Risk Analysis

WILEY

ORIGINAL ARTICLE OPEN ACCESS

Globally Critical Infrastructure: The Unique Risks and Challenges

Zachary Kallenborn[1,2,3,4] | Henry H. Willis[5,6]

[1]Department of War Studies, King's College London, London, UK | [2]Emerging Threats Group, University of Oxford, Oxford, UK | [3]Center for Strategic and International Studies, Washington, USA | [4]Schar School of Policy and Government, George Mason University, Arlington, Virginia, USA | [5]RAND Center on AI, Security, and Technology, Pittsburgh, Pennsylvania, USA | [6]RAND School of Public Policy, Pittsburgh, Pennsylvania, USA

Correspondence: Zachary Kallenborn (zkallenborn@gmail.com)

Received: 5 May 2025 | **Revised:** 28 August 2025 | **Accepted:** 20 October 2025

Keywords: critical infrastructure | global infrastructure | risk management | risk analysis

ABSTRACT

Critical infrastructure is typically identified at the national level. However, disruption to certain infrastructure systems, facilities, and assets can have negative consequences for global societies. Such globally critical infrastructure entails a distinct risk profile for both countries dependent on the infrastructure, and countries that have such infrastructure in their territory. The goal of the article is to provide an initial framing and definition of "globally critical infrastructure" as a concept worthy of attention and explore the unique risk analysis and management challenges to support future, more rigorous examinations. For dependent countries, globally critical infrastructure exists outside of their border (or possibly outside any country's border), under sometimes drastically different economic, political, governance, and threat environments. Risk management entails unique challenges, because countries dependent on that infrastructure may have no legal or regulatory authority to shape risk management practices at facilities in other countries. Consequently, risk management may extend beyond the domains of the typical homeland or internal affairs agencies to include capabilities and responsibilities of ministries of foreign affairs, trade and commerce, and defense. However, those challenges also imply new risk management demands and options, such as new avenues for international cooperation on infrastructure protection and resilience, international funding, and enhanced monitoring. Having a globally critical infrastructure system in its borders changes the risk dynamics for a nation state, creating potential leverage over dependent nations and new avenues to garner international support, but also creates new risks to national sovereignty. Recognizing these common dependencies can better enable the global community to engage stakeholders to develop and implement systemic risk management approaches worldwide.

1 | Introduction

> "Whatever highway may be constructed across the barrier dividing the two greatest maritime areas of the world must be for the world's benefit, a trust for mankind, to be removed from the chance of domination by any single power, nor become a point of invitation for hostilities or a prize for warlike ambition." Former American President Grover Cleveland regarding ownership rights of a potential canal joining the Atlantic and Pacific oceans, December, 1885 (Quoted in Weld 1889)

Over the centuries, the international community has come together to establish norms and treaties to safeguard common interests and protect global commons. This has included the law of the sea, outer space law, the Antarctic treaty system, and developing numerous international fora to identify common opportunities, and litigate disputes. Yet, academic and policy discussions of critical infrastructure have largely focused on national policy. When global discussions occur, the focus tends

to be on common themes experienced globally but manifesting primarily at the local or national levels. However, the strong and growing connections between global societies mean that common infrastructure dependencies are growing too. Consider the response to COVID-19. In March 2020, two Pfizer facilities, one in Puurs, Belgium, the other in Kalamazoo, Michigan, were selected to manufacture COVID-19 vaccines at industrial scale (Silver n.d.). Pfizer claims the two facilities produced 100 million doses per month collectively and have shipped vaccines to 166 countries (Silver n.d; Pfizer n.d.). The scale of production implies the global reach: just 1 year of production would generate enough vaccines for about 15% of the world's population.

However, no academic or policy analysis has focused on the challenges of identifying, assessing, and managing risks to such globally critical infrastructure. A Google scholar search for the term "globally critical infrastructure" on September 28, 2024 returned only 10 results, only one of which appears to use the term in the same sense as intended here. However, that study by Chris Demchak focused primarily on global cyber infrastructure (Demchak 2012). Google searches for the term "globally critical infrastructure" primarily return results of the form "globally, critical infrastructure" referring to global behaviors regarding critical infrastructure. Of those, two results are relevant. The first, a study on improving climate resilience to the Suez Canal offered general lessons to "other globally critical infrastructure assets" (Barnes et al. 2022). The second, the June 2020 meeting notes of NASA's International VLBI Service for Geodesy and Astrometry explicitly notes, "The concept of 'critical infrastructure' is only defined on a national level. There is no global equivalent" (Behrend 2020). Narrowed Google searches of "globally critical infrastructure" to UN.org, OECD.org, WEForum.org, the .gov and .eu domains, as well as prominent think tanks (RAND.org; RUSI.org; IISS.org; Chathamhouse.org) produced only one additional relevant document: a summary of a 2008 inspector general's report noting that the Department of Homeland Security international activities should include "better understanding globally critical infrastructure" (Committee on Homeland Security and Governmental Affairs 2008.)

Although several studies use the term "critical international infrastructure," none appear to identify, define, and analyze the set as a common class, but rather use the term as a descriptor for specific types of infrastructure (see e.g., Scott-Hayward 2024; Rapp et al. 2012; Ganz et al. 2024). The use of "international" also implies a different and much broader scope. Similarly, some studies use the term "global critical systems," though again do not define or explore the systems as a comprehensive class (Mani et al. 2021; Kemp et al. 2022). Although it remains possible other studies use another term that has been explicitly defined and explored, we have been unable to locate them.

Nonetheless, specific forms of globally critical infrastructure do have existing literature, sometimes extensive, such as studies on the Suez (e.g., Lee and Wong 2021) and Panama canals, space infrastructure, cyber infrastructure (Clemente 2013), automobile manufacturing (Farooq et al. 2024), and trade chokepoints (Bailey and Wellesley 2017). Previously, the United States developed a list of foreign infrastructure it depends on through the Critical Foreign Dependencies Initiative, but items in this list may be unique dependencies for the United States and not necessarily global dependencies (Arce 2015). Further, the list is also no longer maintained and considered relevant, though some initial efforts to build a new version are ongoing (Interview With Former Department of Homeland Security Officials 2024).

Globally critical infrastructure is defined here as systems and assets, whether physical or virtual, so vital to societies around the world that the incapacity or destruction of such systems and assets would have a debilitating impact on numerous countries across multiple geographic regions (derived from The White House 2013). Disruption to such infrastructure could entail far greater and far broader consequences to many countries and to global society compared to national critical infrastructure disruptions.[1] The nature of the systems entails unique risk analysis and risk management challenges, owing to a different range of threats and hazards, more complex stakeholder relationships, and differing national and global risk governance responsibilities and capabilities. Although infrastructure systems that could be considered globally critical have long been considered in isolation, defining and conceptualizing them as a common class has benefits for both fundamental understanding of policymaking and practical application for risk governance in both academia and government:

1. The common concept calls attention to the unique risk analysis and management challenges of this infrastructure class, which should be accounted for during risk analysis and management;
2. Recognizing the common geopolitical challenges of globally critical infrastructure may reveal novel opportunities for global collaboration and risk reduction, which, to the degree those opportunities do or do not emerge, deserves academic inquiry;
3. Focusing on common global infrastructure may call focused attention, research, and analysis into those systems, to include identifying systems whose attention is not proportional to their importance; and
4. Growing attention to global catastrophic risks like climate change and COVID-19 as well as various long-term oriented philosophies, suggests a need to focus attention on protecting and supporting humanity's common infrastructure.

To begin developing and exploring the globally critical infrastructure, this article will begin with a discussion of the emergence of globally critical infrastructure, including a framework for identifying such infrastructure. Then, the article will explore the unique risk analysis and management challenges, highlighting differing risk profiles, and the vastly more complex political and stakeholder environment. Next, the article discusses the potential policy implications implied in recognizing globally critical infrastructure as a unique set of systems, facilities, and assets meriting global attention. The conclusion offers next steps in developing and implementing the concept in real-world policy.

2 | The Emergence of Globally Critical Infrastructure

Globally critical infrastructure has become prominent because the world is far more interdependent and interconnected than

it has ever been, and countries have encouraged and exploited global interdependence to advance policy and economic goals. In 2022, world trade volume was roughly 45 times higher than it was in 1950 (World Trade Organization n.d.). It is not just trade that is connecting the world.

