In the Polycrisis Era, Infrastructure Defenders Need to Broaden, not Tighten, Their Focus

Andrew Bochman[1]

[1] Senior Grid Strategist, Idaho National Laboratory Homeland Security Directorate, andybochman@gmail.com

Abstract

Marked by multiple concurrent overlapping and interconnected challenges, the Polycrisis Era portends an unprecedented mix of threats to infrastructure protection and demands more resilience planning and preparation than ever before. This article explores some distinct facets of the Polycrisis Era, tracing its emergence, its unique characteristics, and the societal implications of failing to adequately address these challenges. Importantly, the case is made that infrastructure defenders in the operational technology (OT) cyber space and those primarily concerned with physical climate risks should consider enhanced communication and collaboration with each other. Put another way, in an age of simultaneous, interwoven crises, it is advantageous for infrastructure defenders to think beyond their traditional domains. In order to examine this topic and to facilitate productive collaboration, an exploratory typology is advanced.

The Polycrisis Era

From wars and industrial revolutions to the dawn of cyber threats, infrastructure defense has evolved in tandem with the nature of challenges faced. However, the evolving Polycrisis Era is distinct, marking an epoch of compounded and multifaceted vulnerabilities. The term "Polycrisis" denotes a period characterized by multiple, overlapping crises. These are not isolated incidents but are interconnected, often exacerbating each other. As early as five years ago, the National Academies of Sciences, Engineering, and Medicine predicted some of these challenges:

> Climate change and extreme weather grab headlines and present a fundamental challenge to the ability of infrastructure to protect communities. But beneath the seemingly endless cascade of catastrophes lie consistent, systemic failures in current approaches to infrastructure. One common failure is an overconfidence, bordering on hubris, in the ability to tightly control complex social

doi: 10.18278/jcip.4.1.6

> and ecological systems through the management of technological systems. Another is the failure often associated with managing interdependent infrastructure systems. And there are failures in the ability of institutions that manage infrastructure to generate, communicate, and utilize knowledge.[1]

What differentiates this era from the past includes, but is not limited to:

- *Complex Interdependencies*: Crises are no longer isolated. For instance, climate change intensifies natural disasters, which in turn disrupts socio-economic systems and challenges digital infrastructures. As global temperatures rise and weather patterns shift, the intensity and frequency of natural disasters such as hurricanes, floods, and wildfires have notably increased. These environmental calamities don't just wreak havoc on the natural world; they also severely disrupt socio-economic systems, causing dislocation, impacting supply chains, and challenging critical infrastructures—including high priority digital networks. In the tightly knit global landscape, it is evident that challenges in one domain can have cascading effects on others, prescribing the need for more comprehensive solutions.

- *Rapid Technological Advancement*: The rate of technological innovation, while beneficial, has introduced a slew of vulnerabilities. These vulnerabilities, especially in our increasingly interconnected digital networks, pose compound threats. For example, cyber-attacks can destabilize power grids.[2] When such critical infrastructures are compromised, the cascading effects may be profound, impacting vital sectors like healthcare and transportation, potentially leading to widespread disruptions and crises.

- *Economic Repercussions*: A single crisis—whether emanating from the OT cyber side or a major climate disaster—can snowball into global economic downturns, leading to unemployment, inflation, and societal unrest. Economies are more intricately interwoven now than ever before. A disturbance in one sector or region can have a domino effect, leading to global financial downturns. Examples from the 2008 financial crisis or the economic impacts of the COVID-19 pandemic serve are harbingers of the cascading impacts we will witness in this new era

[1] Rethinking Infrastructure in an Era of Unprecedented Weather Events, National Academies of Sciences, Engineering and Medicine, Winter, 2018.

[2] This risk will become greater still as the U.S., fueled by federal funds from the Bipartisan Infrastructure and Inflation Reduction Act, will stimulate enormous amounts of new distributed energy resources (DERs). These will be deployed over the next five to ten years. Otherwise known as inverter-based resources (IBRs), inverters are sourced almost entirely from the U.S.'s main cyber adversary: China. So as we make DERs responsible for a higher percentage of generation, we will also potentially be enabling China to hold that higher percentage at risk.

