THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 1, 73-92
https://doi.org/10.55682/cdr/qw13-9v8c

RESEARCH ARTICLE

Lights Out: What Hurricanes Reveal about Cyberattacks and Blackouts

Tom Johansmeyer

Irregular Warfare Initiative, Washington, DC, USA
Institute of Cyber Security for Society (iCSS), Canterbury, UK

It is time to critically reassess the fear that a hostile state will launch a cyberattack on energy infrastructure to plunge a society into darkness and civil unrest. Not only has it never happened, but the component parts of the chain required in such a scenario are fragile. A lot must go wrong for an effort of that kind to achieve even partial success. This article offers an original contribution by examining the risk of cyberattack against the energy grid as a driver of civil unrest. In the absence of direct historical precedents, the analysis draws on adjacent cases from blackouts unrelated to cyberattacks to assess the potential societal impact of mass outages. While energy infrastructure remains a frequent target for cyberattacks, the existing security architecture has largely held, provided it continues to adapt. Persistent fear surrounding this threat may therefore misdirect resources and attention from more pressing security challenges.

Keywords: cybersecurity, security strategy, international security, economic security, cyber war, energy security.

Corresponding author: trj5@kent.ac.uk

INTRODUCTION

The fear is real – even if the risk may not be. Many worry that a hostile state could launch a cyberattack against the United States or its allies, plunging them into darkness and sparking widespread civil unrest. According to this logic, ensuing riots would be catastrophic, marked by looting, destruction, and indiscriminate violence. The costs to society would be immense, and that is even after an expensive effort at both systems remediation and the physical repair of the power grid. This scenario foregrounds the potential consequences of a hostile cyberattack on a nation's capacity to generate and transmit electricity. However, executing such a large-scale attack is extremely difficult, and even if it were feasible, historical cases suggest the outcomes would be far less severe.

This article examines the specific scenario of a hostile cyberattack targeting energy infrastructure with the intent of instigating civil unrest through widespread power outages. While this focus may appear narrowly defined, the scenario warrants careful consideration. It is a unique problem in that it is widely feared (as discussed in the next section), partially realized in several cases involving different aggressor and target states, and has reference points for mass blackouts outside the scope of hostile cyberattacks. These precedents support a case study approach, enabling comparative analysis to assess both the impact of such an attack and the likelihood of ensuing civil unrest. What makes the problem particularly compelling is the contrast between prevailing fears and the growing body of evidence suggesting that such fear may be misplaced.

This article stems from the author's extensive experience in the insurance and reinsurance industry. When presented with historical cases that challenge prevailing fears about cyberattack-induced blackouts, the author was confronted with questions such as, "What about riots?" This reflects a broader belief that cyberattacks could be used to foment civil unrest. While blackouts may lead to various consequences, civil unrest is frequently used as shorthand for severity. Because damage from cyberattacks is often reversible, the occurrence of widespread civil unrest is seen as an indicator of a particularly high-impact event. There are many reasons to protect energy infrastructure that do not rise to this level of social impact, but ensuing civil unrest signifies an extreme impact that is often discussed but which remains remote.

To assess the potential effects of cyberattacks on the power grid, and ensuing civil unrest, several blackout events are compared, revealing not only the absence of significant civil unrest but also that cyberattack-induced blackouts have, to date, been less severe and easier to remedy than feared. The seductively intuitive chain of events from cyberattack to blackout to societal and economic chaos lacks historical support. This is reinforced by research arguing that such acts of cyber aggression are unlikely to produce (Brooking and Lonergan 2023; Rid 2011; Gartzke 2013). This article investigates past blackout examples to demonstrate that the risk of a major cyber-induced blackout – one affecting tens of millions– is highly improbable,

and even if it were to occur, the likelihood of blackout-driven civil unrest remains very low.

The argument in this article primarily reflects U.S. and allied-state contexts, focusing on the concerns and fears that adversaries of those states will execute cyberattacks intended to induce blackouts and instigate civil unrest. However, the findings of the case study analysis in this article are likely portable to the perspectives of U.S. adversaries, as well.

LITERATURE REVIEW

Government experts agree that cyberattacks on the energy sector are a critical concern for several reasons. However, there is little historical evidence of widespread outages caused by cyberattacks. Therefore, the author proposes the use of data from significant outages caused by natural disasters. The discussion requires consideration of which catastrophic events trigger civil unrest. This includes both natural disasters and human-made catastrophes. While a key argument of this paper is that widespread power outages are unlikely to cause civil unrest, based on the preponderance of historical examples, it is necessary to understand why civil unrest generally has not arisen following blackouts and why that is unlikely to change.

To fully understand the problem of civil unrest following both natural and unnatural disasters, clear definitions are essential. According to the United Nations Office for Disaster Risk Reduction (UNDRR n.d.), a *disaster* is "a serious disruption of a community or a society at any scale due to hazardous events interacting with conditions of exposure, vulnerability and capacity, leading to one or more of the following: human, material, economic and environmental losses and impacts." To further qualify a disaster as natural, the Swiss Re Institute (2025), which is part of one of the world's largest reinsurance companies, uses the expression "caused by natural forces". Essentially, a naturally occurring event must not only strike with impact, but it must also affect people. Without human impact, a naturally occurring event cannot be considered a "disaster".

Civil unrest is more challenging to define. It is a broad term that covers the spectrum of political violence, described by Oyefusi (2010) as ranging from "peaceful protests" to "militarized struggle." This article takes a narrower view, though, requiring at least some level of violence. Must and Rustad (2019) help reduce the scope offered by Oyefusi, defining "civil unrest as demonstrations, protests, and the use of political violence". As with the treatment of natural disasters, this analysis focuses on major events, rather than small demonstrations that involve no violence or a minimal government response. Events under consideration in this analysis must involve violence or unrest that is directly and overtly political.

Drivers of Civil Unrest: Grievance and Opportunity Cost

Grievance is a key factor in understanding the risk and emergence of civil unrest. However,

as Wood and Wright (2016) note, grievance alone is not the problem, as it "may be pervasive within a society." It becomes a driver of unrest when an event "exacerbate[s] existing tensions between state and society" (1447-48). Although this insight stems from their study of natural disasters, it applies more broadly. Civil unrest tends to erupt when grievances are inflamed in ways that weaken state capacity and legitimacy, creating openings for violent resistance and disrupting economic development, deepening inequality, marginalizing groups, or triggering mass migration (Nel and Righarts 2008).

When civil unrest follows an event such as a natural disaster, it may arise from what Oyefusi (2010) calls an "opportunity structure" or what Nel and Righarts (2008) describe as a reduced "opportunity cost." Simply put, victims are more likely to act when they have less to lose. The factors that intensify this post-disaster calculus vary: grievances may predate the disaster or stem from dissatisfaction with the government's—or other institutions'—response. While corruption and self-serving aid distribution are frequently observed (Kim 2021), unrest may also result from the state's diminished capacity to deter violence after being overwhelmed by a natural disaster (Ghimire and Ferreira 2013).

