"Black Sky" Infrastructure and Societal Resilience Workshop

Monday 16th January 2017 | The Royal Society, London

CENTRE FOR THE STUDY OF EXISTENTIAL RISK

ICIF INTERNATIONAL CENTRE FOR INFRASTRUCTURE FUTURES

EIS COUNCIL

“Black Sky” Infrastructure and Societal Resilience Workshop

Monday 16th January 2017

The Black Sky Infrastructure and Societal Resilience Workshop was organized by the EIS Council, in cooperation with:

CENTRE FOR THE STUDY OF EXISTENTIAL RISK
UNIVERSITY OF CAMBRIDGE

The Centre for the Study of Existential Risk, Cambridge University

ICIF
INTERNATIONAL CENTRE FOR INFRASTRUCTURE FUTURES

The International Centre for Infrastructure Futures

The organizers wish to thank the Royal Society, London, for hosting the event.

Executive Summary

Problem Statement

In the modern world, our lives are empowered, enriched and sustained by unprecedented access to clean water, electricity, food, health care and pharmaceuticals, and a wide range of other vital products and services. In most modern nations, when disasters strike and the interconnected infrastructure networks that supply these goods and services fail, utilities, corporations, government agencies and mass care NGOs have always been able to depend on the continued availability of these networks in most of the country, setting aside other priorities to come to the aid of the affected region.

In Black Sky hazards, long duration, potentially nationwide power outages and associated cascading failures of all lifeline utilities will drastically limit availability of such “external” support, precisely at the time when it is desperately needed by the population. Thus “scaling up” disaster plans that depend on such external support will be insufficient to meet the unique needs of these severe scenarios.

In addition, to sustain or restore its services, each utility sector typically depends on products and services it receives from other, interdependent sectors. In a Black Sky outage, advance preparations of any one sector, without common, well-coordinated preparations across many sectors, will be unsuccessful due to the lack of these sector-external products and services.

Solution Approaches

Given adequate, well-coordinated advance planning and associated limited, prioritized investment, preparing for these uniquely severe hazards is well within the capabilities of UK corporations and their government and NGO partners. However, since no single sector today can function without the partner sectors each depends on, coordinated planning and engagement is critical. To resolve the problem of sector interdependencies in highly disrupted environments, such planning must be remarkably broad, addressing the full range of essential sectors. It must also be operationally focused, designed to ensure each sector’s planning addresses its unique Black Sky mission, with associated recommended “internal” requirements or resilience measures to be taken by that sector, and recommended “external” requirements representing a sector’s needs for support from other sectors.

Key Discussion Points

Black Sky Hazards should be high on decision makers’ agendas. As Lord Rees put it, “our power grids are becoming ever more crucial. Cities will be paralyzed without electricity, and the lights going out will be the least of the consequences… everything else that urban life depends on is vulnerable to breakdowns, errors, or even intentional sabotage of the system.”

We need to be concerned with low-probability high–consequence events. "The most worrying events are those that haven't yet happened but where even one instance would be too many," Lord Rees point out.

The principal malicious Black Sky hazards are cyber-attack, Electromagnetic Pulse attack (EMP), caused by the high-altitude explosion of a nuclear warhead for example by a rogue nation or terrorist organization, and coordinated physical attack on the electrical grid.

A prolonged widespread power outage would cause cascading failures of other systems. As Lord Toby Harris said, "our lives are so now dependent on electricity that it's almost impossible to envisage what our daily existence would look like without it." Among the most serious impacts could be failure of water and waste water systems that would make cities uninhabitable and break down of the food distribution system that could unleash civil chaos.

Detailed cross-sectoral planning will be needed if our societies are to weather Black Sky events. Avi Schnurr of EIS Council explained that such planning must include, firstly, robust resilience investment to protect a core set of critical hardware and secondly, "there needs to be very good cross-sector planning to support restoration of infrastructures."

It is important to raise awareness of the threat at all levels of organizations. As Lord James Arbuthnot put it, "We must recognize that this is not an IT problem; it's a problem for everyone; it's an issue of culture and education."

Infrastructure systems are connected through complex interdependencies. Agent-based Modelling can be a powerful tool for real-world infrastructure analysis as it allows the agents and nodes to be defined uniquely and hence more accurately than standard network node analysis.

In the US, EIS Council is engaged in building a national, cross-sector resilience community. This work is centered on sector playbooks that disseminate best practice resilience investment and recovery planning, and regular cross-sector exercises, most prominently the Earth Ex series.

Black Sky hazards may be understood on a systems level as an emergent property of complex infrastructure interdependencies and relationships. These interdependencies may be physical, digital, geographical or functional. As Professor Miguel Centeno put it, "Emergent risk arises from individual parts that are connected to the whole, but they can't be reduced to a single bad apple. It's the fact that you put all these apples in the barrel that creates the problem. Trying to regulate the bad apples won't help you because the real problem is the fact you're trying to put all these apples together."

Systems can fail, even if everything works as it is supposed to; "even if there is no stupid person, no greedy person or no terrorist. If the system is so complex there's no way the various parts are well integrated," said Miguel Centeno.

Cross-sector infrastructure planning processes can minimize the adverse impacts of interdependencies and also achieve opportunities to gain extra value from interdependencies.

We need to put resilience at the center of infrastructure planning. "We get what we measure in our infrastructure," as John Beckford put it. Currently in the UK, efficiency, not resilience is the main outcome parameter that is measured and incentivized. High performance at low cost, rather than robustness receives political and financial rewards.

Senior leadership turnover is a serious shortcoming in Western governments' ability to undertake long term sustained resilience planning: "I think all of our developed countries have exactly the same systemic problem at the top, change of leadership and complete, not only loss of, but almost conscious destruction of corporate memory, which is even worse in some ways," declared Professor Brian Collins.

The critical importance of infrastructure is not well understood. In a recent World Economic Forum survey that asked senior decision makers to rank leading global risks, the failure of critical infrastructure comes 25th on the list.

Exercising emergency plans is critical. A plan that is not rehearsed until an actual emergency hits will fail. It helps to use vivid and realistic scenarios. Mark Abbot from the National Grid said, it's only when people start to see reality in front of them that actually they start to engage with it fully and start to understand."

The scale of the risks to infrastructure is vastly disproportionate to the current scale of investment in resilience. As Professor Brian Collins said, "we must start thinking in the trillions, and what we're currently doing in terms of preparedness, which is in hundreds of millions. That ratio is not in the right place."

Introductory Session

Setting the Context - Emerging Black Sky Hazards

In this session, three leading experts set out the nature of Black Sky threats, explained why we need to take them very seriously and discussed how we should approach their mitigation.

Lord Rees warned that as all aspects of modern life become increasingly dependent on electricity, the power system becomes more vulnerable to breakdowns, errors and intentional sabotage. A prolonged, mass outage could have catastrophic, cascading impacts. “The most worrying events are those that haven't yet happened but where even one instance would be too many,” he declared.

Avi Schnurr of EIS Council noted the high importance of this meeting as an opportunity for leading academic researchers to bring their expertise to bear on the critical threats to infrastructure. He enumerated the main natural threats as severe earthquakes, severe weather and very severe solar weather caused by coronal mass ejections. The principal malicious hazards are cyber-attack, Electromagnetic pulse attack (EMP), caused by the high-altitude explosion of a nuclear warhead for example by a rogue nation or terrorist organization, and coordinated physical attack on the electrical grid.

He argued that only detailed cross-sector planning can prepare us to survive such threats. Such planning must include, firstly, robust resilience investment to protect a core set of critical hardware. Secondly, Schnurr said, “there needs to be very good cross-sector planning to support restoration of infrastructures.”

Lord Toby Harris described the effects of a Black Sky level outage. He noted in particular the dangers that failure of water and waste water systems could make cities uninhabitable and that break down of the food distribution system may unleash civil chaos. Harris conclude that even of the probabilities of such events are small, their seriousness more than justifies the investments needed to protect against and mitigate their effects.