- *Societal Fragmentation*: Discontentment stemming from unaddressed crises can result in polarization, mistrust in institutions, and potential civil unrest. Simultaneous crises have historically produced societal discord, leading to a rise in extremist ideologies and a breakdown of social cohesion. An underlying sentiment of inequality (real or perceived), gets exacerbated, leading to larger rifts in society, and if anything, AI promises to sow further distrust.

- *Environmental Degradation*: Beyond the preservation of critical infrastructures, ignoring the environmental components of a polycrisis might lead to irreversible ecological damage, impacting biodiversity and human survival. Climate change-induced natural disasters, coupled with infrastructural collapses, can wreak havoc on ecosystems, making regions uninhabitable, leading to the mass migration of both humans and wildlife.

- *Socio-political Tensions*: Geopolitical discord, stemming from territorial disputes, ideological differences or other factors, can escalate into crises where the attack surfaces of adversaries are exploited in a highly concentrated fashion. Supply chains can be severely impacted. Whether launched by state-sponsored entities or groups affiliated with particular governments, cyberattacks may target a nation's critical infrastructure, impact large regions or metropolitan areas, or spread misinformation to destabilize societies. It is axiomatic that state actors will attempt to hijack sensitive data to gain strategic advantages. As the digital realm increasingly joins with the physical, addressing such threats requires wholistic, cross disciplinary thinking.

Black Skies and Black Swans

I first met Dr. Paul Stockton at the 2018 Winter meeting of the National Association of Regulatory Utility Commissioners (NARUC). Paul had previously served as Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, where he was responsible for Defense Critical Infrastructure Protection, Western Hemisphere security policy, domestic crisis management, continuity of operations planning, and a range of other responsibilities. He served from 2009–2013 with distinction, but, by far, his greatest test came in the form of a hurricane named Sandy, a so-called superstorm.

As one climatologist put it, Sandy "was a hurricane wrapped in a nor'easter"[3] which produced a storm more than 1,000 miles across with a super powerful punch. Paul's job in October 2012 was to hold things together, as best he could, keeping food and fuel flowing not just to Department of Defense bases, but playing his part orchestrating restoration of energy and water services up and down the eastern seaboard. At the NARUC meeting, drawing from lessons from San-

[3] https://patch.com/new-jersey/tomsriver/not-just-hurricane-what-made-sandy-superstorm

dy, Paul addressed disaster preparedness and the implications of extended power outages. Called “black sky” events, these are outages lasting a month or more that affect multiple states. They have the potential to turn natural or human induced disasters into catastrophes. No matter their cause—weather, cyberattack or terrorism—no one wants to have experience a black sky event, but they must prepare nevertheless. In a supporting document he added:

> Commissioners also face the risk of outages lasting even longer and covering a wider area than those caused by Sandy. A range of natural and manmade hazards could create “worse than Sandy” events. Federal and State emergency management agencies are treating preparedness for such catastrophes as a rapidly growing priority. These extraordinary and hazardous events will pose special risks to the resilience of electric utilities. Accordingly, State Commissions may wish to proactively consider assessment frameworks for investments in resilience that are structured to account not only for Sandy-scale major outage events, but also for black sky days.[4]

And indeed, most infrastructure defenders would admit that the longer duration events Stockton spoke of in 2014 are, if anything, even more likely ten years hence.

Another type of darkness we’d prefer not to encounter is the oft-referenced *Black Swan* event. A book on response strategies and the psychology of disaster preparedness by Nassim Nicholas Taleb, addresses rare outlier events having catastrophic impact. Central to his thesis is the perspective that we should not attempt to predict Black Swan events, but rather to build robustness and resilience regardless of this type of extreme event or its timing—sounds at first blush like resilience to all hazards.

Taleb’s guidance syncs well with the left of boom-right of boom construct developed in the context of improvised explosive devices (IEDs) in Iraq that wreaked havoc on U.S. soldiers. The “boom” referred to the explosion. Efforts developed to detect roadside bombs and to disrupt the insurgents before they armed and planted them became known as left of boom activities.[5] On the other side, a variety of specialized skills were formulated to make progress on “IED Defeat.” The technicians and soldiers who devised those techniques, married expertise from a range of disciplines, including explosives, chemistry, communications, cybersecurity, and physics. The challenge demanded mental agility and flexibility in evaluating candidate approaches.

