SUMMIT REPORT

IX/18


ELECTRIC INFRASTRUCTURE SECURITY SUMMIT

THE NINTH ANNUAL WORLD SUMMIT ON INFRASTRUCTURE SECURITY

EPRO Executive Steering Committee

Summer, 2018
Electric Infrastructure Security Summit IX/18
London, United Kingdom

Working Together to Secure Our World

Building multi-sector, international resilience to extreme hazards
Introduction

The resource networks that sustain our world have merged. Food, fuel, clean water, health care, a sustainable environment - our lives today depend on hyper-connected supply chains that span the globe. EISS IX explored best-in-class approaches, worldwide, to build coordinated resilience to extreme, “Black Sky” hazards that could fracture our interconnected world.

This Summit reflected substantial progress. In previous years much of the focus was on building awareness. Leading organizations in key sectors have now gone beyond that and have made solid progress in Black Sky planning and, in some of the most important sectors, increasing progress in implementation.

This represents an excellent beginning. Of course, given the sheer size and scope of the many interdependent sectors, most of the work remains to be done. Primary, high priority areas include expanding the sectors involved, improving advance Black Sky planning and investment across the full scope of each sector, and improved cross-sector coordination.

This was highlighted by many corporate and government executives. After noting the progress, they turned their attention to the highest priority gaps in planning and implementation that must be addressed. In this report, we attempt to summarize the primary gaps in planning and implementation for complex catastrophes that were identified as next steps by industry and government leaders.

Key Points

Scope of the Threat

A prolonged multi-region Black Sky power outage “represents an existential, civilization-scale issue, and is critical to life, safety and security,” as Scott Aaronson put it. General Mark Bowman added, “There is going to be a Black Sky event. We need to get past the question of “Will this happen?” Yes, it will.” Protecting against Black Sky threats is an imperative. As Sergo Braunstein of Israel Electric Corporation described the decision to implement EMP protection, “It is not a matter of choice. When there is a question of survival, it is simply essential to get to work, and build a capability to do what must be done.” Addressing the seriousness of the EMP threat, Randy Horton acknowledged that the E1 EMP pulse could damage relays and SCADA and the E3 could cause voltage collapse.

The threat posed today by cyber to electrical infrastructure is severe. U.S. intelligence reports that adversaries are actively probing the power grid for cyber vulnerabilities. “The cyber threat is existential today for corporations. Soon it will be existential for nations,” Yosi Shneck warned. A further source of cyber risk is rapid technology change providing new points of access for hackers. Carla Baker noted that there has been a roughly 600% increase in Internet of Things attacks, and 8000% increase in crypto attacks and a 300% increase in supply chain attacks in the past year.
Steps Being Taken

Implementation of EMP protection has begun. Speakers noted that whereas previously there was talk about doing this, now major utilities including Israel Electric and Dominion Energy are taking practical steps. Chris Beck presented the EIS Council - DTRA - SARA - Dominion partnership to test generation component vulnerability to EMP and make the information available to industry. Beck said, “this is the first time in history that comprehensive testing of the vulnerability, and potential for protection, of critical generation components has taken place.” Terry Boston added that we are seeing more rapid and concrete progress in preparation against threats to critical power infrastructure than ever before.

Gaps and Recommendations to Address Them

Cross-sector planning remains lacking. Electricity is a fundamental, critical need, but only one part of the full set of interdependent infrastructure networks. The Electric Subsector cannot solve this problem alone. It is a shared, social responsibility and requires a joint, integrated effort, including the public, private and NGO sectors. Robert Kolasky stressed that this cross-sector dimension is one way in which disasters affecting critical infrastructure are essentially different in their nature and scale from ordinary disasters. EIS Council’s Earth Ex annual event, the largest ever cross-sector Black Sky exercise aims to help fill the cross-sector planning gap.

One of the biggest cyber security vulnerabilities is the component supply chain. It is essential to incentivize buyers to purchase secure products. EIS Council’s new CPIC initiative aims to generate solutions to the acute problem of cyber supply chain security through international cooperation. The greatest cyber risk is people; several speakers stressed that training staff in good “cyber hygiene” practices reduces the risk of attack dramatically.

Utilities must partner closely and systematically with the public sector, if we are to reach a level that could allow us to survive a Black Sky event. Alan Brown of Tesco’s noted the immense capabilities that a firm like his can contribute to aid recovery.

The importance of emergency communications came up repeatedly. A Black Sky event is likely to bring down normal communications channels. Without a resilient, interoperable emergency communications system, recovery would be extremely challenging, if not impossible. Scott Aaronson noted that emergency exercises almost always assume – unrealistically - the existence of excellent communications. Avi Schnurr updated delegates on the progress of EIS Council’s BSX system that aims to fill this vital gap. Alongside emergency communications, a means of mapping infrastructure interdependencies and providing decision support is also needed. John Organek and Joey Schnurr presented and the GiNOM™ project that is planned to fulfill these functions.

Utilities plans for a “black start” of the grid after a massive outage needed to be reviewed and upgraded in the light of the closure in recent years of many coal plants that were the backbone of black start capacity. Scott Aaronson urged that electrical systems need to be designed with redundancy, minimizing single points of failure and hyper-critical assets. Andy
Andy Ott expressed serious concern about whether the utilities’ fuel security plans could adequately support the black start and restoration process. Avi Schnurr added that shortfalls of emergency generators and adequate fuel storage in many sectors “is not, primarily, because they’re so expensive -- they’re not. It’s because the need is not taken seriously enough.” Such generators’ availability in key sectors will be crucial to the civilian population’s ability to “shelter in place” in a Black Sky event. This depends critically on the continuation of water and wastewater services, and on at least limited availability of other essential services.
On Day One, speakers and delegates reviewed malicious Black Sky hazards and highlighted some of the most critical resilience gaps, along with best practice approaches to address them. Speakers reviewed both sector-specific and cross-sector gaps and resilience approaches.
Avi Schnurr briefly described how the “electrification of everything” and our unprecedented network of interconnected infrastructure systems have enabled our ever-improving living standards, yet also created acute vulnerabilities. In particular, our societies are exposed to the threat of “Black Sky events” – massive, long-term, wide area power outages that would cause cascading failures of dependent infrastructures.

This problem is created by interdependence and can only be solved by recognizing our interdependence. It will require exceptional levels of cross-sector collaboration to achieve resilience to Black Sky hazards. Schnurr stressed the responsibility that infrastructure managers and operators will need to feel for sectors that are dependent on them. “Can we get to the point where we feel a level of pain if we don’t provide what other sectors, other people, other human beings whom I’ve never met, need in order to be sustained, and to restore their systems?” Schnurr asked.
Session One

Challenges and Best Practices for Specific, Malicious Black Sky hazards
Session One
Challenges and Best Practices for Specific, Malicious Black Sky hazards

Session Chair: The Rt. Hon. Lord James Arbuthnot,
EIS Summit Co-chair, Member, House of Lords

Lord Arbuthnot succinctly defined the problem that the Summit would address: “The Western world has become totally dependent on one thing, electricity. Everything works through electricity: our money, communications, water, chain of command, food, just-in-time systems. If the world has a single point of failure, somebody is going to see if they can bring that down.”

Arbuthnot warned against thinking that the problem is too big to think about or too complex to solve. “There are answers to this problem,” he declared. “Amongst the participants here today, you will have almost all of the answers to this problem.” He also advised against the unrealistic belief that in a Black Sky event, “calling out the army” would be sufficient. The British army is not large enough to undertake this task and has its own vulnerabilities that will be disrupted like other organizations in a massive power outage. A third pitfall that Arbuthnot warned against was to believe that, “someone is thinking about this, somebody’s dealing with it.” “They’re not,” he stressed. “So we’ve got to do it for them. We’ve got to galvanize the people.”