Welcome and Comments on the Nature of Existential Risk

Lord Martin Rees OM FRS, Astronomer Royal, Founder - Centre for the Study of Existential Risk, Cambridge University

Lord Rees described how globalization makes extreme risks more dangerous. This trend demands that we protect and mitigate against the possibility of previously unthinkable events.

“Black Sky events should indeed be higher on everyone's agenda,” he declared. “Our power grids are becoming ever more crucial. Cities will be paralyzed without electricity, and the lights going out will be the least of the consequences… everything else that urban life depends on is

vulnerable to breakdowns, errors, or even intentional sabotage of the system. That's why indeed infrastructure security should be high on the agenda. It needs collaboration between central government, civic government, and of course the relevant industries.”

> Black Sky events should indeed be higher on everyone's agenda

He added that the more extensive the event, the more likely would be the failure of interdependent infrastructure and the harder it would be to mobilize resources to restore affected systems: “the more widely the outages cascade, the less feasible it is to send help from outside. And of course, if a whole region is affected, it's far worse. And if the effects spread across borders, it's catastrophically worse”

Lord Rees argued powerfully for why we should be concerned with low-probability, high-consequences events: “the most worrying events are those that haven't yet happened but where even one instance would be too many,” he warned. “These are the hardest, of course, to study and quantify because generally there's as of yet no data.”

He posited that “we have entered a new geological era, the Anthropocene, where the most extreme threats, the near-existential ones even, come not from nature anymore but from humans. They're worse because we are more globalized.” While affirming that globalization is, overall, immensely beneficial, Rees pointed out that it can exponentially amplify the reach, impact and speed of spread for large-scale disasters, such as financial crises, pandemics or infrastructure failures. “In our ever-more-connected world, the risk of disaster spreading internationally, even globally is rising.”

> The most worrying events are those that haven't yet happened but where even one instance would be too many,

He concluded, “an important mantra is that the unfamiliar is not the same as the improbable.” We must keep our minds open to how transformative advances in technology are creating opportunities but also dangers that were previously unimaginable. “

Overview and Canonical Black Sky Hazards

Avi Schnurr, CEO EIS Council

Avi Schnurr began by noting the rare and important opportunity provided by this meeting for academia and industry to come together and examine extreme risks for critical infrastructures. “It's going to be important that the very best minds available can help lead the way doing the research on Black Sky hazards,” he stressed.

Schnurr went on to outline some of the features of Black Sky hazards that make such threats uniquely challenging to prepare for. The root of the problem, he suggested is a shift in how we treat resources. “For almost all of history, resources were local affairs; today all of our critical lifeline infrastructures are interconnected. The flip side of interconnection is interdependency. And

not only are they interconnected, but they are national, international and global in scale. The corollary of this interconnectedness is that major infrastructure failures can have national and global impact.”

It's going to be important that the very best minds available can help lead the way doing the research on Black Sky hazards,

Another unique challenge of Black Sky events is that “we have no 20/20 hindsight:” we must evolve adequate means of addressing them without a Black Sky event actually occurring. Moreover, “if we have a problem which is national or even near-national in scale, the cavalry will not be able to come. The problem will have to be resolved from inside the affected community.” This can only happen of the response is carefully preplanned. However, “the preplanning is going to have to occur without the help that normally we get from repeated disasters.”

Schnurr continued that the necessary cross-sector planning needs to have two critical elements.

- The first is robust resilience investment at least to protect a core set of critical hardware. Without a core of surviving critical infrastructure, “you can’t sustain society long enough for restoration.”
- Secondly, there needs to be very good cross-sector planning to support restoration of infrastructures.

If we have a problem which is national or even near-national in scale, the cavalry will not be able to come. The problem will have to be resolved from inside the affected community.

Schnurr emphasized that the planning goals we set must be robust and ambitious enough, taking into account the severity of black sky hazard impacts: “timid goals will not be able to ensure the continuity of society through any of these black sky hazards.” Moreover, he added, these aggressive goals must be attainable through cost-effective measures. Otherwise, they will not be funded and won’t happen.

He concluded by enumerating the key Black Sky hazards. Natural hazards include severe earthquake zones, severe weather and very severe solar weather caused by coronal mass ejections. The principal malicious hazards are cyber-attack, Electromagnetic pulse attack (EMP), caused by the high-altitude explosion of a nuclear warhead for example by a rogue nation or terrorist organization, and coordinated physical attack on the electrical grid.

Timid goals will not be able to ensure the continuity of society through any of these black sky hazards.

Civil and Societal Impacts of Severe, Long-Duration Power Outages, Regardless of Cause

Lord Toby Harris, UK Coordinator, EIS Council; Member, Joint Committee on National Security Strategy, UK Parliament

Toby Harris described the likely consequences of a wide-spread prolonged power outage. While the probability of such an event might be low, the consequences would be so severe that it is amply justified to devote serious time and resources to planning against such eventualities.

He related how “the lights would go off; heating or cooling systems would stop working. Refrigerators and freezers fail. Landline telecommunications stop. Computer screens go dark.” Harris stressed that, “our lives are so now dependent on electricity that it's almost impossible to envisage what our daily existence would look like without it.”

He recalled the four-day power cut a year earlier in Lancaster as a result of a severe flooding described as a once in a hundred years' event. A substation was inundated, affecting more than 60,000 homes and businesses, and at least 100,000 people.

Harris detailed some of the impacts of this event: “A review conducted by the Royal Academy of Engineering found this event disrupted transport, communications, and the ability of the emergency services to reach people in need. Text messaging is one of the first services to go, followed by digital radio and the internet, and shops soon lost their tills. ATM machines went out of action. And garages were unable to dispense fuel as their pumps need electricity to operate. Traffic lights stopped working. … 75 emergency generators had to be brought to Lancaster from as far away as the southwest of England and Norther Ireland.”

> Our lives are so now dependent on electricity that it's almost impossible to envisage what our daily existence would look like without it.

The Lancaster incident was comparatively localized and manageable yet was still immensely disruptive of basic services and technologies that we take for granted. It gives us an inkling as to how bad a far more extensive power outage could be. Extrapolating from the effects of the Lancaster incident, he suggested that some of the most serious impacts of a more serious outage would be in the areas of schools, hospitals, nuclear plant cooling, water, waste-water and sewage treatment.

He pointed out that “a city without fresh water or a city where wastewater and sewage cannot be removed rapidly becomes uninhabitable.” Moreover, the effects of power failure on food supplies could also be disastrous. How long, Harris asked would “refrigerators and freezers in homes, in small retailers, major supermarket outlets last? And in these days of just-in-time deliveries, how well will wholesale supplies hold up.” He noted that, according to a famous MI5 warning, “the UK is four meals away from anarchy… It is not hard to imagine the implications for civil order of this sort of disruption to food supplies.” Furthermore, in Lancaster, the ATMs stopped working, “so how long would the financial system continue to function?” Harris asked.

> A city without fresh water or a city where wastewater and sewage cannot be removed rapidly becomes uninhabitable.

While individual sectors all have contingency plans, a crucial shortcoming is that these plans tend to assume that other infrastructures are still functioning – that the phones still work, internet is accessible and transport is operating. “But the reality is that they are all interconnected, interrelated, and interdependent.” Restoration planning for a scenario where key infrastructures are badly damaged simultaneously is much more difficult and has barely been attempted.

> The UK is four meals away from anarchy… It is not hard to imagine the implications for civil order of this sort of disruption to food supplies.

Keynote address

Infrastructure Interdependencies and the Nature of Complex Systems

Professor Liz Varga, Professor of Complex Infrastructure Systems, Cranfield University

Professor Liz Varga gave an overview of complexity science and how it can help us to understand interdependent infrastructure systems. Modern society relies heavily on effective functioning of critical infrastructure networks to provide essential public services and the foundation for our economies. However the tight interdependence of these systems increases their potential vulnerability.

The complex, multiply interconnected interdependence of these systems raises the possibility that “things are so intricately interconnected that as humans we can't possibly understand the magnitude and consequence of those interconnections.” This leads to what complexity scientists call “VUCA” environments, which are volatile, uncertain and ambiguous, where volatile indicates instability, ambiguity refers to a lack of information and uncertainty is our consequent inability to fully understand causing events.

