Electricity Infrastructure Security Council – Written evidence (RSK0099)

Requirements and Opportunities for UK Societal Sustainment in Complex Catastrophe Events

Addressing critical resilience gaps in today's tightly interdependent infrastructure, resource and supply chain networks

"Complex systems are disrupted if any of their components fail."

- California's Office of Emergency Services, summarizing the fundamental, new systemic vulnerabilities introduced by heavily interconnected lifeline infrastructures and the industrial base that supports them.

I. Background

The infrastructures, utilities, global supply chains and resource networks that sustain the UK and other modern nations represent a new and extraordinarily complex, tightly interdependent system: a "meta-grid" that has brought with it unprecedented capabilities. But these interdependencies have also brought a new class of vulnerability: the risk that a major crisis in one sector could cause cascading failures in all other sectors, disrupting society's infrastructure bedrock on massive geographic scales.

The tragic worldwide impact of COVID-19 has given us a hint of this new risk. And in addition to future, potentially even more dangerous pandemics, the meta-grid could be severely disrupted by a range of other natural and manmade hazards:[1] Extreme terrestrial or space weather, focused infrastructure attacks, large scale cyber or EMP attacks and others.

As the interdependencies spanning business sectors and supply chains become ever tighter, the thresholds at which such "Black Sky"[2] hazards could cause catastrophic, cascading infrastructure breakdown are falling. Without diligent, collaborative public and private sector resilience planning and investment, this emerging reality will mean unacceptable, unrecoverable risk to societal continuity in communities across the United Kingdom.

Over the last decade, the Electric Infrastructure Security (EIS) Council, a US-based international nonprofit resilience research and planning hub, has hosted high level, focused working groups to help define the most critical resilience gaps and solutions, working with operational leaders from many sectors and nations. The material provided below is designed to summarize some of the most important, current assessments of this effort.

---

[1] "Black Sky-class" hazards: Highly disruptive natural or manmade events that could cause multi-week or longer cascading infrastructure failures, on national or subcontinental geographic scales.

[2] Ibid.

II. Critical Black Sky-class resilience gaps and solutions: Research highlights

Research Conclusion: *Two classes of resilience preparations are required to ensure continuity of the rapidly changing, modern, tightly interconnected infrastructures that sustain communities in the UK.*

Preparations for relatively short duration, conventional crises*: Typically managed with conventional, widely available emergency resilience capabilities and tools.*

Preparations for Black Sky-class[3] catastrophes: *Recoverable, but only if decision makers have invested in the unique resilience capabilities and tools that will be essential in such scenarios.*

A key question that must be addressed: Does the UK wish to be capable of surviving Black Sky-class scenarios, based on affordable but diligent preparations? The recommendations below become relevant if public and private sector leaders conclude that the answer to this question is "yes."

A. Essential Black Sky-Class Resilience <u>Capabilities</u>:

Critical Emergency Supplies and Services

The capabilities summarized here are meant to be representative of broader requirements, and should not be construed as comprehensive. Nevertheless, the specific items shown summarize particularly critical elements of such a comprehensive plan, and are thus offered as an initial, crucial priority.

1. Basic emergency generation and fuel

For conventional, relatively short-duration hazards, critical resource and supply chain facilities critical to sustaining communities, people and the economy require adequate emergency generation capability to maintain basic functionality.

Generators should be cyber and EMP protected, and located well above the local maximum flood plain, with provisions for regular maintenance, testing and personnel training.

On-site emergency fuel/energy storage should provide for continuous operation of at least 7 days. Actual stored fuel/energy quantities may vary for different facilities. However, water systems that depend on electricity to pressurize pipes

---

[3] **Black Sky-class catastrophes**: This refers to complex catastrophes associated with seven hazard classes which, if occurring at sufficiently extreme levels, could cause widely distributed damage of bulk power systems and other utilities, resulting in multi-region, extended power cuts (weeks to months) and cascading failures of other critical infrastructures. Hazards that can fall into this class include severe cyber or EMP attacks, kinetic attacks on key infrastructure facilities, extreme pandemics or solar storms, or extreme terrestrial weather. Of particular concern is the potential for malicious attacks to be launched concurrent with natural disasters, complicating recovery.

and treat water and sewage must ensure their fuel supplies are adequate for a one-week minimum, with a goal of two weeks.

2. **Supplemental Prioritized emergency power (PEP)**

In addition to the basic emergency generation system, all critical facilities should include a small emergency power system, typically <<5% of the size of the basic emergency generation system, designed with prearranged voltage regulators, transformers and related equipment to provide continuous emergency lighting to the key facility center and continuous power to the most critical instruments, communication devices etc.

This system should be sized to allow for multi-hour operation with an embedded battery pack, with a small external generator (e.g., propane) with adequate fuel to continue recharging the battery pack for at least 30 days.

3. **National Emergency Fuel Supplies**

For the UK to be capable of recovering from a (typically multi-week) Black Sky-class event, a national emergency fuel delivery plan will be required, with embedded planning for hardened refineries, fuel storage and distribution to designated public and private sector emergency facilities.

4. **National Emergency Food and Pharmaceutical Supplies**

Similarly, since basic food and pharmaceutical supply chains will typically be disrupted in a Black Sky-class disaster, arrangements should be made to incentivize major food and pharmaceutical corporations to harden at least a substantial fraction of their basic production, storage and distribution systems, to be capable of surviving the full set of Black Sky hazards.

