DJIM
Volume 7 – Fall 2011
djim.management.dal.ca

Watts At Stake?: Protecting North America's Energy Infrastructure From Cascading Failure And Terrorist Threats

Alexander Szumilas, Bryce Swerhun, Jeannette Lye

Abstract: Due to rising consumption, electrical infrastructure has grown in size and complexity. This has allowed for an increased vulnerability of the infrastructure. Under the caveats of high-reliability organizations (HRO) theory and normal accidents theory (NAT), this paper examines two predominant threats to the North American energy sector: cascading failures and terrorism. A key consideration underlying the analysis is that NAT and HRO are not mutually exclusive; it is within both theories to suggest that redundancy and organizational learning are essential for the operation of critical energy infrastructure. This paper argues that while energy infrastructure has several characteristics of an NAT organization, the high-consequence nature of infrastructure operations lends to a predisposition towards HRO strategies for risk identification and management. Energy infrastructure must be highly reliable, because society expects it to be so – the capacity for meeting periods of high demand must not be disabled by accidents or attacks.

About the Author(s): Alexander Szumilas is a Master of Public Administration student in the School of Public Administration at Dalhousie University. Alexander holds a Bachelor of Science in Environmental Sciences from the University of Guelph in Guelph, ON. Apart from his scholarly work, Alexander participates in a number of extra-curricular leadership activities, including the Dalhousie University Senate, the Dalhousie Student Union and the Dalhousie Association of Graduate Students. He intends to pursue federal government employment after graduation.

Bryce Swerhun completed his undergraduate studies in political studies and philosophy at Queen's University. He also holds a Master of Arts in political science from the University of Stellenbosch and is currently studying for the Master of Public Administration at Dalhousie University. He gave a presentation titled "Fairness for Economic Recovery: Stimulus, Bailouts and the Difference Principle" at the recent annual conference of the Atlantic Provinces Political Science Association. In addition to his academic studies and research he serves as the Vice President for Academic Affairs at the Dalhousie Association of Graduate Students.

Jeannette Lye is graduate student in the School of Public Administration at Dalhousie University. She holds a Master of Science in Cultural Psychology from Brunel University and an undergraduate degree in psychology from Acadia University. Jeannette is the former research coordinator for the Refugee and Immigrant Advisory Council in St. John's, Newfoundland. Most recently, she co-authored The Economic Impact of Post-Secondary International Students in Atlantic Canada, a study commissioned by the Council of Atlantic Ministers of Education and Training. She currently serves on the Nova Scotia Population Committee, investigating strategies for rural repopulation, immigration and retention.

1.0 Introduction

Organizational theories may be applied to a variety of critical infrastructure sectors to explain how and why these sectors function the way they do. Two dominant theories, Normal Accidents Theory (NAT) and High-Reliability Organizations (HRO) theory, have both been employed in academic literature and in practice to explain the energy sector in North America. Although NAT offers a compelling account of risk to energy infrastructure, this paper argues that HRO, and not NAT, best explains the risk environment faced by the energy sector; should critical infrastructure managers and policymakers adopt HRO theory, risks can be more successfully mitigated than with NAT. A literature review of the competing theories is followed by an examination of the energy sector in North America through the 2003 Northeast Blackout and the omnipresent threat of terrorism on critical energy infrastructure. Lastly, a section of identified lessons follows the literature review and presents recommendations for policymakers with regards to power grids.

2.0 Organizational Theories

Normal Accidents Theory and High-Reliability Organizations theory provide insights into how critical infrastructure systems may operate. Depending on the theory ascribed to by managers, different options may be appropriate to ensure long-term functioning of the critical infrastructure sector (if applicable).

2.1 Normal Accidents Theory

Normal Accidents Theory argues that due to the complexity and the tight coupling present in systems, accidents are inevitable (Perrow, 1999, p.4). Accordingly, Perrow (1999, p.4) states that risk can never be eliminated from high-risk systems and can only be marginally controlled, if at all, through improvements to organization, design, quality control and other aspects of infrastructure.