As the opportunity costs of engaging in civil unrest decrease—particularly when affected populations feel they have nothing left to lose—the risk of upheaval grows. This risk is also shaped by the level of repression within a society. Highly repressive regimes tend to suppress unrest altogether, while fully open democracies often provide legitimate avenues to address grievances, reducing the likelihood of violent outcomes (Pfaff 2020; Drury and Olsen 1998). The highest risk appears to lie in between—within semi-democracies or "anocracies"—which allow some political participation but lack robust mechanisms to resolve public discontent (Regan and Bell, 2010). Such states, as researchers note, "permit some means of participation through opposition group behavior but have incomplete development of the mechanisms to redress grievances" (748-749).

Historically, disaster-induced unrest has been difficult to quantify. Efforts to track its frequency often overstate its prevalence (Johansmeyer 2022). In this author's own case study analysis (Johansmeyer 2024c), only twenty-two relevant instances were identified—suggesting that such events are far less common than estimates by Nel and Righarts (2008) would imply. The strongest indicator of post-disaster unrest remains a history of previous unrest, a finding noted by Brancati (2007), Pfaff (2020), and Drury and Olson (1998, 155), who observe that "one can expect that prior political unrest will be positively related to post-disaster unrest." While informative, this predictor offers limited practical utility for forecasting.

Ultimately, it is not the disaster itself—natural or man-made—that drives civil unrest, but the presence of unresolved grievances and a shift in opportunity costs. This perspective informs comparisons between natural and cyber catastrophes, particularly within the insurance industry, where assessing extreme-event risk and capital exposure is central

(Johansmeyer 2025). Since at least 1998, such analyses have shown that natural disasters produce significantly greater economic losses than cyber events (Johansmeyer 2024c). This contrast frames the present discussion on cyber threats to society, especially through attacks on critical energy infrastructure.

Modeling vs. Reality: The Economic Scale of Cyber Risk

Concerns about a blackout caused by a hostile cyberattack have been of sufficient concern to fuel nearly a decade of extensive research. In 2015, global insurance company Lloyd's of London and the University of Cambridge's Centre for Risk Studies released a study, which projected that such an attack could leave 93 million people without power and result in economic losses ranging from $243 billion to over $1 trillion (Ruffle et al. 2015). To reach such levels of economic impact would require profound cross-sector implications, spanning financial services, government response and emergency aid capabilities, access to food and water, and other basics of survival. It is a concern entertained by other insurance industry stakeholders, who are doubtless aware of the Lloyd's of London report. Munich Re (2018), one of the largest insurance and reinsurance companies in the world takes a nearly apocalyptic view of the cyber threat, claiming, "The major concern is the potential impact on critical infrastructure: communication and transport, heating and water supply, production processes and trading, emergency services (fire, police, ambulance), hospitals, financial trading, cash machines and supermarkets." Such fears, which Munich Re believes culminate in civil unrest, are grounded in experience with natural disasters and then assumed to scale upward.

However, the scale of impact raised in the examples above is difficult to imagine. To contextualize this, the 2003 blackout across the northeastern United States and southern Canada affected approximately 50 million people (Eyewitness News 2023) and caused economic losses of under $10 billion (Electricity Consumers Resource Council 2004). Even accounting for inflation, technological advances, and increased connectivity, it is difficult to reconcile how doubling the number of affected individuals would amplify the economic impact by more than twenty-four times. The 2015 Lloyd's scenario, while influential, appears significantly misaligned with historical evidence. Further, while there have been natural disasters that cause the sort of strain imagined by Lloyd's, Munich Re, and others (Beazley 2023), they have been extremely rare and do not justify the sorts of extrapolation to cyberattacks, as imagined here.

Lloyd's released a new study in 2023, focused on the economic losses that cyberattacks on the financial system could cause. While the report does not focus on blackout scenarios, it offers a useful reference point for estimating the economic consequences of a cyber-induced blackout. Developed by the Cambridge Centre for Risk Studies, the scenario projects $3.5 trillion in losses—an alarming figure that underscores the perceived severity of such threats. Yet, this projection stands in stark contrast to historical data: no past cyber incident has

resulted in economic damages exceeding $40 billion (unadjusted for inflation), and the last major event of this magnitude occurred in 2004 (Johansmeyer 2025). In total, aggregate economic losses from catastrophic cyber events—defined as those causing at least $800 million in inflation-adjusted damages and affecting a large population (Johansmeyer 2024b)—amount to only approximately $326.4 billion since 1998 (Johansmeyer 2024a), illustrated by year in Figure1. Once again, the hypothetical scale advanced in such modeling appears largely disconnected from historical precedent.

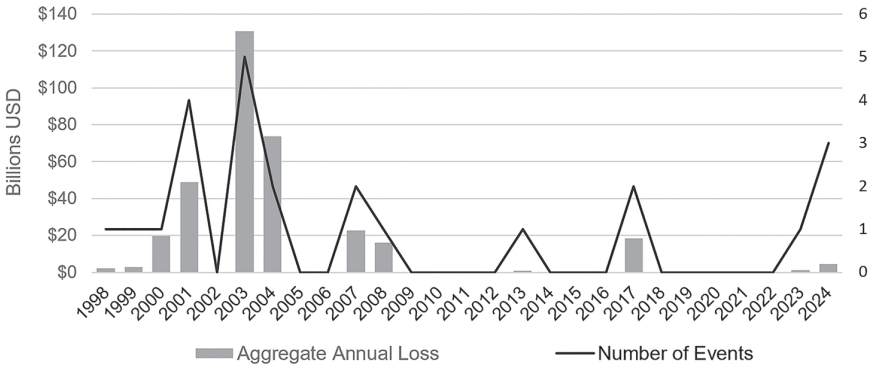

Figure 1. Economic Losses from Cyber Catastrophes from 1998-2024 (Johansmeyer 2024a)

Evidence from the Council on Foreign Relations Cyber Operations Tracker

Cyberattacks on energy infrastructure have become increasingly common (Morehouse 2023), reflecting a belief that disrupting power supply could destabilize societies across multiple security domains. The loss of power for an extended period would have commercial, societal, and political ramifications. Food and water security would presumably be threatened, and the government's ability to respond to acute need would presumably be impaired. Some of the most well-known cyberattacks in recent history have targeted energy infrastructure, including Stuxnet, the Colonial Pipeline attack, and the 2015 Ukraine blackout. Yet, none produced lasting disruption. Historical patterns suggest a prevalence of near misses and events with limited impact.

A review of the Council on Foreign Relations Cyber Operations Tracker (2024), which includes 873 incidents from 2005 to 2023, supports this view. Only eight cases involve cyberattacks on energy infrastructure, resulting in data destruction or sabotage. This figure excludes defacements or website disruptions unrelated to energy operations but includes attacks on nuclear facilities potentially linked to weapons development. If additional attacks occurred but were not recorded, their absence from public datasets may imply limited consequences. In light of this, the dramatic economic damage projected in modeling studies appears increasingly implausible.

State and state-like actors have so far failed to generate a substantial impact through major hostile actions in the cyber domain. Cyber weapons are costly, short-lived, and often of limited value (Smeets 2018), particularly given the reversibility of the damage they inflict. As discussed below, cyber weapons have generally failed to produce meaningful disruption. They are unlikely to "land a punch" and even when they do, reversibility means that the impact is typically transitory. According to Gartzke (2013), cyber war is, in actuality, a myth—with states seeking to inflict costs through hostile acts being more likely to choose kinetic alternatives (Schulze and Kerttunen 2023).