Arbuthnot declared that the solution lies in harnessing the huge ingenuity of the Western World. The key action steps are “Discuss, Educate, Train, and Practice. In order to do that, we need to start with discussion. Get this issue out into the public debate.” He also recommended that all organizations must begin to audit their vulnerabilities.

“...The Western world has become totally dependent on one thing, electricity. Everything works through electricity: our money, communications, water, chain of command, food, just-in-time systems. If the world has a single point of failure, somebody is going to see if they can bring that down.”
Scott Aaronson stressed what the stakes are for the electric sector in building resilience to Black Sky events. “We care about this because it is crucial to the continuity of our civilization,” he declared, adding that the sector takes seriously the responsibility of being “critical to the life, health, and safety of our customers and critical to our national and economic security.” Aaronson added that this belief entails “putting your money where your mouth is,” and making the necessary investments to build resilience.

Aaronson compared the response and recovery to the three biggest storms that struck the United States during Summer 2018. Hurricanes Harvey and Irma were extremely powerful category 4 storms that hit Texas and Florida respectively. Harvey, which struck the fourth largest metropolitan area in the US caused 350,000 people to lose power. Irma, left 8 million in Florida without power. Within five days 95% had power restored. Aaronson praised these feats of resilience. By contrast, Hurricane Maria caused a 100% power outage in Puerto Rico. “We are still dealing with the impact nine months later,” said Aaronson. The relative lack of preparation in Puerto Rico was extremely costly. He concluded by emphasizing, that “we can’t do this alone; This is a shared, social responsibility.”
Mark Ghilarducci, Director,  
California Governor’s Office of Emergency Services

Mark Ghilarducci spoke about the critical importance of public-private partnership for building disaster resilience. He emphasized that, “this is a whole of community challenge. Public, private, non-governmental, philanthropic and faith-based organizations, have to come together in a coordinated manner.”

Ghilarducci described how the California state operations center has embedded within it an organization called the California Utility Emergency Association made up of all of the utilities, public, private, municipal, non-governmental. They are integral to the state's planning and response cells, helping set priorities, and training alongside state teams as first responders. Ghilarducci, added that California’s private sector emergency partners include UPS, Apple, FedEx, Marriot, companies that bring immense capabilities that government lacks.

Robert Kolasky, Acting Deputy Undersecretary for the National Protection and Programs Directorate (NPPD), U.S. Department of Homeland Security (DHS)

Robert Kolasky’s central point was that disasters affecting critical infrastructure are essentially different in their nature and scale from ordinary disasters. He enumerated what needs to change:

1. “We need to recognize that catastrophic planning isn’t just a version of traditional planning. It requires a different way of doing things.” Catastrophic event response will involve senior leadership and government more intensively. It poses a different decision process.

2. Private sector involvement in response operations is critical. It will also be crucial to aggregate data and information that may lie between the government and industry as a basis for making decisions. “We need to refresh our way of thinking, and of deciding what is critical, in particular through effective use of data to make a difference in these scenarios,” he said.

3. Raising the importance of the lifeline functions: transportation, water, communications, energy which includes electricity and fuel, and banking and finance as first-order priorities. Life sustainment and restoration depends on functioning infrastructures.
Kolasky listed four areas that DHS is working to strengthen in order to reach these goals.

1. Rethinking risk analysis. “We’re taking a functions-based approach to understand the critical functions that communities and national security depend on,” Kolasky said.

2. Utilizing a public-private-sector model that is now in place across 16 critical infrastructure sectors, including coordinating councils and cross-sector partnerships for risk management.

3. New data and modeling capabilities to aggregate real-time information for incident response

4. Dynamic prioritization process. Setting cross-sector priorities, matching information and analysis to identify unmet needs and enable a more flexible and nimble response.
Brief Interview
Breaking EMP News and Special Announcements
Session Interviewer: Rt. Hon. Lord James Arbuthnot

Sergo Braunstein, Vice President of Transmission, Israel Electric Corporation

Sergo Braunstein declared that Israel has begun to protect itself against EMP because it has no choice: “When it becomes a question of survival, it is simply essential to get to work, and build a capability to do what must be done,” Braunstein said. As an energy island, Israel cannot call on the support of its neighbors in a Black Sky event. It must therefore protect its grid to survive all eventualities.

Although Israel has been considering the EMP threat for almost ten years, in the last few years it has begun implementing real steps. In particular, its new Automatic Distribution Management Systems and Transmission Management Systems will have built-in EMP protection. Braunstein added Israel Electric Corporation is developing critical systems with EMP protection built in at the design stage.

“When it becomes a question of survival – as in the case of EMP protection – it is simply essential to get to work, and build a capability to do what must be done,”
Naomi Etzion, EMP Committee Chair, Israel Electric Corporation

Naomi Etzion from Israel Electric added, “we are defining risk and protection priorities, and looking at requirements to achieve restoration within 10 days of an event. We are testing to assess component and system vulnerability, such for EMP and protection requirements for Emergency Generators.” She elaborated on the ways in which IEC is also working to harden existing systems.

She emphasized the importance of identifying critical loads, having backup diesel generators to support them and hardening systems that support critical services including fuel, communications, water and waste water. Israel Electric is also working with all sectors of the Israeli economy to protect against the EMP threat. “The goal is to survive,” Etzion concluded, “with minimal disruption to the electric system.”

David Roop, Director, Electric Transportation Operations & Reliability, Power Delivery Group, Dominion Energy

David Roop reported on progress in his company, Dominion Energy, in protecting systems from EMP. His key points were:

- Dominion is using a layered protection approach for its substation facilities to reduce the E1 pulse impacts on digital equipment. Dominion has moved to a new control enclosure for its substations and has changed grounding and shielding techniques for substations.
- Dominion has tested older substation enclosures and will try a new steel shell design to overlay an existing structure to attenuate E1 pulse. This work will be completed in 2018.
- In August 2018, Dominion conducted field testing of substation equipment. This project undertaken with EPRI, (the Electric Power Research Institute) tested the effectiveness of MOV (Metal Oxide Varistor) arresters to clip the conducted E1 waveform. The testing aims to provide validation on best practices for attenuation that will be shared with the industry.
Dominion is working with the Defense Threat Reduction Agency (DTRA), Scientific Application & Research Associates, Inc. (SARA), and EIS Council to conduct testing of frequently used generation digital control systems to determine their capacity to withstand EMP.

Dr. Chris Beck, Vice President of Policy & Chief Strategist, EIS Council

Chris Beck from EIS Council reported on a research partnership that EIS Council is undertaking together with DTRA, the Defense Threat Reduction Agency. Beck noted that “DTRA, like other parts of the U.S. military, has understood the danger of electromagnetic pulse since 1962. But that information has been under wraps for security reasons until just a few years ago.”

Beck described how Michael Rooney from DTRA helped to release some EMP data that was included in a report that EIS Council worked on with a subcontractor of DTRA, Scientific Applications of Research Associates (SARA) called “Electromagnetic Black Sky Responses of Power and Control Equipment.” The report will shortly be available on the EIS Council website.

The report includes DTRA testing on relays and battery chargers for transmission substations. The tests found many relays to be vulnerable, but readily implementable protections exist. Beck added, “We want to also propose a way to fix it that’s cost-effective and that is going to enhance your systems’ survivability.” The next stage of the partnership will focus on the EMP resilience of the power generation sector. Beck concluded that the goal of the project is to get useful, actionable information on EMP resilience and protection into the hands of utility operators who can use it to protect their systems. He stressed that, “this represents the first time in history that any comprehensive testing of the vulnerability of critical generation components has taken place.”
Panel 1
The EMP Threat

Session Chair: Rt. Hon. Lord James Arbuthnot.