[4] https://pubs.naruc.org/pub.cfm?id=536F42EE-2354-D714-518F-EC79033665CD

[5] https://leftofboomconference.com/

Critical Function Assurance: Finding the Hidden Vulnerabilities Left of Boom

Developed at Idaho National Laboratory (INL) in collaboration with partners, while initially intended for cybersecurity risks from top-tier adversaries, Critical Function Assurance (CFA) is a proactive and purposefully cross-discipline strategy. It identifies an organization's vulnerabilities and mitigates them before they become liabilities. In some important respects, CFA is the art of finding an organization's Achilles Heel, and then doing something about it before Paris' arrow strikes. It seeks to prioritize risk based squarely on impact, not probability. That is accomplished by determining how an organization's most critical, mission-supporting functions are delivered. In so doing, it reinforces a focus on what matters most and illuminates overlooked sources of risk. As the INL team defines it:

> CFA is an approach to prioritize and address risk based on impact and is rooted in a holistic understanding of how critical functions are delivered. It provides rapid focus to what matters most and illuminates elements and areas of risk that otherwise are often overlooked. This focus enables effective application of available security resources to the most vital areas of a business/mission/entity and provides the foundation for optimizing greater security strategy and policy efforts.[6]

Today we increasingly rely on digitization and cloud services to increase efficiency, but this reliance also creates complex technological dependencies. Consider the supply chain disruptions that have recently roiled manufacturing operations, and the present and increasingly disruptive impacts of climate change—each presents its own constellation of challenges. Whether it's a ransomware attack compromising a firm's financial system, extended heatwaves affecting data centers, or malign actors targeting a nation's electrical grid, critical infrastructure defenders must anticipate a growing volume of significant threats and prepare for them well in advance.

Digitization and cloud services are making companies more efficient but at the cost of making them more dependent on other organizations and increasingly complex technologies. These factors will compound by orders of magnitude when AI technologies permeate operations. At the same time, climate change is driving rapid onset extreme weather events like heatwaves, wildfires, floods and freezes, as well as slower moving droughts, melting permafrost, and coastal inundation from sea level rise.

[6] Gellner, J., et al. 2023.

Staying One or More Steps Ahead of Disaster

From the perspective of an individual organization, it is difficult-bordering-on-impossible to know in what form disaster will strike, but here are some candidates:

- Ransomware bricks a billing system and it turns out that back-up files didn't include the necessary configuration information. And paying off the attackers didn't work when they took the money and disappeared.

- A two week-long heat dome that shutters a primary data center(s) neutralizes the ability to serve on-line customers which account for 80 percent of sales

- The same extreme heat event melts runways so that air carriers have to reroute for weeks

- A company that owns hundreds of data centers projects that the water they depend on for cooling will become scarce due to drought in several operating regions

- A region's electric grid and many of the larger generation plants and key substations have been immobilized by coordinated physical and cyber attacks.

While these situations may sound hopeless, and others marginally manageable, the main point about CFA is that it aims to make conditions "less bad" in the face of a crisis. As former DHS executive and presidential advisor Juliette Kayyem says in *The Devil Never Sleeps: Learning to Live in the Age of Disasters*:

> "Every institution has the capacity to assess its single points of failure, to assume that the last line of defense is not that, and then focus on avoiding losses that are not inevitable."[7]

She forcefully makes the case for a broadened perspective among all infrastructure defenders:

> Despite best efforts, the "boom" will arrive. The boom may be a crack, a surge, an electric fizzle, a howl, a deadly quiet. They are all booms: disaster management is about being ready for any boom in any shape, for whatever the devil brings. This concept, known as *all hazards* planning, does not focus on one specific hazard but instead on all of them. Some specialized threats may need specialized reactions—a fire is, in fact, different from a cyber-attack—but fewer specialized reactions than we may think. Accepting both the commonality and the frequency of disasters on the few key skills needed to manage them rather than highly specialized measures

[7] Kayyem, J. *The Devil Never Sleeps*. 2022. P. 108.

> that belong to limited environments. Beings can be slow or fast, wet or dry, hot or cold, silent or loud, visible or invisible. It does not, it should not, matter. It will come. So, we must focus on the right-of-boom activities, which are all those things we do to respond, recover, and build more resilience once the devil has arrived, again.[8]

Thus, another dimension of CFA is not about absolute prevention but is more attuned to enhancing an organization's crisis response. As Kayyem concludes, every entity (though few do comprehensively) can identify its most profound vulnerabilities, eschew over-reliance on final defenses, and strive to prevent avoidable losses.