Noting that “black sky disruptions are characterized by long duration, widespread impact, and cascading failures,” she defined cascading failure as “the idea that successive parts of the system fail as a consequence of a failure somewhere else.” In systems that are tightly coupled together, such as modern infrastructures, a small fraction of affected nodes in one network can produce an iterative cascade of failures in other networks. As an example of a case where

> Things are so intricately interconnected that as humans we can't possibly understand the magnitude and consequence of those interconnections.

interconnections were not understood, she cited the recent accident where an Australian dam overflowed and disrupted telecommunications equipment which meant that the people operating the dam could not warn the people in the valley that the water was coming, and consequently a number were killed.

Varga pointed out that although interconnectedness can produce cascading failures, it also provides opportunities to design systems with greater resilience. For example green spaces can be deliberately used as a buffer against flooding. She went on to discuss various types of resilience from a systems perspective. Varga defined resilience as the capacity of a system to bounce back to its normal state after a serious interruption. A key dimension of societal resilience is the availability of substitutes for key services. For example energy substitutes might include batteries, generators and other short-term solutions. Water substitutes might include bottled supplies. Regarding business resilience, businesses can be forced to cease operating immediately without contingency plans in place; they are also heavily dependent on societal resilience to keep functioning.

Turning to definitions and common features of key infrastructure, Varga noted that they include energy, water and waste, transport, telecommunications food and finance. Critical infrastructures have some common features: “they can lead to people not having access to critical services. There's rapid and growing demand for these services. There are resource constraints. They all operate in heavily regulated markets. There's strong interdependencies with environment, with climate, and the general development of urbanization and densification is putting pressure on these systems. Security is a fundamental issue.”

> Cascading failure is the idea that successive parts of the system fail as a consequence of a failure somewhere else.

Interdependencies

Varga cited Rinaldi’s seminal 2001 paper which analyzed four types of interdependency between critical infrastructures: physical, cyber, geographic, and logical. Physical interdependencies occur when one system depends on the material outputs from another, so there's some physical interaction between the systems. Cyber involves a dependency on information between systems. Geographic entails physical location interdependency, and the logical is “almost anything else.” “Interdependencies are varied and they might arise indirectly. You needn't be in the same place but you can be interdependent through another path to these other systems.” Varga went on to map the interdependencies between four overlapping critical infrastructure systems: energy, telecoms, water and waste. She emphasized the wide range of different overlaps between the systems and that the scale of the overlap is often unknown.

Resilience of complex systems is a function of their ability to adapt. Some of the ways systems adapt are through substitutes, contingencies, backups, training and human ingenuity. On the other hand, some of the things that make systems inflexible and unadaptable are restrictive legal and regulatory regimes including health and safety standards. Although such standards are designed to help us, they can sometimes prevent intelligent, adaptive action. Agents in a system need to be able to act and interact flexibly to respond to serious disruption.

Varga alluded to the UK Cabinet Office's useful "5R's framework" for thinking systematically about infrastructure resilience "where do you think about resistance - how do you protect your infrastructure before it gets into that situation? What redundancy do you have - the flexibility you have to recover? Reliability - what maintenance are you doing beforehand. And then your actual response and recovery processes."

Varga concluded her talk with three suggestions for how to strengthen resilience in increasingly interdependent systems. The first is information sharing, education or learning across networks to improve efficiency and resilience. The second is exploiting geographical or physical interdependencies, if we can understand them well enough to share assets. "A good example for this is energy storage, Varga explained. "Store it where it's produced rather than distributing it and redistributing." The third is taking advantage of some integrative opportunities. Smart infrastructure and Internet of Things information provided by the telecoms network; could be made available to energy, transportation and other networks.

In the question period, Avi Schnurr asked whether network analysis is advanced enough to project detailed approaches and methodologies for particular industries. Vargas answered that one of the limitations of network science in this respect is that it treats nodes as homogeneous, which in the real world they are not; they have different traits and sizes. She suggested that Agent-based Modelling can work better for real-world infrastructure analysis as it allows the agents – nodes to be defined uniquely and hence more accurately.

One of the limitations of network science is that it treats nodes as homogeneous, which in the real world they are not; they have different traits and sizes. Agent-based Modelling can work better for real-world infrastructure analysis as it allows the agents – nodes to be defined uniquely and hence more accurately.

Panel 1

The Coordination Challenge and Implications

This panel addressed the broad challenges of coordination that are necessary to prepare for and deal with Black Sky level events.

Lord Arbuthnot insisted that civil society and all levels must be prepared and that it is illusory to think that the military would step in and clear up the crisis. He suggested a number of practical steps to support preparedness, including regular exercising of recovery plans, utilities storing essential spare parts and the establishment of a national cyber audit for key utilities and government bodies.

John Hetzel described the cross-sector utility resilience planning process that EIS Council is hosting in the US. The work is centered on the sector playbooks that document best practice in resilience investment and recovery planning for each sector. The playbooks are developed through an Iterative process of consultation with utility and emergency managers in the field and are crucial resource for cross-sector planning.

Communications are a particular focus, out of a recognition that without adequate surviving communications after a Black Sky event, recovery would be virtually impossible. Exercising recovery plans is also a major focus; in August 2017, EIS Council will be running the first ever Earth Ex cross-sector exercise.

Meir Elran discussed how resilience is being implemented in Israel. He noted the gap between the high level of resilience of the general public and the relative tardiness of the government in implementing necessary resilience measures. He argued for a more urgent awareness among decision-makers of the dangers of a major power outage and the need to take action to prevent and mitigate such an event.

National Security Implications for Severe Black Sky Hazards

Rt. Hon. Lord James Arbuthnot, Director SC Security

Lord Arbuthnot outlined some of the implications of a Black Sky threats and suggested constructive ways to mitigate the threats. He began by challenging the assumption that in any crisis such as this, the military will step in and solve the problem. He assured the audience that the military is overstretched and unprepared to deal singlehandedly with a Black Sky event. “They say there's no evidence that anyone is planning a major attack on our infrastructure. They may be right, but they did say that about 9/11,” cautioned Lord Arbuthnot.

The worst-case scenario

Lord Arbuthnot sketched out a plausible scenario of “a multifaceted attack involving a dirty bomb in Waterloo Station, combined with a cyberattack on the ambulances and the national health system, and an electromagnetic pulse attack delivered by drone on the National Grid, all at the same time.” He opined that if there to be a state-on-state war, “I'm sure that's exactly how it would begin.”

He warned how shockingly easy it could be to launch a major cyber-attack on critical infrastructure. He described a recent demonstration of this by risk expert Dr. Sally Leivesley who showed how, with a few minutes one could download the instruction manual for the operation

They say there's no evidence that anyone is planning a major attack on our infrastructure. They may be right, but they did say that about 9/11

system of a major European power company, including the default password. “Engineers installing operating systems don't change the default password. And you may be surprised to hear; in over 50% of companies, neither do the operators,” Arbuthnot reported. “People will do almost anything in the interests of convenience.”

Arbuthnot made five suggestions for improving planning and preparedness. First, we must raise awareness of the threat at all levels of organizations. “We must recognize that this is not an IT problem; it's a problem for everyone; it's an issue of culture and education.”

Second, plans need to be practised. “If the first time you try something out is when you're under attack, your plan will fail.” The plan needs to involve the highest levels of decision making, up to the Prime Minister.

We must recognize that this is not an IT problem; it's a problem for everyone; it's an issue of culture and education.

Third, utilities need to store critical spare parts. We need to recognize that multiple redundancy is not a waste of money. It's a sensible exercise in resilience,” Lord Arbuthnot declared.

Fourth, there must be a plan in practice for recovery and it must be practiced.

Fifth, critical infrastructure organizations should establish an annual cyber audit. “Organizations should be encouraged to include in their annual reports the steps they're taking to defend against cyberattacks. This should be led by industry, not by government, because government can never keep up with technological change.
At first, it should be by encouragement, and then it should in the longer term be obligatory.”