Dr. Zvi Rosenstock, Head of EMC Section, RAFAEL

Dr. Zvi Rosenstock compared the reliability requirements of civilian and military infrastructure systems, from his unique vantage point as a senior manager at Rafael, one of Israel's leading military technology companies, which also has a large civilian technology transfer program.

Dr. Rosenstock drew a distinction between military infrastructures, which need to work 24/7, and civilian infrastructures which may function at an adequate level even if there are temporary failures. Rosenstock coined the phrase “Acceptable Shutdown Time” (AST) to describe the maximum period for which we can tolerate a system not functioning. As an example, he posited that “if we lost power for four days, maybe more, it would be unpleasant, but society would still be functioning. For each system we need to define what that period is.” Answering this question requires analyzing the impact of each system's failure on the functioning of society.
Davidson Scott endorsed Rosenstock’s distinction between military systems where disruption must be eliminated and civilian systems where it must be minimized, citing U.S. Presidential Directive 21 as support. He argued that ultimately the issue is one of leadership. “Developing a sense of urgency to execute EMP protection is a challenge that we need to help organizations overcome.” Scott praised the work that Israel Electric has accomplished to begin protecting its grid from EMP, and also the research work that EIS Council is doing together with DTRA and EPRI. He stressed that much work remains on implementation.

Discussion

Avi Schnurr remarked how impressed he was by the leadership on EMP protection being demonstrated by Dominion, Defense Threat Research Agency, Israel Electric Corporation, EIS Council and EPRI. He asked how those initiatives can be expanded more broadly throughout the power industry. Dave Roop answered that the EPRI-DTRA research projects are likely to have a strong motivating effect. “Once you get science and fact behind the problem, it makes it a whole lot easier to look at cost-effective solutions,” he commented.

Lord Harris asked two questions: firstly, whether the same measures that protect against EMP are also effective against coronal mass ejections from the sun; secondly, what thought has been given to rolling out this protection for sectors other than electrical power.

Dave Roop answered that Dominion has shared a good deal of its EMP knowledge with its partners in the gas sector and also with the North American Transmission Forum. Chris Beck responded that while there is considerable overlap between the protection needed against CME and EMP, nuclear EMP generates very short-wave pulses that are harmful to micro-electronics, but which are not produced by a CME solar flare. Regarding other sectors, Beck agreed that “other critical infrastructures all use quite similar command-and-control supervisory control and data acquisition systems.” Consequently, measures that protect the electric sector are transferable.

“Developing a sense of urgency to execute EMP protection is a challenge that we need to help organizations overcome.”

“Major utilities have clearly taken note of the EMP threat and are starting to take action,”
Lord Arbuthnot concluded by noting that the Summit was turning out to be one of the most hopeful meetings on this subject that he had ever attended. He praised the important and dedicated work of infrastructure managers, saying, “major utilities have clearly taken note of the EMP threat and are starting to take action.”
Brief Interview

Cyber Update – The United Kingdom, Israel and the US Electric Sector

Session Interviewer: Rt. Hon. Lord James Arbuthnot

The Rt. Hon. Lord Desmond Browne, former UK Secretary of State for Defense

Lord Browne made some remarks on the current threat environment to critical infrastructure. He noted the prominence of the cyber threat and the successful cyberattack on the Ukrainian grid in 2015, probably by Russia. Browne referenced a recent U.S. intelligence report, which argued that the U.S. capacity to defend critical civilian infrastructure will lag behind the offensive abilities of states like Russia and China for the next decade. He added that he was not sure the U.K. was in a better position than the U.S. in this regard.
Rafael Franco described how Israel National Cyber Directorate is moving towards “a societal / functional model” in its cyber protection strategy. Information sharing is key and ensuring that such sharing takes place effectively is essential.

Franco declared that the biggest source of cyber risk is organizational culture. He stressed that such risk extends not just to users of technology products. Suppliers are also part of the problem. Therefore, “buyer incentivization” is key to supply chain security. “We need to encourage buyers to buy secure products,” he said. In Israel, the cyber regulatory authority helps vendors to do this, and also hosts joint exercises encompassing users and suppliers.

Rafael Franco, Deputy Director General for Cyber Robustness, Israel National Cyber Directorate

Jim Robb argued that Security, like reliability, is a community responsibility. That means that, although not all information is shared, cross-sector sharing is the key to buying down Black Sky risk.

Robb praised the work of the E-ISAC, the Electric Sector Information Sharing and Analysis Center, which has substantially expanded sharing of information within the power sector. He noted that one of the difficult issues is getting critical information out to industry in a timely fashion.

Jim Robb, CEO, North American Reliability Corporation (NERC)

“Buyer incentivization is key to supply chain security. We need to encourage buyers to buy secure products;
Carla Baker, Senior Manager, Government Affairs, Symantec

Carla Baker described some of the increased sources of cyber vulnerability. A new, rapidly growing area of vulnerability is the Internet of Things, (IOT) through which millions of devices and pieces of equipment are connected to the internet, making them susceptible to cyber-attack. Baker noted there has been a dramatic 600% increase in cyber-attacks on the Internet of Things in the past year. She also noted a sharp increase in attacks on cyber supply chains, which have increased three-fold in recent years. Poor supply chain security is the largest single cyber vulnerability, with potential adversaries like Russia and China covertly controlling companies that supply cyber components worldwide.

Based on a recent infrastructure survey, there is a major hostile effort going on to exploit infrastructure cyber access for disruption. Baker remarked on the increased sophistication of nation-state sponsored cyber-attacks. Not only are their capabilities growing, but they are also better at leaving no fingerprints of their involvement, making attribution harder.
Lt. General (Ret.) Mark Bowman, former Director, Command, Control, Communications and Computers (C4)/Cyber, Chief information Officer, joint Staff, J6/CIO, the Pentagon

General Bowman addressed the probability of Black Sky and declared unequivocally, “there is going to be a Black Sky event. We need to get past the question of “Will this happen?” Yes, it will.”

He reiterated concern about over-reliance on the internet of things and said that our desire for convenience often translates into vulnerability. He asserted, “we need to bake in cyber security at all levels of system design” and acknowledged that no matter how effective a particular system or patch is, a counter to that level of security is only one smart idea from the adversary away. Bowman spoke of his concern that there are fundamental gaps in our knowledge of how our infrastructure “system of systems” works. “You cannot protect what you do not understand,” he stressed. Interoperable, interconnected systems create vulnerabilities as unintended consequences.

Bowman argued that cyber weapons are displacing Weapons of Mass Destruction and conventional arms as the lowest cost, highest impact systems, both for terrorists and for nation states. He gave two recent disruptive examples: a) the successful attack through an HVAC system on a major retailer’s financial systems; and b) successful attacks against the Democrat National Committee during the 2016 elections. Bowman urged that industry, government and citizens work together and argued we must focus on people as they prove consistently to be the weakest link in cyber security.

“There are fundamental gaps in our knowledge of how our infrastructure system of systems works. You cannot protect what you do not understand.”
Yosi Shneck described a worsening geostrategic environment for utilities. Cyber is one of the most serious threats, ranking high both on the scales of likelihood and consequence. “The cyber threat is existential today for corporations. Soon it will be existential for nations,” he warned. Moreover, technology change presents ever greater protection challenges. “We are living in the Smart Grid age. That means distributed production and autonomous, fully unattended supply chain operation is coming fast. It will, therefore, be critical to address these new realities, Shneck said.

He described the widening range of channels through which adversaries can attack. In addition to targeting IT and OT systems, there are a host of vulnerable indirect channels. For example, most appliances now have remote controls, and these are entirely unsecured. If one could take over 20% of the air conditioner remote control devices in Israel, one would be able to cause a sudden 10% fluctuation in total electricity demand, enough to crash the whole grid.