The track record of cyberattacks and their results complicates the effort to assess the actual risk. The contrast between dire projections, such as those from Lloyd's, and the relatively modest impacts recorded in the Cyber Operations Tracker may lead some to dismiss the possibility of a successful attack on energy infrastructure, especially one capable of triggering civil unrest.

Blackouts and Unrest in Context

There is always room for the belief that "the big one" just has not happened yet. Addressing such concerns requires more than a review of historical records of cyber incidents. It is also essential to examine the potential for civil unrest following any large-scale blackout – regardless of whether a cyberattack was the immediate cause. This broader approach enables the analysis of different links in the causal chain. Natural disasters provide a particularly useful reference point, given the frequency with which they cause blackouts.

Neither of the scenarios presented by Lloyd's has materialized. In fact, no major blackout, cyber-induced or otherwise, has approached the scale of disruption or economic loss outlined in their projections. Of course, the scale of economic damage alone may not predict the likelihood of post-event civil unrest. This can be gleaned from a comparison of not only the 2003 blackout but also those caused by natural disasters, which can result in widespread and long-lasting power outages. As mentioned earlier, the existing scholarship on civil unrest suggests that preexisting grievances are the most likely triggers for civil unrest following a natural disaster (Drury and Olsen 1998). However, empirical evidence of disaster-induced civil unrest remains limited.

The Property Claim Services (PCS) database by Verisk,[1] which catalogs natural and manmade catastrophe events in the United States since 1949 (and their attendant industry-wide insured losses), includes no instances of civil unrest linked to natural disasters, even in cases involving extensive power outages such as major hurricanes.[2] This includes major

1 Property Claim Services (PCS) by Verisk. https://www.verisk.com/solutions/claims/investigation/catastrophe-claims-data/

2 Hurricane Ida affected many more states than Louisiana, but the scope here is limited by the focus on Louisiana. The economic loss provided in the Table 1 includes Alabama and Mississippi. In using the industry-wide insured losses reported by insurance data/analytics organization PCS as a proxy, the overwhelming majority of the economic loss can be ascribed to the storm's impact in Louisiana. Disclosure: This author led PCS through May 2023, covering both the period of the storm's impact and the post-storm reporting period.

natural disasters that have occurred in recent years, during a period marked by broader societal challenges in the United States. Estimates vary, but some studies suggest there have been as few as twenty-two instances of disaster-induced civil unrest worldwide since 1970 (Johansmeyer 2022). It should, however, be noted that this recent analysis represents a sharp departure from earlier studies that placed the total between 176 (Ide et al. 2020) and 225 (Nel and Righarts 2008). Given this uncertainty, comparisons with non-cyber blackouts are instructive, though far from straightforward.

The 1977 blackout in New York lasted twenty-five hours and affected 9 million people (Latson 2015). It is believed that up to 80% of the economic damage from that event came not from the loss of power but from the attendant civil unrest (Corwin and Miles 1978). Notably, the 1965 Northeast blackout, which affected New York under similar conditions, did not trigger civil unrest. These divergent outcomes underscore the challenge of predicting unrest, even under seemingly similar circumstances. As a result, using civil unrest following blackouts to inform an analysis of civil unrest risk after cyber-induced blackouts is a fraught exercise.

Ultimately, the absence of civil unrest following decades of major energy infrastructure disruptions in the U.S. – to use a large and mature economy frequently impacted by blackout events not induced by cyberattacks (e.g., by natural disasters and human error) –suggests that the threshold for such an event remains extraordinarily high, questioning the plausibility of such an event in a developed economy with both mature infrastructure and experienced and tested emergency response mechanisms. Meanwhile, cyberattacks on energy infrastructure, with an aim to cause blackouts, continue to fall short of even modest benchmarks set by natural disaster-induced outages. The historical record, therefore, challenges the plausibility of the "hacking the grid" scenario often emphasized by Lloyd's and echoed within parts of the insurance industry.

COMPARATIVE CASE ANALYSIS

This article assesses the risk of civil unrest resulting from a widespread power outage caused by a cyberattack. Although both offensive and defensive cybersecurity strategies can affect energy infrastructure, historical evidence shows that such impacts have been limited. Understanding this gap is crucial: overstating the threat can lead to misallocated security resources—vulnerabilities in their own right. The goal here is not to "de-securitize" the energy–cyber nexus, but to recalibrate the perceived threat in light of historical evidence.

While blackouts are common worldwide, prolonged outages are not. A study presented at the 2016 IEEE International WIE Conference identified only 34 major global blackouts lasting over 100 hours from 1965 to 2015, most of which were caused by natural disasters (Rahman et al. 2016). The historical rarity of extended outages—whether from natural, cyber, or other causes—acts as a constraint on current risk estimates. While the absence of precedent doesn't preclude future escalation, claims of unprecedented impact require strong

justification. The examples cited below were selected precisely because they represent some of the most extreme—and unusual—blackout cases to date.

Beyond the outages themselves, this article explores conditions that might lead to civil unrest in their aftermath. Historically, such unrest has been rare. To this end, the analysis draws on cases of disaster-induced civil unrest, using natural disasters as analogues. Admittedly, this analysis is limited by the absence of the scenario it investigates: a large-scale blackout caused by a hostile cyberattack has not yet occurred. Yet, fear of such an event remains widespread. Drawing on adjacent historical cases, this article offers a grounded, corrective perspective on the discourse surrounding cyber-induced blackouts and civil unrest.

In the absence of a directly relevant case of a cyberattack on energy infrastructure causing a mass blackout and ensuing civil unrest, three adjacent examples are compared to triangulate the plausibility of the "hacking the grid" scenario. The examples were selected for their significant economic impact and their relevance to the type of risk under examination. Collectively, they help qualitatively illustrate the gap between perceived threats and historically observed outcomes. These events have also been extensively studied over time, providing a foundation for meaningful insights. The 2025 Iberian blackout, for instance, lasted less than 24 hours (Larson 2025). Although it is still too early for definitive economic assessments, initial estimates range from "tens of millions of euros" (Butler, Barnes, and Lahiri 2025) to as much as 2.25–4.5 billion euros (Reuters 2025). The lack of precision—an undefined lower bound and a wide upper range—undermines confidence in the reliability of these figures, limiting the example's usefulness for case study analysis.

The cases selected are predominantly U.S.-centric, with the exception of the 2015 blackout in Ukraine. This reflects a combination of factors: greater data availability and credibility, a higher likelihood of major blackouts, and sufficient economic activity to produce measurable impacts. U.S. cases also benefit from related precedent events, enabling richer qualitative analysis. While protracted outages have occurred elsewhere—such as following the 2023 Kahramanmaraş earthquake in Turkey, which left some areas without power for two months (UNOSAT 2023)—such events are too recent and lack the comparative data needed for robust analysis.

These three examples are the 2003 blackout event in the northeastern United States and southeastern Canada, Hurricane Ida in Louisiana, and the 2015 cyberattack by Russia on Ukraine's power grid. The 2003 blackout illustrates the effect of a major power outage on a large population. Although a cyberattack did not cause it, it demonstrates the breadth of its impact. Hurricane Ida, on the other hand, reveals a significant depth of impact, with a highly concentrated group of people left without power for an extended period (some nearly twice the 100-hour threshold described above). Finally, the 2015 attack on the Ukrainian grid was the most impactful such cyberattack, despite having far less impact than the other events discussed.