It is important to note that NAT refers to accidents being inevitable and does not address the frequency at which accidents occur (Perrow, 1999, p.5). Given that new, increasingly complex and specialised systems are sure to continue emerging, the learning that can be done from past accidents is limited (Perrow, 1999, p.12). Under the NAT paradigm, acts of terrorism are not accidents and are otherwise not addressed (SINTEF, 2004, p.8). Also of importance to the debate in this paper is the notion that not all accidents are, in fact, accidents; according to NAT, an accident disrupts the system or subsystem, and not just constituent parts (Clarke, 2005, p. 65).

A final thought in accordance with NAT is that because failures are inevitable and may have cataclysmic results, society must determine if such activities should even be conducted. For example, if genetic engineering is sure to result in hybrid species that will inevitably

contaminate the food chain, a proponent of NAT would, at the very least, advocate a cost-benefit analysis to determine if this technology should be used.

2.2 High–Reliability Organizations

La Porte & Consolini (1991, p.3) state that there are large-scale and highly complex organizations that have committed to failure-free operations and nearly always live up to this commitment. Such HROs include nuclear power plants, air traffic control operations, radioactive and toxic-waste management systems, and the management of blood supplies used for transfusions (La Porte & Consolini, 1991, p.20). Society demands that these systems be both employed and used in a way that ensures failures never occur.

High-reliability organizations are large, internally dynamic, and can be intermittently, intensely interactive (La Porte & Consolini, 1991, p.21); they are highly hierarchical in organization. Depending on the circumstances in which the HRO is operating, further layers of experts and hierarchy may even be added to the system to maintain constant operations (La Porte & Consolini, 1991, p.32). To further guarantee smooth operating, HROs spend considerable effort on emergency scenario planning so that the system can react in such a way that ensures potential crises do not manifest into actual failures (La Porte & Consolini, 1991, p.33). Accordingly, the underlying assumption in HROs is that operators of systems can know enough to deal with all situations that arise and further training can ensure that errors do not occur (La Porte & Consolini, 1991, p.25). Since this expertise is abundant, it must be maintained and frequently used to learn from.

HROs are unlike failure-tolerant organizations, where the benefits of “lessons learned” are greater than the costs of failure; HROs have other distinct properties. These include the coupling of organizational units so tightly that one failure may potentially compromise the entire system, operational failures being visible by the public, and significant resources being allocated towards high-reliability operations, leading to reliability being the primary concern within HROs (La Porte & Consolini, 1991, p.23).

2.3. NAT and HRO: Competing or Compatible?

A consideration influencing this paper is that critical energy infrastructure has attributes that align with both NAT and HRO theory. Hartley & Swaim (2007, p. 383) suggest that while NAT organizations may be commonplace, HRO management is expected (and often unavoidable) in high-consequence operations. Undeniably, some aspects of normal accidents are of relevance to the energy sector. For example, given the geographically broad, inter-jurisdictional nature of energy infrastructure, the NAT notion of increasingly complex, aggregated parts of a system is significant.

Recent theorists suggest that both the NAT and HRO theories oversimplify the cause of risk (Marais, et al., 2004, p. 11). High-Reliability Organization theory underestimates the problems

of uncertainty; conversely, NAT recognises the challenges associated with uncertainty but underestimates the potential for strategic intervention. It has been proposed that NAT and HRO are not mutually-exclusive when it comes to power critical infrastructure. The Foundation for Scientific and Industrial Research (SINTEF) report (2004, p. 35) argues that organizational learning will occur in both HRO and NAT organizations either deliberately or inadvertently, as system operators explore new technologies and the boundaries of safe operations. Thus, the capacity for organizational learning should not be underestimated as an instrument for risk identification and management. Further, while NAT warns that redundancies may increase the likelihood of accidents, the theory does not claim that system redundancy should be avoided. Therefore, it is within the reason of both theories to suggest that while difficult to manage, redundancy is essential for the operation of critical energy infrastructure.

3.0 Energy Infrastructure Overview

Society demands failure-free performance from electrical systems and, despite Perrow's admonition, such a high-risk system seldom fails (Hopkins, 2007, p.4). Due to rising modern consumption, infrastructure systems that provide electrical power have grown in size and complexity into vast technical networks. This expansion has substantially increased their vulnerability at the operational level, and also within the intricately interconnected broader critical infrastructure; conditions which Perrow's theory suggests substantially increase the likelihood of normal accidents. When a singular accident or disruption does occur to a critical system such as electric power, it can lead to compounding disruptions across the electrical network (Chang et al., 2007, p. 337).