Turning to solutions, Shneck recommended:

- The current rigid technological standards perception should be more flexible and dynamic.
- Electrical infrastructure cyber resilience design should be integrated to the borders of interconnection.
- Cyber by Design methodology (where cyber defense is integrated at the earliest system design stage) should be implemented among all the players of the electrical supply chain.

“The cyber threat is existential today for corporations. Soon it will be existential for nations.”
Brief Interview

Terrorism and the Evolving Asymmetric Physical Threat

Dr. Uri Ben Yaakov, Senior Researcher and Project Manager at the International Institute for Counter-Terrorism (ICT), Herzliya, Israel.

Uri Ben Yaakov described evidence that terrorists are planning to attack critical infrastructure. We know this from Jihadist literature, actual attacks that have taken place in the Middle East, Syria, Africa, and Hezbollah’s attempts to attack critical infrastructure in Israel. Terrorism studies defines threat level as motivation to attack multiplied by the ability to do so. Without effective ways to lower terrorists’ motivation, law enforcement authorities need to lower their ability to attack.

Currently, terrorists can readily buy cyber-attack tools from criminals or nation states. Law enforcement agencies must cooperate with private companies to restrict the gaps an adversary can identify and exploit. We need more effective monitoring by internet providers to provide early identification of risks and support efforts to counter cyber threats.

Finally, Ben Yaakov spoke of the need to examine regulatory underpinnings so as to identify and close vulnerabilities.
Panel 3

Terrorism and the Asymmetric Physical Threat – Geostrategic scenarios and resilience strategies

Major General Richard Hayes, Adjutant General, Illinois National Guard

General Hayes spoke about the Laws of War and argued that they need to be updated and rewritten for the cyber age. Issues such as what constitutes a casus belli, what is proportionate response, and whether a preemptive strike against an adversary planning an attack is justified, have not been properly defined or thought through in the cyber context.

General Hayes also discussed the nationwide GRID EX emergency exercise, which Illinois used as an opportunity to develop a full-scale planning and exercise event and review its emergency playbooks.
Bill Bryan discussed risks associated with emerging new technologies including block chain, machine learning and 3-D printers, that regulators and law enforcement agencies have yet to adequately address. Machine learning can now accurately identify faces, while 3D printing is advancing rapidly to the point where for example, criminals will soon be able to use them to create drugs. New technology development is driving IT and OT product evolution faster than cyber security assurance can keep up. Bryan argued that current laws limit DHS ability to combat these threats.

Paul Stockton commented from the floor that that “if we have plans to sustain lives on a large scale and defeat the adversary we will reduce the likelihood that the adversary will attack. Adversaries act to achieve political and military effects. In the event of an attack there will be information warfare where the adversary will use social and mass media to incite panic.”
Session Two

HAZARD-INDEPENDENT STRATEGIES for BLACK SKY vs CONVENTIONAL THREATS: UNIQUE CHALLENGES, AND COMMUNICATION AND COORDINATION CAPABILITIES NEEDED TO ADDRESS THEM
Coordination and Communication Challenges and Opportunities
Coordination Planning and Real Time Implementation Frameworks:
the EPRO Handbook III Template

Dr. Paul Stockton, Managing Director, SONECON, Former U.S. Assistant
Secretary of Defense.

Paul Stockton introduced the recent published EPRO Handbook III. He described the book’s two central propositions:

1. Infrastructure owners and operators, government agencies, and non-governmental organizations will require collaborative decision-making mechanisms in a Black Sky event.

2. Survivable communication and coordination systems are of core importance for infrastructure sustainment and restoration.

The book describes the multi-sector planning that will be necessary, analyses how such collaboration can be structured in a way that is consistent with the U.S. Constitution and discusses Black Sky prioritization. It also details the operational specifications and social architecture of a survivable communications system, as well as the characteristics of BSX, the leading such candidate system. Stockton concluded with his gratitude to all those managers and practitioners in the field whose suggestions and contributions to the Handbook were invaluable.
The Private Sector: The Role for Emergency Communications and Coordination Capabilities in a Black Sky event

Alan Brown, Group Security Director, Tesco

Alan Brown spoke of the role of the private sector and the critical importance of close coordination between the public, private and NGO sectors. He emphasized that the private sector has immense capabilities that are currently not harnessed by the public sector for emergency relief. “Just my company, Tesco has greater emergency capabilities than the whole public sector,” he argued.

Achieving this kind of cooperation will require overcoming traditional suspicions between public and private sector and the public sector overcoming its siloed organizational structure. “We need a synergy of effort between the public and private sectors,” Brown said. “And we need to find a mechanism to get public and private sector structured to coordinate.”

Communication in a Black Sky event will be a special challenge if the mobile phone network is down, Brown warned. “We haven’t thought about that. We need to do it now.” Concluding, Brown expressed his appreciation for EIS Council “as thought leaders in this area.”
Avi Schnurr, CEO and President, EIS Council

Avi Schnurr pointed out that in a Black Sky emergency, all communication will fail after a few days. While many people realize that emergency communications will be needed across emergency services, Schnurr argued that “that’s only the beginning. All the other sectors need to be in communication. Emergency communication will be need to be able to talk to all critical sectors.”

A Black Sky emergency communications system will need to be interoperable with all other communications devices. It should have the ability to connect to the internet. A further core requirement is that nodes are deployed at all critical facilities. In addition, it must have backup power, power duty cycle management to prioritize who will be on the line, pre-planned situational awareness function, and decision support for restoration priorities. The BSX system under development is designed to meet all these specifications.

While many people realize that emergency communications will be needed across emergency services, that’s only the beginning. All the other sectors need to be in communication. Emergency communication will need to talk to all critical sectors.
Dr. Fiona Twycross, Deputy Mayor of London

Dr. Twycross spoke about the London Resilience Partnership. It comprises 170 agencies and organizations spanning multiple sectors that are working together on pre-disaster planning and resilience. The overall goal is to help Londoners prepare for an emergency.

She warned that there would be limited water, health care, communication and food in a major disaster. Dr. Twycross stressed that neighbourhood practices develop neighbourhood and community response, a powerful force for resilience. She pointed out that some people respond better to faith or education-based institutions rather than geographic communities.
Multi-Sector Situational Awareness and Decision Support for Complex Catastrophes: The GINOM™ Strategy

**John Organek**, Administrative Director, Infrastructure Simulation, EIS Council

John Organek introduced EIS Council’s GINOM™ initiative, a project to capture and model our complex societal system of systems in a broad computational simulation. The aim is to provide decision makers with the mission-focused situational awareness and decision-making capability necessary to understand, prioritize and assure the vital support needs of lifeline infrastructures.

---

**Joey Schnurr**, Technical Director, Infrastructure Simulation, EIS Council

Joey Schnurr described the need for the GINOM™ tool, arising from the threat that hyper-connectivity across all sectors could lead to societal collapse in a long blackout resulting from a Black Sky outage.

He explained GINOM’s™ potential role in “enabling and guiding national and global scale restoration and population sustainment plans and real-time actions in complex catastrophe.” GINOM™ is assembling a world class team to build unprecedented, evolving global infrastructure simulation.
The goals for such simulations are:

- Restoration plan assessment
- Decision support for coordinated restoration and population sustainment
- Creating a large-scale exercise platform

Schnurr described two facets of GINOM’s™ infrastructure simulation scope:

"As is modeling," to map the current configurations of infrastructures: This will be a geospatial repository for Emergency Management / Infrastructure data, tracing multi-sector supply chain connections. It will be updated continuously with real time operations information. The “as is” model will be hosted on the ArcGIS® platform by ESRI, a leading computer mapping company.

**Forecasting Service:** This will run time forward from the As-Is Model state, calculate dynamic supply chain interactions for testing and refinement of restoration plans and set the stage for real-time decision support guidance. The forecasting service will be hosted at SpatialOS®, a prominent cloud-based platform for games. The plan is for the As-is and Forecasting capabilities to be merged later.