A 2011 McKinsey report estimated that the Internet accounted for 10% of GDP growth from 1996 to 2011 among the most advanced economies, and the overall rate doubled from 2006 to 2011 to 21% (Manyika, and Roxburgh 2011). More recently, UN Trade and Development estimated that global e-commerce jumped to $26.7 trillion in value during COVID-19 (UN Trade and Development 2021). Global communities increasingly rely on the Internet for critical transactions, like paying rent or utilities, whereas global shifts to remote and hybrid work structures during COVID-19 meant global commerce became even more dependent on Internet connectivity and enabling services like Zoom.

Similarly, space-based communication and position, navigation, and timing services are critical for numerous aspects of global infrastructure. For example, the United Kingdom estimates that 17% of annual GDP is dependent on satellite services, and a 5-days disruption alone could cause losses as high as 3.2 billion pounds (House of Commons Science and Technology Committee 2022). Other, traditional infrastructure sectors depend on space too. The National Institute of Standards and Technology has noted how time synchronization is critical for financial markets to manage incoming transactions, power grids to monitor real-time loads and locate faults, and mobile communication networks require synchronized timing to ensure operations are synchronized (Lombardi 2021).

The global community has also increasingly recognized the world faces an array of potential globally catastrophic or existential risks from climate change to large magnitude volcanic eruptions and near-Earth objects (Bostrom and Cirkovic 2008; Willis et al. 2024). Infrastructure to reduce these risks would necessarily be globally critical, because the risks they address are globally impactful. For example, the Svalbard Global Seed Vault in Norway is intended to provide a "global backstop" with seeds from tens of thousands of food crops from across the world (Ministry of Agriculture and Food 2007). Although disruptions to global seed stores may not be impactful in the near-term, it could be globally catastrophic if disruptions correspond with a larger catastrophe where the seed stores prove critical, but unavailable. Likewise, active research and development activities seek to develop future infrastructure to, for example, cool super-volcanoes to prevent catastrophic eruptions, and release particles into the atmosphere to reduce global greenhouse effects (Cox 2017). Once solar geo-engineering to reduce global warming has begun, disruption could lead to rapid warming, creating greater global harms than climate change on its own, and also coming with potential opportunity costs of lost time and resources on alternative approaches to reduce climate change risks (Tang and Kemp 2021).

Potential examples of globally critical infrastructure span a broad and diverse range of systems, services, and assets. As a first step in advancing efforts to assess and govern risks of this type we offer a framework for identification grounded in definitions of three key terms: *infrastructure*, *critical*, and *global* and criteria for which each might lead an infrastructure to be considered globally critical. Anchoring governance of globally critical infrastructure on these definitions allows focused identification of cases that warrant special attention without distracting efforts away from the equally important domain of nationally critical infrastructure.

2.1 | Defining Infrastructure

The Oxford English Dictionary gives the etymology of infrastructure as 1875, combining the Latin roots *infra* meaning below, or part of, and *structure*, "relating to the action or process of construction and to the condition or quality of being constructed." (Oxford English Dictionary 2025) The term most commonly refers to "the basic systems and services … that a country or organization uses in order to work effectively" (Cambridge Dictionary 2025; Oxford English Dictionary 2025). Governments around the world have adapted this definition to include a variety of systems and services upon which society depends. For example, as shown in Table 1, the United States and European Union define an overlapping set of infrastructure sectors that span physical, economic, and societal systems that include intertwined logistical, transactional, and governance layers (Cybersecurity and Infrastructure Security Agency n.d.; European Commission 2025; Weber et al. 2023).

National priorities for critical infrastructure management vary widely. A global review of 194 countries identified 100 published assessments of critical infrastructure. Focus on the problem varies widely across countries; 96% of countries in Europe and North America have published critical infrastructure lists compared to 42%, 49%, 29%, and 28% for Latin American and the Caribbean, Asia, Oceana, and Africa, respectively (Weber et al. 2023).

Similarities across the references included in Table 1 demonstrate some common understanding across nations. There is consensus on some sectors; such as energy, information and communications technology, transport, finance, government and administration, and health. Differences reveal variations in governance and oversight as well as underlying priorities. Sectors related to research and education, food, and water are included less consistently. In addition, sectors are organized differently in different regions. For example, the US sectors for communications and information technology are largely captured by the European Union digital infrastructure sector. In addition, the United States includes a nuclear sector, whereas the European Union includes a space sector. Accordingly, these lists have changed over time as priorities and shifts in governance structure resulted in inclusion, exclusion, or reorganization and renaming of sectors.

Although not typically included as critical infrastructure, some risk governance frameworks also recognize the importance of *green infrastructure* which provides:

> "a strategically planned network of natural and semi-natural areas with other environmental features designed and managed to deliver a wide range of ecosystem services… …[incorporating] green spaces (or blue if aquatic ecosystems are concerned) and other

TABLE 1 | Critical infrastructure sectors defined by the United States, the European Union, and a global review of 194 countries.

United States critical infrastructure sectors	European Union critical infrastructure sectors	Sectors identified through global review of critical infrastructure governance
• Chemical • Commercial facilities • Communications • Critical manufacturing • Dams • Defense industrial base • Emergency services • Energy • Financial services • Food and agriculture • Government services and facilities • Healthcare and public health • Information technology • Nuclear reactors, materials, and waste • Transportation systems • Water and wastewater	• Energy • Transport • Banking • Financial market infrastructure • Health • Drinking water • Wastewater • Digital infrastructure • Public administration • Space • Production, processing, and distribution of food	• Energy • Information and communication technologies • Health • Transport • Food • Water • Public services • Economy and finance • Research and education • National security

> physical features in terrestrial (including coastal) and marine areas" (European Union 2013)

Inclusion of green infrastructure expands the systems to include resources that support global biomes and terrestrial, oceanic, and atmospheric systems. To the degree global focus on climate change continues to grow, emphasis on green infrastructure can be expected too, some of which may be globally critical like geo-engineering systems.

When identifying globally critical infrastructure, it is important to consider elements that could exist across the broadest set of sectors that nations deem important.

2.2 | Defining Criticality

Criticality stems from the benefits society obtains (or seeks to obtain) from infrastructure and the risk of loss when that infrastructure is disrupted, degraded, or destroyed. Empirical studies of risk perception reveal a range of outcomes that people care about related to health and safety (Fischhoff and Morgan 2013; Florig, et al. 2001), the environment and natural ecosystems (Willis et al. 2004), and homeland and national security (Lundberg 2013; Willis et al. 2018). Governments have focused these outcomes to encompass effects on national security, economic security, public health or safety, or any combination of those matters (The White House 2013). Because weighing such values is necessarily a subjective, often political process, actors will vary in the relative weight placed on different outcomes as well as the overall approach to identifying and managing risks. Social, political, and environmental changes may also change the relative weight countries and people place on those outcomes over time. In practice, some degree of at least limited consensus is required on what constitutes critically to support collective decision-making.

In considering assessment of global catastrophic risks that could threaten human civilization or lead to human extinction, five dimensions of consequences from disruptions to globally critical infrastructure can be identified based on Willis et al. (2024):

- Mortality and morbidity: deaths and injuries resulting directly from infrastructure disruptions
- Economic instability: economic losses of varying degrees
- Governance instability: governance failures of varying degrees, to include threats to national security
- Ecosystem instability: degradation or destruction of the functions and services that support biomes and global terrestrial, oceanic, and atmospheric systems
- Reduced human capabilities: degradation of significant aspects of well-being such as a general sense of security, justice and freedoms, and basic human needs and dignities (Nussbaum 2011).

On each of these dimensions, defining criticality requires considering criteria that would specify infrastructure as globally critical such as

- Intensity: the impacts in terms of all five dimensions of outcome, which could be reflected in both measures of magnitude and quality
- Geographic extent: how the effects span across national jurisdictional boundaries to extend across a region or subregion, a continent, a hemisphere, or globally
- Duration: do the impacts manifest over a period of months or less, years, decades, or centuries or more; including whether effects are expected to be permanent and irreversible.

Measurement of criticality will necessarily rely on mixed methods and interdisciplinary approaches. Some types of consequences are amenable to quantitative estimation; such as estimation of deaths and injuries, amounts of species or habitat affected, or economic losses. In cases where globally critical infrastructure is generated by interconnected systems, methods of graph theory and estimates of centrality can be leveraged (Dunn and Wilkinson 2012). Other types of consequences, such as instability of governance or reductions in human capabilities, may require reliance on qualitative analysis, indices, or information about public perceptions.