Event	Location	Year	Economic Impact
Northeast Blackout	Northeastern U.S. and Southeastern Canada	2003	< $10 billion
Hurricane Ida	Louisiana	2021	$27-40 billion
Hurricane Florence	North Carolina	2018	$16-20 billion
Hurricane Laura	Louisiana	2020	$25-30 billion
NotPetya cyberattack	Ukraine, U.S., UK, others	2017	$10 billion
Ukrainian power grid cyberattack	Ukraine	2015	Unavailable[3]

Table 1: Economic Impacts from Natural and Cyber Disasters
Sources: Elcon 2004; Stevens 2021; Davidson 2018; Byrne 2020; Johansmeyer 2019.

New York Blackout (2003)

Fifty million people across seven states (and parts of Canada) lost power for a period of at least 29 hours in 2003, likely due to damage to a transmission line in Ohio. New York, the largest metropolitan area in the U.S., was among the hardest hit: traffic lights failed, and the subway system came to a standstill. While the experience was far from pleasant, particularly in the summer heat, there was no civil unrest, minimal looting, and widespread displays of community resilience, from people helping each other out to stoop parties and restaurants selling off perishable food at discounted prices (Brick Underground 2023). Far from societal collapse, the blackout revealed a capacity for solidarity.

Remarkably, the largest blackout in U.S. history produced no unrest, mirroring the outcome of the second-largest event, the 1965 New York blackout. The absence of violence in both cases suggests that scale alone does not determine the likelihood of civil unrest. Post-blackout rioting with substantial economic impact is exceptionally rare. Further, duration does not appear to be decisive: The 29-hour outage in 2003 was managed without major incident, and even longer blackouts, such as those following Hurricane Sandy, did not provoke widespread unrest. Instead, they often led to similar community responses, with local businesses adapting and neighbors supporting each other.

Hurricane Ida (2021)

If the 2003 Northeast Blackout was severe, and Superstorm Sandy worse, then the effects of Hurricane Ida in 2021 should be considered nearly catastrophic. The Category 4 storm left over one million households in Louisiana without power for more than a week, with nearly half still without electricity a week later. Occurring in late August, the blackout was compounded by extreme heat and limited access to food, water, and shelter. More than 80 deaths were attributed to direct and indirect causes, including heat exhaustion (Beven et

3 With the blackout lasting only 1-6 hours for the people affected, it would be difficult to calculate an economic effect, and for only 230,000 people, one would have to expect that impact to be small, given the historical economic losses and scales detailed in the tables above.

al. 2022). Yet, despite these conditions, civil unrest did not occur. This pattern is consistent across other recent hurricanes. In 2022, Hurricane Ian left over 5 million without power (Shivaprasad and DiSavino 2022). Four years earlier, Hurricane Florence, though smaller in scale, resulted in nearly one million outages (Kumar 2018). In none of these cases did power loss lead to civil unrest.

What makes Hurricane Ida particularly notable is the context in which it occurred. Just a year earlier, Louisiana endured Hurricane Laura, a Category 5 storm, causing over 568,000 outages (Pasch et al. 2021). The state was also among the hardest hit by the COVID-19 pandemic, which was still exerting severe pressure on hospitals during and after Hurricane Ida. The social and political environment was tense, marked by pandemic-related polarization, inflation, and shortages of essential goods and materials, all during peak summer heat. By the time Hurricane Ida passed, Louisiana's 4.7 million residents had endured two major hurricanes in only twelve months, a global pandemic, economic strain, and extreme weather—all without triggering unrest. Even in the aftermath of Hurricane Katrina, fifteen years earlier, reports of looting and violence were largely exaggerated (Tierney et al. 2006). Despite these patterns, the belief persists that a blackout—especially one caused by a hostile cyberattack—could spark widespread civil unrest. To evaluate this claim further, we turn next to the 2015 cyberattack on Ukraine's power grid.

Cyberattacks on the Ukrainian Power Grid (2015 and 2022)

Russia's occupation of parts of Ukraine in 2014 triggered a wave of cyberattacks and information operations, which have continued through the 2022 invasion (Council on Foreign Relations 2022b). Among the early incidents were three major cyberattacks on critical Ukrainian institutions, including a 2015 attack on the power grid (European Parliament 2022). This is the closest real-world case to the "hacking the grid" scenario outlined by Lloyd's in 2015. Despite being launched by a hostile state with clear destabilization goals, the attack had a limited impact. The key concept here is *reversibility*—the relative easeand speed with which the damage from an attack can be undone (Johansmeyer 2023). Unlike nuclear or kinetic attacks, cyberattacks tend to be more reversible, a pattern supported by past incidents. The 2015 attack caused outages for 230,000 people lasting between one and six hours—a modest impact by any standard (European Parliament 2022). Compared to large-scale natural disasters or the 2003 Northeast blackout, the footprint and duration were minimal. Even accounting for population density, the severity remains difficult to argue.

Beyond Ukraine, India successfully thwarted a Chinese cyberattack on its grid in 2022 (Council on Foreign Relations 2022a). Earlier examples, including cyber activity targeting Estonia, Lithuania, and Georgia in 2007 and 2008, similarly lacked significant consequences (Gotsiridze 2019). Despite these underwhelming results, cyberattacks remain a recurring feature of modern conflicts, including the ongoing war in Ukraine. The cyber campaign

has largely been deemed ineffective, with the most generous assessment that cyberattacks "amount to an occasional and secondary threat to Ukrainian connectivity" (Bateman 2022).

One incident that warrants closer examination is the failed April 2022 cyberattack on Ukraine's power grid. Though ultimately unsuccessful, it was poised to become the largest cyber-induced blackout ever recorded (O'Neill 2022). Despite being a near miss, the event remains important. First, there are no other major cyber-induced blackouts with meaningful breadth of effect. The review of the CFR's Cyber Operations Tracker reveals a landscape dominated by espionage rather than sabotage, with most entries reflecting unsuccessful or limited attacks, and few disclosing the number of people affected. The 2015 event above stands out for its size, which implies a ceiling on effect, at least with regard to past events. In this context, evaluating what the 2022 attack might have achieved is critical, even if its failure complicates its use as a model.

The 2022 attack followed the pattern of earlier Russian operations against Ukraine's power grid in 2015 and 2016, but with a key innovation: malware designed to hinder service restoration, directly targeting reversibility (Bateman 2022). Initial reports claimed nine substations were affected, though these were later disproven. Had the intended impact—disrupting power to 2 million people—been realized, the scale would have far exceeded previous attacks. The prospect of a longer duration through impeded reversibility marked a notable escalation in technical sophistication. While it is impossible to fully gauge the consequences of a successful execution, the disruption would almost certainly have surpassed the 2015 blackout, which affected 230,000 people for 1 to 6 hours. The actual duration of a successful outage however remains uncertain. As Bateman notes (2022), the malware's design targeted reversibility, implying a potentially longer disruption. Still, drawing from comparisons like Hurricane Ida, it seems unlikely that a cyber-induced outage would extend to a week or more. Unlike physical infrastructure damage from natural disasters, cyber disruptions tend to be more localized and amenable to faster remediation.