Schnurr also gave a live demonstration of GINOM™. He stressed that, “like the systems that it models, GINOM™ will continually evolve, growing to map an ever-greater number of infrastructure sectors and subnetworks that together define the complex organism of our society." He ended with the hope that GINOM™ will become an essential tool for both resilience and disaster recovery.
Matt Hogan presented a graphic representation of how a massive power outage could impact London’s critical infrastructure sectors. The water sector would suffer from pumping failures that could cut off supply. Telecoms would likely experience the failure of internet and VOIP systems, as well as of mobile base stations. The transport sector would be hit by loss of passenger information systems, trains stopping, trapped passengers, airport diversions and major disruption to national transport. Health systems would become dependent on emergency generators with their finite fuel supplies and would probably have to stop treating non-emergency and critical patients. In addition, many businesses and financial institutions would shut down, ATMs would stop working, schools would close and patients in nursing and residential care centers would be at serious risk.
Among the key points of the day to emerge from the Concluding Remarks were:

- We need to start creating task prioritized decisions tackling the difficult questions of who gets which resources, when and how in a crisis, and how will such decisions be taken.
- The vital importance of Communications – to any action.
- There was discussion about the status of fielding 5G networks for emergencies.
- Despite progress, much work must still be done in communicating Black Sky risks to policy makers.
- Scott Aaronson noted that the threats represent a true existential threat to our societies.
DAY TWO

Tuesday June 26, 2018

On Day Two, leaders from the utility, private sector, NGO and government sector groups highlighted some of the key missions, internal measures and external requirements needed by each sector to achieve Black Sky resilience.
Introduction: The EPRO SECTOR Executive Committee, Summer 2018

**Terry Boston**, EPRO SECTOR Executive Committee Chairman; Board Vice Chair, Grid Protection Alliance; Energy Security Advisor to the President of the United States; Board Member and CEO Emeritus, PJM Interconnection

Introducing Day Two, Terry Boston said that we are seeing more rapid and concrete progress in preparation against threats to critical power infrastructure than ever before. Among the tangible results that he cited is that the DTRA (Defense Threats Reduction Agency) is now sharing technical information about the effects of EMP that is specific enough for the utilities to protect their relays.
Session Three

BLACK SKY RESILIENCE IN THE UTILITY SECTORS
Session Three

Black sky resilience in the utility sectors

Session Chairman: Anthony Pugliese,
Chief of Staff, Federal Energy Regulatory Commission (FERC)

Introducing Session Three, Anthony Pugliese stressed the need for all sectors to work collaboratively and to be “nimble and focused” to meet the growing threats to infrastructure. Nation states have demonstrated their ability to conduct cyber-attacks on electric companies. Enemies of the U.S. are developing the ability to launch an EMP attack that could imperil the very survival of the U.S. while physical attacks such as the 2013 acts of sabotage on pipelines cause increasing concern.
Enabling Investment for the Sector’s Black Sky Mission: Progress and Gaps

Andrew Ott, CEO and President, PJM Interconnection

Andy Ott noted three key dimensions of resilience for his utility: the power grid itself, its gas network and telecoms systems. Ott declared that PJM challenges itself with the question, “how can we get better at all three?” Regarding the grid itself, PJM has certain especially critical substations; Ott asked, “can we make substations less critical, for example by building in alternative pathways and redundancies?”

Severe weather combined with an attack on the grid would also expose particular vulnerabilities. In the area of fuel security, PJM is studying vulnerabilities associated with transportation. For example, emergency generators are a potential single point of failure, since they need reliable fuel – something which, given good planning, should not be hard to secure.

Finally, he raised the question of how cost-recovery should be arranged for the essential resilience investments that PJM needs to make.
Richard Fox, Executive Vice President. and Chief Operating Officer, Aqua America

Richard Fox set out challenges of ensuring resilience in the water sector. Fox noted that the average American uses 100 gallons of water per day. In a crisis however, consumers would need to reduce their water use to 10 gallons per day devoted to cooking, drinking and sanitation.

A major challenge to water sector resilience is the aging state of its infrastructure. Many water mains and pipes were laid in the early to mid-20th century with a lifespan of 75-100 years. 240,000 water main breaks occur each year in the US and an estimated $1 trillion investment in water infrastructure is needed over the next 20 years. Moreover, the industry is highly fragmented, making implementation of resilience measures very difficult. There are over 52,000 community water systems in the U.S. and fewer than 1% of these serve more than 100,000 people.

Aqua America’s approach to resilience is based on customer communications and preparedness. Emergency Operations Center (EOC) coordination, advance contracts for critical supplies, communication with regulatory agencies, intra-state cooperation, stakeholder relationship-building, employee training, and exercise participation.

In subsequent discussions, Chris Beck of EIS Council noted that the inefficiency of the water system is also a lack of resilience, because leaky pipes are more fragile. He urged those present to use their clout and influence to help get water pipes repaired and upgraded.

Joseph McClelland, Director, Office of Energy Infrastructure Security, Federal Energy Regulatory Commission (FERC)

Joe McClelland focused on the challenge of how to protect power infrastructure that is privately owned, but which also serves critical defense installations. If we can effectively protect critical military facilities, this could serve as a deterrent to nation states from attacking the U.S. McClelland stressed that regulation alone cannot solve this problem. One may assume, he warned, that adversaries read new regulations before they are even issued. McClelland too raised the question of cost recovery for resilience investments that protect defense infrastructure.

He concluded that FERC can help in four main ways:

1. By informing industry of threats, giving classified briefings and issuing special clearances.
2. Promoting and sharing best practices resilience measures.
3. Undertaking assessments of utilities’ preparedness.
4. Providing cost recovery for resilience investments.
Track 1
Cyber and Physical Security: Protecting the Grid and Other Critical Infrastructures

Moderator: Steven McElwee, Information Security & IT Compliance, PJM Interconnection

Steven McElwee opened by noting that hostile states have moved from committing acts of sabotage to more active attacks to the grid. He said that we must evaluate the cost of innovation to protect against these attacks and asked where the government stands in coordinating these efforts.

Tim Roxey, Vice President, Chief E-ISAC Operations Officer, Interim Chief Security Officer NERC

Tim Roxey gave an overview of recent cyber-attacks affecting the U.S. grid. He said that nation states can currently carry out banking-200 billion bytes per second attacks and that a 1 trillion byte per second attack would be very challenging to defend against. We need to know our adversaries and their capabilities to know how to counter them, Roxey said.
Yosi Shneck, Senior Vice President, IT & Communications, Chief Cyber Officer, Israel Electric Corporation

Yosi Shneck described the Israeli experience in responding to cyber-attacks. The Israeli cyber department was formed as early as 1992. He said that while we keep on talking about strategic risk and “critical” infrastructure, we need to determine what our adversaries think is critical. Shneck argued that the public and private sectors still need an operational basis for joint actions to reduce risk. He also highlighted the vulnerabilities in new SCADA systems that use open source architecture, which make it vital to establishing a supply chain procurement list.

Bob Kolasky, Acting Deputy Undersecretary, for the National Protection and Programs Directorate (NPPD) U.S. Department of Homeland Security (DHS)

Bob Kolasky discussed the role of the federal government in partnership with the private sector. He said that DHS has made risk-based decisions for the U.S. government but does not make such assessments for the public/private partnerships. It will, however, help the private sector develop decisions for itself. He noted that several federal agencies have responsibility for information warfare.*
Stephen Bates, Business Development Executive, Forcepoint

Stephen Bates discussed private sector response to cyber protection. He urged the audience to consider the entire value chain of electricity, from: Power Generation, Transmission and Distribution, Transmission and Metering and the regulatory bodies, commercial entities, and consumers.

