When smart systems fail: the ethics of cyber-physical critical infrastructure risk

Caitlin Grady
Department of Civil and Environmental Engineering
Rock Ethics Institute
Penn State University
University Park, PA USA
cgrady@psu.edu

Sarah Rajtmajer
College of Information Sciences and Technology
Rock Ethics Institute
Penn State University
University Park, PA USA
smr48@psu.edu

Lauren Dennis
Department of Civil and Environmental Engineering
Penn State University
University Park, PA USA
lud93@psu.edu

***Abstract*— Critical infrastructure remains an important part of daily life in support of providing basic goods and services. Cyber-physical connections between critical infrastructure systems and sectors continue to increase with the development and integration of new technology. We study the emerging threat landscape and ethical implications of cyber-physical connections within critical infrastructure. Using both a comprehensive literature review and a coupled epistemic-ethical analysis, we provide evidence that new approaches in science, technology, and policy are necessary. We propose future research directions and emphasize the need for value transparency throughout the science policy landscape.**

Keywords*— *critical infrastructure; ethics; risk; cybersecurity; cyber attack; responsibility

I. Introduction

Everyday life is supported by a web of interconnected infrastructures. From the moment we turn on the light in the morning, to the trucks, trains, ships, and planes supporting our globally connected food supply, we rely on provisioning services across a variety of sectors. As defined by the United States Department of Homeland Security, critical infrastructure (CI) encompasses 16 sectors such as communications, transportation, energy, agriculture, and financial services, whose physical or virtual systems, networks and assets are so vital to the country that their disruption or destruction would have a debilitating effect on physical security, economic security, and public health [1], [2]. Protecting these assets has remained a government priority across multiple administrations and parties [1], [3]. The cyber-physical connections across and within CI sectors have increased over the last decade or more, resulting in new and challenging threats [4].

In the United States, over the last decade, an increasing focus has been placed on the connections between cyber and physical infrastructure and how those connections present risks to system functioning. A new federal agency, the Cybersecurity and Infrastructure Security Agency (CISA) was created in 2018 to lead the protection of the nation's infrastructure. The White House has reported over 1,900 cyber breaches across all critical infrastructure sectors [5]. In 2020, U.S. government assets were subject to perhaps the largest cyber-attack in history through a months-long well-resourced campaign by Russian government entities that gained access to U.S. government agencies, critical infrastructure, and private sector organizations [6], [7]. The impacts of this intrusion are still not fully realized. If these examples are any indication of the threat landscape to critical infrastructure moving forward, disruptions may be more frequent and lead to vulnerabilities we have yet to understand. These highly connected systems influencing our daily lives bring important societal questions to the forefront of technology advancement.

In fact, the very use of the word "critical" suggests a specific, value-laden, ethical framework raising several further questions. For whom are these systems critical? Who is responsible for their protection? What happens to these systems and to broader society when they are subjected to risk? If services of interconnected systems are interrupted, who is responsible for addressing this disruption, determining what is most critical, and preventing future disruption? While the national security community in the United States has shown significant concern about threats to CI and has sought efforts to understand and mitigate them [4], we have not yet seen widespread efforts to specify ethical parameters within the public interest for interventions in this space. A few previous scholars have articulated the importance for considering human needs when managing critical infrastructure [8]–[11]. Clark et al., for example, argue for using a human capabilities approach to define what sectors should be considered most critical and further utilizes Maslow's Theory of Human Motivation to hierarchically arrange these critical sectors based on their provisioning of basic human needs [9]. Other scholars have articulated the need for utilizing social vulnerability assessments and minimum supply considerations to guide CI governance and failure [10]. Privacy and data collection have also been highlighted as ethical challenges surrounding CI management [11]. Missing from these dialogues are several important considerations which form the basis of our work. To further previous scholars, we explore moral responsibility and the ethics of cyber-physical CI by explicitly analyzing ethical issues that arise from a unique threat landscape using an epistemic-ethical analysis framework.

II. Methods

This paper examines the role of changing cyber threats and critical infrastructure risk within a framework tied to the ethical questions generated when critical infrastructure is disrupted. The aim of this paper is to articulate a set of epistemic and ethical concerns stemming from advanced cyber-physical CI connections. We argue over the course of this paper that the prioritization or devaluation of specific sectors, the ownership of these sectors, and the decisions around how to address risks across and within sectors involve ethical choices. Our focus throughout is on the United States, acknowledging that other jurisdictions may have different ownership and regulatory frameworks and are at varying stages of adoption of emerging technologies for critical infrastructure.

Given this frame, our investigations are precipitated by a series of questions: For whom are these systems critical? Who is responsible for their protection? What happens to these systems and to broader society when they are subjected to risk? If services of interconnected systems are interrupted, who is responsible for addressing this disruption, determining what is most critical, and preventing future disruption? We expand upon previous work by not only furthering discussions around risk and ethics but also addressing gaps in previous literature that fail to describe how the unique challenge presented by increasing cyber connectedness underlying physical infrastructure further complicates choices and amplifies the ethical imperative of managing these systems with care.

This paper is structured into five sections. The next section articulates the current state of what we mean by "threat" as well as the myriad of shifting motivations and emerging types of harm to cyber-physical CI. Section 4 provides our analysis of responsibility, ethics, and moral principles at play given these threats. Section 5 builds upon our findings in Sections 3 and 4 to present and debate a future agenda for science and practitioners. Finally, we end with a brief conclusion of our key findings.

III. The Emerging Threat Landscape

A 2019 report of the National Consortium for the Study of Terrorism and Responses to Terrorism (START) [12] determined there to have been 130 "significant disruptive cyber-physical attacks" between January 2009 and November 2019. These 130 attacks were determined as meeting three key inclusion criteria: 1) originating in the cyber domain; 2) targeting a critical infrastructure sector as defined by the Presidential Policy Directive 21 (PPD-21); 3) representing a disruptive cyber-physical incident or a disruptive cyber-operational incident. Crucially, the report indicates that these events have been steadily increasing in frequency over the years, with the largest jump between 2015 (8 total attacks) and 2017 (30 total attacks). This trend parallels steep increases in the frequency and severity of cyber incidents more broadly - both domestically and internationally, in both industry [13] and government sectors [14]. Just this summer, the National Security Agency (NSA) and the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) released a joint Activity Alert [15] recommending immediate action to secure internet-accessible operational technology assets in response to malicious cyber activity against critical infrastructure in recent months.