4.0 Case Study: 2003 Northeast Power Outage

While the power system in North America is commonly referred to as "the grid," there are actually three independent power grids or "interconnections" (Minkel, 2008). The Eastern Interconnection, of relevance to this paper, includes the eastern United States and Canada from Saskatchewan to the Maritime Provinces. Though the interconnectedness of the electrical grid allows the system to compensate for local variations in demand and power generation, it also lends to a greater risk of cascading failure over a wider channel, should a disruption occur. The Northeast Power Outage that occurred on August 14th, 2003 exemplifies the complications associated with this risk.

In 2004, a joint U.S.–Canadian task force traced the origin of a widespread power outage to northern Ohio, where a series of electrical, human, and computer incidents led to cascading failures in the North American electrical grid. The Task Force investigation found that a generating plant in a Cleveland suburb went offline during a time of high electrical demand, putting a strain on high-voltage power lines that later went out of service due to "tree-to-line"

contact (U.S.-Canada Task Force, 2004). Further complicating the electrical failure was a software bug that stalled the network control room alarm system.

The alarm malfunction resulted in a queue of unprocessed electrical failures, causing an overload in the backup server and its eventual breakdown. It took over an hour for IT support operatives to become aware that the computer system had failed. While incidences of power failures were telephoned into the control room, system operators did not pursue the issue due to a lack of supporting technical evidence. The cascading effect that resulted ultimately forced the shutdown of more than 250 power plants, leaving approximately 50 million residents of the United States and Canada without electricity. Power was not restored for four days in some parts of the United States, while parts of Ontario suffered rolling outages for more than a week before full network capacity was restored. Estimates of the total costs resulting from the outage in the United States range between $4 billion and $10 billion. In Canada, there was an estimated net loss of 18.9 million work hours (U.S.-Canada Task Force, 2004).

4.1 Beyond a "Fly-Fix-Fly" Approach to Safety

The Task Force cautions that a cascade is a dynamic phenomenon that is difficult to contain by human intervention once started. What stopped the cascade from progressing further was the stability of higher capacity power generators in parts of New England and the Maritime Provinces. This observation aligns with NAT, as the theory presumes that failures are inevitable and can only be marginally controlled. Perrow's theory further asserts that complexly interactive and tightly-coupled systems are bound to fail at some time due to inherent failures built into the system design. Widespread electrical outages, however, are more frequently caused by human error or natural phenomena, which may be part of the system itself but not necessarily part of its technical design (Roe & Schulman, 2008, p.210). While complex and tightly coupled, the grid's interconnectedness offers many opportunities for "multiple strategies of resistance, resilience, and recovery after failure" (Roe & Schulman, 2008, p.205).

Supporting the Task Force's argument, Hines et al. (2008, p.7) suggest that while cascading blackouts may be inherent in the grid's complexity, there is room for improvement through rigorous standard setting and training. In this way, the electrical industry operates under the HRO assumption that while failures can occur, system operators can have the necessary training required to detect the failure before it becomes catastrophic. If failures are inevitable, an HRO develops the skills to detect errors and to contain these errors at early stages (SINTEF, 2004, p. 33). To this end, individuals working at power facilities would be trained to respond to would-be failures and to employ any number of strategies to prevent the failure.

Improving the reliability of the electric power system requires a more stringent approach than compliance with guidelines (Apt et al., 2006, p.7). Appropriate branches of government in the United States and Canada have taken action as required to make reliability standards mandatory and enforceable, and to provide penalties for noncompliance (U.S.-Canada Task

Force, 2004). Based on the Task Force's recommendations, new reliability standards have been developed by an independent, international electric reliability organization. These standards cover what is referred to as the three Ts: "trees, training and tools" (Minkel, 2008).

Maintaining reliability is a complex enterprise that requires skilled operators, sophisticated computers and communications, and careful planning and design. Planning and operating standards have been put in place to ensure that the grid remains in a reliable condition even if a contingency occurs, such as the loss of a key generator. In addition, system operators are trained in emergency procedures for a range of possible scenarios in order to prevent a total collapse of the electric system. The North American Electric Reliability Corporation's standard PER-003, for example, requires that operating personnel have at least the minimum training needed to recognise and deal with critical events in the grid (Minkel, 2008).