If the first time you try something out is when you're under attack, your plan will fail.

Hosting a Black Sky Coordinated Resilience Planning Process in the U.S: Utilities, Government Agencies, NGOs, Corporations

Brigadier General (ret.) John Heltzel, Director of Resiliency Planning, EIS Council

John Hetzel outlined EIS Council's work on building and implementing a national resilience community model that could enable our societies to recover from a complex catastrophe.

Describing the organization's focus, Hetzel noted, "98% of all our emergencies are handled, every day, by our first responders. We've got another 1% which are regionalized, which the state or region will take care of it. That other half percent is what we spend our time talking about, these Black Sky events."

EIS Council's approach is to move the focus from emergency management and emergency response to restoration activities. "How do we bring the sectors together to work to ensure that restoration process starts as soon as possible, and is as effective as it possibly can be?" Hetzel described three main tiers of effort towards this goal:

The foundational tier is the development of sector playbooks, which convene and disseminate a best-practice and inter-sectoral approach to mitigating and recovering from Black Sky hazards.

The middle tier is built around Black Sky communication protocols. "How do we communicate? When do we communicate? How do we share information? What's the most critical information?"

At the very top of pyramid is the Black Sky doctrine, which Hetzel termed a "phase synchronization matrix of who needs to take what actions at what times to ensure that we save lives, and protect property. It's easy to say; it's not easy to do, especially when communications will be mostly not working."

How do we bring the sectors together to work to ensure that restoration process starts as soon as possible, and is as effective as it possibly can be?

EIS Council has appointed coordinators for each of the major sectors who are building Playbooks, coordination events and exercises for their sectors, including the electric sector, the water sector, the US Federal sector, the state sector, NGO sectors, oil and gas and the regulatory sector. Food, transportation, medicine and finance will shortly be added. Twice a year, EIS Council holds major seminars to ensure that the information and processes laid out in the Playbooks are developed and widely shared.

EARTH EX - an EIS Council-supported exercise.

The EARTH EX exercise, set to take place for the first time in August 2017, "will give senior decision makers and operational decision makers the opportunity to apply the things in the playbooks and put them into practice, Hetzel explained. "Our overarching objective is to improve community resilience to these long-duration power outages through this cross-sector exercise."

The Broad Definition of Resiliency:
How is it Being Implemented in Israel?

Brigadier General (ret.) Meir Elran, Head of the Civilian Sector,
Israel National Security Studies (INSS)

Meir Elran began by noting that Israel has experienced serious, periodic interruptions to its national life, all of them caused by security challenges.

Elran contrasted the remarkable resilience of many communities in Israel with the resilience efforts of the state. Communities, he reported, “are not only initially resilient, but they are actually investing a lot of their own capacities, their own capital to enhance their own resilience.” The outcome is

encouraging. At the national level, on the other hand, “you see quite a different picture.” He posed the question: “why is it the case that when you look at the national level, you see not enough is being invested in order to promote the restoration capacity of infrastructure systems?”

He suggested a number of steps that could be taken at the national level to increase infrastructure resilience.

Firstly he proposed that it is necessary to identify the threshold of national functionality, primarily in the area of electric supply; what is the minimum power capacity that Israel needs to function?

Secondly, Elran emphasized, the country must construct the necessary power capacity that will ensure the system's capacity to bounce back and restore itself within days, following a major disruption possibly.

Thirdly, there needs to be a much stronger and clearer awareness of the dangers of a massive prolonged power outage and the urgency of taking measures to protect against it.

Finally, he declared, “we have to lessen dependency on the bureaucracy that prevents the system from operating in a more flexible manner, and to set the necessary priorities to be able to restore the system under attack.”

Elran concluded that although these observations are based on his experience from Israel, “I would suggest that they are not exclusive to our own case.” These common features between countries make the sharing of knowledge at internationals gatherings like this especially fruitful.

We have to lessen dependency on the bureaucracy that prevents the system from operating in a more flexible manner, and to set the necessary priorities to be able to restore the system under attack.

Discussion

The Coordinating Challenge and Implications

Moderator: Lord Martin Rees

In response to a question about whether the Playbooks allow responders sufficient flexibility in an emergency, John Hetzel emphasized that “Playbooks provide the information that's required in an emergency, outline the interdependencies that exist, and how we would coordinate between sectors.” He added that a key 2017 Playbook task is understanding the sectors’ resource supply chain “who's the supplier and who's their supplier's supplier? What critical resources need to be on the ground or immediately available in a Black Sky event?”

Brian Collins from University College London questioned the assumption that utilities know what is in their asset bases. Given that utilities are often privately and internationally owned, and that rapidly changing software is a key part of the asset base, this is immensely challenging. Liz Varga replied that resilience planning provides a valuable opportunity to compile all of this knowledge. James Arbuthnot maintained that today, when systems are controlled by continuously updating software, it is simply impossible to know what is in one’s asset base

Mark Workman from Imperial College London noted the importance of mapping multidisciplinary activities for decision making under Black Sky events. Chris Rogers, from the University of Birmingham suggested that extreme future scenario analysis done in a rigorous manner can play a role in understanding the potential dimensions of problems, an also the capability one would need then to address them.

In response to a question about the global dimensions of Black Sky events, Liz Varga remarked that we learned quite a lot about this from the ash cloud that spread across Europe after the volcanic eruption in Iceland affecting the finance, travel and transportation industries.

Panel 2

Infrastructure Interdependence and Resilience

In this panel, systems theorists and infrastructure experts took a systems approach to infrastructure resilience.

Dr. Neil Carhart proposed that Black Sky hazards are an emergent property of infrastructure interdependencies and a product of the relationships between the parts of complex systems. He analyzed four types of interdependency: material, digital, geographical and organizational. Carhart argued that the latter two are neglected in planning and need more attention.

Dr. Ges Rosenberg described how intersectoral planning of infrastructure can help minimize the adverse effects of interdependencies and maximize positive synergies. He noted the tendency of people and organizations to working in silos, “whether it's supply chains, public/private, regulatory barriers that can often thwart people coming together.”

Dr. Tom Dolan also took a systems approach to infrastructure and suggested that the banking crisis of 2008, “a high-profile cascade failure impact that was society wide” could provide an illuminating parallel to potential large scale infrastructure failure.

Dolan argued strongly that “we need to make a case putting resilience at the center of all of our decision making. It's not and can't be a bolt-on to how we currently operate.”

Planning and Managing Infrastructure Interdependencies

Dr. Neil Carhart, University of Bristol

Dr. Neil Carhart talked about infrastructure interdependencies and proposed that we need to understand them more broadly. He argued that Black Sky hazards and resilience are emergent properties of infrastructure interdependencies. “I'm a systems theorist,” Carhart declared, which can be summed up by this philosophy: The whole is greater than the sum of its parts. But we have a tendency in infrastructure to look at the parts independently of one another.

“Infrastructure exists in silos. We take infrastructure and the problems infrastructure piecemeal, bit

by bit.” But, as Carhart explained, emergent properties of systems are features that emerge as a product of the relationships between parts. “As a systems theorist, I'm interested in understanding what those relationships are,” he stated.

“I argue that black sky hazards are, in part, an emergent property of those interdependencies and relationships. But also the capabilities and abilities associated with resilience are emergent properties of the interdependencies of the infrastructure system.”

Carhart referred to a seminal article on infrastructure interdependencies that analyzed four types of interdependency: material, digital, geographical and organizational. The first two, functional, interdependencies which include, for example needing power to pump water, or the outputs of a SCADA system being essential for communications are relatively well understood; the second two, by contrast, tend to be neglected.

> Black sky hazards are, in part, an emergent property of those interdependencies and relationships.

For example, where two infrastructure systems are collocated in the same physical space, and therefore, if one is disrupted it can disrupt another. “In 2011, Carhart recalled, “a pump in Trafalgar Square fountains failed. That caused a leak and overflow of the fountain, which disrupted its power supplies. It disrupted the power supplies at Charing Cross Station, which took out the Bakerloo line temporarily. Is the Bakerloo line functionally dependent on Trafalgar Square fountains? Or do we need a richer set of words and descriptions to be able to capture these kinds of interdependencies?”