Thresholds for criticality will involve interactions among the factors of intensity, geographic extent, and duration. For example, a complete disruption of the global positioning system may not be significant if it only lasts fractions of a second, yet a permanent 25% reduction in the shipping capacity through the Suez or Panama canals could have immense economic impacts. Given tradeoffs across these factors and across consequences, the process of setting thresholds will require policymakers to capture and reflect value-based priorities.

2.3 | Defining Globally

In general, infrastructure that is globally critical will tend to be systems and assets around the world that numerous national-level infrastructure systems and assets depend on for their own function, as well as systems and assets to address uniquely global challenges such as global governance institutions, security of global commons, and planetary defense and protection. Infrastructure may be globally critical because of three potential properties of an identified infrastructure.

First, the benefits of infrastructure could be the result of its *existence and operation as a global system*. This value exists beyond any value that might be generated by national or regional elements of the global system. For example, each nation has established financial networks to enable financial transactions, whereas the existence of the Society for Worldwide Interbank Financial Telecommunications (SWIFT) provides a unique service to provide messaging and transactions across national networks, as well as developing and propagating related standards (Scott and Zachariadis 2014).

Second, infrastructure may deliver a globally singular or distinctive service that is not easily replaceable. Examples include the Svalbard Global Seed Vault (i.e., food), the ITER magnetic fusion device in France (i.e., research), or the International Atomic Energy Agency (i.e., energy and public administration). Expanding the construct to include green infrastructure motivates inclusion of unique ecosystems and features that influence global ecosystems, such as the Amazonian forests, polar ice shelves, and infrastructure enabling activities like stratospheric aerosol injection (Reynolds 2019).

Finally, a specific infrastructure asset may serve a special role in a global system because of the connectivity it enables or the magnitude of the contributions it provides. For example, the Suez and Panama canals represent global chokepoints for global container shipping and Taiwan Semiconductor Manufacturing is responsible for 92% of global manufacturer of the most advanced semiconductors (Varas et al. 2021). Although disruption of chokepoint infrastructure like the Suez Canal may not completely end shipping, because ships could transit around, the increased time and costs could still create global disruption and impacts, especially for products dependent on parts or components to produce other goods.

These three properties illustrate that the network typology and, consequently, vulnerability and management, of globally critical infrastructure systems can vary greatly. Certain infrastructure like the canals is highly localized and bound to a geographic area. Meanwhile, certain global services could, in theory, be located anywhere, but may be difficult to reconstitute elsewhere for various political and economic reasons. Global systems like the submarine cable network are highly distributed with numerous potential points where disruption can occur.

"Globally" critical infrastructure can be understood as a subtype of foreign dependent infrastructure. As summarized in Table 2, national infrastructure is well-recognized as having different geographic scopes from local water treatment plants to national-level institutions like stock exchanges or defense industrial bases. Similarly, foreign infrastructure upon which a country depends can vary in geographic scope too from bilateral infrastructure where only one other country depends on it, to regional where multiple states in the same geographic region depend on it, to the focus of this study, truly global infrastructure. Note that the importance of foreign infrastructure will typically be simultaneously important through many types of dependency relationships. As a result, global infrastructure may also carry importance at bilateral, regional, and national levels. For example, Taiwanese semiconductor manufacturing is global infrastructure that is also important foreign infrastructure at the regional level (the European Union), and the bilateral level (e.g., specific exchanges between the United States and Taiwan), as well as serving as nation-wide infrastructure for Taiwan.

Of course, nations may differ in their degree of dependence on any particular globally critical infrastructure system, so disruption might have disproportional effects. Some countries might be affected extremely by disruptions, whereas others might not. For example, a highly digitized society is likely to be far more affected by disruptions to semiconductor production compared to countries with very limited access to or use of computers.

TABLE 2 | Level of infrastructure.

Infrastructure level	Sublevel	Example
National	Local	Municipal water treatment facility
	Regional	The Hoover dam
	Nation-wide	National stock exchange
Foreign	Bilateral	United States–Canada integrated power grid
	Regional	Nord Stream pipeline
	Global	Taiwanese semiconductor manufacturing companies

TABLE 3 | Examples of globally critical infrastructure.

		Relevant dimensions of criticality				
Global nature of infrastructure	**Examples of infrastructure sector/asset**	**Morbidity and mortality**	**Economic stability**	**Governance stability**	**Ecological stability**	**Enablement of human capabilities**
Global system	Space launch (transport)		X	X	X	X
	SWIFT (Finance)		X			
	GPS (space)	X	X	X		
	Undersea cable network (telecommunications)		X	X		
Singular global service	Svalbard Global Seed Vault (Food)	X			X	
	ITER (research/energy)		X			X
	International Atomic Energy Agency (energy/government)	X	X	X		
	Amazonian forests (green infrastructure)	X	X		X	X
	World Trade Organization (Government)		X	X		
	Gavi Vaccine Alliance (Healthcare)	X				X
Global chokepoints	Suez Canal (transport)		X	X		
	Taiwan semiconductor manufacturing companies (manufacturing)		X	X		
	Ultra-high purity quartz mines (critical minerals)		X	X		

2.4 | Identifying and Describing Globally Critical Infrastructure

These definitions and dimensions provide a framework that could facilitate identification and characterization of globally critical infrastructure. Table 3 provides a list of examples of infrastructure and the reasons each infrastructure may be considered globally critical. These characterizations can in turn provide a basis from which to consider analyzing and managing globally critical infrastructure.

As can be seen, numerous potential examples of globally critical infrastructure exist, and many contribute to several dimensions of critical outcomes, albeit to differing degrees. Notably, almost every identified infrastructure system contributes to economic outcomes, which reflects the observation that the drivers criticality for much of what could be considered globally critical infrastructure is the pervasiveness of global trade and economic interconnectivity. Further, the list also illustrates the broad range of globally critical infrastructure, as the list covers most forms of traditional infrastructure.

3 | Analyzing Risk to Globally Critical Infrastructure

Kaplan and Gerrick (1981) describe risk analysis as answering three questions: "(i) what can happen? (i.e., what can go wrong?); (ii) how likely is it to happen?; and (iii) If it does happen, what are the consequences?". On all three questions, globally critical infrastructure has major differences from typical national critical infrastructure.

A defining feature of globally critical infrastructure is that the effects of disruptions extend far beyond national borders. That means priority threats and hazards for globally critical infrastructure will often differ from (though may still overlap with) those that affect national infrastructure, along with associated likelihood assessments. For example, although an infrastructure-hosting and infrastructure-dependent country may face terrorist threats, the ideology, technical capacity, and preferred tactics may differ drastically. Similarly, infrastructure-hosting states may differ in their regime type, economic system, degree of governmental and private sector corruption, human rights record, regulatory and policy environment, national control over infrastructure, geopolitical landscape, threat actors, and natural hazards all of which may affect the successful operation of the infrastructure system. For example, the five biggest importers of Saudi Arabian oil are China, India, Japan, South Korea, and the United States (Observatory of Economic Complexity n.d.). None of the five are monarchies located in the Middle East facing direct threats from Iran and regional proxies. In the 2019 Abqaiq–Khurais attacks, Iranian drone strikes on Saudi Aramco oil refining facilities resulted in a 50% cut in Saudi oil production, amounting to 5% of global oil production (BBC 2019). Although China, India, Japan, South Korea, and the United States may not worry about Iranian drone attacks on their national infrastructure, the threat still had and could have a significant impact on infrastructure operations.

On the one hand, the global dependence of infrastructure means an actor could harm numerous adversaries by disrupting this infrastructure to reduce the magnitude or quality of services that it provides. For example, if Russia wanted to harm American trade, disrupting the Panama Canal would certainly be extremely impactful. On the other hand, common, global dependencies on the infrastructure may generate self-deterrence effects. Russian ships also travel through the Panama Canal, so disruption would affect trade there too (France24 2022). However, conversely, globally critical infrastructure might attract the attention of actors who may be delighted to generate global harm, either as part of an asymmetric coercion strategy or to achieve larger ideological gains. Various extremist groups, for example, increasingly hold accelerationist ideologies focused on generating larger social collapse. Those organizations have and will likely continue to focus on targeting critical infrastructure to radicalize and recruit members, advance their narratives, and generally cause damage, because infrastructure is a necessary component of maintaining modern society (Clarke 2023). All this means states providing globally critical infrastructure may face unique threats to their sovereignty from more powerful states and a range of other hostile actors.