Critics of HRO argue that organizational learning must extend beyond a "fly-fix-fly" approach to safety (Marais et al., 2004, p. 10). Rather than relying on past experience and ad-hoc scenario training, organizational learning must be supplemented with increasing emphasis on intervention at the first sign of disaster through the use of hazard analysis, design for safety, and safety assurance techniques. The aforementioned changes to the electrical operating procedures address these critical concerns and acknowledge that while the system may vulnerable to risk (as suggested by NAT), the potential for catastrophic failure can be reduced.

5.0 Case Study: Terrorism and Public Utility Infrastructure Protection

Following the events of the 2003 Northeast Power Outage, reports circulated of a possible association with Al-Qaeda activities. While the 2004 Task Force found no evidence that terrorists caused or contributed to the power outage, the cascading blackouts were a sudden admonition to the possibility of a purposeful, malicious attack on North America's vulnerable electrical grid (Amin, 2003, p.1).

The threat of terrorism has challenged the way risk is perceived and managed in North America's energy infrastructure. Prior to recent developments in security strategy, such as Canada's 2004 National Critical Infrastructure Assurance Program, energy infrastructure protection was concerned primarily with risks to individual physical assets. Emphasis is now placed, however, on examining the energy infrastructure as a whole system (Shull, 2006, p.3). The explanation for this change has to do with the nature of terrorism itself, namely the fact that it is no accident at all, and a realisation that risk exposure and potential damage magnitude are not spread evenly across the energy infrastructure.

Energy generation and transmission systems have been designed to compensate quickly for failures, partly because it is not feasible to hold electricity in reserve while damaged system components are fixed. Consumer demand is left wanting the very instant that the grid goes

down (Shull, 2006, p.2). Even short-term power outages result in significant economic costs: for example, the aforementioned 2003 Northeast Power Outage resulted in approximately $10 billion in associated costs (Ness, 2008).

5.1 Redundancy and Vulnerability in the Energy Sector

To reduce the likelihood of service interruption as a result of accidents, the North American energy infrastructure was designed with an N minus 1 redundancy system, which means that each electrical grid is capable of servicing its demand in the absence of its largest contributing energy source (National Research Council, p.182). In other words, consumers should not notice a major disruption if a power generating station or transformer goes offline in their region. The N minus 1 system fits well with NAT because it anticipates that power generation and transmission systems will inevitably suffer breakdowns throughout their useful lives, and thus provides a loose coupling mechanism in the power grid so periodic shocks do not cause destabilisation (Clarke, 2005, p.92).

Notably, the N minus 1 system does not offer adequate protection against terrorist attacks (Shull, 2006, p.2). In a normal operating environment, it may be rare for a grid to lose more than one major energy source at the same time. A terrorist attack, however, lacks the characteristics of a normal accident; the attack may be strategic and coordinated as multiple targets can be hit simultaneously, and it may be directed, targeting the most sensitive assets (Ness, 2008). North America's electricity grids are designed to handle accidents, not intentional harm.

Given the importance of everyday demand for electricity in Canada, the safety of energy infrastructure must be highly reliable. As Shull notes, "an attack on the energy infrastructure would have devastating economic costs. There would certainly be a drop in consumer confidence following an attack, increased costs of security, costs of repair, consequential loss due to supply interruption, and decreased production" (2006, p.13). Perhaps the greatest threats to human life and economic security through energy infrastructure are found in generating facilities (such as nuclear power plants) and centralised distribution networks (such as natural gas pipelines) (Shull, 2006, p.7, 11). Numerous studies have been conducted to examine the consequences of plane crashes and other forms of terrorist attacks against nuclear facilities (Fedorowicz, 2007, p.6), underscoring a common principle of HRO: that ongoing training and learning can significantly reduce risk exposure (La Porte & Consolini, 1991, p.25). Training those working in power plants to cope with these worst-case scenarios and understand that they could occur may help them respond with greater confidence and mitigate further failures to the system.

Then again, a strong focus on individual generation and transmission sites fails to capture risks to other parts of the system. Consider the thousands of kilometers of oil and natural gas pipes across the country, and how vulnerable they are to terrorist attack relative to fortified central

facilities. It would be far easier to strike a remote section of pipe than a well-protected urban distribution pipe (Shull, 2006, p.8).