Carhart described a study showing that large models of the National Grid and water distribution networks use input/output interoperability modeling approaches. But these methods only model the physical and digital interdependencies. They completely overlook and are actually incapable of effectively modeling geographic and all those other types of logical interdependencies. As an alternative, Carhart showed a matrix-based approach that mapped physical, digital, geographic, and logic between major infrastructure projects planned to be developed in the UK over the next 40 years. “What's really interesting,” he pointed out, “is the fact that while 47% of the identified interdependencies were physical, a big chunk of them, 13% were geographic, and an even bigger chunk 26% were those organizational/logical interdependencies, the things that our modeling approaches overlook.”

> We tend to focus on functional interdependencies, but we also need to think about nonfunctional interdependencies, and systems theory has much to offer in terms of being able to capture, manage, and understand those other interdependencies.

Carhart concluded, “we tend to focus on functional interdependencies, but we also need to think about nonfunctional interdependencies, and systems theory has much to offer in terms of being able to capture, manage, and understand those other interdependencies.”

Developing Black Sky Hazard-Resilient Infrastructure: The Benefits of a Collaborative Approach to the Planning and Management of Infrastructure Interdependency

Dr. Ges Rosenberg, University of Bristol

Ges Rosenberg described his experience working with the UK Treasury on major UK infrastructure projects including the High Speed Two rail link. He focused on how planning can minimize the adverse impacts of interdependencies and also achieve opportunities to gain extra value from interdependencies.

This requires addressing the practical barriers to bringing people together. “The first one already referenced is about working in silos, whether it's supply chains, public/private, regulatory barriers that can often thwart people coming together.” Another, design and engineering related set of problems are what Rosenberg termed “pattern-repeating practices… we've always done is this way so we do it that way. We just scale up but don't look at redesign.”

Another set of interdependency challenges are wicked and super wicked problems. Wicked problems are “very complex and pernicious and difficult to solve. Solve one bit, and it pops up somewhere else.” Super wicked problems are those where “the interests that are creating the problem don't have necessarily the interest to align to solve that particular problem. There's a lack of incentive and potentially a lack of leadership to find solutions.”

He described the projects’ efforts to develop a collaborative approach, to break down silos and do co-design, co-production co-creation. He noted the need to improve the tool sets we have for valuation and distribution of co-benefits. Rosenberg also discussed principles such as stewardship that could evolve appropriate collaborative governance and leadership for

infrastructure. Leadership was provided by Infrastructure UK and the Department of Transport.

Rosenberg concluded that “to plan and manage interdependencies we need an interconnected, open-systems approach; if we're going to do that we've got to recognize there are a number of different stakeholders that are going to be involved. That takes us to collaboration, co-production, and co-design.”

He emphasized that this approach is equally applicable for risk management as well as for identifying beneficial interdependencies.

> To plan and manage interdependencies we need an interconnected open-systems approach;

Multi-Disciplinary Perspectives on Infrastructure Resilience and Can We Learn From the Banking Crisis?

Dr. Tom Dolan, Research Associate and Centre Coordinator for the International Centre for Infrastructure Futures (ICIF), UCL

Tom Dolan spoke about resilience based on his work for Infrastructure UK that focuses especially on measuring the performance of infrastructure.

He stressed the importance of seeing infrastructure protection as a systems problem, as we view

climate change. From this perspective, hardening a particular asset is of limited value if we do not also improve the resilience and effectiveness of the web of interdependent activities in which the asset is embedded.

Dolan posed the question of what we can learn from the banking crisis that might help us better understand infrastructure resilience. “The reason I ask this,” he explained “is that it's a high-profile cascade failure impact that was society wide.”

There was a culture of denial prior to the 2008 crash. Positive feedback loops were predominant, so success was seen as proof of concept, reinforcing what bankers doing. Certain actions decreased resilience.

He concluded that “we need to make a case putting resilience at the center of all of our decision making. It's not and can't be a bolt-on to how we currently operate.”

We need to make a case putting resilience at the center of all of our decision making. It's not and can't be a bolt-on to how we currently operate.

Discussion

Infrastructure Interdependence and Resilience

Moderator: Lord Harris

Peter Van Manen from Living PlanIT picked up on the idea of a Black Sky event being an emergent property of a complex system and pointed out that, “the nature of emergent properties is if you look for them early enough you will see them coming. Can we learn more from near-misses or tremors in the systems to be able to anticipate the black sky events?” he asked.

Panelists agreed that by better understanding the structure of these complex systems, their components and the relationships between them it could be possible to put in place early warning triggers suggesting that the system may be heading towards catastrophe.

Panelists also discussed the dangers of building vulnerabilities into the system. For example, although infrastructure hardware differs, if there are common software components and modules across different sectors then there could be massive, correlated failures under certain conditions. Testing and modelling are important for reducing these risks.

Mark Abbot from National Grid asked for an example nonfunctional interdependence in a potential Black Sky scenario. Neil Carhart cited as an example an incident a couple of months earlier in which pumping station failed and the area flooded, taking out an electrical substation next door. Though not a Black Sky hazard, this was a triggering event of the kind that has the potential to cause or exacerbate a much larger failure.

He referred to the engineering concept of functional resonance, explaining, “that is where a hazard can emerge when no component within the system has actually failed. Each component within the system has some kind of accepted tolerance of variability in its function. If those accepted tolerances happen to combine in a particular way, then the emergent property at the whole system level is that the whole system collapses.”

Sarah Mukherjee, Director of Environment at Water UK noted that all the panelists touched on the idea of collaboration but asked whether someone needs to take overall responsibility and if so, who? “We have found even when there is a critical moment, people still cling onto their hierarchies, and cling on to their little silos. Someone needs to help to break that down,” she argued. Brian

A hazard can emerge when no component within the system has actually failed. Each component within the system has some kind of accepted tolerance of variability in its function. If those accepted tolerances happen to combine in a particular way, then the emergent property at the whole system level is that the whole system collapses.

Collins agreed and replied that in his experience of the Iceland volcanic ash eruption episode, the British Prime Minister took responsibility and charged the Chief Scientific Adviser with making and executing a plan.

John Beckford, commented on the implicit assumption underlying the discussion "of the controlling mind somewhere, continuance of some form of central government that guides, governs, and makes all this possible."

> We have found even when there is a critical moment, people still cling onto their hierarchies, and cling on to their little silos. Someone needs to help to break that down,

Panel 3

Resilience, Systems, Risk and Perception

This panel examined different perspectives on the interplay of risk and resilience. John Beckford argued that in the infrastructure space we get what we incentivize and we incentivize what we measure. Over recent decades in the UK, efficiency has been the parameter that has been overwhelmingly measured and incentivized. Resilience is not measured, indeed we do not even know how to measure it. Resilience investment has, therefore, inevitably been neglected.

Miguel Centeno strongly concurred that today most of the political and economic incentives favour producing high performance "Porsches" rather than robust and resilient "Volkswagens." He argued that global infrastructure risk is an emergent property of complex, interconnected systems. "It arises," he argued, "from individual parts that are connected to the whole, but you can't be reduced to a single bad apple. It's the fact that you put all these apples in the barrel that creates the problem. Trying to regulate the bad apples won't help you because the real problem is the fact you're trying to put all these apples together."

He also listed some of the fundamental causes of global systemic risk, including "specialization of production, comparative advantage, diversity of consumption, much less on reserve, a low-inventory culture with high reliance on technology. You have the belief that tomorrow will be just like yesterday, the hubris of over confidence, silos of information, selfish behavior, the difficulty of modeling, moral hazard and malfeasance. All these possibilities combine to create the potential for a collapse."

Finally, Paul Larcey discussed risk perception in infrastructure from the perspective of project finance for developing world infrastructure projects.