5. **Critical national spare parts inventory**

In the event of a serious Black Sky event, widely distributed damage of power grid facilities and other key utilities is one likely consequence. Planning for restoration from such disruption requires prepositioning regional, well-maintained stores of replacement components and systems, with continuing product flow-through, as older inventory is sold to users to make way for updated inventory to keep products current. Listings of equipment to be included in this system will require input from utilities and other critical facility stakeholders.

6. **Preplanned emergency transportation measures**

In a Black Sky scenario, as the duration of the catastrophe expands, people will begin looking for opportunities to escape megacities. Even small changes in traffic patterns can cause gridlock, and maintaining continuous through-ways for critical supplies and services will be essential to sustain such urban areas. This will require advance planning by government agencies to secure lanes on highways and other predesignated routes.

7. **Black Sky hazard protection**

Although prearranged Black Sky-class resilience capabilities and tools will be essential in such scenarios, these can only help in sustaining an affected population if basic protection measures are taken by critical utilities to address the full set of Black Sky hazards. Thus, for example, power grids, water utilities and emergency communication systems all require best-in-class, affordable protection against the expanding Cyber threats, EMP or IEMI events, kinetic attacks to critical grid nodes, and extreme pandemics and solar weather.

8. **Critical personnel resource planning for a highly disrupted environment**

While infrastructure protection to minimize damage, coupled with preplanned key Black Sky-compatible capabilities and tools will all be essential, they can only be useful if there are sufficient trained, expert personnel available to work through the restoration process in each affected infrastructure. Such experts are typically a scarce resource in normal times, since human involvement in design, repair and related activities is increasingly being replaced by expert systems.

In a complex catastrophe however, such people will become a critical resource. Attention should be paid to allocating appropriate resources to expand the availability of such personnel in key industries, to improve their availability when critically needed in extreme disasters.

Essential Black Sky-Class Resilience <u>Tools</u>:

1. **All-hazard-scenario emergency communication**

Problem

Extended, multi-region power cuts are the most fundamental disruptions associated with Black Sky hazard scenarios. Such disruption, in turn, quickly shuts down most normal means of communication, making restoration and recovery actions almost impossible.

Even when individual corporations or government organizations have effective, internal emergency communication systems that can continue operating, the inability to connect to critical resource and service suppliers, critical interdependent utilities or facilities, government agencies and geographically distributed stakeholders poses an insurmountable obstacle for such events.

For example:

When the scale of a blackout becomes large enough, restarting and restoring the grid will take weeks or months. Yet existing communication systems can only operate for hours or a few days in a blackout. Without communication spanning all relevant facilities, suppliers and other services, grid restart and restoration will not be possible.

In fact, power cuts thus far have been limited in scale, so grid restart (technically, grid "black start") has never been necessary, and existing emergency communication systems have been adequate for the critical initial phase of restoration. Power industry leaders have advised us that in a large-scale blackout, the core grid restart effort will take far longer. It will not be possible without an all-hazard, widely deployed communication system that can continue to operate for days or weeks without grid power.

Solution

All-hazard protected, IP-based communication systems that establish self-forming networks with essentially unlimited scalability could be widely deployed to key decision makers across both the corporate and government landscape.

Architectures and off-the-shelf hardware solutions meeting such requirements now exist. For example, finding and initial deployment of such a system has been a primary objective of EIS Council for more than five years, resulting in successful, early phase deployment of one such system (BSX®)[4] in utilities and power companies in the US and Israel.

2. Black Sky-compatible situational awareness and AI-based decision support

Problem

In a long duration, multi-region scale blackout, recovery will only be possible with machine-enhanced decision support and excellent, real time, multisector situational awareness.

With our tightly interdependent utilities and infrastructures, any hope of preparing for or dealing with complex catastrophes will require excellent, real time information on the interdependent status of all relevant supply chains and service providers. This would be provided in the context of multicorporate simulations that continually update the relevance of that information, and recommend critical actions. Yet few companies are willing to share their private data, which has become a key problem that, until now, has blocked any progress toward developing such a capability.

Solution

The fundamental requirement needed to address this problem is development of an AI-enhanced crisis decision support and situational awareness multi-corporate operating system that can interlink the operating systems of essential corporations and government agencies in both advance crisis simulations and in real time catastrophe scenarios – and do so without requiring proprietary data sharing.

In addition to all-hazard emergency communication, this represents one of the most serious resilience shortfalls for our modern, hyper-connected industrial society, and finding a solution has been a high priority objective of EIS council for more than three years. The result was initial development work on

[4] For more information, write info@eiscouncil.org

GINOM®, a state-of-the-art multisector simulation (a multicorporate operating system), representing a new approach designed to avoid the pitfalls of previous, large scale but failed attempts to develop "mega-models" that would attempt to build a single, massive model that duplicates and continually updates all relevant corporate operating systems and data. The initial baseline design met all the fundamental requirements but one – at some level, all participating entities would need to supply updated proprietary information, at least during a catastrophe.

Last year, building on GINOM's baseline design, an innovative, unique capability was developed (now patented) that resolves this roadblock, and early development has been proceeding, utilizing multiple government and foundation grants. This new approach will make it possible to *functionally integrate* the operating systems of any number of utilities, suppliers, and other corporations, and to do so in a way that does not require any sharing of proprietary data.

May 2021