He noted that according to the EIA, in 2017, the US generated 4T kWh of electricity from utility-scale facilities, of which 17% was from renewables. This is a big change in the generating mix. Policy makers’ goal is a diversified, reliable, secure energy/electricity supply at low cost with high security — storage and transmission. The resilience implications of this shift need further study.

Bates added that we need more sensors built into the transmission system. He also stressed that people are the weakest link, a problem accentuated by the ease of use of new mobile devices and wearables.

Discussion

Key points emerging from the discussion were that more training is needed in how to recognize attacks and how to counter; protecting the procurement supply chain is critical; the respective roles of government and private sector in cyber protection need clear definition. Responding to Steve Bates’ remarks on the vulnerability of new consumer technologies, Chris Beck noted the potential cyber weaknesses of electric cars and discussed how a vehicle was recently hacked by the Idaho National Laboratories.
Track 2
Balancing Utilities’ Operations Efficiency and Resilience Posture

Moderator: Terry Boston, Chair, EPRO SECTOR Executive Committee; CEO Emeritus, PJM Interconnection

Rear Admiral (Res) Yoram Laks, Security Director, Energean

Admiral Laks analysed key challenges to the surety and resilience of utilities, drawing on his experience as Israel’s Head of Naval Intelligence and as Security Director for Energean, a leading oil and natural gas developer.

Bill Chiu, Director, Grid Resiliency & Public Safety, Southern California Edison

Bill Chiu discussed how Southern California Edison (SCE) made the decision to better organize itself to deal with resilience issues on a company wide basis. Most of their immediate focus was on dealing with the wildfire situation in California, but they also regularly face extreme heat, droughts, mudslides, and earthquakes regularly. The company’s current posture is that resilience considerations are prioritized and built in to planning, design, and operations, rather than only reacting to emergencies after-the-fact.
Track 3
Public and Private Sector Collaboration: Building Partnerships for Resilience

Moderator: Shandi Treloar, Private Sector Committee Chair, National Emergency Managers Association (NEMA), and Private Sector Coordinator, EIS Council

Shandi Treloar, Private Sector Committee Chair, National Emergency Managers Association (NEMA), and Private Sector Coordinator, EIS Council

Introducing the discussion, Shandi Treloar noted the near universal recognition of “how critical it is for the private sector to be included in planning, in responding, and restoring after major disasters.” She also pointed out the important distinction between utility private sector companies and non-utility private sector companies. The latter group are also critical for their role in the supply chain.

Simon Lewis, Head of Emergency Planning & Respond, British Red Cross

Simon Lewis emphasized the critical importance for all emergency planners of building cross-sector relationships before a disaster strikes. “The more peace-time relationship building one can do, the better prepared everyone will be in the response,” he argued.

He strongly supported involving the private sector in emergency response. As a senior manager in the British Red Cross, he described the immense value to the organization of private sector sponsors like Tesco’s “time, talent and treasure.” Lewis recounted one of the lessons from the 2017
Grenfell Tower fire in London was the importance of community groups as first responders. Perhaps the Red Cross was “a bit too much perhaps focused on the auxiliary-to-government role and less on the auxiliary to the community function,” he said. Shandi Treloar said that FEMA in the U.S. has a community directed initiative called “You are Help Until Help Arrives”.

Thomas F. Minton, Manager, Corporate and Information Security Service, Exelon

The key government-industry interdependency, as Thomas Minton put it, is that “the government owns the intelligence that the private sector needs to protect critical infrastructure, while private industry owns and operates the infrastructure that needs to be protected.”

Minton cited the development of state-run, federally funded “fusion centers,” which combine intelligence from multiple sources from government and industry sources as a big step. They make intelligence available to industry in real time. The Electric Subsector Coordinating Council ESCC – formed 6 years ago – included White House officials and utility CEOs to enhance cooperation.

Minton cited large research projects on the EMP threat as an area where future cooperation is crucial. No private sector company has the resources to devote to this. Finally, he highlighted resilient Black Sky communications as a critical challenge where the government can play an important supporting role.

Mark Ghilarducci, Director, California Governor's Office of Emergency Service

Mark Ghilarducci described California's development of a unique model for their State Emergency Operations Center. This focus for public-private cooperation is crucial for both stabilization and restoration after a disaster. Fiber optics, cell-phone communication and water delivery are vital for recovery; in these areas, the private sector plays a major role in restoration. Ghilarducci concluded, “because of this integrated effort, amazing amounts of resources, logistic support, transportation, technology, personnel, funding from multiple kinds of organizations can be mobilized.”

“The government owns the intelligence that private sector needs to protect critical infrastructure, while private industry owns and operates the infrastructure that needs to be protected.”
Discussion

Shandi Treloar pointed out a striking example of supply chain dependency from the Puerto Rico Hurricane disaster of 2017: “a lot of people didn’t realize before that saline solution bags are produced in Puerto Rico. It’s the only place these bags which are ubiquitous in hospital treatment are produced.” Mark Ghilarducci noted the key importance of holding drills in schools. These exercises educate not just children but also families about emergency procedures.
The ERPO Sector, Overview and Black Sky Playbooks: Multi Sector Planning:

Brig. Gen (Ret.) John W. Heltzel, Director of Resilience Planning, EIS Council

John Heltzel defined the ERPO initiative as a response to “a world with ever-increasing interconnectedness and dependence on critical life-line infrastructures.” Given the growing risk and potentially devastating impact of a variety of threats, “inclusive partnerships will be required in order to prepare and to become more resilient.”

Heltzel also gave a short progress report on EIS Council’s resilience metrics project, which aims to develop usable, meaningful metrics to track our progress in resilience investments, sector by sector. The key components of the resilience metrics are a threats analysis, an impact analysis for critical sectors, and assessment of resilience goals and objectives and of cross-sector dependencies and coordination.
Ranger Dorn, Exercises Coordinator, EIS Council

EARTH EX: Black Sky Sector-Specific and Multi-Sector Exercises, and Coming Soon – EARTH EX Black Sky Planning Workshops

**Ranger Dorn** presented EIS Council’s extensive exercise program. EIS Council has developed. Delivered and customized Black Sky exercises for numerous groups of senior decision makers and managers across the United States over the past year, including multiple FEMA Regions. Turning to EARTH EX, EIS Council’s flagship cross-sector Black Sky exercise, Dorn reported that the inaugural 2017 EARTH EX attracted thousands of participants from 500 organizations in 14 countries. Dorn defined the three key concepts underlying EARTH EX as:

- We need better plans, planning tools and planning processes
- We need a comprehensive set of processes and procedures to acquire the situational awareness needed for cross-sector coordination to ensure the restoration
- We need investment in resilience, planning, training, exercising and hardening of systems.

Among the compelling features of EARTH EX are that it is a come-as-you-are exercise for executive and operational managers to test and refine policies and procedures for responding to a long duration power outage. No ramp up or pre-exercise work is required; EARTH EX is self-facilitated, self-assessed and self-evaluated, with participation lanes for 33 sectors and sub-sectors.
Session Four

BLACK SKY RESILIENCE IN THE GOVERNMENT, NGO AND PRIVATE SECTORS
AFTERNOON PLENARY SESSION
Black Sky Missions and Requirements: Gaps and Approaches

Shandi Treloar, Private Sector Committee Chair, National Emergency Managers Association (NEMA) and Private Sector Coordinator, EIS Council.

Shandi Treloar argued that the private sector, including utilities, and other private sector companies, is critical to the response and restoration of any infrastructure and of the community overall. Private sector and non-profit organizations bring significant logistical, technological and financial resources, that are not available in the public sector. Public-Private Partnerships need to be formalized and baseline standards to be developed. Treloar noted that emergency services in many public sector jurisdictions do not currently partner with the private sector.