The different risk sets also imply different organizations are needed to conduct risk assessment, particularly with a much greater emphasis on agencies that enable shared awareness among nations. A country dependent on a globally critical infrastructure system may have limited insight into the risk management activities of other countries, except to the degree the country elects to share them. Countries providing the infrastructure may be quite hesitant to share risk-related data, because it may be security sensitive, economically sensitive, or fear sharing the information may prompt undesirable actions. This is especially likely to be the case regarding internal security threats that may upend or disrupt governmental functioning.

By definition, many countries depend on globally critical infrastructure, and that infrastructure will rarely (and perhaps never) exist within their national borders. The external locus of control implies that states need to assess risks to globally critical infrastructure upon which they are dependent seperate from national critical infrastructure. Researchers have concluded that the most important factor in realizing the economic benefit of the Suez Canal is the stability of the Egyptian regime (Chorev 2023). So, Suez risks might include factors like Egyptian monetary and fiscal policy; human rights records; and democratization (Zaki 2017; Mansour 2025). Consequently, risk assessment will also require different types of regional and functional subject matter expertise to appropriately assess and account for the larger range of risks. That will require the risk assessing state to either develop the indigenous knowledge and capability to critically assess such risks, or build relationships with other states, such as the infrastructure provider, who can share that knowledge. However, as the Suez illustrates dependent states may have mismatched risk perceptions: For European countries and others, the Suez is external, global infrastructure, but for Egypt it is also critical national infrastructure.

Even small disruptions to globally critical infrastructure may be globally consequential and major disruptions could amount to a global catastrophe, especially when globally critical infrastructure systems are geographically concentrated (Mani et al. 2021). In March 2021, the Ever Given container ship became trapped in the Suez Canal for 6 days (BBC 2021). Lloyd's list estimates the ship held up $9.6 billion per day in global trade, while the Wall Street Journal notes it simultaneously worsened shortfalls in critical goods like semiconductors (Harper 2021; Stahl 2021). The event generated global headlines even months later (Yee and Glanz 2021). Similarly, disruption to mass vaccine production facilities just before or in the midst of a new global pandemic could result in millions more people dying who might not otherwise would have, because vaccines are not available or achieving herd immunity is postponed. Although not every disruption may be so impactful and not every infrastructure system is so sensitive to disruption, the growing interconnectivity of infrastructure means disruptions may have significant consequences in unexpected ways. Influential risk researcher Yacov Haimes noted that modern societies are complex large-scale system of systems: "Each system is composed of numerous interconnected and interdependent cyber, physical, social, and organizational infrastructures (subsystems), whose relationships are dynamic (i.e. ever changing with time), non-linear (defeating a simplistic modeling schema), probabilistic (fraught with uncertainty), and spatially distributed (agents and infrastructure with possible overlapping characteristics are spread all over the continent(s))." (Haimes 2008) This complexity coupled with worldwide dependence on

globally critical infrastructure means that disruptions can be expected to have major downstream consequences on other forms of critical infrastructure. Even if most countries have adequate preparedness and resilience to handle the effects of a disruption, some may not. Simultaneous disruptions to multiple globally critical infrastructure systems could be especially harmful, as disruptions combine in uncertain and complex ways.

4 | Managing Risk

Haimes (1991) offers another set of three questions to capture risk management: "What can be done? What options are available and what are their associated trade-offs in terms of all costs, benefits, and risks? And what are the impacts of current management decisions on future options?" Again, globally critical infrastructure will have unique answers to all three questions.

Traditional domestic policy, regulatory, and legal tools may have little value in encouraging or coercing protective behavior for globally critical infrastructure that operates in another jurisdiction. Consequently, traditional, domestic-focused critical infrastructure bureaucracies may be limited, instead shifting responsibility to externally focused ministries of foreign affairs, trade and commerce coordination, and defense.

Similarly, the benefits from, responsibilities for, and capacity to steward globally critical infrastructure might not align well with national boundaries. By its nature, globally critical infrastructure affords benefits that extend beyond national borders. This could create responsibilities for nations that host globally critical infrastructure, while also creating interests and associated responsibilities for other countries. The resources available or priorities within the host country may not support or align with sustaining the globally desired infrastructure to meet the interests of other states. Aligning these interests, responsibilities, and capacities adds additional complexity to managing globally critical infrastructure and several considerations related to infrastructure as a tool of global power, implications of infrastructure and conflict, governance structures for risk management, and coordination of risk management.

4.1 | Infrastructure as Global Power

Hosting globally critical infrastructure creates opportunities for states to use infrastructure as a tool of geopolitical power (This point is made well in Farrell and Newman 2019). Global dependency on infrastructure gives the owner/operator of the infrastructure system some power over dependent states. An owner/operator may revoke access to one or more states as a coercive or punitive measure to support the owner/operator's goals. For example, in April 2023 Kazakhstan seized Russian property at the Baikonur Cosmodrome, the world's largest spaceport, and barred Russian leadership from leaving the country, because Kazakhstan demanded $26 million in unpaid debts (Eckel 2023). The seizure opened questions about Kazakhstan's continued support to create the new Zenit-M space launch facility, necessary for Russia's launch of new Soyuz-5 rockets (Eckel 2023). Similarly, in February 2022 Turkey closed the Bosphorus and Dardanelles straits to warships in opposition to Russia's war with Ukraine, though it is unclear whether all warships or just Russian and Ukrainian warships were banned (Mongilio 2022; Pedrozo 2022). Article 19 of the 1936 Montreux Convention which governs transit through the straits allows Turkey to prohibit access to warships in conflict, and all warships if Turkey is party to the conflict (Pedrozo 2022).

Fears of infrastructure being used as a form of power may also motivate states to decouple from globally critical infrastructure. This is perhaps most notable in the case of North Korea, whose governing ideology is based on *Juche* philosophies of self-reliance in political, economic, and military matters (Kim 2017). Similarly, how and whether Europe should divorce Russian natural gas dependence continues to be a fraught political issue (Gross and Stelzenmüller 2024).

4.2 | Infrastructure and Conflict and Cooperation

Risk management for globally critical infrastructure can become major matters of global conflict. On October 29, 1956, Great Britain, France, and Israel launched a combined attack on Egypt following Egypt's nationalization of the Suez Cana (Wright et al. 1980). In 1885, the United States supported a rebellion in Panama pushing for independence from Colombia in large part because the United States desired control over the yet-to-be-built Panama Canal (Wicks 1980). Then during Operation Just Cause in 1989, the United States invaded Panama, in part, to "protect the integrity of the Panama Canal Treaty" after General Manuel Noriega declared a military dictatorship (Bush 1989). Although the United States did not respond militarily following the September 2019 attacks on Saudi oil processing facilities at Abqaiq, former President Trump stated the United States was "locked and loaded" and issued a new round of economic sanctions on Iran (Rampton and Mohammed 2019). Other examples exist too.

The presence of globally critical infrastructure in a state party to a conflict may also change the geopolitical dynamics of that conflict. Taiwanese semiconductor facilities have been described as a potential "silicon shield," because they would provide a strong incentive for the United States to support intervention in a conflict with China on Taiwan's behalf (Lee et al. 2021). Similarly, US security guarantees to Saudi Arabia have long been recognized to be a product of Saudi Arabia's criticality to American and global oil production (Spalding 2023).

But globally critical infrastructure is not just a cause of conflict. The infrastructure may also present diplomatic opportunities to improve relations. Russia–United States collaboration on the International Space Station has been a hallmark of science diplomacy for decades. Increasing the resilience of commonly shared globally critical infrastructure could be an opportunity to broaden those benefits. When risks manifest, the collaborative response can catalyze larger diplomatic efforts for peace and security (Kelman 2018). Of course, geopolitical sensitivities may preclude cooperation on threats or infrastructure with strong security relevance; however, opportunities might exist for security-neutral resilience, such as improving canal resilience to natural hazards. Certain common threats may also justify cooperation on

security-sensitive issues, such as US-Russian counter-terrorism intelligence sharing (McDermott 2004).

4.3 | Governance Structures for Risk Management

The global nature of globally critical infrastructure risk means a much broader range of stakeholder groups will be involved in analyzing, mitigating, and governing risk. By definition, a broad range of states, international organizations, multinational corporations, nongovernmental organizations, and others will have a stake in the functioning of globally critical infrastructure. On a day-to-day basis, these actors may not concern themselves with the infrastructure's operations, as they may have other priorities; however, disruptions to effective operations may generate global concern and attention. Some globally critical infrastructure may also be inherently transnational, such as undersea cables which may originate and terminate in two separate countries, subjecting the cable to different terminology, regulations, permitting, and other factors (Bowden et al. 2024). The broad stakeholder interest may also lead to novel risk governance approaches, such as the 1956 proposal for an international "Suez Canal Users' Association" comprised of 15 countries with a common interest in the canal (UK Parliament 1956).