Resilient Systems and Quality

John Beckford, John Beckford Consulting

John Beckford analyzed the strengths and weaknesses of modern infrastructure through the lens of how we measure what we expect infrastructure to do. “Our siloed fragmented infrastructure works remarkably well most of the time,” he declared. “But when we put it under stress it has a tendency to fail. One of the reasons it does that is because we get what we measure in our infrastructure.”

Efficiency has been the main goal for UK infrastructure over the past 30 years and consequently it is what managers attempt to measure. This is just one of the reasonable markers for assessing utility performance: “those of you who are directors of utilities will know that a director's obligation is to maximize return to the shareholders in the privatized utility, and we do that by managing our costs. We say we made this profit, this much surplus, this much return on investment, this much EBITDA.”

Outputs are measured by regulators who assess, for example that the water produced by a utility is clean and penalize those who fall short. Efficiency means producing the required outputs at a low cost.

In a regulated yet profit-oriented industry there are strong incentives to outsource risks, either by insuring them or by delegating responsibility for a risky area to an external supplier. In these ways risks are shifted out of the core areas of performance measurement, at the cost, however, of directly addressing them as part of the utility’s essential functioning.

> Our siloed fragmented infrastructure works remarkably well most of the time. But when we put it under stress it has a tendency to fail. One of the reasons it does that is because we get what we measure in our infrastructure.

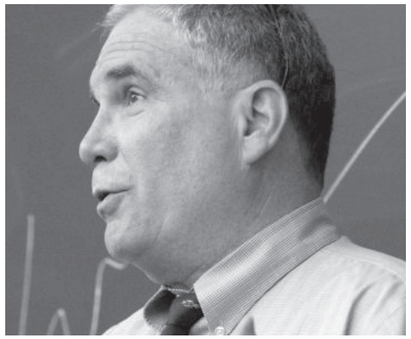
A better, more sophisticated approach, Bedford argued, would be to have an integrated, systematic understanding of how the different aspects of a utility’s functioning interact to produce either resiliency or vulnerability. This would require that we begin to measure and incentivize greater resilience which in turn would help us to build Black Sky resilient infrastructure.

Global Systemic Risk: A Research Agenda

Miguel Centeno, Musgrove Professor of Sociology, Professor of Sociology and International Affairs; Chair, Department of Sociology

Miguel Centeno spoke about global systemic risk. He endeavored to explain some of the acute vulnerabilities inherent in global interdependence. “We have been constructing the Global System for the last 30 or 40 years,” he warned. It is ever more complex, ever more demanding, essentially a tower of Babel. The tower itself will collapse.”

Centeno defined globalization as a complex system that is a set of tightly coupled interactions that together allow for the continued flow of information, money, goods, services, and people. “If you want to think about it, what we have constructed is a massive plumbing system spanning the entire globe, filling all sorts of various flows and reacting to one another.”



Centeno argued that some 20% of the world’s countries and the top 20% of the populations of other countries are entirely dependent on the effective functioning of multiple global networks. This engenders increasing social vulnerability in the face of any accidental or intentional disruption.

Centeno cited the economist Frank Knight’s well-known distinction between risk and uncertainty. Risk is quantifiable; uncertainty is not, because we do not where the uncertainty is going to come from.

Centeno identified emergent risk as a major source of global instability. This is not the same as the problem of how “does the bad apple, whether it's the stupid banker, the malfeasant terrorist, destroy the basket of apples?” Emergent risk, on the other hand results from interconnection. “It arises from individual parts that are connected to the whole, but they can't be reduced to a single bad apple. It's the fact that you put all these apples in the barrel that creates the problem. Trying to regulate the bad apples won't help you because the real problem is the fact you're trying to put all these apples together.”

> Emergent risk arises from individual parts that are connected to the whole, but they can't be reduced to a single bad apple. It's the fact that you put all these apples in the barrel that creates the problem. Trying to regulate the bad apples won't help you because the real problem is the fact you're trying to put all these apples together.

A further source of vulnerability is our heavy emphasis on efficiency rather than robustness. Centeno used the analogy of a Porsche compared to a Volkswagen Beetle. “A Porsche is a much more effective and more efficient system. If you were driving down a German autobahn,

you'd certainly want to drive the Porsche. If, however, you're trying to cross the Sahara, you're probably better off in a robust Volkswagen, which can be fixed with some duct tape and a stick. All our institutions are designed to build Porsches," Centeno claimed, "because that in a sense is what gets you the institutional and social rewards."

There are additional sources of uncertainty that are built into the system and do not require malfeasance or incompetence to create serious problems need malfeasance. One such source is normal accidents. As a system generates more tightly coupled, numerous interactions, the likelihood of an accident becomes more and more normal.

A Porsche is a much more effective and more efficient system. If you were driving down a German autobahn, you'd certainly want to drive the Porsche. If, however, you're trying to cross the Sahara, you're probably better off in a robust Volkswagen, which can be fixed with some duct tape and a stick. All our institutions are designed to build Porsches,

The vulnerability of interconnected, global systems to catastrophic collapse is, Centeno argued, "a wicked problem." Whereas capitalism is global, governance is local. Whose responsibility is managing the global system and where are the mechanisms that can do so? Centeno described the work of his team at Princeton in studying "the network of networks," to understand where critical vulnerabilities in the global system may lie. He noted that the global food system one of the key areas of risk. "In the pursuit of efficiency, the global food system has become ever more degraded and much more susceptible to some kind of catastrophic collapse… we're only three square-meals away from anarchy."

Centeno concluded with an incisive taxonomy of some of the common structure causes of global systemic risk. "We have specialization of production. We have comparative advantage. We have diversity of consumption. We have much less on reserve. It's a low-inventory culture with high reliance on technology. You have the belief that tomorrow will be just like yesterday, the hubris of over confidence, silos of information, selfish behavior, the difficulty of modeling, moral hazard and malfeasance. All these possibilities combine with the structural elements to create the potential for a collapse."

Risk Perception in Infrastructure Funding:

Paul Larcey, Department of Engineering, University of Cambridge

Paul Larcey discussed infrastructure risk from the perspective of the of project finance, with a particular focus on large infrastructure investments in the developing world.

There is a serious shortfall of global infrastructure, especially in the developing world. A McKinsey report shows that by 2030 there will be a 70 trillion shortfall in global infrastructure, of which the energy element is 13 trillion. There are many trillions of funds looking for double digit returns from infrastructure investments, but they are also seeking excellent risk mitigation and good liquidity. As Larcey put it, "If you're a fund manager or investor, you say, do I want to put a billion into this project which for the first three years is going to be a hole in the ground worth about 100 million, if I bought all the concrete and steel together."

Larcey, cited rapidly growing African countries such as Nigeria and Ghana that are starving for the electrical power that their economies need to grow. However, with poor planning, limited technical expertise and minimal access to finance solutions and structures in these countries, there is a shortage of bankable, de-risked infrastructure projects.

Larcey pointed out that the aftermath of the 2008 financial crash has worsened this situation. The new Basel III regulations that are designed to prevent a reoccurrence include higher capital bases for banks, decreasing of loan lengths redefining project finance as high risk. This has led to a decrease in bank financing of large infrastructure projects. Larcey was critical: "it's trying to paper over an issue these guys created, and the knock-on effect is going to affect the developing world in its financing of infrastructure."

If you're a fund manager or investor, you say, do I want to put a billion into this project which for the first three years is going to be a hole in the ground worth about 100 million, if I bought all the concrete and steel together.

New investors, in particular insurers, are starting to enter infrastructure finance now, "but they're not putting it into the parts of the world that truly need it," Larcey cautioned. The mismatch between investors seeking a 25-35% return and the projects available for finance is still wide.

Discussion
Resilience, Systems, Risk and Perception

Miguel Centeno stressed that systems can fail, “even if everything works as it is supposed to… even if there is no stupid person, no greedy person or no terrorist. If the system is so complex there's no way the various parts are well integrated. This is a classic example of emergence; a characteristic of the system that cannot be attributed to the individual parts.”

Avi Schnurr noted the point about incentives that drive in the wrong direction, to produce effective “Porsches” rather than resilient “Volkswagens,” for example. He asked whether it is possible “to agree to design Porsches or investment instruments that in principle look good, but have the capability of defaulting into a Volkswagen?”