Randy Garrett, Director, Disaster Relief, Arkansas Baptist Convention

Randy Garrett pointed out that for the NGO sector to fulfill its role in a Black Sky disaster emergency generation, it will need to meet its own needs for diesel distribution, redistribution, consumables and emergency communication.
Dr. Shlomo Wald, Consultant to Joint Research Council (JRC,) European Union

Shlomo Wald outlined some of the measures that Israel has taken to protect its grid from EMP, in partnership with EIS Council. Wald stressed that despite Israel being probably the first country to begin taking action at a national government level to protect its grid, a great deal of work remains to be done.

Andrzej Kawalec, CTO, Head of Strategy and Innovation, Vodafone Enterprise Security Services

Andrzej Kawalec declared that human beings are inherently poor at projecting risk. In business and in life, people’s decisions about what risks to protect against and how much to invest in protection often bear little relationship to the real risks and costs involved. Consequently, we need to find effective tools to help people recognize and assess risk, even if they’re not natively and naturally good at it.

He also noted that it is important for businesses to begin viewing and pursuing resilience as a business opportunity, not a cost.
Steve Broughall raised the question of whether it is the government or NGO’s primary job to educate the public. In Broughall’s view, NGOs carry out the role much better than governments. Randy Garrett replied that governments play a vital role too; FEMA public information presentations in advance of the hurricane season have been effective. He noted the messaging challenge of developing education and training materials that can catch the attention of the young, who want to receive all information on their smartphones and the older generation that still reads print media.

A number of speakers noted how extremely rare it is for organizations in the public sector to prepare or exercise for an outage on the scale of a Black Sky event. Broughall highlighted the 2018 Earth Ex exercise as an opportunity to do just that.
John Vonglis, Chief Financial Officer, U.S. Department of Energy

John Vonglis responded, “there’s also an obligation that any company has, if it’s a public company, to their shareholders and to the community, to protect against the reputational risks and financial risks associated with prolonged outages.” To be sure, he added, the government also has a role. The right balance needs to be struck between private and public sector involvement but it is no longer an option for private industry to avoid responsibility.

Joseph McClelland, Director, Office of Energy Infrastructure Security, FERC

Joe McClelland stressed that the cyber security problem can be solved. McClelland said that applied to cyber, the oft-repeated maxim that 20% of effort yields 80% of benefits, should be adapted to “5% effort yield 90-95% benefits.” This is because, “the end objective isn’t to be perfect, but rather is to introduce enough uncertainty to the attacker that they go somewhere else.” A nation-state will probably not launch an attack unless it believes there is at least a 90% chance of success.

Turning to regulation, McClelland said “you can’t regulate your way out of this but, that’s not to say regulations aren’t important.” Regulation provides a baseline and an initial reason to take action, but utilities need to go further than government can meaningfully regulate; companies need imagination to conceive of the full range of threats they face and to mitigate them. Finally, he highlighted the importance of protecting against future threats, and tagged machine-driven attacks powered by Artificial Intelligence as an imminent concern.

“...The end objective of cyber protection isn’t to be perfect, but rather to introduce enough uncertainty to the attacker that they go somewhere else.
Randy Garrett, Director, Disaster Relief, Arkansas Baptist State Convention

Randy Garrett emphasized the exceptional value to the NGO sector of its strong relationships with corporations. Arkansas Baptist State Convention has a partnership with Tyson Foods, the leading meat producers in the U.S. where the company will truck any of the NGO’s equipment needed, free of charge. Similarly, a relationship with Walmart allows ABSC to pick up any necessary equipment in a disaster from a Walmart branch with only a single phone call by the store manager.

Discussion

Steve Broughall raised the question of whether it is the government or NGO’s primary job to educate the public. In Broughall’s view, NGOs carry out the role much better than governments. Randy Garrett replied that governments play a vital role too; FEMA public information presentations in advance of the hurricane season have been effective. He noted the messaging challenge of developing education and training materials that can catch the attention of the young, who want to receive all information on their smartphones and the older generation that still reads print media. A number of speakers noted how extremely rare it is for organizations in the public sector to prepare or exercise for an outage on the scale of a Black Sky event. Broughall highlighted the 2018 Earth Ex exercise as an opportunity to do just that.
Scott Aaronson asserted that the key to resilience is partnership. He recalled that the very first recommendation of the president’s National Infrastructure Advisory Council in 2010 was that “there needs to be better dialogue between senior executives and senior government officials.” He noted the important role of ESCC in fostering the dialogue since then, and the value of utility CEOs on that body. He described such organizations as “trust communities” that facilitate information sharing.

He underscored the importance of cross-sector work, noting that each infrastructure needs different policies. The water sector, for example comprises by some measures 160,000 separate entities, whereas the power sector is made up of a few dozen utilities. Aaronson reported on a new initiative underway to establish a cross-sector Strategic Infrastructure Coordinating Council based on sectors that are the foundational to our society including electricity, telecommunications, and finance.

Aaronson concluded that “the best way to protect critical infrastructure is to not have it.” Systems need to be designed with redundancy, minimizing single points of failure and hyper-critical assets.
Richard Fox, Executive Vice President and Chief Operating Officer, Aqua America

Richard Fox acknowledged “there’s not a lot of cooperation between my water company and the electric companies.” He described how Hurricane Harvey caused severe impacts on water systems in the Houston area which compelled Aqua American to deepen its working relationships with the other utilities. Fox expressed the paramount importance of continuing this work. Scott Aaronson commented that in the 2017 hurricane season there was a lot of ad hoc coordination between sectors that was made possible by relationships built through the different coordinating councils.

Fox added that one of the most important questions he would need answered in a long-term outage would be “how long is the power going to be out? If I have three or four days’ worth of fuel and power will be out for two weeks, I’m going to treat that fuel differently than if it’s just six hours and it’s a normal outage.”

Sergo Braunstein, Vice President of Transmission & Substations, Israel Electric Corporation

Sergo Braunstein described how, in a country as small as Israel, planning, functioning and operations for the electricity and water industries are closely interconnected. A further reason for the close cooperation between the sectors is the heavy reliance of the water sector on desalination and other electricity-intensive technologies. Israel’s total national consumption is 2.1 billion cubic meters a year of which 600 million cubic meters is desalinated water.

Israel's security situation requires that the emergency plans for critical sectors are coordinated. “When it comes to emergencies, we exercise and tackle real problems together on a daily basis.” Braunstein explained that for a range of historical and practical reasons, the Israel Electric Company has been the sector that set down operational and emergency rules, and the other sectors followed. Braunstein said that Israel Electric’s critical customers are very well defined. Their system could suffer 25% load shedding and the most critical customers would not suffer. Israel Electric reviews its list of critical customers four times per year.
Discussion

John Organek commented that since Israel is a world-leader in technologies like desalination, ozonation, and membrane filters their water sector is especially dependent on electricity. In certain parts of the United States, such as Phoenix, Arizona and California, Organek said, “there is an Israel-like situation, where the water people have to talk intensively with the electric sector. Avi Schnurr said that “given that in the United States we’ve got 155,000 water companies, we need to find mechanisms to spread the coordination process between the electric and water sectors very, very fast.” Richard Fox responded that the crucial channel is to work with the American Water Works Association, of which virtually all water utilities, large and small are members. Scott Aaronson praised the GINOM™ project as having the potential to make an immense contribution to understanding, mapping and managing inter-sector dependencies.

“Given that in the United States we’ve got 155,000 water companies, we need to find mechanisms to spread the coordination process between the electric and water sectors very, very fast.
Track 6
Advanced Electric Power System Restoration Requirements

Moderator: Frank Koza, Special Projects Coordinator, EIS Council
Roger Kemp, Professional Fellow, Lancaster University

Professor Roger Kemp described what was learned about resilience and infrastructure interdependency when Storm Desmond caused a major outage in the town of Lancaster, U.K. in 2015. The lessons were published in a report called “Living Without Electricity.”