Managing risk to globally critical infrastructure will also necessarily imply focus on a different set of infrastructure systems, facilities, and assets. After WikiLeaks released a classified list of American critical foreign dependencies, economist Daniel Arce analyzed the list and concluded that "what the United States identifies as critical international infrastructure differs significantly from what is defined as the national critical infrastructure" (Arce 2015) Managing risk to globally critical infrastructure can be expected to require a significant expansion of managed systems, facilities, and assets, necessarily requiring new resources.

Managing risks to globally critical infrastructure is likely to involve different organizational equities too. Infrastructure protection is typically the remit of global ministries of internal affairs/security. In the United States, for example, the Department of Homeland Security's Cybersecurity and Infrastructure Agency leads interagency efforts to reduce critical infrastructure risk, whereas Department of Defense plays a supporting role in certain areas around homeland defense and the defense industrial base. This is appropriate, because a country's critical infrastructure typically falls under the jurisdiction of that country's legal, regulatory, and policy architecture. However, globally critical infrastructure may be owned and managed by other countries. As such, ministries of foreign affairs become essential, because any influence (or not) that a state may have over another will necessarily exist in the context of the overall relationship between the two states. If one state is concerned that another is leaving open vulnerabilities to global critical infrastructure upon which the first depends, that issue will need to be addressed through formal diplomatic channels. Similarly, because globally critical infrastructure is "globally" critical, other states are likely to take an interest in risk management policies and procedures. That means if a state has concerns, they may also need to navigate a complex geopolitical environment. International affairs offices within ministries of interior affairs might be sufficient for some bilateral or even multilateral discussions, but formally trained diplomats and appointed ambassadors will be necessary at times to navigate the political complexities.

In practice, the broad range of organizational equities means risk mitigation is likely to require significant interagency and international coordination. Homeland and internal affairs ministries responsible for national-level critical infrastructure will be necessary to anticipate the impacts of a disruption on national-level infrastructure; however, collaboration with academia, nongovernmental organizations, and international partners may be necessary to fully understand and anticipate the effects, because second- and third-order effects are likely. For example, it should be easy to determine the value of trade in a given country that flows through the Suez Canal; however, trade in critical parts or materials needed for a downstream manufacturer may be disrupted too. Close communication and collaboration between private and governmental critical infrastructure owners and operators at the inter and intrastate level are likely to be necessary. All those perspectives need to be linked with defense, foreign affairs, and trade perspectives to develop aligned and comprehensive programs, policies, and strategies.

4.4 | Coordination of Risk Management

Coordinating risk reduction will also be a challenge because states that own and are responsible for globally critical infrastructure may have different risk perceptions compared to dependent countries. External states that depend on the infrastructure may be narrowly interested in the protection of that infrastructure, whereas the states where infrastructure is located must juggle a range of competing domestic and international priorities. The states where infrastructure is located will necessarily have limited budgets for infrastructure protection activities and may choose to prioritize other, national-level infrastructure. Differing priorities could and have emerged as sources of conflict between infrastructure dependent and infrastructure-providing nations.

Infrastructure-dependent states may also face internal tensions between risks management, and the larger foreign policy goals of the dependent states. During the Suez Crisis of 1956, the Eisenhower administration in the United States feared the British-French-Israeli invasion of Egypt would prompt a Soviet intervention, ultimately leading to greater Soviet influence in the Middle East (Department of State n.d.). The United States supported a UN resolution denouncing the invasion, and pressured Britain and France to accept a ceasefire (Department of State n.d.). The United States paid a price for the approach in temporarily damaged relations with Britain and France (Department of State n.d.). These competing priorities may also create decision-making challenges if critical leaders weigh the risks differently.

Of course, risk management and larger foreign goals are not inherently at odds. Positive relations between states on risk management could bleed into larger collaborative relationships that strengthen interstate ties. For example, the United States Department of State and Homeland Security might collaborate to support Taiwan in building a national exercise program and improving its emergency response system, which could help reduce risk to semiconductor protection while also supporting Taiwanese emergency management more generally and

strengthening bilateral ties (Bosner and Chang 2020). Likewise, the Odyssean Institute proposed the use of preferential trade agreements to enhance global trade resilience (Odyssean Institute n.d.). And even when there is conflict, it may not rise to a major crisis.

Another challenge is coordination across potentially numerous public–private entities. Aggregated infrastructure systems like the Internet depend on the successful operation of a multitude of physical and digital infrastructure and enabling services owned and managed by a multitude of governmental and private sector entities. These include data centers, subsea communication cables, Internet exchange points, Internet service providers, and management of the domain name system. More broadly, non-state actors typically own and manage globally critical infrastructure, and their activities may be covered under multiple legal jurisdictions. Thus, risk management takes place in a highly complex stakeholder environment, and stakeholders may hold different values, and risk perceptions (Luhmann 1990). In turn, that may lead to underinvestment and free-riding, as actors prioritize values other than security and risk.

4.5 | Capacity Differences

Infrastructure-hosting and infrastructure-dependent countries can also be expected to differ, sometimes significantly in their capacity to manage risks. Numerous countries all around the world depend on globally critical infrastructure, to include countries that may lack significant economic, technological, military, and governance capacity. If a less powerful state is concerned about threats to global infrastructure they depend on, they may have few tools available to encourage or influence risk management practices. Conversely, infrastructure-hosting countries may have limited capacity to address the risks they face. Although the legacy of post September 11th counter-terrorism means the United States faces limited direct threats from sophisticated, hierarchical terrorist organizations, Middle Eastern states like Egypt and Saudi Arabia face major direct regional threats from Iran-sponsored terrorist organizations like Hamas, Hezbollah, and the Houthi rebels. Those terrorist groups pose significant threats comparable to state-level militaries, and consequently, Egypt and Saudi Arabia have often relied on help from the United States to repel the threats. Similarly, countries may differ in the broad legal, regulatory, and governance regimes to support risk reduction, that may either restrict or enable approaches. For example, countries with greater nationalization and state control of the private sector may be able to insist on infrastructure providers adopting various measures that countries with greater public–private separation could not.

5 | Conclusions/Next Steps

In summary, globally critical infrastructure entails unique risk assessment and management challenges. The biggest of which is that infrastructure providers reside outside the control of states dependent upon them. This means the sets of hazards facing this infrastructure, the tools for managing them, and the stakeholders involved will all differ from traditional risk management. The consequences of disruptions will often be quite high, because harms will spread to multiple sectors in multiple nations, creating high potential for cascading consequences. Unfortunately, global governments and civil society are not looking at this class of infrastructure in a comprehensive way. So, what should academics and policymakers do now?

To further develop the concept, a critical next step is to develop a formalized approach to more precisely, and systematically identify globally critical infrastructure across not only traditional infrastructure sectors, but also infrastructure that may transcend typical infrastructure boundaries and is necessary for, but not typically considered, as critical infrastructure (e.g., international standards bodies). Developing a common list of globally critical infrastructure is likely to be difficult, but not insurmountable. First, a methodological issue exists of determining the threshold for "global" criticality as opposed to simply national or regional. Waterways like the Jordan River might be regionally important to states relying on it, but be minimally important globally. However, a globally critical infrastructure system will almost certainly be national and regional in importance. Second, states may be unwilling to share information about the infrastructure they depend upon for fear international rivals may misuse the information.

In practice, identification of globally critical infrastructure will almost certainly be a political process rather than an academically robust methodology. One potential solution is for global criticality to be self-nominated with the global community accepting or rejecting that nomination. Assume for the sake of argument that the United States considers the Panama Canal a critical foreign dependency, and that determination is classified information. If the government of Panama nominated the Panama Canal as globally critical and provided a case why, the United States could choose to support (or not) based on the merits of the case and the larger international politics. The United States might choose to support Panama's bid ostensibly either to support bilateral ties, support allies, or simply because Panama made a good case that they are important, without acknowledging the classified determination that the United States is deeply dependent on the canal. American diplomats might also work quietly behind the scenes to encourage either Panama making its case, or others to support the bid. Although the specifics should depend on context, at face value, a self-nomination approach seems to provide numerous means for states to create plausible deniability regarding their interest in a particular globally critical infrastructure system. States in which globally critical infrastructure exists would also have an incentive to seek designation, because it may unlock various international economic, political, and technological support to improve their country. In practice, sympathetic global governments could convene international tiger teams of infrastructure and foreign policy experts as part of multilateral fora like the G-7 or five-eyes to explore common approaches to identifying and governing globally critical infrastructure.