Exploring the Cyber and Physical Climate Interface in Polycrises

Defenders need to open their risk apertures. Based on the foregoing, regardless of where we sit on critical infrastructure defense continuum, we all need to get into the Mission Assurance space. We would then be Mission Assurors—determined, and equipped to confront any and all hazards, proactively and reactively. This necessitates leveraging our primary areas of expertise, but also extending our capabilities well beyond the threats we were first trained on.

A clear-eyed approach that enables all mission assurers to expand the breadth of their situational awareness and proficiencies is required. For example, infrastructure defenders in the OT Cyber space and those primarily concerned with climate risk should consider enhanced communication and collaboration. From a different vantage point, in an age of simultaneous, interwoven crises, it is advantageous for infrastructure defenders to think beyond their traditional domains.

In order to examine this topic and to facilitate productive collaboration, an exploratory typology is presented in Figure 1. It is intended to reveal areas where selected defender skills and capabilities may be transferable to other threat categories.

Two infrastructure defense domains that have much in common are OT cybersecurity and climate physical risk, via resilience (asset hardening) and process adaptation strategies. While these initially may seem to be so different in kind as to render any comparison unproductive, the types of knowledge and skills defenders require for success are substantially similar. Perhaps the two most important resources that can be brought to bear against both threat types are a deep understanding of the characteristics of the system(s) being defended, as well as experience gained from defending similar threats in the past. There are additional areas of overlap, however, where defender capabilities in cyber scenarios might be cross-applied to climate physical risks, and vice versa.

[8] Kayyem, J. *The Devil Never Sleeps*. 2022. P. 11.

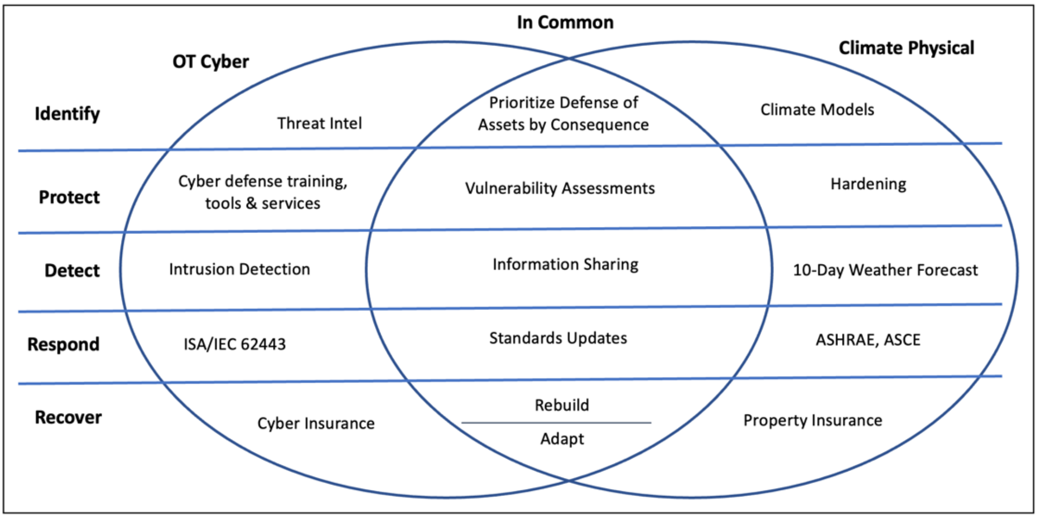

Figure 1: OT Cyber/Climate Physical Venn Diagram

Figure 1 draws its structure from the original NIST Framework[9] for cyber defense in the left-most column breaking the challenge into five, roughly discreet, roughly sequential tasks: identify, protect, detect, respond, and recover. Of course, the activities required to successfully defend against cyber attacks conducted by human actors are quite different than those necessary to thwart the physical forces generated by a warming atmosphere and ocean. Yet they do share some similarities that may be leveraged to good effect:

Identify

What mission are you trying to protect? What are the critical functions that must not be allowed to fail and what, in terms of people, process and technology, enable them?

Protect

What defensive strategies can be deployed to make the adversary's job more difficult in the case of cyber, or to ensure that infrastructure elements can withstand and continue to operate in the face of more-extreme natural conditions? In the case of the former, some basics like closing unused ports, segmenting networks, employing robust access controls, and granting least privilege authentication rights are significantly helpful.