There are several reasons for observed increases in cyber attacks, broadly, and cyber-physical attacks, specifically. With increased automation, complexity, and interdependence inherent in smart systems, a new threat landscape is developing for cyber-physical critical infrastructure. Following, we argue that this landscape is meaningfully distinct from past counterparts, highlighting three emerging trends.

A. Trend 1: Emerging vulnerabilities in cyber-physical systems

Fundamentally, the integration of new technologies into cyber-physical infrastructure and industrial control systems (ICSs) increases the number of system access points. In addition to physical incidents having physical consequences, cyber incidents can have physical consequences as well. Connected systems are susceptible to IT commodity malware and ransomware (see Table I), while automation can result in unanticipated permutations of functioning and subsequent opportunity for smart attackers [16], [17]. The primary classes of attack on computers and servers have been a subject of research for decades, and general mitigations for these attacks are known. However, the specific vulnerabilities, risks, threats and impacts of new cyber-physical technologies embedded within Smart Cities will only be understood as these systems are introduced and breached. The 2017 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure [3] highlights migration to the cloud as part of its defense strategy. While the cloud offers scalability and flexibility, it also expands the attack surface and allows malicious actors to deliver attacks faster, farther, and more inexpensively.

Adding complexity, modernization and automation of cyber-physical infrastructure is being rolled out inconsistently and, in many sectors, without clearly defined industry standards and practices as a guide [16]. Old and new systems and software interoperate with more or less congruence and transparency, resulting in widespread network vulnerabilities. System updates may be difficult or prohibitively expensive to implement, especially in the case of essential infrastructure for which lengthy lags in functionality are particularly disruptive. At present, the 2018 Cybersecurity Framework developed and shared by the National Institute of Standards and Technology (NIST) serves as a primary reference for standards, guidelines and practices to promote the protection of critical infrastructure [18]. A first version of the voluntary Framework was released in 2014, in response to a 2013 Executive Order [19]. The Framework represents voluntary guidance, created through collaboration between industry and government stakeholders. Beyond this document, each sector has managed its own dissemination of recommendations and best practices with varying coverage. A listing of these resources is maintained by NIST [18]. They represent an assortment of reports, assessments, and guidance, conspicuously lacking a clear, unified set of standards cross-cutting services and sectors, targeting interoperability and interpretability of connected cyber-physical systems.

This work was partially supported by NSF Award Number 1941657

Of course, a major impediment to interoperability amongst cyber-physical infrastructure is its ownership structure. As much as 85% of the nation's critical infrastructure is privately owned [24]. Collaboration and information sharing between government and private sector partners, and amongst private sector partners themselves, is balanced against safeguarding proprietary information and competitive advantage. To facilitate voluntary collaboration and information sharing within and across CI sectors, the government has established coordinating councils. Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) represent two such bodies that bring together private stakeholders to collect and share information amongst communities of interest [20]. These groups, however, face important challenges. Ideally, stakeholders must be willing to participate in reciprocal information sharing. They should receive and provide threat information in a way that protects appropriate permissions, in particular for sensitive information. And, they should be able to do so rapidly during critical events and emergencies. Herein, we call upon the community of researchers to study the structures and incentives necessary to overcome these challenges.

Finally, physical infrastructure in the US is aging. That is, the average age of physical infrastructure in the US is increasing and costs to improve it are high and rising [21]. In 2009, FEMA identified 2,047 "high hazard" dams [22]. The American Society of Civil Engineers (ASCE) classified 12% of the nation's 600,000 bridges as structurally deficient, and declared 14% of bridges functionally obsolete [23]. The issue of aging infrastructure is closely tied to insufficient funding. The ASCE has estimated that the United States needs to invest $2.2 trillion to meet future infrastructure needs, of which $1.1 trillion is currently unfunded. Here as well, private ownership of infrastructure bears critical relevance as safety and security compete with economic factors, and as these factors differentially impact systems and sectors. These vulnerabilities not only influence the safety and security of cyber-physical critical infrastructure, but also present important questions of moral responsibility which we elaborate on in section 3.

B. Trend 2: Increased sophistication of attacks

In parallel to development of increasingly sophisticated cyber-physical systems and the rollout of Smart City technologies, of course, cyber attackers are also leveraging artificial intelligence (AI) to revolutionize their approaches. Threats themselves are becoming increasingly automated and increasingly smart. Bots, or simple pieces of software, are much better than humans at simple, repetitive tasks. They can ping a system in search of vulnerabilities with greatly reduced time, effort, and cost. Moreover, emerging, intelligent threats will be able to respond to non-automated security software in real time, forecast and circumvent defensive responses [24]. Early examples of machine learning in cyber attacks include models which defeat CAPTCHA systems [25], [26] and automate tests of stolen usernames and passwords across websites [27, p.]. More recently, we have begun to see attacks using smart malware, stealthy spyware, and synthetic fishing trained by deep learning. AI has enabled software that observes, learns, and mimics patterns of normal user behavior inside a network to remain hidden from security tools. Moving forward, AI will be deeply integrated in targeting, deployment and concealment of cyber threats (see [28] for a survey).

Another critically important challenge within the emerging cyber threat landscape is the challenge of attribution. According to the 2019 START report, 66 of the 130 incidents identified (51%) were unattributed [12]. Unattributed threats are problematic for a number of reasons. From a strategic perspective, difficulty attributing cyber threats complicate questions about deterrence and retaliation [29], and the security community has called for a reimagining of deterrence in the context of cyber threat where attribution is imperfect [30]. From a technical perspective, challenges with attribution undermine our understanding of adversaries' cyber capabilities and subsequent preparedness for response. In cases of cyber espionage and cybercrime, these challenges undermine our appreciation of potential impacts and downstream consequences of these attacks.