Nonetheless, academic insight may still have a role in attempting to identify this infrastructure in a systematic and rigorous way. In fact, academic-led work could also be a simple solution to the information sharing problem in providing a common, open-source baseline that states can react to. Academics thinking about and debating how criticality and global-ness manifest could provide useful insight into policy-development processes, as well as developing novel ideas around risk governance.

At the national level, states will differ in their degree of dependency on any particular globally critical infrastructure, national-level efforts are needed to determine which infrastructure that particular country is dependent on and the country's general strategic approach to ensuring access and reducing risk. Nationally identified infrastructure should receive dedicated risk analysis to account for the broader scope of hazards that might exist with appropriate inclusion in national risk registers. This should include scenario analyses and sensitivity analyses to better characterize how risks may manifest, and their consequences for the national system. States should also create or designate an entity to lead risk analysis and management efforts around globally critical infrastructure. For example, the United States might designate the Department of State or Commerce as the lead Sector Risk Management Agency for globally critical infrastructure, responsible for leading interagency coordination and collaboration (Cybersecurity and Infrastructure Security Agency n.d.). This would ensure risk management activities are conducted consistent with and supporting larger foreign policy goals. Alternatively, because globally critical infrastructure necessarily crosscuts traditional infrastructure sectors, the American National Security Council could establish an interagency policy committee that includes representatives from the Departments of State, Defense, and Intelligence Community to develop an approach to governing and managing risk to globally critical infrastructure.

Countries should also collaborate at relevant international fora to identify and assess common dependencies among members, and collaborate to develop, implement, and improve risk management approaches. For example, the final assessment report of an EU-NATO task force recommended: "Developing regular Parallel and Coordinated Assessments of the threats to critical infrastructure…" which could include threats to globally critical infrastructure of interest to the EU and NATO (NATO 2023). Similarly, the Organisation for Economic Co-Operation and Development (OECD) might raise the topic in the High-level Risk Forum to identify common infrastructure dependencies among member states and identify and develop common governance strategies. The OECD might also coordinate tailored risk assessments of specific globally critical infrastructure systems and identify opportunities for member engagement. International defense fora like NATO and five-eyes intelligence sharing community may also allow for more candid discussion of classified assessments and categorizations of globally critical infrastructure. At the United Nations, the United Nations Security Council could order reports on global security threats to globally critical infrastructure, whereas the United Nations Disaster Risk Reduction agency could create a funding stream dedicated to reducing natural hazard risk to globally critical infrastructure. The G20 is also a potentially useful forum for raising the topic of globally critical infrastructure, owing to their broad participation from both states and civil society and on-going work on global infrastructure generally.

Given that so much of global infrastructure is owned and operated by private sector entities, the private sector will need to play a leading role. There is a solid basis for doing so. Although the American government led early development of the Internet, Internet governance has become largely privatized (Sherman 2020). Governments continue to exercise influence through laws, building infrastructure, and setting norms and standards, but private sector entities typically finance and develop subsea cables, data centers, and cloud services all of which affect both the structure of the Internet and risks to it (Sherman 2020). Insights from experiences governing risk to Internet infrastructure and working across the public–private divide may be useful for reducing risk to other globally critical infrastructure.

Another specific group of entities who should play a role is international development agencies and banks. States use multilateral development banks to fund and support development in middle and low-income countries, which has and could include infrastructure projects (Avellán et al. 2024). Globally critical infrastructure exists not only in developed states, but middle- and low-income states too. Providing funding to those states to help support various risk and disaster management activities around globally critical infrastructure would be valuable not only for the middle- and low-income states but also for the global community. International development agencies and banks should create dedicated funding streams for this purpose to encourage and solicit support from wealthy nations.

Globally critical infrastructure should also be considered in relevant hazard-specific analyses at all levels. It is especially critical to explore scenarios where the same hazard—or some combination of hazards—harms multiple globally critical systems, facilities, and assets, because that could create compounding and cascading consequences. One obvious hazard worth focus is climate change. Climate-induced hazards like rising sea-levels, more frequent and higher intensity natural hazards, and global instability could potentially impact a broad range of globally critical infrastructure, compounding larger threats to international economic and social systems.

Finally, a new focus on globally critical infrastructure may open the aperture of critical risk management to global systems not typically considered infrastructure, such as green infrastructure as discussed above. Another possibility is the global system of scientific discovery and innovation. Considering scientific discovery and innovation as a critical function of critical infrastructure has some basis: In the American Cybersecurity and Infrastructure Security Agency's National Risk Management Center designated "research and development" a national critical function, whereas the German Federal Agency for Cartography and Geodesy has pushed to designate the Geodetic Observatory Wettzell as critical infrastructure (Behrend 2020). Scientific discovery certainly has implications for all relevant dimensions of criticality. Without the germ theory of disease and the discovery of bacteria and viruses, humanity would have been ill-equipped to respond to COVID-19 or any other pandemic; the economic benefits of the Internet and digitization could not exist without the development of computers. Although immediate harms may be minimal except for certain facilities or in certain circumstances (e.g., disruption to the ability of scientists to share information about a new pathogen right when a pandemic breaks out), long-term consequences could be catastrophic. What happens if a supervolcano erupts before humanity can discover how to prevent it or respond?

Today, global societies are more interconnected than ever before. But greater interconnectivity means greater interdependency and vulnerability. Critical infrastructure risk analysis and

management needs a paradigm shift to look beyond national borders to the infrastructure upon which all of us depend.

Acknowledgments

The authors would like to thank Steve Abott, Salman Ahmed, Bilal Asghar, Bob Kolaksy, Lara Mani, Susan Stevens, James Sullivan, Nicholas Vernon, Seth Weinberger, and attendees of Strategic Multilayer Assessment and Military Operations Research Society speaker series for providing thoughtful comments and input. Any errors or awkward turns of phrase are the author's own.

Conflicts of Interest

The authors declare no conflicts of interest.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Endnotes

[1]We use "disruption" as a catch-all term to include any event preventing infrastructure from generating desirable outcomes. In practice, we expect differing risk dynamics between the physical destruction of infrastructure, narrowly operational disruptions (e.g., a temporary power outage), loss of social trust in infrastructure systems, and other events; however, we reduce these all to "disruption" for the sake of linguistic simplicity.

References

Arce, D. G. 2015. "WikiLeaks and the Risks to Critical Foreign Dependencies." *International Journal of Critical Infrastructure Protection* 11: 3–11. https://doi.org/10.1016/j.ijcip.2015.07.004.

Avellán, L., A. J. Galindo, G. Lotti, and J. P. Rodríguez. 2024. "Bridging the Gap: Mobilization of Multilateral Development Banks in Infrastructure." *World Development* 176: 106498. https://doi.org/10.1016/j.worlddev.2023.106498.

BBC. 2019. "Saudi Arabia Oil and Gas Production Reduced by Drone Strikes." *BBC News*. September 14. https://www.bbc.co.uk/news/world-middle-east-49703143.

BBC. 2021. "*Egypt's Suez Canal Blocked by Huge Container Ship*." BBC News, March 23. https://www.bbc.co.uk/news/world-middle-east-56505413.

Bailey, R., and L. Wellesley. 2017. *Chokepoints and Vulnerabilities in Global Food Trade*. Chatham House. https://www.chathamhouse.org/2017/06/chokepoints-and-vulnerabilities-global-food-trade.

Barnes, A., N. Faull, L. Ghatauray, and A. Goodman. 2022. *High Seas: Enabling a Climate Resilient Suez Canal. March McLennan*. March McLennan. https://www.marshmclennan.com/assets/insights/publications/2022/december/Enabling_climate_resilience_in_the_Suez_Canal_insight_v6.pdf.

Behrend, D. 2020. "42nd Directing Board Ersatz Meeting II—Minutes." International VLBI Service for Geodesy and Astrometry. https://ivscc.gsfc.nasa.gov/about/org/board/dbmeet42-e2.pdf.

Bosner, L., and I.-W. J. Chang. 2020. *Taiwan's Disaster Preparedness and Response: Strengths, Shortfalls, and Paths to Improvement*. Global Taiwan Institute. https://globaltaiwan.org/wp-content/uploads/2022/08/GTI-Taiwans-Disaster-Preparedness-and-Response-Oct-2020-final-1.pdf.