The war in Ukraine offers a rare opportunity to directly compare cyber and kinetic methods in targeting energy infrastructure. The April 2022 near miss stands in stark contrast to the November 2022 kinetic attacks, which left 4.5 million people without power (Bateman 2022). As noted by the German think tank SWP (Schulze and Kerttunen 2023), conventional bombings succeeded where cyber operations failed—shutting down 40% of Ukraine's power grid. Cyberattacks proved insufficient and were ultimately replaced by traditional means.

DISCUSSION

Are Close Calls Really Close?

Cyberattacks targeting energy infrastructure are frequent, but their effectiveness has been limited, as discussed above. The 2015 Ukraine attack and the thwarted 2022 attempt remain the most serious cases—and yet, their impact was modest. The Ukraine outages

lasted hours and affected hundreds of thousands, not a scale to trigger societal disruption or destabilization, as evidenced by the comparison with the millions impacted by natural disasters like Hurricanes Ida or Ian. After all, the outage caused by the 2015 cyberattack on Ukraine's grid and the 2022 attempt, arguably the last such attack with any meaningful scale, was only a quarter of the breadth of that from Hurricane Ida and less than a twentieth of that from Hurricane Ian.

When anticipated crises fail to materialize or reach the levels feared, the fallback is often that an event could have been worse—or that what has happened so far is not indicative of what could transpire in the future. This logic sustains the notion of the "near miss," as discussed above. Yet, as Rid (2011) and Gartzke (2013) argue, the lack of a theoretical foundation for cyber war, the absence of compelling empirical evidence, and the comparison to more severe—but non-malicious—power outages raise important questions. One could accept this evidence at face value or, alternatively, attempt to rationalize why past experience might not apply to future scenarios. Admittedly, this position is deliberately provocative: It suggests that the persistence of such beliefs resembles doomsday forecasting—predictions that endure despite repeated disconfirmation. While a large-scale blackout caused by a hostile cyberattack may be possible—provided one uses large-scale within the historical context and without positing the possibility of outages far more severe than have occurred without specific support—claims of its imminence remain speculative and unsupported by historical precedent.

Several high-profile cyber incidents, such as the 2017 NotPetya attack (Smith 2019) are frequently cited as close calls or near misses. Some in the insurance industry still anticipate a so-called "Hurricane Andrew of cyber" (Orcutt 2017)—shorthand used for a market- and society-changing event—"is coming." However, the same events that *could* have been worse also *could* have been far less severe—an asymmetry rarely acknowledged by alarmist narratives. WannaCry and NotPetya, for example, are among the events that could have been worse, according to some, "if EternalBlue had been a true zero-day vulnerability with no available patch or advanced notice for mitigations" (Laux et al. 2024). While near misses deserve attention and can inform improvements in security strategy, treating them as inevitabilities may distort a genuine understanding of the risk and how to respond to it. These comparisons highlight the need to recalibrate expectations. Rather than merely dismiss the notion that a destabilizing cyberattack-induced blackout is a profound threat, it is more productive to acknowledge its existence while aligning security planning with realistic scenarios. Hostile cyber activity is a real threat. Energy infrastructure remains an important and coveted target, as evidenced by the frequency of attacks, and society's reliance on energy infrastructure is undeniable. At the nexus of energy security and cyber security, strategy has led to action, and action has been effective. The focus should be on maintaining and improving existing safeguards—not overreacting to speculative threats.

Civil Unrest as an Unlikely Consequence

If a vulnerability remains in the cyber-blackout scenario, it is likely not technical but societal. Historical blackouts suggest that the breadth and depth of the outage is less an indicator of societal impact than other factors, especially the existence of preexisting grievances (Drury and Olsen 1998). This may suggest the possibility of targeting states with preexisting grievances via the cyber domain. However, the rarity of post-event civil unrest in general – to include natural disasters – indicate that attempting to engineer an instance of civil unrest can be uneven via the power outages.

The 1977 New York blackout is frequently cited as an example of blackout-induced unrest. But it was short-lived, localized, and occurred in a context of intense preexisting grievances. It is important to remember also that it remains an outlier. To the best of this author's knowledge, no comparable riot has followed any blackout since. This is supported by the fact that major blackouts were overwhelmingly caused by natural events, and the scarcity of disaster-induced civil unrest has been established (Johansmeyer 2024c). Although this may not be exhaustive, it is certainly indicative. Further, using industry-wide insured losses as a proxy for economic impact,[4] there have been fewer than 15 civil unrest events in the U.S. since 1949 according to PCS, the division of data/analytics firm Verisk that estimates the impact of disaster effects on the insurance industry (Johansmeyer and Gregory 2021). Of those events, only two had industry-wide insured losses of over $1 billion (adjusted for inflation) – the Los Angeles Riot of 1992 (Sams 2020) and the George Floyd Riot of 2020 (Johansmeyer 2021).

Some may argue that the United States has entered a period of heightened vulnerability to unrest since the 2020 events, and that a targeted cyberattack causing a blackout in a population with preexisting grievances—similar to conditions that sparked the 2020 riots—could be destabilizing. This assumption, though, overlooks just how rarely large-scale civil unrest occurs. Using natural disasters as a proxy, only twenty-two instances if disaster-induced unrest events have been identified since 1970 (Johansmeyer 2024c). While this figure may be incomplete, it highlights how fragile and specific the conditions must be to spark such events.

In this light, the prospect of a cyberattack on energy infrastructure triggering civil unrest appears exceedingly remote. Cyberattacks, the temporary and often limited nature of blackouts, and the complex conditions required for unrest all point to a low-risk scenario. Rather than fear the extremes, cyber threats should be contemplated within the available economic context, not to mention the realities of affecting such an outcome, as offered by Lewis of the Center for Strategic & International Studies: "It is easier to imagine a catastrophe than to produce it" (Lewis 2020). The number of fatalities from cyberattacks has been minimal (Horne et al. 2024), physical damage has been scarce (with LockerGoga's impact on

4 One limitation of this approach is its exclusion of events that caused substantial economic damage to uninsured structures (e.g., the "Capitol Riot" of January 6, 2021)

Norsk Hydro a rare example; Johansmeyer 2025b), and instances of cyber attacks' economic effects reaching above even 0.2% of GDP has occurred only twice since 1998 and not since 2004 (Johansmeyer 2025a).

Lewis (2018) argues that the "real damage" from cyberattacks is "political," undermining "confidence in government and on relations between states, encouraging a sense of instability and unease that increases as our dependency on networked devices grows". This insight is especially relevant when cyberattacks are paired with a domestic or geopolitical context that amplifies public fear—often of improbable worst-case scenarios. Yet, smaller and more localized incidents remain far more likely (Johansmeyer 2025b). As seen in natural disasters, such events tend to trigger well-practiced responses: unaffected regions mobilize aid, and recovery begins swiftly. Blackouts are familiar disruptions, and even a severe but realistic cyber-induced blackout would likely follow established remediation patterns.

IMPLICATIONS FOR CYBER DEFENSE STRATEGY

The absence of catastrophic consequences from cyberattacks should not justify minimizing or deprioritizing cyber defense strategies. On the contrary, part of the reason cyberattacks have not caused large-scale disruption is precisely because of improved security over the past two decades. It is no coincidence that over 90% of aggregate cyber catastrophe losses since 1998 occurred between 1998 and 2008 (Johansmeyer 2024a), and that no cyber incident has surpassed 0.2% of U.S. GDP since 2004 (Johansmeyer 2025a). These trends reflect the success of defense—not a lack of threat.