5.2 Connecting Terrorist Threats to Theory

The vulnerability of remote oil and gas pipes raises issues for both risk theories. A proponent of NAT might argue that the infeasibility of protecting all remote pipelines means that a terrorist attack is inevitable, and so society must determine whether or not the benefits of the oil energy industry are truly worth the risk. Proposals to transition North America's power generation to highly dispersed generating sites with low terrorist-related risk, such as thousands of windmills in wind farms, fit well with Perrow's argument that the targets of terrorist attacks (even entire populations) should be dispersed (Perrow, 2007).

An HRO defender would likely dismiss this concern, and argue that since damage to minor remote infrastructure would not result in catastrophic outcomes, individual components of the energy infrastructure can afford to be more risk tolerant than the system as a whole. Rural pipelines are open targets for terrorist attack, but they are not critical aspects of the highly reliable energy infrastructure.

Consider the string of bombings against gas pipelines in northern British Columbia. From October 2008 to January 2010, six bombs were detonated on Encana pipelines located in rural environments (Edmonton Journal, 2010). The use of threatening notes from the bomber supported suspicions that these events constituted terrorist attacks. Although the work of foreign-based terrorists was not suspected, ominous information came from Al-Qaeda affiliated websites, which had previously suggested Alaska oil pipelines as potential targets for would-be terrorists (Pemberton, 2006). Given the interest that terrorists have expressed in bombing rural pipelines in the vicinity, and considering the attacks that have already occurred, why has northern British Columbia not received more attention? There are likely multiple reasons, but the lack of sufficient risk to energy infrastructure posed by these attacks is a reasonable explanation.

Risks to the infrastructure are not evenly distributed. To the extent that some accidents or attacks cannot be avoided or feasibly prevented, the infrastructure is subject to normal accidents. However, given that the energy infrastructure provides on-demand services to the population and underpins almost all sectors of the economy, it must deliver to the standards of a highly reliable organization.

6.0 Recommendations

Based on the above case studies, three recommendations can be made to critical energy infrastructure operators and managers. These recommendations pertain to the capacity for learning, scenario-planning and command and control tenets of HRO.

6.1 Test New Methodologies on Proxy Systems

The Northeast Power Outage was exacerbated by a software bug that delayed the alarm system from sounding when problems arose. In the future, such software should be tested on an isolated, proxy grid in a number of scenarios, before being implemented across the grid. If this is not possible, alternative measures should be taken. Since the software in 2003 did not indicate that databases were on the verge of collapse, organizations could add levels of redundancy into these databases to also send warnings to operators' mobile phones, for example (provided the technology still is functional). Further, such warnings could be sent to other power plants utilizing the same grid as the threatened or failing energy system, so that other operators would know to isolate their own station from the grid. Alternatively, the databases could be monitored and incorporated into a decision-support system (DSS) that could later be drawn on (perhaps even through mobile phones) when the system is at elevated risk, provided there is sufficient time to do so. Indeed, Shen and Grivas (1996) note that a DSS approach allows for a systematic approach to processing information for management decisions, which is in accordance with HRO.

6.2 Modify Systems in Anticipation of Terrorist Attacks

A terrorist attack does not have to happen in order to learn from it. Scenario planning, central to HROs, could be expanded to a number of hypothetical, terror-based situations. Additionally, given that the N minus 1 energy grid may not function after direct terrorist attacks, the system should be redesigned. An option to explore is the further subdivision of the grid into loose interconnections so that damaged portions would not be able to cascade their malfunctions throughout the grid.

6.3 Enhance the Communications Network between Stakeholders

The 2003 Northeast Power Outage demonstrated that the lines of communication before, during and after a disaster may not be sufficient to mitigate damages or even figure out what those damages are. Lessons identified from this include the importance of having a reliable broadcast function in the energy sector. Operators, media, government authorities, security authorities and the public should all be aware or impending disasters or attacks so that they can react and, ideally, contribute to the damage mitigation. This could happen through pre-emptively creating groups of volunteers that could provide food and shelter to elderly people that may not be suited to cope alone without electricity, for example, and also by giving government decision-makers access to the system's DSS. Additionally, the public could be informed that energy supply will be severely limited. In turn, some individuals using electronic devices could be encouraged, through an internet or television broadcast, to minimise their power usage and prevent further damages to the grid.