Bostrom, N., and M. Cirkovac. 2008. *Global Catastrophic Risks*. Oxford University Press.

Bowden, M. T. E., G. A. Lipsham, and D. A. Johnson. 2024. "Diving Deep: Britain's Critical Submarine Cable Infrastructure." pp. 272–289. In *Maritime Britain: In the 21st Century*, edited by K. Jamieson, K. Rowlands, and A. Young, Britannia Publishing: Dartmouth.

Bush, G. 1989. "Fighting in Panama: The President; a Transcript of Bush's Address on the Decision to Use Force in Panama." *New York Times*. December 21. https://www.nytimes.com/1989/12/21/world/fighting-panama-president-transcript-bush-s-address-decision-use-force-panama.html.

Critical Infrastructure Sectors. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

Chorev, S. 2023. "The Suez Canal: Forthcoming Strategic and Geopolitical Challenges." In *The Suez Canal: Past Lessons and Future Challenges*, edited by C. Lutmar, and Z. Rubinovitz, 3–26. Springer International Publishing. https://doi.org/10.1007/978-3-031-15670-0_1.

Clemente, D. 2013. *Cyber Security and Global Interdependence: What is Critical?* Chatham House. https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0213pr_cyber.pdf.

Committee on Homeland Security & Governmental Affairs. 2008. *IG Report Indicates Dhs Must Improve International Activity Efforts*. Committee on Homeland Security & Governmental Affairs. https://www.hsgac.senate.gov/media/dems/ig-report-indicates-dhs-must-improve-international-activity-efforts/.

Cambridge Dictionary. 2025. "*Infrastructure*." Cambridge Dictionary. https://dictionary.cambridge.org/us/dictionary/english/infrastructure.

Clarke, C. 2023. *The Targeting of Infrastructure by America's Violent Far-Right*. Combating Terrorism Center at West Point. https://ctc.westpoint.edu/the-targeting-of-infrastructure-by-americas-violent-far-right/.

Cox, D. 2017. "*NASA's Ambitious Plan to Save Earth From a Supervolcano*." *BBC*. August 17. Accessed October 24, 2025: https://www.bbc.com/future/article/20170817-nasas-ambitious-plan-to-save-earth-from-a-supervolcano.

Cybersecurity and Infrastructure Security Agency. n.d. *National Critical Functions Set*. Accessed October 24. https://www.cisa.gov/national-critical-functions-set.

Demchak, C. C. 2012. "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)." *Journal of Comparative Policy Analysis: Research and Practice* 14, no. 3: 254–269. https://doi.org/10.1080/13876988.2012.687619.

Dunn, S., and S. M. Wilkinson. 2012. "Identifying Critical Components in Infrastructure Networks Using Network Topology." *Journal of Infrastructure Systems* 19, no. 2: 157–165. https://doi.org/10.1061/(ASCE)IS.1943-555X.0000120.

European Commission. 2025. *Critical Infrastructure Resilience at EU-Level*. European Commission. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience-eu-level_en.

Eckel, M. 2023. *Sunset for Baikonur? A Contract Dispute with Kazakhstan Flashes Warnings for Russia's Legendary Spaceport*. RadioFreeEurope.

"*EU-NATO Task Force on the Resilience of Critical Infrastructure: Final Assessment Report*, 2023. NATO. https://commission.europa.eu/system/files/2023-06/EU-NATO_Final%20Assessment%20Report%20Digital.pdf.

European Union. 2013. "Green Infrastructure (GI)—Enhancing Europe's Natural Capital." European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013DC0249.

Farooq, S., A. Naseem, Y. Ahmad, M. Awais Akbar, and M. Ullah. 2024. "Identification and Prioritization of Risks for New Entrants in Automobile Sector Using Monte Carlo Based Approach." *Scientific Reports* 14, no. 1: 12571. https://doi.org/10.1038/s41598-024-62803-8.

Farrell, H., and A. L. Newman. 2019. "Weaponized Interdependence: How Global Economic Networks Shape State Coercion." *International Security* 44, no. 1: 42–79. https://doi.org/10.1162/isec_a_00351.

Fischhoff, B., and G. Morgan. 2013. "The Science and Practice of Risk Ranking." pp. 393–403 In *Risk Analysis and Human Behavior*, edited by B. Fischhoff. Routledge. https://doi.org/10.4324/9780203140710.

Florig, H. K., M. G. Morgan, K. M. Morgan, et al. 2001. "A Deliberative Method for Ranking Risks (I): Overview and Test Bed Development." *Risk Analysis* 21, no. 5: 913–913. https://doi.org/10.1111/0272-4332.215161.

France24. 2022. Protestors Urge Closure of Panama Canal to Russian Ships. France24, March 3. https://www.france24.com/en/live-news/20220303-protesters-urge-closure-of-panama-canal-to-russian-ships.

Ganz, A., M. Camellini, E. Hine, C. Novelli, H. Roberts, and L. Floridi. 2024. "Submarine Cables and the Risks to Digital Sovereignty." *Minds and Machines* 34, no. 3: 31. https://doi.org/10.1007/s11023-024-09683-z.

Gross, S., and C. Stelzenmüller. 2024. *Europe's Messy Russian Gas Divorce*. Brookings. https://www.brookings.edu/articles/europes-messy-russian-gas-divorce/.

Haimes, Y. 1991. "Total Risk Management." *Risk Analysis* 11, no. 2: 169–171. https://doi.org/10.1111/j.1539-6924.1991.tb00589.x.

Haimes, Y. Y. 2008. "Systems-Based Risk Analysis." In *Global Catastrophic Risks*. Oxford University Press. https://doi.org/10.1093/oso/9780198570509.003.0011.

Harper, J. 2021. "Suez Blockage is Holding up $9.6bn of Goods a Day." *BBC News*. March 26. https://www.bbc.co.uk/news/business-56533250.

Mongilio, H. 2022. "Turkey Closes Bosphorus, Dardanelles Straits to Warships." *USNI News*. February 28. https://news.usni.org/2022/02/28/turkey-closes-bosphorus-dardanelles-straits-to-warships;.

House of Commons Science and Technology Committee. 2022. *UK Space Strategy and UK Satellite Infrastructure*. House of Commons Science and Technology Committee. https://committees.parliament.uk/publications/31490/documents/176763/default/.

Interview With Former Department of Homeland Security Official. 2024.

Kaplan, S., and B. J. Garrick. 1981. "On the Quantitative Definition of Risk." *Risk Analysis* 1, no. 1: 11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x.

Kelman, I. 2018. "Disaster Diplomacy." In *The Encyclopedia of Diplomacy*, edited by G. Martel, 1st ed. 1–6. Wiley. https://doi.org/10.1002/9781118885154.dipl0086.

Kemp, L., C. Xu, J. Depledge, et al. 2022. "Climate Endgame: Exploring Catastrophic Climate Change Scenarios." *Proceedings of the National Academy of Sciences* 119, no. 34: e2108146119. https://doi.org/10.1073/pnas.2108146119.

Kim, S. K. 2017. "Juche (Self-Reliance) in North Korea." In *The Wiley-Blackwell Encyclopedia of Social Theory*, edited by B. S. Turner, 1st ed. 1–3. Wiley. https://doi.org/10.1002/9781118430873.est0820.

Lee, J. M., and E. Y. Wong. 2021. "Suez Canal Blockage: An Analysis of Legal Impact, Risks and Liabilities to the Global Supply Chain." *MATEC Web of Conferences* 339: 01019. https://doi.org/10.1051/matecconf/202133901019.

Lee, Y., N. Shirouzu, and D. Lague. 2021. "SPECIAL REPORT-Taiwan Chip Industry Emerges as Battlefront in U.S.-China Showdown." *Reuters*. December 27. https://www.reuters.com/article/technology/special-report-taiwan-chip-industry-emerges-as-battlefront-in-us-china-showdow-idUSL4N2TC0JE/.

Lombardi, M. A. 2021. NIST Technical Note 2189: An Evaluation of Dependencies of Critical Infrastructure Timing Systems on the Global Position System (GPS). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/TechnicalNotes/NIST.TN.2189.pdf.

Luhmann, N. 1990. "Technology, Environment and Social Risk: A Systems Perspective." *Industrial Crisis Quarterly* 4, no. 3: 223–231.