Miguel Centeno responded that “some of that is achievable through modularity, where even if the system starts failing you can close out one part of it, and you can maintain say two-third of the system.” The major issue with incentives is that of time-discounting. Political and corporate incentives tend to be short term whereas successful resilience investment pays off over the long term. “We have to change that incentive structure so there is some robustness measure inside the incentive structure,” he stressed

John Beckford pointed out the formidable planning coordination problems of fragmented infrastructure. “Where you have siloed utilities trying to get them all in the room at the same time is difficult enough, let alone getting any of them to make a decision together.”

Systems can fail, even if everything works as it is supposed to… even if there is no stupid person, no greedy person or no terrorist. If the system is so complex there's no way the various parts are well integrated.

Brian Collins noted the problem of senior leadership turnover, another serious shortcoming in Western governments’ ability to undertake long term sustained resilience planning: “I think all of our developed countries have exactly the same systemic problem at the top, change of leadership and complete, not only loss of, but almost conscious destruction of corporate memory, which is even worse in some ways.”

Panel 4
Learning and Perspectives

This panel surveyed different models for individual and organizational learning that can help build societal resilience in the face of Black Sky events.

Ruth Deakin-Crick discussed learning for resilient agency. Resilient agency, she explained, is an essential capacity to develop in people who need to respond to crises. It consists in qualities such as flexible problem solving abilities, creativity and the capacity to identify with and act on the top-level mission of the organization. She argued that we know how to develop resilient agency In people and organizations; programs that do so effectively exist.

Gilead Shenhar described how Israel has, and continues to, inculcate resilience in its population after 69 years living with periodic, severe threats. Government works closely with all sectors towards this goal. School children are taught emergency drills from the age of ten and play an important role in educating their families. One of the most remarkable resilience learning institutions in the country is a week-long annual emergency exercise spanning all levels of society from the Prime Minister to the general public, some 60-70% of whom participate.

In the discussion speakers stressed the value of exercising emergency plans using vivid and realistic scenarios. Mark Abbot from the National Grid said, it's only when people start to see reality in front of them that actually they start to engage with it fully and start to understand.”

They also considered the role of the media in educating the public and the double-edged role of social media.

Learning for Resilient Agency for People, Supply Networks, Business Models; Resilience Dashboard

Prof. Ruth Deakin-Crick, University of Bristol and University of Technology Sydney

Professor Deakin Crick emphasized that a vital ingredient of resilient infrastructure systems consists in the resilience of the people who work in them. She made four points:

Firstly, she declared, “if we want to develop resilient infrastructure systems, then we have to develop resilient agency in the people who design, deliver, and use those infrastructure services. All data and technical systems are embedded in human systems, and are dependent on human decision making for their success.”

Secondly, we now understand more about what resilient agency looks like in people. It consists in qualities such as flexible problem solving abilities, creativity and the capacity to identify with and act on the top-level mission of the organization. In systems thinking, as she put it, the “why” of organizational mission becomes merged with the “how” of detailed execution. “We know how to develop it,” she stressed, “and significantly, to measure it.”

Thirdly, we can design learning systems, both human and virtual, which enhance and encourage the development of resilient agency in individuals, teams, and organizations. New techniques such as decisioning engines, social network analysis, and interaction, knowledge curation and rapid analytics, support such learning systems.”

Fourthly, “these learning systems can be integrated into business processes, so that learning and the development of resilience agency becomes part of business as usual, not only in business, but also in community, and can drive transformation and processes.” As an example, she cited an Australian water company that, rather than just following the normal regulatory framework, started asking employees questions about a particular leak. This led to uncovering extensive unmetered water and a gap between the construction company and the water company, where water was leaking that nobody knew about.

If we want to develop resilient infrastructure systems, then we have to develop resilient agency in the people who design, deliver, and use those infrastructure services. All data and technical systems are embedded in human systems, and are dependent on human decision making for their success.

In summary, she concluded, “we must attend to the development of resilient agency in people if we want resilient infrastructure services. We know what resilient agency looks like and how to measure it. And we can design it into our business and technical architectures.”

Lessons Learned over 68 Years in Israel: Developing a Resilient Society in a Constantly Changing, Threatening Environment

Col. (Res.) Gilead Shenhar, Spokesman of the Israeli Home Front Command

Colonel Shenhar explained how Israel develops a resilient society and population in the face of periodic emergencies He noted that the relevant threats include terror, war, chemical and cyber-attacks as well as the danger of earthquakes.

The two overriding goals are too save lives and for the economy to continue to function, so that

there will be food, health and communications. Some of the key elements of Israel's preparedness include training for the whole population, courses, a command-and-control system, emergency equipment and risk and crisis communication system.

Emergency preparedness involves many organizations, spanning government, including 255 local authorities, private sector, NGOs and volunteers who need to work together not just during the event, but also on advanced planning. "The goal is that every individual, family and community should always be ready to cope with emergencies," Shenhar emphasized.

Shenhar described the annual national emergency preparedness exercise that Israel conducts every year. "It starts from the Cabinet, all the government agencies, the private sector, local authorities and the population are all a part of it." He noted that 60-70% of the public fulfills the exercises that the Home Front Command requests of them during the exercise week, what we are asking them to do, resulting in a sharp rise in public awareness.

Shenhar also referred to his role as national spokesman for the Home Front Command. His responsibility is to ensure that the public has accurate information so that they know exactly what to do in order to reduce their vulnerability, and to save life. His job also includes combatting disinformation, "killing any rumours when they are small."

He noted the challenge of striking the right balance, for example during the 2014 Gaza war between "telling the people for 52 days, sit in a shelter and don't go out, and on the other hand, encouraging people to continue their normal life."

Shenhar stressed in conclusion that preparing a country for emergency scenarios takes a lot of time, as well as investment and effort from decision makers. "It doesn't just happen from today to tomorrow."

> The goal is that every individual, family and community should always be ready to cope with emergencies.

Tactical Lessons for Black Sky Resilience from the UK Energy Emergency Executive Committee (E3C) and Local Resilience Forums

Mark Abbott, Head of UK Resilience, National Grid, UK

Mark Abbot of National Grid UK described some of the resilience structures and initiatives in the UK power industry. As one of the largest utilities in the U.K. involved in electricity transmission, gas distribution, generation and with substantial assets in the North East USA, the National Grid is a major player in the power, oil and natural gas sector.

The coordinating group for power sector resilience in the UK is the Energy Emergency Executive, EEE, which comprises the Government Department for Business, Energy and Industrial Strategy, Ofgem the regulator, and National Grid. This group looks at the risks to supply of gas and electricity for consumers in the U.K.

Below that, there is a working group, consisting of about 25-plus groups from the U.K. government and industry "from upstream oil and gas through generation, gas distribution, electricity distribution and transmission, all the way through the supply chain of energy to businesses and premises." This body works on detailed emergency planning. Currently, there are seven task force groups, working from electricity and gas through to pandemic, cyber, and a new one around black start.

Abbot described another joint initiative the "self-purge and relight project." In a major disruption to gas in the U.K., with tens or hundreds of thousands of customers cut off from their gas supplies,

it is necessary to isolate the system and the turn it on customer by customer. With several hundred thousand customers that could take months. This group is putting in place some simple processes and procedures for customers to turn their gas back on safely.

Another piece of joint work addressing SCADA control systems is developing a lab to examine cyber impacts on infrastructure and try to improve the resilience of the technology to cyberattack.

The UK also has local resilience forums, regional resilience meetings and also a number of exercises that take place throughout the country involving multiple agencies.

In summary, Abbot concluded, "there are processes in place for identifying and mitigating risks and good collaboration throughout the energy industry, and at the community level. However, to deal effectively with a Black Sky event, engagement at the strategic level is needed."

"There are processes in place for identifying and mitigating risks and good collaboration throughout the energy industry, and at the community level. However, to deal effectively with a Black Sky event, engagement at the strategic level is needed."