Along those lines, emerging threats have opened doors to new motivations and harms. Kinetic attacks on CI (e.g., terrorist attacks [31], [32]) have traditionally sought, primarily, to inflict physical damage to the infrastructure and consequent disruptions to service. Psychological damage and geopolitical maneuvering have sometimes been parallel aims [32]. However, according to the 2019 START report [12], espionage was the most common identified motivation amongst cyber-physical attacks studied between 2009 and 2019 (29 of 88 total incidents). Cybercrime was another important motive (28/88), equally important to destruction (28/88). Analysis of attacks specifically directed at the US parallels this breakdown (7/18 espionage, 6/18 cybercrime, 4/18 destruction, and 1/18 proof of concept). This shift points to a broader spectrum of losses associated with attacks on cyber-physical systems as compared to their offline counterparts. The dual of these potential harms are, of course, tangible gains for would-be attackers.

C. Trend 3: The impact of cyber-physical disruptions are increasingly difficult to predict

Critically, the widening set of motivations associated with cyber threats and associated set of consequences complicate projections of impact. Attackers with access to control systems can steal information about system status, operations, and environment. In some cases (e.g., [33]), this is done covertly and over an extended period of time, furnishing attackers with critical details to facilitate physical disruption. In others, this information may include personal or sensitive individual data records (e.g. [34]). Psychological impacts of cyber attacks are often magnified as well. Attacks originating in the cyber domain can cause confusion and uncertainty, in addition to damage (e.g., [35], [36]). Beginning and endpoints of these operations are not necessarily clear, nor are their ways and means, or next steps.

A paramount challenge to understanding, predicting, quantifying and ultimately mitigating the impact of disruptions to cyber-physical critical infrastructure, whether due to failure or attack, is the connectedness of interacting systems. Physical, cyber, geographical, social and financial interdependencies within and between infrastructures allow impacts to propagate or even escalate through these networks [37]–[39].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TTS.2021.3058605, IEEE Transactions on Technology and Society

An early example of this was the 2003 blackout across the Northeast US and Canada, caused by a software bug in the alarm system at an electric utility in Ohio. The outage affected an estimated 50 million people, cost the US between 4 and 10 billion dollars, generated significant impact for power generation, water supply, transportation, and communication, and resulted in the rapid shutdown of nine nuclear power plants. The incident was a harbinger for technologists and policymakers alike; leaders from both countries stood up a task force to explore mitigation strategies for similar future events [40]. Several other recent examples of multi-sector cyber-physical disruptions, specifically originating through cyber attacks, are listed in Table I. Looking forward to Smart Cities (and megacities) of the near future, we must prepare for cascading impacts amongst cyber-physical systems at unprecedented scale. Richly interdependent cyber-physical infrastructure, including autonomous vehicles, vehicle-to-vehicle and vehicle-to-infrastructure communications systems, automated or semi-automated resource distribution and safety monitoring systems, coupled with unprecedented urban growth will both add complexity and raise the stakes. Finally, the physical, social, economic landscape underlying CI is itself becoming more tenuous. As global populations shift to urban areas [41], population will place a greater strain on infrastructure. Against this backdrop, CI will face the existential threat of climate change. Rising sea levels are forecasted to cause damaging episodic flooding to coastal infrastructure [42] and extreme weather events are anticipated to put stress on water treatment and energy infrastructures [43], [44]. CI under the stress of excessive demand will be particularly vulnerable to both failures and attack, and critically, these systems will be less resilient to disruptions when they occur.

As CI becomes increasingly connected and automation increasingly common, the great promise of Smart Cities is apparent. Integrated cyber-physical technologies and infrastructure are envisioned to improve quality of life and support environmental and economic efficiency [4]. Smart systems will be agile and robust, predicting resource needs, careful monitoring availability, planning and directing resources accordingly, and rapidly compensating for system failures. In order for these promises to be realized, however, within a complex and dynamic landscape, we argue that: 1) infrastructure control systems must be interoperable; 2) interdependencies amongst systems (including non-CI) must be transparent and well-understood; 3) inter- and intra-sectoral standards for security and operability must be established and maintained. These suggestions are given both as foundational to robust, resilient connected CI and to precursor to the study and determination of risks and responsibilities related to the management of these systems.

TABLE I. EXAMPLE CYBER PHYSICAL CI ATTACKS[a]

Event	Primary CI impacted	Secondary CI	Impact	Cyber approach	Reference
Maroochy Water Breach - 2000	Waste and Wastewater Systems	Healthcare and Public Health	1 Million Liters of sewage leaked into local waterways	Hacker accessed the Supervisory Control and Data Acquisition system (SCADA)	[45]
Estonian cyber attacks - 2007	Information Technology, Government	Communications, Financial Services	22 days of interrupted services on commercial and government servers	DDoS	[36], [46]
Stuxnet worm - 2010	Nuclear	Information Technology, Communications Government	Damage >1000 centrifuges at an Iranian uranium enrichment facility	Malware attack	[47]
Iranian infiltration of New York Dam - 2013	Dams	Information Technology	Information on status and operation of the dam collected, for 3 week period	Cyberspies hacked into control system of the dam	[33]
Ukrainian power grid attacks - 2015, 2017	Power	Information Technology	3 energy distribution companies impacted; approximately 225,000 people lost electricity for a number of hours	Cyberspies used phishing emails followed by credential theft to gain access to systems further infecting them with malicious firmware	[48]
NotPetya Maersk Shutdown - 2017	Information Technology	Transportation systems	NotPetya impacted multiple CI in many countries, example includes $200-$300 million in damages to Shipping Company Maersk, shut down of port of NYNJ	Ransomware attack	[35]
Hollywood Presbyterian Medical Center - 2016	Healthcare and Public Health	Communications	Computers offline for over one week, hospital paid $17,000 in bitcoin to the hackers	Ransomware attack	[34]
San Francisco transit hack - 2016	Transportation Systems	Communications	Loss of two days revenue	Ransomware attack	[49]
Ports of Barcelona and San Diego hacks - 2018	Transportation Systems	IT	undisclosed	Ransomware attack	[50], [51]

[a] Exemplary past cyber attacks which have influenced multiple CI system and are intertwined with cyber-physical connections. This table does not serve as an artifact of every cyber-physical attack on CI but rather as a starting point for discussing past events and future threat landscape throughout section 2.