However, the goal should not be absolute prevention or deterrence at all costs. Instead, strategy must shift toward more pragmatic and effective models. Historical blackouts—and the cyber domain's failure to replicate them—underscore one enduring lesson: the ability to recover quickly is crucial. Prevention should remain a goal but cyberattacks will inevitably breach even the best defenses. What happens next is critical. Response and remediation must be swift, predictable, and rehearsed.

This approach aligns with the inherently transitory nature of cyber weapons (Smeet 2018). Their damage is often reversible, and their strategic impact diminishes quickly. As Rid (2011) has noted, cyberattacks have failed to reach Clausewitzian levels of warfare. The economic record similarly shows limited impact. The faster a target recovers, the less effective the attack—and the less harm suffered by the population.

Prioritizing remediation and recovery alongside prevention has important implications for resource allocation. It also challenges how the security strategy perceives the cyber domain. Traditional deterrence relies on the threat of unacceptable consequences—an "all or nothing" logic that is poorly suited to the cyber domain, where stakes are lower. A more nuanced strategy emphasizes resilience and response, asking not only "what vulnerabilities exist?" but also "what happens when we are attacked?"

While a prolonged, nationwide cyber-induced blackout may be implausible, examining the possibility yields importance insights about balance and proportionality in cybersecurity strategy. Over-securitization can lead to distorted priorities. Historical experience suggests that the most effective strategy is one of preparedness—before and after a breach—with the aim of minimizing disruption. Rather than focusing on prevention at all costs, the better goal may be to recover so rapidly that the attack fails to deliver meaningful results.

CONCLUSION

The notion that a cyberattack on energy infrastructure could trigger civil unrest remains largely hypothetical, and its likelihood is low. Natural disasters have caused longer, wider outages without provoking such unrest, despite causing comparable or greater disruption. The belief that cyber-induced outages will lead to social collapse is built on a series of improbabilities. Civil unrest itself is rare and rooted in complex, multifaceted causes. The blackout scenario taps into deep societal anxieties—fear of the unknown, sudden disruption, and loss of control. But history tells a different story: one of resilience and adaptation. In most cases communities respond to outages not with chaos, but with collective adjustment and mutual aid.

Cyber threats to energy infrastructure are real and warrant attention—but must be contextualized. The risk is serious (Department of Defense 2023), but proportionality is essential. Overstating the threat may appear cautious, but it can distort security priorities, possibly leading to to less—or less appropriate—protection for society. One might argue that cyber-induced unrest shouldn't be dismissed merely because it hasn't happened. After all, the 9/11 attacks were later described as a "failure of imagination".[5] But as Lewis (2020) notes, strategy should be grounded in what is executable—not merely imaginable. Cybersecurity for energy infrastructure should not be neglected, but the nexus of cyber and power grid security requires disciplined, targeted, and reality-based strategies. The feared blackout scenario has not materialized, despite repeated attempts by hostile actors. While the theoretical payoff may appear high, the practical costs and complexity consistently outweigh it, and past outcomes have yielded only brief, reversible disruptions.

The risk landscape is not uniform worldwide (Rahman et al. 2016). The U.S. experience may not be fully generalizable, but it offers valuable insight. In some regions, infrastructure may be more vulnerable, yet the consequences of attack may be less severe, or the state may not be a strategically attractive target. In areas with already irregular power access, the impact of an outage might be lower than in highly developed economies. Nonetheless, the U.S. experience—enduring frequent blackouts without unrest—demonstrates a level of societal tolerance that is at least comparable to, if not greater than, that of less developed states.

5 National Commission on Terrorist Attacks upon the United States. 2004. *The 9/11 Commission Report*. July 22. https://govinfo.library.unt.edu/911/report/911Report.pdf.

This article has shown that historical experience with both blackouts and cyber incidents can recalibrate fears, offering a clearer basis for security planning. There is a difference between threats that haven't yet occurred but plausibly could, and those built on flawed premises. The author argues that the scenario of cyber-induced civil unrest via a power grid attack falls into the latter category. Recognizing this distinction enables more balanced and effective cyber and societal security strategies going forward.

ABOUT THE AUTHOR

Tom Johansmeyer is a POLIR Ph.D. candidate at the University of Kent, Canterbury. His research is focused on the role of cyber insurance in economic security, with a specific interest in the role of hyperbole with regard to systemic risk as an impediment to the flow of capital. Tom has an MA in global diplomacy from the School of Oriental and African Studies at the University of London, an MBA in accounting from Suffolk University (in Boston), and an AB in philosophy and history from Ripon College (in Wisconsin). He speaks and publishes regularly. Based in Bermuda, where he also works in the reinsurance industry, Tom was previously the head of Property Claim Services (PCS) at data and analytics firm Verisk, which provides data on industry-wide insured loss events for both natural and man-made disaster events. Thus, Tom is a recognized leader in understanding the cost of natural and man-made disasters in both insured loss and economic terms. Also, he is a U.S. Army veteran, serving in both active and reserve roles from 1994-1999. Finally, Tom co-leads the Instruments of Power area of practice with the Irregular Warfare Initiative and is an early career researcher member of the University of Kent's Institute of Cyber Security for Society.

REFERENCES

Bateman, Jon. 2022. "Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications." *Carnegie Endowment for International Peace*, December 16. https://carnegieendowment.org/2022/12/16/russia-s-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications-pub-88657.

Beazley. 2023. "Leaders Need to Lead on Catastrophic Cyber." January 13, 2023. https://www.beazley.com/en-US/articles/leaders-need-to-lead-on-catastrophic-cyber.

Beven, John II, Andrew Hagen, and Robbie Berg. 2022. "Hurricane Ida." *National Hurricane Center Tropical Cyclone Report*, April 4, 12. https://www.nhc.noaa.gov/data/tcr/AL092021_Ida.pdf.

Brancati, D. 2007. "Political Aftershocks: The Impact of Earthquakes on Intrastate Conflict." *Journal of Conflict Resolution* 51 (5): 723. https://www.researchgate.net/publication/249728741_Political_Aftershocks_The_Impact_of_Earthquakes_on_Intrastate_Conflict#fullTextFileContent.

Brick Underground. 2023. "Where Were You during the 2003 Blackout? New Yorkers Share Their Stories." August 14. https://www.brickunderground.com/live/2003-nyc-blackout-stories.

Brooking, Emerson T., and Erica Lonergan. 2023. "Welcome to Cyber Realism: Parsing the 2023 Department of Defense Cyber Strategy." *War on the Rocks,* September 25. https://warontherocks.com/2023/09/welcome-to-cyber-realism-parsing-the-2023-department-of-defense-cyber-strategy/.

Butler, E., A. Barnes, and I. Lahiri. 2025. "Spain and Portugal Power Outage Costs 'Likely to Be in Tens of Millions'." *euronews*, April 28, 2025. https://www.euronews.com/business/2025/04/28/how-spain-and-portugals-economies-could-be-hit-by-the-blackout.

Byrne, Kevin. 2020. "Hurricane Laura to Cause $25 Billion to $30 Billion in Economic Damage." *AccuWeather,* August 26. https://www.accuweather.com/en/hurricane/hurricane-laura-to-cause-25-billion-to-30-billion-in-economic-damage/800854.