The storm flooded a substation that supported the entire town of 100,000 people. All street lights went off. Communications ceased. The mobile phone networks went down and internet was lost within a few minutes. Most organizations, even large ones had no contact whatever with emergency planning infrastructure. The hospital functioned thanks to its emergency generator and backup fuel. Most doctors’ surgeries, however, had to close. A care home with 70 frail patients barely continued functioning.

“Pretty well all ATMs failed,” Kemp recalled. “There was no way of getting cash.” Many shops closed. A supermarket that stayed open could not order stock or take credit card payments. Transport was seriously disrupted. “There were no traffic lights. There were no petrol pumps - gas stations.” Rail networks continued but trains could not stop at the local station as there were no platform lights. People in apartments on high stories lost water as pumps failed. Kemp noted that “there was quite a big social divide between the people who could ride out that problem, who generally are representative of the decision makers, and the people who couldn’t ride out that sort of problem.”

Summarizing, Kemp said, “people learned a lot about what does and doesn’t work when you’ve lost your electricity. The biggest problem was communications; those who thought they were managing things had no way of talking to any of the people who thought they were being managed.”
Andrew Ott, CEO and President, PJM Interconnection

Andrew Ott surveyed how black start plans and capabilities in the U.S. are currently evolving as the power industry changes. With the spread of renewable generation and the closure of coal plants that were fundamental to black start generation, black start plans are having to change. Ott explained, “there were coal plants that were always essentially running, that could be used in Black Start. However, the economics changed so dramatically that it started to cost millions and millions of dollars to keep those things running.” Moreover, renewables rely on electronic inverter equipment that may well fail in an EMP or GMD event, making them unreliable for black start.

Another problem is that ever fewer black start units today are able to run on dual fuel and may not work if only natural gas is available to power a black start. An additional difficulty is changes in critical load where customers do not update the utility: We had a gas pipeline that was busy converting its gas compressors to electric, but they didn’t talk to us or the power company. That makes a system less resilient and black start plans less accurate,” Ott said. He flagged these problems as a “call to action: we need to update the black start plans, have more resilience in those plans and get rid of single-points of failure, whether in the cranking-path definition or in the issue of dual fuel. He ended with a warning: “I feel very insecure about our black start plans today because of all this change. We have a lot of work to do.”

Dr. Randy Horton, Senior program Manager, Electric Power Research Institute

Randy Horton reviewed findings with respect to resilience that have emerged from EPRI’s ongoing research assessing the impacts of high-altitude EMP on the bulk power system. Results so far suggest that the E1 very high frequency pulse emitted by an EMP blast would damage substation electronics, including control cables, signal cables, relays and SCADA communication systems. Another important finding is that the E3 pulse from an EMP attack could cause a voltage collapse in the power grid. This would seriously hamper black start plans.

Turning to mitigation options, Horton stressed that effective, readily available mitigation measures exist for these threats. He noted that U.S. military standard protection is probably not needed for substations. Horton noted a potential problem with mitigation measures, that, “if you fit the filters
that you typically would put on AC power supplies and DC power supplies in the circuits that are connected to protect the relays, you could actually introduce a reliability issue. The research needs to be done to make sure we’re providing the proper fix to the power system.” Horton also discussed software tools EPRI is developing that can optimize black start paths. Finally, he reiterated the paramount requirement of an effective, reliable Black Sky communications system.

Discussion

Roger Kemp said that citizens in Lancaster have improved their preparedness as a result of the 2015 outage, but the city authorities have been slow to implement lessons. With much infrastructure now privately owned, “chains of command go all over the place” Andrew Ott emphasized that “black start is a very small expense on a customer’s bill,” and a highly worthwhile investment. Terry Boston raised the problem of how to protect hospital emergency generators given that approximately over half of those in Manhattan failed during Hurricane Sandy, many due to flooding. Paul Stockton amplified Andrew Ott’s concern over the loss of dual fuel black sky plants, “there’s been very little understanding of the loss of redundant supply-chain capacity due to that reliance on a single supply chain, with only a tiny handful of refineries, none of which are hardened against EMP, much less normal cyber hazards.”
Summarizing highlights of the day, Terry Boston quoted Sergio Braunstein’s comment on the absolute existential necessity of EMP threat mitigation: “we had to protect the system at the end of the day.” Boston commented, “We need a lot more of that thinking.” Boston recalled that he had been struck by how unscientific most of our assessments of risk are: “I was blown away by the fact that Dominion has a bunch of PhDs working on probabilistic risk assessments like you would do for a nuclear reactor, assessing the risk and cost of the risk for different events.” Much more such work is necessary, Boston said.

The question of food supply becomes critical by day 3 of major outage, yet we talk about food less than about power, water and finance, Boston said, quoting the MI5 report of 2004 that “the UK is four meals away from anarchy.” Boston reiterated the scale and importance of the challenge of protecting power grids and congratulating Avi Schnurr and the EIS Council team on their work.
EIS IX Conclusions. What Have We learned? What are the next steps? How will we measure our Separate and mutual Progress?

Avi Schnurr, noting key points to emerge from the Summit. He stressed that “failure is not an option” in preparing for a Black Sky event. Schnurr noted that the U.S. National Infrastructure Advisory Council to the President has said that 100 million Americans could be at risk in a Black Sky outage, a marker for what is at stake. Schnurr quoted Paul Stockton’s statement that survival will depend on people’s ability to shelter in place and warned that this will be next to impossible if water and sanitation cannot be maintained. Schnurr picked up on the comment by Andrzej Kawalec from Vodafone that human beings are unusually bad at projecting risk and emphasized the importance of effective tools to help people assess risk better.

Turning to the electric sector, Schnurr underscored Tim Roxey’s point on the importance of being able to configure the electric grid in the most resilient way if we know that a serious hazard will hit in a short time. He also highlighted Andy Ott’s comment that fuel security and the availability of dual fuel generators must improve if we are to be able to manage a Black Sky level black start. Schnurr questioned the widely held belief that renewable energies such as solar and wind are an obvious resource for a Black Start. In fact, since their inverters contain quite complex electronics, they are likely to be damaged by a Black Sky event. Schnurr recommended meeting with renewables and inverter leaders to discuss how they can be more resilient.

“Survival in a Black Sky event will depend on people’s ability to shelter in place. This will be next to impossible if water and sanitation cannot be maintained.”
“Emergency communication came up over and over again, as it always does,” Schnurr noted. Scott Aaronson pointed out that emergency exercises make the highly problematic assumption that there will be excellent communication, because otherwise the exercise will fail. As well as resilient emergency communication, we will also need allied capabilities to map interdependencies, and mechanisms for decision support. Schnurr cited the BSX emergency communications system that EIS Council is developing and added, “one way or the other, the emergency communication space has to be filled.”

Schnurr endorsed Richard Fox’s comment that utility managers need to know as accurately as possible the likely duration of an outage so that they can know how to deploy their emergency fuel. Fuel resupply for emergency generators still hasn’t been solved. “This has to get fixed,” Schnurr said. Likewise, replacement generators will be needed because generators will fail after running for days at a time. Moreover, there are still not enough emergency generators in the world for a Black Sky event. “The only reason for that is not because they’re so expensive, because they’re not. It’s because no one takes the need for them seriously enough,” Schnurr said.

In the area of regulation, Schnurr echoed Joe McClelland’s comments that regulation, while necessary, cannot solve this whole problem, and welcomed the statements from FERC representatives that greater agility is needed on the government side. Finally, Schnurr urged participants to play in the upcoming Earth Ex and Grid Ex exercises.

The reason for the shortage of emergency generators is not that they’re so expensive; they’re not. It’s because no one takes the need for them seriously enough.