IV. Moral Responsibility and Ethics of Cyber-Physical CI: Research and Management Futures

As described in Section 2, we argue that the new threat landscape of cyber-physical infrastructure risk is meaningfully distinct from past counterparts. This distinct threat warrants careful consideration of risks and responsibility. Building upon multiple disciplines, we utilize a coupled ethical-epistemic framework to argue there are important choices associated with both the management of interdependent critical infrastructure and future research directions in the cyber-physical CI landscape. These choices drive moral responsibilities across a variety of actors.

Modern political theory contends with the functions and responsibilities of the state with respect to public welfare and the satisfaction of basic needs for its citizens [52], [53]. Advanced, industrialized countries have seen increasing emphasis on individual responsibility and contraction of scope of and access to public benefits [54]. In the US, a new role for government has developed under welfare capitalism, coordinating public and private efforts for the finance and delivery of social welfare [55].

The social vulnerability studies literature focuses this broader theory on questions of minimum supply for goods and services such as electricity, water, and food. Moving beyond basic provisioning, this framing also discusses how minimum supply requirements are perceived to differ between different social groups (rich v. poor, single elderly v. households, etc.) as well as between different types of CI [10]. In linking CI management, social vulnerability, and minimum supply, authors Garschagen and Sandholz argue that there is a need to assess socially differentiated vulnerabilities towards critical infrastructure failure from both a scientific and politically relevant perspective [10]. In addition to provisioning of basic goods, various CI have large potentials for generating, creating, and storing personal information about citizens thus balancing the need for individual privacy and national security remains a challenging ethical issue [11].

A small group of scholars have begun to ask and answer the question- what are the ethical stakes surrounding disrupted critical infrastructure [9]–[11]. Clark et al. (2018), utilized both a Human Capabilities Approach and Maslow's Hierarchy of Needs to argue that a handful of CI sectors are necessary to provide several fundamental tenets of basic human needs [9]. Of the 16 sectors defined by the United States government as critical, they argued that four were critical to life and basic physiological needs (emergency services, public health, water, and agriculture) and four sectors were necessary for the safety and bodily integrity of others (transportation, national defense, financial services, IT). The remaining sectors provided services and securities above the two basic levels of human capability and hierarchy of needs thus represented less important CI sectors [9]. Additionally, this analysis called into question the entire approach of categorizing CI by sector instead of categorizing CI by the services certain components provide to citizens, since many of the sectors rely on each other though represent different components of basic human needs.

To further previous scholars, we utilize this section to showcase overlap and differences between moral responsibility and the ethics of cyber-physical CI by explicitly analyzing ethical issues that arise from the threat landscape we have articulated throughout section 2. We employ a coupled ethical-epistemic lens to identify both ethical and epistemic values related to these threats and further elaborate on ways in which these values influence three main themes relating to moral responsibility and the ethics of cyber-physical CI management. In using *epistemic values*, we adopt a definition relating to the works of philosophers such as McMullin, Tuana, Kuhn, and others who have utilized this phrase to identify values that promote truth-like character of science and that if pursued, helps attain knowledge [56], [57]. *Ethical values* on the other hand, govern and guide behavior and define what is right and wrong within communities and societies.

TABLE II. Emerging Ethical and Epistemic Values

Threat Trend	Emerging Epistemic Values	Emerging Ethical Values	Primary Ethical Theme	Secondary Theme(s)
Trend 1	Consistency Robustness of evidence Accuracy	Responsibility Privacy Reliability	Theme 1	Theme 3
Trend 2	Scope Fruitfulness	Justice Human well-being Privacy Responsibility	Theme 2	Theme 1 Theme 3
Trend 3	Accuracy Predictive power Methodological soundness	Citizenship Caring Justice	Theme 2	Theme 3

Coupled ethical-epistemic analyses have been used to elicit meaningful advancements in the field of climate science to promote ensuring scientific integrity in complex value dimensions [56], [58]. In utilizing this approach, we provide conclusions relevant to both the scientific and practitioner communities. To begin, Table II outlines our organization of emerging epistemic and ethical values related to each threat trend and identifies the theme in which these values will be further explored throughout this section.

A. Theme 1: Who is in charge? The responsible management of cyber-physical CI

Complicated cyber-physical system risks across various CI are further exacerbated by varied management across public and private entities. Variation in ownership arrangements create uncertainties regarding risk, responsibility, and regulatory influence. For physical infrastructure, in the United States there are some CI assets that are fully government owned as well as some assets fully owned by private corporations. There are also some assets owned through public-private partnerships or community-based ownership arrangements. This variation makes responsibility for disruptions incredibly hard to articulate clearly, particularly for events that have yet to unfold [59]. In the cyber-physical landscape, this ownership variation produces dangerous security gaps due to a lack of coordination and ad hoc responsibility definitions that make it difficult to adequately balance risk and investments in the future [4]. In this section, we refer to responsibility to relate to the responsibility of the actor managing various cyber-physical CI.

As highlighted in our discussion of threat *Trend 1,* to overcome challenges faced by the myriad of ownership arrangements, at a minimum the owners and managers of these systems must be willing to participate in reciprocal information sharing to enable connected cyber-physical risk management. Unfortunately, this remains a challenge in the cyber-physical CI management domain. Future research in this area is important to understand the structures and incentives necessary to overcome these challenges under multiple frameworks of regulatory and non-regulatory approaches. For example, since the current NIST standards, guidelines and practices to promote the protection of critical infrastructure are voluntary in nature [18], it would be helpful to build greater understanding around incentives to comply with these standards if they remain voluntary as well as what the impacts would be if various forms of non-voluntary regulations were put in place to govern the responsible behavior of cyber-physical CI owners and managers. The lack of uniform and regularly updated cybersecurity regulations and challenges with coordination for critical infrastructure managers also presents several important ethical issues around privacy. Works relating to the ethics of data sharing [60], regulating IoT devices and connections [61], and ethics of AI and cyber conflict [62] are all related to privacy risks further exacerbated by complex ownership arrangements and vague voluntary cybersecurity guidelines.