Corwin, Jane L., and William T. Miles. 1978. *Impact Assessment of The 1977 New York City Blackout*. July 1978. https://www.ferc.gov/sites/default/files/2020-05/impact-77.pdf.

Council on Foreign Relations. 2022a. "Targeting of the Indian Power Grid." *Council on Foreign Relations*, April. https://www.cfr.org/index.php/cyber-operations/targeting-indian-power-grid.

Council on Foreign Relations. 2022b. "Targeting of Ukrainian Power Stations." *Council on Foreign Relations,* April. https://www.cfr.org/index.php/cyber-operations/targeting-ukrainian-power-stations.

Council on Foreign Relations. 2024. "Cyber Operations Tracker." *Council on Foreign Relations*, February 2024. https://www.cfr.org/cyber-operations/.

Davidson, Paul. 2018. "Hurricane Florence, Despite Destruction, Will Likely Have Small Impact on US Economy." *USA Today*, September 18. https://eu.usatoday.com/story/money/2018/09/18/hurricane-florence-likely-have-modest-impact-us-economy/1339315002/.

Department of Defense. 2023. *Summary: 2023 Cyber Strategy.* https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF.

Drury, A. Cooper, and Richard Stuart Olsen. 1998. "Disasters and Political Unrest: An Empirical Investigation." *Journal of Contingencies and Crisis Management* 6 (3): 155. https://doi.org/10.1111/1468-5973.00084.

Electricity Consumers Resource Council (ELCON). 2004. T*he Economic Impacts of the August 2023 Blackout*. February 9, 2004. https://www.nrc.gov/docs/ML1113/ML111300584.pdf.

European Parliament. 2022. "Russia's War on Ukraine: Timeline of Cyber-Attacks." *European Parliamentary Research Service*, 3. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Eyewitness News. 2023. "'From Lights Out to Lights On': 20 Years Since the 2003 Blackout." *abc7NY*, August 14, 2023. https://abc7ny.com/2003-blackout-nyc-20-years-power-outage/13646160/.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73. https://doi.org/10.1162/ISEC_a_00136.

Ghimire, R., and S. Ferreira. 2013. "Economic Shocks and Civil Conflict: The Case of Large Floods." *Proceedings of the 2013 Georgia Water Resources Conference*, April 10–11: 2. https://ageconsearch.umn.edu/record/142587?v=pdf.

Gotsiridze, Andria. 2019. "The Cyber Dimension of the 2008 Russia-Georgia War." *Rondeli Foundation,* August 9. https://gfsis.org.ge/blog/view/970.

Hevia-Koch, P., and Brent Wanner. 2025. "The Iberian Blackout Has Highlighted the Critical Importance of Electricity Security." *International Energy Agency,* June 16, 2025. https://www.iea.org/commentaries/the-iberian-blackout-has-highlighted-the-critical-importance-of-electricity-security.

Horne, Si, Gareth Mott, and Jamie MacColl. 2024. "Ransomware: A Life and Death Form of Cybercrime." *RUSI Commentary*, June 25. https://www.rusi.org/explore-our-research/publications/commentary/ransomware-life-and-death-form-cybercrime.

Ide, Tobias, Michael Brzoska, Jonathan Donges, and Carl-Friedrich Schleussner. 2020. "Multi-Method Evidence for When and How Climate-Related Disasters Contribute to Armed Conflict Risk." *Global Environmental Change* 62: 3. https://doi.org/10.1016/j.gloenvcha.2020.102063.

Johansmeyer, Tom. 2019. *Could NotPetya's Tail Be Growing?* Jersey City, NJ: PCS, a division of Verisk Analytics. https://www.verisk.com/4a25ed/siteassets/media/pcs/pcs-cyber-catastrophe-notpetyas-tail.pdf.

Johansmeyer, Thomas. 2021. "How 2020 Protests Changed Insurance Forever." *World Economic Forum Agenda*, February 22. https://www.weforum.org/agenda/2021/02/2020-protests-changed-insurance-forever/.

Johansmeyer, Tom. 2022. "This Is How to Avoid Climate Crises Becoming the Trigger for Social Unrest." *World Economic Forum Agenda*, October 18. https://www.weforum.org/stories/2022/10/civil-unrest-climate-disaster/.

Johansmeyer, Tom. 2023. "How Reversibility Differentiates Cyber from Kinetic Warfare: A Case Study in the Energy Sector." *International Journal of Security, Privacy, and Trust Management* 12 (1): 5. https://aircconline.com/ijsptm/V12N1/12123ijsptm01.pdf.

Johansmeyer, Tom. 2024a. "Recent Cyber Catastrophes Show an Intensifying Trend – but They Are Manageable." *The Loop: ECPR's Political Science Blog*, September 25, 2024. https://theloop.ecpr.eu/recent-cyber-catastrophes-show-an-intensifying-trend-but-they-are-manageable/.

Johansmeyer, Tom. 2024b. "Surprising Stats: The Worst Economic Losses from Cyber Catastrophes." *The Loop: ECPR's Political Science Blog*, March 12, 2024. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

Johansmeyer, Tom. 2024c. "The Growing Danger of Natural Disaster Disinformation." *Binding Hook*, May 23. https://bindinghook.com/articles-hooked-on-trends/the-growing-danger-of-natural-disaster-disinformation/.

Johansmeyer, Tom. 2024d. "Why Natural Catastrophes Will Always Be Worse than Cyber Catastrophes." *War on the Rocks*, April 5, 2024. https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/.

Johansmeyer, Tom. 2025a. "Bad Decisions Have Consequences: How Cyber Security Could Fall Victim to Climate Change." *British Actuarial Journal* 30 (e15): 1–15. https://doi.org/10.1017/S1357321725000091.

Johansmeyer, Tom. 2025b. "Look Again: Learning from Smaller Cyber Catastrophes." *The Actuary*, March 7. https://www.theactuary.com/2025/03/07/look-again-learning-smaller-cyber-catastrophes.

Johansmeyer, Tom, and Ted Gregory. 2021. *PCS Information-Only Bulletin: Riot and Civil Disorder Risks in the United States.* January. https://pcs.iso.com/globalnews/pcs_information_only_bulletin_srcc_jan_2021.pdf.

Kasper, Daniel. 2023. "Insights from the 7th ASTIN Cyber Working Group." *Cyber Economics*, no. 2 (November): 4.

Latson, Jennifer. 2015. "Why the 1977 Blackout Was One of New York's Darkest Hours." *Time*, July 13. https://time.com/3949986/1977-blackout-new-york-history/.

Larson, A. 2025. "Understanding the April 2025 Iberian Peninsula Blackout: Early Analysis and Lessons Learned." *POWER Magazine*, May 8, 2025. https://www.powermag.com/understanding-the-april-2025-iberian-peninsula-blackout-early-analysis-and-lessons-learned/.

Laux, John, Josh Knapp, Doug Fullam, Ethan Spangler, and Ty Zeno. 2024. *Three Degrees of Separation: Understanding Cyber Tail Risk with Counterfactual Analysis.* https://insights.cybcube.com/three-degrees-of-separation-understanding-cyber-tail-risk-thank-you.

