irias answered that his utility recommends people to keep one gallon per person per day for a minimum of seven days. He added that realistically the requirement should be higher; after a major earthquake, it could take months to restore supply to some individual customers.

Bridgette Bourge was asked to review some of the main safety precautions people should take when using generators in their homes. She answered, “keep it maintained… make sure you have fuel on hand. Don’t run it in your bathroom. Remember, it has an exhaust.” She also recommended solar-powered generators since batteries eventually run out and no one knows for sure how long it will take until power is restored.
Jacob (Kobi) Wimisberg, Defense Attaché Coordination, NATO & Organizations Unit, Policy Bureau, Israel Ministry of Defense

International Cooperation

Kobi Wimsberg spoke about the critical importance of international cooperation, collaboration and coordination to tackling major threats on infrastructure. International cooperation, he showed, has been essential for security from the Delian League an association of Greek city states against piracy founded 2500 years to the allies of World War II up to the present. Today, Wimsberg argued, the evil that is Islamic State can only be defeated through international collaboration.

Some of the effective mechanisms of security cooperation include knowledge and intelligence sharing, joint R and D projects, emergency assistance and joint exercising, which can all contribute to the safety of nations.

The need for international cooperation against cyber and EMP

The concept of collective security responsibility is enshrined in NATO’s article V which declares that an attack on one is an attack on all of us. However, no equivalent international mechanism exists for cyber or EMP attacks. “Nobody has thought about moving towards creation of an international mechanism to strengthen our ability to cope with EMP.” In the interconnected world of cyber, Wimsberg argued creation of such a mechanism is especially urgent; “if we take cyber, there are no borders. There are no limitations. It’s a net around the world.” “Why is there no such mechanism?” Wimsberg asked. There are a range of reasons from a justified fear of information leaks that could endanger lives to a less noble opposition to sharing glory for achievements with other countries and agencies.

Wimsberg posited that, given our increasing urbanization, interconnectedness and dependence on technology, the next major
global disaster will be one that attacks critical infrastructures and resources. It will be very difficult, he warned, for any one country to handle the results of such a disaster on its own.

Greater international security cooperation will require, firstly the will to cooperate, and secondly the development of detailed plans. The will to work together depends on recognition that the Western world is under threat, identification of potential partners and understanding that only together can we meet the threats effectively.

Wimsberg credited EIS Council with creating much international will to cooperate on EMP saying, “I probably would not be here with my colleagues from NEMA and others if one night I had not find myself with the Minister of Homefront Defense Avi Dichter and four people entered including James Arbuthnot, Cong. Trent Franks and Avi Schnurr and they explained to us there is something called EMP, and we need to be part of this community that is dealing with it.”

Turning to the development of a plan, Wimsberg said, “We need to create an international plan. I’m not going into details, but the plan needs to identify what are the missing points in our preparedness, in our security, what can be done, what can be shared, what kind of exercises we need to do internationally, what level of intelligence we want.” He emphasized that such a plan must include the private sector: “we government agencies cannot afford to ignore them.”

Wimsberg concluded by “calling to the international community and decision makers to have a leaders’ summit or conference on these important issues. GMD and EMP are important enough to put on the table of the leaders of the free world. This is an important topic to deal with and we have to deal with it, and better now and not later.”
Conclusions: “Where are We?” Highlights and Summary from EISS VIII

Summing up the day, Avi Schnurr began by underscoring Kobi Wimsberg’s emphasis on cooperation. “Security forces and the Pentagon expect that infrastructure will be core to future conflicts,” he declared. “That being the case, since infrastructures today are all global, that means that global and international cooperation is absolutely essential. And we can only accomplish what we need to accomplish, as you pointed out Kobi, if we have adequate motivation.”

Reviewing some of the main points to emerge, Schnurr noted that although speakers had generally distinguished between natural and malicious hazards, there is a danger that they will be combined if, for example, “antagonists who are out there wait for opportunities to use natural disasters as an amplifying factor.”

On the theme of cooperation, he stressed that in addition to international cooperation, cross-sector cooperation is essential, since the real need will include both “the resilience that is required from within each sector on its own, and then what they’ll require from their partner sectors.”

On cyber, Schnurr amplified Erez Kreiner’s points that “cyber is now bringing back to the homeland in the United States for the first time in a very, very long time a direct threat taking place on U.S. soil. And the response for cyber is not something the government can solve. Primary responsibility for cyber can reside only with the utility managers and the corporate managers who control the vast majority of the resources in the United States.”
Turning to EMP, he noted that the morning’s speakers had presented new data, some of it quite alarming, particularly in regard to the vulnerability of high-power relays. He also referred to the evidence presented that EMP will affect satellites, adding another risk factor to many other concerns for whether satellite phone systems will be usable after an EMP attack.

Addressing terrestrial weather, Schnurr averred that many presentations showed the significant progress made in addressing terrestrial weather hazards on the scale that we have seen before. However, projections that terrestrial weather events are becoming worse raises the possibility that we could face Black Sky hazards for which we are not prepared.

Briefly summarizing the key messages on space weather, Schnurr noted, “there is a national action plan. That’s a good thing. It is not yet implemented, however, so there is a lot of work to do.” Moreover, he observed, while “there are standards, these standards do not seem to be based, on the 2012 CME, for which that we have all the data that experts agree should be the benchmark for the space weather threat.

Regarding earthquakes, he noted with concern the strong correlation between maps of high-density gas pipelines, electric transmission systems, and the New Madrid Seismic Zone. He also highlighted the Israeli efforts to devise systems to safeguard reservoirs and evacuate schools within the 30-60 seconds period that could be available for warning of an imminent earthquake, and suggested that these may well be global best practices for emulation.

Schnurr emphasized the observation that food distribution today is local and, consequently, local food distribution centers need to be on the map as priorities for protection and power restoration.

Concluding with some summary observations of the whole day, Schnurr said, “on sector resilience, there is a lot of work to do and it is absolutely key. A lot of work has begun and it is those of you in this room today who are the reason that work is beginning and going forward. Cross-sector cooperation has begun and it needs to grow. It needs to be enhanced. It needs to spread to other sectors and it needs to spread internationally.”