Under a market-based system, consumers would have the ability to influence both public and private owners to take part in responsible decisions to mitigate several types of risks identified in *Trend 1,* for example, adoption of cybersecurity measures and future investment in aging infrastructure. This condition would require consumers to have the ability to choose services from actors who are enabling those values. With regard to most critical infrastructure sectors, however, choice does not manifest to the level of the consumer. For example, water infrastructure is often only provided by one company or government provider due to the significant costs associated with access, treatment, and distribution of that basic resource. Likewise, only about 5 percent of the United States electricity load for residential consumers is sold by competitive suppliers [63]. For agricultural and food service provisioning, despite the widespread choices available throughout most grocery stores, only about 10 food and beverage companies control the large share of food products worldwide with their network of subsidiaries [64]. As such, stakeholders involved in decision making and responsibility of ethical management of cyber-physical CI generally leave out public citizens.

This opaque distribution of ownership arrangements across sectors and locations raises ethical challenges across all three of our threat trends and relates to all of our ethical themes. These complex systems make it difficult to accurately represent many of the socio-economic and environmental implications of events and actions. As noted, research which seeks to understand the structures and incentives necessary to overcome these responsibility challenges under multiple frameworks of regulatory and non-regulatory approaches could be pursued by several different domains of scholars. Additionally, furthering research efforts to showcase distribution of risk and responsibility under various conditions and scenarios of threat, disruption, and attack, will contribute to a better ability to have meaningful conversations about ethical approaches to cyber-physical CI management.

B. Theme 2: How are impacts felt? The distribution and understanding of risk

Impacts of disrupted physical or cyber infrastructure are not evenly distributed. Electricity outage analyses at different scales have showcased that neighborhoods and counties with higher proportion of disadvantaged groups experience longer power outages [65], [66], yet those outages may be due not to population demographics but rather the provisioning of other priority assets (i.e. other critical infrastructure) such as hospitals [65]. In urban planning literature, the study of transportation disadvantaged groups has articulated that these vulnerable populations face not only problems of social exclusion in location, but also experience greater exposure to multiple social and environmental threats [67], [68]. Implications of spatial trends, locations of infrastructure and critical services, and vulnerable groups have become a larger part of the national dialogue in part due to the effect this provisioning of infrastructure has had on COVID-19 spread (i.e. [69]).

Interdependencies and cascading failures are not only seen in physical CI, but these challenges and complexities extend to both cyber infrastructure and the experience of living in poverty. Economic losses associated with data breaches can push vulnerable individuals over a financial cliff. When individuals who are barely covering their day to day expenses fall victim to a cyber fraud or attack, such as a credit card being stolen or losing access to their smartphone, the cascade of impacts can be catastrophic [70]–[73]. Additionally, government systems, the same systems considered to be critical infrastructure, often support the most vulnerable communities through housing, medical, and food needs. These systems are subject to breach as shown through the 2016 HUD breach and the 2018 Medicare/Medicaid breach.

Not only are CI disruptions not evenly distributed, but the impacts of cyber-physical disruptions are increasingly difficult to predict, model, or understand. Our threat *Trend 3* articulates rationale behind this assertion. Drawing on our emerging epistemic values, scope, consistency, robustness of evidence, and methodological soundness are all threatened by the increased complexity and vulnerability of cyber-physical critical infrastructure systems. Consistency, as defined by Kuhn [57], affirms the need for scientific pursuits and new theories to not only be consistent internally with itself, but also with other currently accepted theories applicable to related aspects of nature. This becomes difficult to achieve when there are no clear theories that govern human nature in an evolving complex and cascading threat landscape. Scope is also an important epistemic value to consider and properly articulate when describing research around cyber-physical CI. At what point do you draw your system boundaries? What are the implications of those boundary drawings? Do the consequences of a researcher scholar's results extend beyond the particular observations? Often research scholars will define system boundaries in methodological articulations, however the assumptions and inferences that those boundaries influence are not often described when discussing outcomes, theories, and implications of approach.

What about the ethical implications of the unequal distribution of risk for cyber-physical CI and the inability to accurately predict disruption? As highlighted in our discussion of threat *Trend 2*, responsibility for cyber attacks varies widely and is not always clear. Thus, the malicious actor is not constrained by norms governing behavior, making ethical actions and reactions unclear. We also know that disruption impacts different groups in different ways, though to date, this knowledge has often focused on evaluating risk to one type of critical infrastructure and not multiple linked systems or cyber-physical systems specifically. Finally, *Trend 3* articulated that impacts of cyber-physical disruptions are increasingly difficult to predict, model, or understand. The three challenges of attack attribution, understanding differential impacts on populations from disruptions in interconnected CI systems, and the difficulty in predicting, modeling, or understanding impacts of cyber-physical disruptions present challenges in studying the ethical landscape of cyber-physical CI due to uncertainties in our understanding of the system. As research advances to address these challenges in our understanding, potential ethical implications should be equally considered.

Scholars have articulated the need to understand socially differentiated vulnerabilities in multiple ways [10] and have primarily done so through a focus on human well-being as it relates to the basic provisioning of goods and services like food, water, electricity, and healthcare [9]. In addition to human well-being are considerations of privacy, justice, citizenship, and caring. For example, in democratic societies citizenship is hailed as a key value governing political construction and representation. Despite this value, the public is often completely absent from decision making around cyber-physical infrastructure management. Even outside of the act of decision making itself, the public is not highlighted in any of the stakeholder groupings represented in the various reports and documents we reviewed for this work. This omission leads into the third ethical theme which relates to how we define the notion of critical and how that definition has ethical implications. An important step forward in building greater understanding around the epistemic and ethical value choices at play here is to involve all stakeholders, particularly those often neglected, in research and management analyses for cyber-physical CI.