Discussion

Learning and Perspectives

Avi Schnurr pointed out that a common theme of all the panelists was different types of learning. He asked whether there are specific approaches than can effectively encourage the kind of learning that will help individuals, communities and organizations to cope with Black Sky situations.

Mark Abbot responded that “the key thing for me is around the exercising. It's only when people start to see reality in front of them that actually they start to engage with it fully and start to understand.”

Gilead Shenhar added that while an exercise is a good opportunity to give the public information and raise awareness, awareness by itself is not enough.

Ruth Deakin Crick agreed that the right kind of exercising can be very helpful. “I think that authentic modeling and simulation is a key way of enabling people to think differently, to listen to different perspectives, and to take a more resilient approach in practice,” she said. She agreed with Mark Abbot that story telling is an important way of making scenarios and threats understandable in a way that is accessible to the public so that they internalize the important messages.

> The key thing for me is around the exercising. It's only when people start to see reality in front of them that actually they start to engage with it fully and start to understand.

Gilead Shenhar described how in Israel children from the age of ten begin learning to overcome different emergency scenarios. In this way they become educational resources for their families “We call the media first responders also,” he added. Through working in partnership with media outlets, rather than giving them orders, the media can play a crucial role in educating the public, Social media is a major opportunity but also a challenge; it has to be monitored for false information and rumours that need to be refuted before they gain traction.

Keynote Address

Infrastructure Decision Making, Stakeholder Engagement and Disaster Recovery

Professor Peter Guthrie, Professor in Engineering for Sustainable Development, Cambridge University

Peter Guthrie discussed a number of long-term trends and cultural issues around infrastructure that impact resilience planning.

He pointed out that while the shift from public to private ownership of infrastructure has increased efficiency dramatically, it also reduces strategic cooperation. Guthrie noted that, in the UK, "we're in the closing stages of a generation where the engineers, as they approach retirement, still have some memory of working in nationalized or quasi-nationalized industries. The impact of working in an only privatized world has yet to be felt in some of the utilities."

Guthrie expressed concern that this could cause a disappearance of the public service ethos that still survives in utilities: "There's a kind of cultural acceptance at the top level of a lot of utilities about a public good, which may not survive into the next generation," he said. Such a cultural change would make long-term investment in resilience more challenging.

He described how the transportation field is dominated by "the dogma of around moving away from private transport to public transport." This leads to building of very large, long-term infrastructure projects like the HS2 rail link in the UK that are inherently inflexible and lacking resilience. Guthrie suggested that there is a better alternative: "technology is now beginning to show us that driverless transport and automated trains and vehicles might get us to a position within a generation where we can have point-to-point personal transport."

He noted that even senior decision-makers have a poor appreciation for the critical importance of infrastructure. Guthrie referred to the World Economic Foundations most recent "Global Risks Report. The 500 top CEOs surveyed about the leading global risks tended to be very influenced in their assessment of risks by the particular events of previous 12 months. Guthrie reported that "the failure of critical infrastructure comes 25th on the list. While we all think that infrastructure is absolutely essential, it is in most decision makers thinking a second order problem. It will be the failure of infrastructure which leads to a risk which other people identify, but the essential nature of infrastructure in civil society is not well understood by people who run most of the rest of society."

> The failure of critical infrastructure comes 25th on the list. While we all think that infrastructure is absolutely essential it is, in most decision makers thinking, a second order problem.

Guthrie warned that "we need to be quite humble and chastened by that revelation because it means that the necessary investment to engage in resistance and resilience to black sky events around infrastructure is going to have to be quite a hard sell."

He also discussed challenges posed by stakeholder engagement around disaster recovery. He described research into the recovery after the 2011 Christchurch earthquake, New Zealand's worst ever natural disaster, which killed 185 people. Research found that trust in the authorities was at a peak in the immediate aftermath of the disaster. "The authorities, engineers, and Christchurch local government could have done almost anything in the immediate aftermath and it would have been trusted." A year later, however the community having survived this shock, started to question the decision. Two and three years later a lot of trust had broken down and engineers proposals for the rebuilding and recovery were stalled and blocked through the stake-holder engagement process.

> We need to be quite humble and chastened by that revelation because it means that the necessary investment to engage in resistance and resilience to black sky events around infrastructure is going to have to be quite a hard sell.

Closing Keynote Address

Professor Brian Collins, University College, London

Professor Brian Collins opened with a telling story about how we need to rethink the scale of the investments we make in key infrastructure resilience. Collins served as technical director of GCHQ, (the British equivalent of the NSA) at the end of the Cold War. At that time, management started to worry about the resilience of their capability to run the mission of GCHQ. So they undertook a survey of GCHQ's resilience posture against, not only what was then a very primitive form of cyberattack, but also against physical attacks, including bombs, etc.

Collins recalled standing outside the GCHQ datacenter which had in those days about a quarter of a billion pounds worth of IT equipment, and insisting to a colleague "that it had to run 24/7 - otherwise you and I are coming to Number 10 to explain to Mrs. Thatcher why she just lost the signal intelligence capability for the country." He looked up a hill and noticed a large concrete wall behind which was a reservoir containing half a million gallons of water. "One bomb in the right place," he realized, "one breach of that wall for whatever reason and I'd lost my datacenter."

We must start thinking about some of those big numbers that we heard earlier in the day, the trillions, and how much we're currently doing in terms of preparedness, which is in hundreds of millions. That ratio is not in the right place.

GCHQ paid for the considerable cost of moving the reservoir to remove the far greater risk to its critical facility, "because you can't compare those two numbers."

Drawing the contemporary lesson for infrastructure protection, Collins argued that given the huge stakes, we must invest much more in resilience. "We must start thinking about some of those big numbers that we heard earlier in the day, the trillions, and how much we're currently doing in terms of preparedness, which is in hundreds of millions. That ratio is not in the right place."

Collins went on to stress the importance of the health sector as part of critical infrastructure. He warned, "if infection rates get to a certain level and that number of people are not at work, then, for people who normally travel to get to work, that really does affect their productivity. So the resilience of the human system in the large is very important."

He also touched on the importance of human resourcefulness in the recovery process saying, "It's the ability to maintain a sense of momentum about recovery. That's a leadership issue. It's about leadership that stands up and says "yes, we can do this", that keeps pushing people to do things which they might otherwise regard as impractical." He connected resourcefulness to innovation: "People who are innovative in their marketplace or in delivering public goods may suddenly have to turn that innovative capability inwards to make the resilience and recovery of whatever it is in front of them better oriented."

Building resilience is essential but not head-line grabbing work. "You don't tend to cut ribbons for having done the business case for generating an extra two million pounds for maintaining something. It's not a media-worthy issue so it tends not to be a politically worthy issue," Collins noted.

Collins also stressed the importance of political leadership, particularly in major cities. "City leadership could be more important than national leadership," he predicted. "I think we're on the cusp of one becoming more important than the other." Collins cited Singapore, a nation-city-state as an interesting model for resilience planning.

He emphasized the importance of emergency exercising and the potential usefulness of gaming theory and software, including new simulation technologies that allow for mental, aural and visual immersion in emergency scenarios. (EIS Council's upcoming Earth Ex exercise, taking place in August 2017 will provide such an opportunity for utility managers across sectors to engage with a simulated Black Sky situation.)

It's about leadership that stands up and says yes, we can do this, that keeps pushing people to do things which they might otherwise regard as impractical.

Collins further observed that "inter-sectoral interdependency and resilience are poorly understood from a systems point of view. We divide things up in order to make it possible to account for them, and to circumscribe the risks that we might have by engaging with them. Silos and sectors is a language that really gets in the way of talking about this subject."

He concluded with a call for cross-sector and international cooperation to address threats to critical infrastructure, noting that UKCRIC, the U.K. Collaboratorium for Research on Infrastructure and Cities, between 14 universities needs to collaborate with other nations, with industry, with government, with educators in order to get the most from its research investment.

You don't tend to cut ribbons for having done the business case for generating an extra two million pounds for maintaining something. It's not a media-worthy issue so it tends not to be a politically worth issue.