Lundberg, R. 2013. *Comparing Homeland Security Risks Using a Deliberative Risk Ranking Methodology*. RGSD-319. RAND Corporation.

Mani, L., A. Tzachor, and P. Cole. 2021. "Global Catastrophic Risk From Lower Magnitude Volcanic Eruptions." *Nature Communications* 12, no. 1: 4756. https://doi.org/10.1038/s41467-021-25021-8.

Mansour, A. 2025. "Egypt Needs Democracy to Fix Its Economy." Foreign Policy. October 27. https://foreignpolicy.com/2023/02/07/egypt-needs-democracy-to-fix-its-economy/.

Manyika, J., and C. Roxburgh. 2011. *The Great Transformer: The Impact of the Internet on Economic Growth and Prosperity*. McKinsey Global Institute. https://www.mckinsey.com/~/media/mckinsey/industries/technology%20media%20and%20telecommunications/high%20tech/our%20insights/the%20great%20transformer/mgi_impact_of_internet_on_economic_growth.pdf.

McDermott. 2004. *Prospects for Collaboration between Russia and the West in Responding to the New Security Challenges Since September 11*. Chatham House. https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0504_rep_prospects.pdf.

Nussbaum, M. C. 2011. *Creating Capabilities: The Human Development Approach*. Belknap press of Harvard University Press.

Odyssean Institute. n.d. "Global Resilient Anticipatory Infrastructure Network (GRAIN)." Accessed October 24, 2025. https://www.odysseaninstitute.org/grain.

Oxford English Dictionary. n.d. "*Infrastructure*." Accessed October 24, 2025: https://www.oed.com/dictionary/infrastructure_n.

Pedrozo, P. (Pete) 2022. "Closing the Turkish Straits in Times of War." *International Law Studies* 99, no. 517: pp. 517–520. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=3016&context=ils.

Pfizer. n.d. *Pfizer Expands Manufacturing Efforts to Increase COVID-19 Vaccine Supply Globally*. Accessed October 24, 2025. https://www.pfizer.com/sites/default/files/investors/financial_reports/annual_reports/2021/story/expanding-covid-manufacturing-efforts/.

Rampton, R., and A. Mohammed. 2019. U.S. blames Iran for Saudi oil attack, Trump says "locked and loaded." *Reuters*. September 16. https://www.reuters.com/article/world/us-blames-iran-for-saudi-oil-attack-trump-says-locked-and-loaded-idUSKBN1W00SD/.

Rapp, R. J., F.-S. Gady, S. S. Parmar, and K. F. Rauscher. 2012. "India's Critical Role in the Resilience of the Global Undersea Communications Cable Infrastructure." *Strategic Analysis* 36, no. 3: 375–383. https://doi.org/10.1080/09700161.2012.670444.

Reynolds, J. L. 2019. *The Governance of Solar Geoengineering: Managing Climate Change in the Anthropocene*, 1st ed. Cambridge University Press. https://doi.org/10.1017/9781316676790.

Saudi Arabia. n.d.. "*The Observatory of Economic Complexity*." Accessed October 24, 2025. https://oec.world/en/profile/[…bespoke].

Scott, S. V. 2014. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community*. Routledge.

Scott-Hayward, S. 2024. "Critical International Infrastructure: A Case for Secure, Sustainable Non-Terrestrial Networking." Strategic Security Analysis 35. https://www.gcsp.ch/sites/default/files/2024-12/ssa-2024-issue35-polymath.pdf.

Sector Risk Management Agencies. n.d. "Cybersecurity and Infrastructure Security Agency." Accessed October 24, 2025. Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

Sherman, J. 2020. "The Politics of Internet Security: Private Industry and the Future of the Web." Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-security-private-industry-and-the-future-of-the-web/.

Silver, K. n.d. "Shot of a Lifetime: How Pfizer and BioNTech Developed and Manufactured a COVID-19 Vaccine in Record Time—Pfizer Investor Insights." Accessed October 24, 2025.

https://insights.pfizer.com/shot-of-a-lifetime-how-pfizer-and-biontech-developed-and-manufactured-a-covid-19-vaccine-in-record-time.

Spalding, J. 2023. *The Deal That Keeps the Oil Flowing*, Harvard University: Epicenter. https://epicenter.wcfia.harvard.edu/blog/deal-keeps-oil-flowing.

Stahl, G. 2021. "Ship Stuck in Suez Canal and Chip Shortages: What Global Supply-Chain Problems Mean for You." *Wall Street Journal*. (March). https://www.wsj.com/articles/whats-wrong-with-global-supply-chains-and-how-it-affects-you-11616763749.

Svalbard Global Seed Vault. 2007. Ministry of Agriculture and Food. https://www.regjeringen.no/en/topics/food-fisheries-and-agriculture/svalbard-global-seed-vault/id462220/.

Tang, A., and L. Kemp. 2021. "A Fate Worse Than Warming? *Stratospheric Aerosol Injection and Global Catastrophic Risk*." *Frontiers in Climate* 3: 720312. https://doi.org/10.3389/fclim.2021.720312.

The Suez Crisis, 1956. n.d. "Milestones in the History of U.S. Foreign Relations—Office of the Historian." Accessed October 24, 2025. https://history.state.gov/milestones/1953-1960/suez.

The White House. 2013. *Presidential Policy Directive/PPD-21: Critical Infrastructure Security and Resilience*. White House. https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf.

UK Parliament. 1956. *Suez Canal Users' Association*. UK Parliament. https://hansard.parliament.uk/Lords/1956-10-31/debates/f0cdb86f-cbdd-4812-9d8d-4309b3a2b5f4/SuezCanalUsersAssociation.

UN Trade and Development (UNCTAD). 2021. "*Global E-Commerce Jumps to $26.7 Trillion, COVID-19 Boosts Online Sales*." UN Trade and Development. https://unctad.org/news/global-e-commerce-jumps-267-trillion-covid-19-boosts-online-sales.

Varas, A., R. Varadarajan, J. Goodrich, and F. Yinug. 2021. Strengthening the Global Semiconductor Supply Chain in an Uncertain Era. Boston Consulting Group (BCG), Semiconductor Industry Association (SIA). https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf.

Weber, V., M. P. Riera, and E. Laumann. 2023. *Mapping the World's Critical Infrastructure Sectors*. German Council on Foreign Relations. https://dgap.org/en/research/publications/mapping-worlds-critical-infrastructure-sectors.

Weld, S. 1889. "The Isthmus Canal and Our Government." *The Atlantic*. March. http://www.theatlantic.com/magazine/archive/1889/03/the-isthmus-canal-and-our-government/634037/.

Wicks, D. H. 1980. "Dress Rehearsal: United States Intervention on the Isthmus of Panama, 1885." *Pacific Historical Review* 49, no. 4: 581–605. https://doi.org/10.2307/3638968.

World Trade Organization. n.d. "Evolution of Trade Under the WTO: Handy Statistics." Accessed October 24, 2025. https://www.wto.org/english/res_e/statis_e/trade_evolution_e/evolution_trade_wto_e.htm.

Willis, H. H., M. L. DeKay, M. G. Morgan, H. K. Florig, and P. S. Fischbeck. 2004. "Ecological Risk Ranking: Development and Evaluation of a Method for Improving Public Participation in Environmental Decision Making." *Risk Analysis* 24, no. 2: 363–378. https://doi.org/10.1111/j.0272-4332.2004.00438.x.

Willis, H. H., A. Narayanan, B. Boudreaux, et al. 2024. *Global Catastrophic Risk Assessment*. RAND. https://www.rand.org/pubs/research_reports/RRA2981-1.html.

Willis, H. H., M. Tighe, A. Lauland, et al. 2018. *Homeland Security National Risk Characterization: Risk Assessment Methodology*. RR-2140-DHS. RAND Corporation.

Wright, W. M., M. C. Shupe, N. M. Fraser, and K. W. Hipel. 1980. "A Conflict Analysis of the Suez Canal Invasion of 1956." *Conflict Management and Peace Science* 5, no. 1: 27–40. https://doi.org/10.1177/073889428000500102.

Yee, Y., and J. Glanz. 2021. "How One of the World's Biggest Ships Jammed the Suez Canal." *New York Times*. July 19. https://www.nytimes.com/2021/07/17/world/middleeast/suez-canal-stuck-ship-ever-given.html.

Zaki, C. 2017. "An Overview of Structural Imbalances in Egypt." *Égypte/Monde Arabe* no. 16: 99–124. https://doi.org/10.4000/ema.3727.