C. *Theme 3: Why is CI critical? Defining what we manage*

In the United States and many other countries worldwide, the definition of critical infrastructure is relevant to security of the State [74], [75]. This State-centered definition of security showcases specific values that influenced decisions about why systems and sectors are classified as critical. Complex ownership relationships and state-sponsored framing has allowed for critical infrastructure systems to "operate as congealed socio-economic and political interests under the mantle of criticality" [59]. One ethical approach to shifting these values to align with human well-being and basic provisioning has called for CI to be structured around service provisioning instead of by arbitrary sector [9]. Even prior to realignment, transparency in agenda setting and defining scope are necessary for just and equitable management of cyber-physical CI. Additionally, the notion of criticality is a function of scale, time, and place. For example, do slow onset events have different ethical implications than rapid onset events for cyber-physical disruption?

As articulated throughout section 3, a coupled epistemic-ethical framework allowed us to explore important considerations across research and management agendas for cyber-physical risk and security. Previous scholars who highlight ethical issues relating to critical infrastructure focus primarily on issues relating to human well-being and justice with a small focus on responsibility. Here, we showcased a much broader set of ethical concerns as well as epistemic values that will be important to consider as researchers move forward in exploring cyber-physical infrastructure systems.

V. Conclusions

Throughout this paper we have argued two important points. First, cyber-physical critical infrastructure faces unique challenges that are meaningfully distinct from past counterparts. Second, both the management of and research about cyber-physical critical infrastructure has important society-wide ethical implications. To defend these assertions, we analyzed the current and future threat landscape across cyber-physical infrastructure in three trends. We then showcased an epistemic-ethical analysis to unearth societally relevant ethical challenges facing cyber-physical critical infrastructure science and management.

We have shown that not only are there important threats and ethical issues surrounding cyber-physical CI, but also that to address multifaceted technology-related problems, we need to integrate efforts in STEM research and technology with multiple disciplines across humanities and social sciences domains. Leading into the future, transparency in values choices, both epistemic and ethical, will ensure both scientific pursuits and policy or management pursuits. Looking to the future, we call for research scholars to articulate values choices throughout the documentation of their risk and resilience work related to cyber-physical critical infrastructure. Additionally, practitioners in this space may utilize our work to further consider and integrate public citizens into the decision making process around cyber-physical CI management. Finally, unpacking each aspect of each epistemic and ethical issue will require a larger group of scholars to engage in questions at the interface of technology, engineering, and society.

Acknowledgment

We would like to acknowledge the Rock Ethics Institute and the Center for Security Research and Education for supporting our efforts to pursue these topics. This effort was partially supported by NSF Grant Award Number 1941657.

References

[1] Executive Office of the President Barack Obama, *Presidential Policy Directive -- Critical Infrastructure Security and Resilience*. 2013.

[2] P. W. Parfomak, "Vulnerability of Concentrated Critical Infrastructure: Background and Policy Options," Congressional Research Service, RL33206, Dec. 2005. [Online]. Available: https://fas.org/sgp/crs/homesec/index.html.

[3] Executive Office of the President Donald Trump, *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. 2017.

[4] "Cyberspace Solarium Commission Final Report," US Cyberspace Solarium Commission, Mar. 2020. Accessed: Apr. 21, 2020. [Online]. Available: www.solarium.gov.

[5] The Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," Executive Office of the President, Washington D.C., Feb. 2018. Accessed: Apr. 21, 2020. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf.

[6] Cybersecurity & Infrastructure Security Agency, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations | CISA," Department of Homeland Security, Alert AA20-352A, Dec. 2020. Accessed: Jan. 06, 2021. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-352a.

[7] T. P. Bossert, "I Was the Homeland Security Adviser to Trump. We're Being Hacked.," *The New York Times*, Dec. 17, 2020.

[8] S. S. Clark and T. Seager, "A Human-Centered Approach to the Prioritization of Critical Infrastructure Resilience," George Mason University, Jul. 2017. Accessed: Apr. 21, 2020. [Online]. Available: https://cip.gmu.edu/2017/07/13/human-centered-approach-prioritization-critical-infrastructure-resilience/.

[9] S. S. Clark, T. P. Seager, and M. V. Chester, "A capabilities approach to the prioritization of critical infrastructure," *Environ Syst Decis*, vol. 38, no. 3, pp. 339–352, Sep. 2018, doi: 10.1007/s10669-018-9691-8.

[10] M. Garschagen and S. Sandholz, "The role of minimum supply and social vulnerability assessment for governing critical infrastructure failure: current gaps and future agenda," *Nat. Hazards Earth Syst. Sci.*, vol. 18, no. 4, pp. 1233–1246, Apr. 2018, doi: 10.5194/nhess-18-1233-2018.

[11] J. Betts and S. Sezer, "Ethics and privacy in national security and critical infrastructure protection," in *2014 IEEE International Symposium on Ethics in Science, Technology and Engineering*, Chicago, IL, USA, May 2014, pp. 1–7, doi: 10.1109/ETHICS.2014.6893417.

[12] S. Sin and R. Washburn, "Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset," National Consortium for the Study of Terrorism and Responses to Terrorism, University of Maryland, Research Brief, 2019. Accessed: Apr. 21, 2020. [Online]. Available: www.start.umd.edu.

[13] Hiscox, "Cost and Frequency of Cyber Attacks on the Rise, yet Companies are Less Prepared to Combat Attacks, According to Hiscox Cyber R," *Bloomberg.com*, Apr. 23, 2019.

[14] Center for Strategic & International Studies, "Significant Cyber Incidents Since 2006," Center for Strategic & International Studies, 2020. Accessed: Aug. 31, 2020. [Online]. Available: https://csis-website-prod.s3.amazonaws.com/s3fs-public/200727_Cyber_Attacks.pdf.

[15] Cybersecurity & Infrastructure Security Agency and National Security Agency, "NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems," Washington D.C., Alert (AA20-205A), Jul. 2020. Accessed: Sep. 11, 2020. [Online]. Available: https://us-cert.cisa.gov/ncas/alerts/aa20-205a.

[16] Office of Cyber and Infrastructure Analysis, "The Future of Smart Cities: Cyber-Physical Infrastructure Risk," Department of Homeland Security, National Protection and Programs Directorate, Washington D.C., Aug. 2015. Accessed: Aug. 31, 2020. [Online]. Available: https://www.us-cert.gov/sites/default/files/documents/OCIA%20-%20The%20Future%20of%20Smart%20Cities%20-%20Cyber-Physical%20Infrastructure%20Risk.pdf.