Lewis, J.A. 2018. *Rethinking Cybersecurity: Strategy, Mass Effect, and States.* January 8. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180108_Lewis_ReconsideringCybersecurity_Web.pdf.

Lewis, J.A. 2020. "Dismissing Cyber Catastrophe." *Center for Strategic & International Studies*, August 17. https://www.csis.org/analysis/dismissing-cyber-catastrophe.

Lloyd's. 2023. "Lloyd's Systemic Risk Scenario Reveals Global Economy Exposed to $3.5trn from Major Cyber Attack." Last modified October 18, 2023. https://www.lloyds.com/about-lloyds/media-centre/press-releases/lloyds-systemic-risk-scenario-reveals-global-economy-exposed-to-3.5trn-from-major-cyber-attack.

Kim, S. J. 2021. "Environmental Shocks, Civil Conflict and Aid Effectiveness." *Conflict Management and Peace Science* 38 (6): 675. https://doi.org/10.1177/07388942211015240.

Kumar, Devika Krishna. 2018. "More than 870,000 without Power as Florence Lumbers Inland." *Reuters*, September 15. https://www.reuters.com/article/uk-storm-florence-outages-factbox-idUKKCN1LV0FE/.

Morehouse, Catherine. 2023. "Extremists Keep Trying to Trigger Mass Blackouts – and That's Not Even the Scariest Part." *Politico*, September 10, 2023. https://www.politico.com/news/2023/09/10/power-grid-attacks-00114563.

Munich Re. 2018. "What If a Major Cyber Attack Strikes Critical Infrastructure?" *Munich Re: Insights*, November 22, 2018. https://www.munichre.com/en/insights/cyber/silent-cyber.html.

Must, E., and S. A. Rustad. 2019. "'Mtwara Will Be the New Dubai': Dashed Expectations, Grievances, and Civil Unrest in Tanzania." *International Interactions: Empirical and Theoretical Research in International Relations* 45 (3): 504. https://doi.org/10.1080/03050629.2019.1554569.

Nel, Philip, and Marjolein Righarts. 2008. "Natural Disaster and the Risk of Violent Civil Conflict." *International Studies Quarterly* 52 (1): 167. https://doi.org/10.1111/j.1468-2478.2007.00495.x.

Orcutt, Mike. 2017. "Insurers Scramble to Put a Price on Cyber Catastrophe." *MIT Technology Review*, April 6. https://www.technologyreview.com/2017/04/06/5143/insurers-scramble-to-put-a-price-on-a-cyber-catastrophe/.

Oyefusi, A. 2010. "Oil, Youths, and Civil Unrest in Nigeria's Delta: The Role of Schooling, Educational Attainments, Earnings, and Unemployment." *Conflict Management and Peace Science* 27 (4): 326. https://doi.org/10.1177/0738894210374399.

Pasch, Richard J., Robbie Berg, David P. Roberts, and Philippe P. Papin. 2021. "Hurricane Laura." *National Hurricane Center Tropical Cyclone Report,* May 26, 10. https://www.nhc.noaa.gov/data/tcr/AL132020_Laura.pdf.

Pfaff, K. 2020. "Assessing the Risk of Pre-existing Grievances in Non-Democracies: The Conditional Effect of Natural Disasters on Repression." *International Journal of Disaster Reduction* 42. https://www.sciencedirect.com/science/article/pii/S2212420919300354.

Rahman, K.M.J., M.M. Munnee, and S. Khan. 2016. "Largest Blackouts Around the World: Trends and Data Analyses." In *2016 IEEE International WIE Conference on Electrical and Computer Engineering (WIECON-ECE)*, December 19–21, Pune, India, 156. http://dx.doi.org/10.1109/WIECON-ECE.2016.8009108.

Regan, P., and S. Bell. 2010. "Changing Lanes or Stuck in the Middle: Why Are Anocracies More Prone to Civil Wars?" *Political Research Quarterly* 63 (4): 749. https://www.jstor.org/stable/25749246.

Reuters. 2025. "Spain, Portugal Switch Back On, Seek Answers after Biggest Ever Blackout." *Reuters,* April 29, 2025. https://www.reuters.com/world/europe/spains-power-generation-nearly-back-normal-after-monday-blackout-says-grid-2025-04-29/.

Rid, Thomas. 2011. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (2): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Ruffle, Simon, Eireann Leverett, Andrew Coburn, Julian Copic, Susan Kelly, Trevor Evan, Daniel Ralph, et al. 2015. *Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid.* Cambridge, UK: Lloyd's of London and the University of Cambridge Centre for Risk Studies. https://www.lloyds.com/news-and-insights/risk-reports/library/business-blackout.

Sams, Jim. 2020. "Insurers May Rethink Property Risks After Unprecedented Losses from Riots." *Claims Journal,* July 6. Accessed February 25, 2024. https://www.claimsjournal.com/news/national/2020/07/06/298012.htm.

Schulze, Matthias, and Mika Kerttunen. 2023. "Cyber Operations in Russia's War against Ukraine: Uses, Limitations, and Lessons Learned So Far." *SWP Comment* 2023/C23. https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf.

Shivaprasad, Ashitha, and Scott DiSavino. 2022. "Over 391,000 Still without Power in Florida after Hurricane Ian." *Reuters*, October 4. https://www.reuters.com/world/us/over-million-customers-without-power-florida-hurricane-ian-2022-09-28/.

Smeets, Max. 2018. "A Matter of Time: On the Transitory Nature of Cyberweapons." *The Journal of Strategic Studies* 41 (1–2): 10–11. https://doi.org/10.1080/01402390.2017.1288107.

Smith, Kate. 2019. "Going Dark." *Best's Review*, June. https://www3.ambest.com/ambv/bestnews/articlecontent.aspx?refnum=285596

Stevens, Pippa. 2021. "Hurricane Ida's Damage Tally Could Top $95 Billion, Making It 7th Costliest Hurricane since 2000." *CNBC*, September 8. https://www.cnbc.com/2021/09/08/hurricane-idas-damage-tally-could-top-95-billion-making-it-7th-costliest-hurricane-since-2000-.html.

Swiss Re Institute. 2025. "Sigma Explorer." *Swiss Re Institute.* https://www.sigma-explorer.com/index.html.

Tierney, Kathleen, Christine Bevc, and Erica Kuligowski. 2006. "Metaphors Matter: Disaster Myths, Media Frames, and Their Consequences in Hurricane Katrina." *The ANNALS of the American Academy of Political and Social Science* 604 (1): 57. https://www.jstor.org/stable/25097781.

United Nations Office for Disaster Risk Reduction (UNDRR). n.d. "Disaster." U*nited Nations Office for Disaster Risk Reduction*. https://www.undrr.org/terminology/disaster.

United Nations Satellite Centre (UNOSAT). 2023. *Power Supply Recovery Assessment Following the Marash / Antep Earthquake (6 February 2023, Mw 7.8) Using Night-Time Light Imagery.* April 20, 2023, p. 14. https://unosat.org/static/unosat_filesystem/3565/UNOSAT_Preliminary_Assessment_Report_LightLight_EQ20230420SYRTUR.pdf.

Wood, R. M., and T. M. Wright. 2016. "Responding to Catastrophe: Repression Dynamics Following Rapid-Onset Natural Disasters." *Journal of Conflict Resolution* 60 (8): 1450. https://doi.org/10.1177/0022002715596366.