For physical climate risks like floods, fires, freezes and extreme heat events, an assortment of engineered "hardening" strategies available like elevating equipment in flood-prone areas, undergrounding or fireproofing equipment in loca-

[9] https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

tions with above average wildfire potential, and winterizing systems to operate reliably at temperatures below or far below previous lows.

Detect

Is it possible to see the threat coming before it actually arrives, as in threat intelligence for cyber and downscaled climate model projections for physical climate risk? The answer to both is yes, with varying degrees of certainty and time to prepare. In the case of cyber, it could be as long as years once a particular attack type or vulnerability exploitation surfaces in the wild, or as brief as just a few seconds. On the other hand, methods for determining the likely arrival date of more damaging climate forces is a problem being worked at science labs around the world. Here the timeframes can be measured in decades, though any particular event (e.g., severe storm, flood, heat dome, etc.) may arrive with only a few days warning by meteorologists.

Respond[10]

There are a number of actions that can be conducted in the event of imminent or near-imminent cyber or climate threats. The concept of "conversative operations"[11] prompts organizations to prioritize resilience even at the expense of efficiency, profit maximization, and even full-services delivery if the threat is perceived to be significant enough to warrant such actions. In cyber this may mean isolating and/or greatly reducing access to the most critical systems. Physical climate risks can be met in ways as familiar as the boarding up of windows on a residential scale, to de-energizing power lines deemed likely to blow over during high wind events in areas with where they might trigger wildfires. In both cases, communicating the inbound threat to governmental and private sector support organizations is crucial.[12]

Recover

Depending on the degree of damage incurred, this phase includes both the restoration of services as quickly as possible, plus taking time to learn from the event to then apply lessons learned to strengthen activities conducted and capabilities achieved in the framework's earlier phases.

[10] The term "respond" obscures the proactive intent of this framework element. It's more about implementing the last lines of defense—potentially operationally limiting actions that bring a higher degree of confidence that an organization will "weather the storm" even if in a degraded fashion, and hasten the return to normal operations.

[11] https://www.jhuapl.edu/sites/default/files/2022-12/PostCyberAttack.pdf

[12] For example, in the energy sector, the Electricity Information Sharing and Analysis Center, or E-ISAC is one such communication and coordination hub, and there are other sector-specific ISACs.

Conclusions

While domain-specific skills are required to prepare for and conduct defensive operations for the two threat types discussed, there are also opportunities for collaboration across specialized defender communities. Since that is the case, then perhaps defenders against other threat types may find similar benefit in coordinating and drawing support in times of need from still other domains. Examples might be found within an organization, as technical SMEs address an imminent or ongoing cyber attack by reducing automation, others might shift to perform those functions in a mode closer to manual operations. This could be the case when other hazards arise, such as earthquakes, solar storms, or as Ukraine has demonstrated, even when critical infrastructure is subjected to continuous kinetic attack, as evidenced by its electric grid's resilience under bombardment.

Author Capsule Bio

Andrew Bochman is Senior Grid Strategist for Idaho National Laboratory's (INL) National and Homeland Security directorate. Mr. Bochman provides strategic guidance on topics at the intersection of grid security, the Energy Transition, and infrastructure climate resilience and adaption to senior U.S. and international government and industry leaders. A Non-Resident Senior Fellow at the Atlantic Council's Global Energy Center, in 2021 he published *Countering Cyber Sabotage: Introducing Consequence-based Cyber-Informed Engineering*. He began his career as a communications officer in the U.S. Air Force, and, prior to joining INL, was a Senior Advisor at the Chertoff Group and the Energy Security Lead at IBM. Mr. Bochman received a BS from the U.S. Air Force Academy and an MA from Har-vard University.

He is currently working on a second book prospectively titled *Defending Civilization: Stories from the Fronts Lines of Critical Function Assurance*. It applies the Critical Function Assurance risk reduction approach to four distinct but overlap-ping digital and physical threat types to critical infrastructure: Cyber, AI, Climate, and Kinetic, with the latter emphasizing lessons from Ukraine. These include how to design, build and operate electric grids and similar infrastructure components under bombardment. Infrastructure operators and defenders and multiple stake-holder types will find lessons for application with as much alacrity as possible. Publication is anticipated in late 2024 or early 2025 by Taylor & Francis / CRC Press.