[17] Cybersecurity & Infrastructure Security Agency, "Recommended Cybersecurity Practices for Industrial Control Systems," Department of Homeland Security, 2020. Accessed: Aug. 31, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf.

[18] NIST, "Cybersecurity Framework Version 1.1," National Institute of Standards and Technology, Gaithersburg MD, Apr. 2018. Accessed: Sep. 10, 2020. [Online]. Available: https://www.nist.gov/cyberframework/framework.

[19] Executive Office of the President Barack Obama, *Executive Order -- Improving Critical Infrastructure Cybersecurity*. 2013.

[20] Cybersecurity & Infrastructure Security Agency, "A Guide to Critical Infrastructure Security and Resilience," Department of Homeland Security, Nov. 2019. Accessed: Sep. 10, 2020. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/Guide-Critical-Infrastructure-Security-Resilience-110819-508v2.pdf.

[21] FEMA, "Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency management," Federal Emergency Management Agency, Jun. 2011. Accessed: Aug. 31, 2020. [Online]. Available: https://www.fema.gov/pdf/about/programs/oppa/critical_infrastructure_paper.pdf.

[22] FEMA, "Identifying High Hazard Dam Risk in the United States," Federal Emergency Management Agency, Article, 2010. Accessed: Aug. 31, 2020. [Online]. Available: https://www.hsdl.org/?view&did=23898.

[23] ASCE, *2009 Report Card for America's Infrastructure*. Reston, VA: American Society of Civil Engineers, 2009.

[24] M. King and J. Rosen, "The Real Challenges of Artificial Intelligence: Automating Cyber Attacks," *CTRL Forward*, Nov. 28, 2018. https://www.wilsoncenter.org/blog-post/the-real-challenges-artificial-intelligence-automating-cyber-attacks (accessed Aug. 31, 2020).

[25] F. Stark, C. Hazırbas, R. Triebel, and D. Cremers, "Captcha recognition with active deep learning," 2015, vol. 2015, p. 94.

[26] J. Wang, J. H. Qin, X. Y. Xiang, Y. Tan, and N. Pan, "CAPTCHA recognition based on deep convolutional neural network," *Math. Biosci. Eng.*, vol. 16, no. 5, pp. 5851–5861, 2019.

[27] E. Ben-Meir, "Sentry MBA: A Tale of the Most Popular Credential Stuffing Attack Tool," *Cyberint*, Mar. 21, 2019. https://blog.cyberint.com/sentry-mba-a-tale-of-the-most-popular-credential-stuffing-attack-tool (accessed Sep. 10, 2020).

[28] N. Kaloudi and J. Li, "The ai-based cyber threat landscape: A survey," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–34, 2020.

[29] S. Baliga, E. B. de Mesquita, and A. Wolitzky, "Deterrence with imperfect attribution," Working Paper, 2019. Accessed: Sep. 10, 2020. [Online]. Available: http://home.uchicago.edu/bdm/PDF/deterrence.pdf.

[30] M. Hayden, *The Cyber Threat*. Washington DC, 2011.

[31] Middle East Online, "One year after gas plant attack in Algeria, security fears linger," *MEO*, Mar. 22, 2018. https://middle-east-online.com/en/one-year-after-gas-plant-attack-algeria-security-fears-linger (accessed Aug. 31, 2020).

[32] D. J. Sinai, "New Trends in Terrorism's Targeting of the Business Sector," *The Mackenzie Institute*, May 09, 2016. https://mackenzieinstitute.com/2016/05/new-trends-in-terrorisms-targeting-of-the-business-sector/ (accessed Aug. 31, 2020).

[33] D. Yadron, "Iranian Hackers Infiltrated New York Dam in 2013," *Wall Street Journal*, Dec. 21, 2015.

[34] R. Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating - Los Angeles Times," *Los Angeles Times*, Feb. 18, 2016.

[35] A. Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, Aug. 22, 2018.

[36] S. Herzog, "Revisiting the Estonian Cyber Attacks," *Journal of Strategic Security*, vol. 4, no. 2, pp. 49–60, 2011.

[37] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, and S. Havlin, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol. 464, no. 7291, Art. no. 7291, Apr. 2010, doi: 10.1038/nature08932.

[38] L. Chen *et al.*, "Hotspots: Failure cascades on heterogeneous critical infrastructure networks," 2017, pp. 1599–1607.

[39] P. Crucitti, V. Latora, and M. Marchiori, "Model for cascading failures in complex networks," *Physical Review E*, vol. 69, no. 4, p. 045104, 2004.

[40] A. Muir and J. Lopatto, "Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations," *US–Canada Power System Outage Task Force, Canada*, 2004.

[41] United Nations, "68% of the world population projected to live in urban areas by 2050, says UN," *UN DESA | United Nations Department of Economic and Social Affairs*, May 16, 2018. https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html (accessed Aug. 31, 2020).

[42] E. Kirezci *et al.*, "Projections of global-scale extreme sea levels and resulting episodic coastal flooding over the 21st Century," *Scientific Reports*, vol. 10, no. 1, Art. no. 1, Jul. 2020, doi: 10.1038/s41598-020-67736-6.

[43] S. J. Khan, D. Deere, F. D. L. Leusch, A. Humpage, M. Jenkins, and D. Cunliffe, "Extreme weather events: Should drinking water quality management systems adapt to changing risk profiles?," *Water Research*, vol. 85, pp. 124–136, Nov. 2015, doi: 10.1016/j.watres.2015.08.018.

[44] N. Abi-Samra, J. McConnach, S. Mukhopadhyay, and B. Wojszczyk, "When the Bough Breaks: Managing Extreme Weather Events Affecting Electrical Power Grids," *IEEE Power and Energy Magazine*, vol. 12, no. 5, pp. 61–65, Sep. 2014, doi: 10.1109/MPE.2014.2331899.

[45] J. Slay and M. Miller, "Lessons Learned from the Maroochy Water Breach," in *Critical Infrastructure Protection*, vol. 253, E. Goetz and S. Shenoi, Eds. Boston, MA: Springer US, 2007, pp. 73–82.

[46] NATO STRATCOM, "Hybrid Threats: 2007 cyber attacks on Estonia," NATO STRATCOM, 2007. Accessed: Aug. 31, 2020. [Online]. Available: https://stratcomcoe.org/hybrid-threats-2007-cyber-attacks-estonia.

[47] J. R. Lindsay, "Stuxnet and the limits of cyber warfare," *Security Studies*, vol. 22, no. 3, pp. 365–404, 2013.

[48] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[49] K. Holland, "Update on SFMTA Ransomware Attack," *San Francisco Municipal Transportation Agency*, Nov. 27, 2016. https://www.sfmta.com/blog/update-sfmta-ransomware-attack (accessed Aug. 31, 2020).

[50] IMarEST: Institute of Marine Engineering, Science & Technolog, "Ports of Barcelona and San Diego hit by cyber attacks," *Marine Professional*, Sep. 28, 2018.

[51] C. Clmpanu, "Port of San Diego suffers cyber-attack, second port in a week after Barcelona," *ZDNet*, Sep. 27, 2018.

[52] P. Streeten, "Basic needs: Some unsettled questions," *World Development*, vol. 12, no. 9, pp. 973–978, Sep. 1984, doi: 10.1016/0305-750X(84)90054-8.

[53] B. E. Moon, *The political economy of basic human needs*. Ithaca: Cornell University Press, 1991.

[54] N. Gilbert, *Transformation of the welfare state: the silent surrender of public responsibility*. Oxford: Oxford Univ. Press, 2004.

[55] N. Gilbert and B. Gilbert, *The enabling state: modern welfare capitalism in America*. New York: Oxford University Press, 1989.

[56] N. Tuana, "Understanding Coupled Ethical-Epistemic Issues Relevant to Climate Modeling and Decision Support Science," in *Scientific Integrity and Ethics in the Geosciences*, L. C. Gundersen, Ed. Hoboken, NJ, USA: John Wiley & Sons, Inc., 2017, pp. 155–173.

[57] T. S. Kuhn, "Objectivity, value judgment and theory choice, in The essential tension: Selected studies in the scientific tradition and change," Chicago, IL, USA: University of Chicago Press, 1977, pp. 356–367.

[58] L. A. Mayer *et al.*, "Understanding scientists' computational modeling decisions about climate risk management strategies using values-informed mental models," *Global Environmental Change*, vol. 42, pp. 107–116, Jan. 2017, doi: 10.1016/j.gloenvcha.2016.12.007.

[59] W. Steele, K. Hussey, and S. Dovers, "What's Critical about Critical Infrastructure?," *Urban Policy and Research*, vol. 35, no. 1, pp. 74–86, Jan. 2017, doi: 10.1080/08111146.2017.1282857.

[60] D. Shou, "Ethical considerations of sharing data for cybersecurity research," 2011, pp. 169–177.

[61] C. A. Tschider, "Regulating the internet of things: discrimination, privacy, and cybersecurity in the artificial intelligence age," *Denv. L. Rev.*, vol. 96, p. 87, 2018.

[62] S. Rajtmajer and D. Susser, "Automated influence and the challenge of cognitive security," in *Proceedings of the 7th Symposium on Hot Topics in the Science of Security*, Lawrence Kansas, Sep. 2020, pp. 1–9, doi: 10.1145/3384217.3385615.

[63] Energy Information Agency, "Participation in electricity customer choice programs has remained unchanged since 2013," Washington D.C., 2019. Accessed: Apr. 22, 2020. [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=41853.

[64] Oxfam, "Behind the Brands," 2014. https://www.behindthebrands.org/about/ (accessed Apr. 22, 2020).

[65] R. S. Liévanos and C. Horne, "Unequal resilience: The duration of electricity outages," *Energy Policy*, vol. 108, pp. 201–211, Sep. 2017, doi: 10.1016/j.enpol.2017.05.058.

[66] D. Mitsova, A.-M. Esnard, A. Sapat, and B. S. Lai, "Socioeconomic vulnerability and electric power restoration timelines in Florida: the case of Hurricane Irma," *Nat Hazards*, vol. 94, no. 2, pp. 689–709, Nov. 2018, doi: 10.1007/s11069-018-3413-x.

[67] A. Delbosc and G. Currie, "The spatial context of transport disadvantage, social exclusion and well-being," *Journal of Transport Geography*, vol. 19, no. 6, pp. 1130–1137, Nov. 2011, doi: 10.1016/j.jtrangeo.2011.04.005.

[68] A. Power, "Social inequality, disadvantaged neighbourhoods and transport deprivation: an assessment of the historical influence of housing policies," *Journal of Transport Geography*, vol. 21, pp. 39–48, Mar. 2012, doi: 10.1016/j.jtrangeo.2012.01.016.

[69] J. Németh and S. Rowan, "Is your neighborhood raising your coronavirus risk? Redlining decades ago set communities up for greater danger," *The Conversation*.

[70] M. Madden, M. Gilman, K. Levy, and A. Marwick, "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans," *Washington Law Review*, vol. 95, no. Rev 053, p. 74, 2017.

[71] M. Madden, "The Devastating Consequences of Being Poor in the Digital Age," *The New York Times*, Apr. 25, 2019.

[72] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 36–49, Jun. 2019, doi: 10.1016/j.ijcip.2019.01.001.

[73] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek, and P. Novotny, "Cascading Impact Assessment in a Critical Infrastructure System," *International Journal of Critical Infrastructure Protection*, vol. 22, pp. 125–138, Sep. 2018, doi: 10.1016/j.ijcip.2018.06.004.

[74] D. A. Baldwin, "The Concept of Security," *Review of International Studies*, vol. 23, pp. 5–26, 1997.

[75] A. Cherp and J. Jewell, "The concept of energy security: Beyond the four As," *Energy Policy*, vol. 75, pp. 415–421, Dec. 2014, doi: 10.1016/j.enpol.2014.09.005.