7.0 Conclusion

Risks are generally identified as the potential weaknesses of an organization, sometimes to the extent that the purpose and expectations of the organization are forgotten. As this paper demonstrates, the risks to energy infrastructure are signified by the degree to which energy infrastructure is valued by consumers and not only by the degree to which things can go wrong. While the energy sector has several characteristics of a NAT organization, the high consequence nature of infrastructure operations lends to a predisposition towards the HRO theory of risk management. The risks are significant, because the output of the organization is significant. Energy infrastructure must be highly reliable, because society expects it to be highly reliable.

References

Amin, M. (2003). North America's Electricity Infrastructure: Are we ready for more perfect storms? IEEE Security & Privacy: IEEE Computer Science Society.

Apt, J., Lave, L.B., Morgan, M.G. (2009). Can the U.S. have reliable electricity? Carnegie Mellon Electricity Industry Center Working Paper.

Chang, S.E., McDaniels, T.L., Mikawoz, J., Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: Power outage consequences in the 1998 Ice Storm. Natural Hazards, 41, 337-358. CrossRef

Clarke, L. (2005). Worst Cases: Terror and Catastrophe in the Popular Imagination. Chicago: University of Chicago Press.

Edmonton Journal (2010). Timeline: Northern B.C. Pipeline Bombings. Retrieved from http://www.edmontonjournal.com/health/Timeline+Northern+pipeline+bombings/2421378/story.html

Fedorowicz, J. (2007). The Ten Thousand Mile Target: Energy Infrastructure and Terrorism Today. Conference Proceedings from the Critical Energy Infrastructure Protection Policy Research Series. Ottawa: The Norman Patterson School of International Affairs.

Hines, P., Apt, J., & Talukdar, S. (2008). Trends in the History of Large Blackouts in the United States. Proc. of the IEEE Power Engineering Society General Meeting, Pittsburgh.

Hartley, R.S., & Swaim, D.J. (2007). A New Causal Factors Analysis to Support a High Reliability Organization. Human Factors and Power Plants and HPRCT 13th Annual Meeting, IEEE, 382-385.

Hopkins, A. (2007). The problem of defining high reliability organisations. Working paper 51, National Research Centre for OHS Regulation: Australia National University.

La Porte, T.R. & Consolini, P. (1991), "Working in Practice but not in Theory: Theoretical Challenges of High Reliability Organizations." Journal of Public Administration Research and Theory. 1, 19-47.

Minkel, J.R. (August 2008). The 2003 Northeast Blackout--Five Years Later. Scientific American. Retrieved from http://www.scientificamerican.com/article.cfm?id=2003-blackout-five-years-later

Marais, K., Dulac, N., & Leveson, N. (2004). Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems. Engineering Systems Division Symposium, MIT, Cambridge, MA.

Ness, L. (2008). Terrorism & Public Utility Infrastructure Protection. Retrieved from http://www.ensec.org/index.php?option=com_content&view=article&id=154:terrorismandpublicutilityinfrastructureprotection&catid=84:energyinfrastructureprotection&Itemid=324.html

Pemberton, M. (2006). Officials: Alaska Pipeline not that Vulnerable. USA Today. Retrieved from http://www.usatoday.com/news/nation/2006-02-12-pipeline- threats_x.htm

Perrow, C. (1999). Normal Accidents: Living with High Risk Technologies. Second Edition. Princeton: Princeton University Press.

Perrow, C. (October 2007). The Next Catastrophe: Reducing our Vulnerabilities to Natural, Industrial, and Terror Disasters. Lecture retrieved from http://mitworld.mit.edu/video/510/

Roe, E., & Shulman, P.R. (2008). High reliability management: operation on the edge. Standford University Press: Stanford, California.

Shen, Yung-Ching and Dimitri A. Grivas. (1996). Decision-support system for infrastructure preservation. Journal of Computing in Civil Engineering. 1, 40-49. CrossRef

Shull, A. (2006). Assessment of Terrorist Threats to the Canadian Energy Sector. Conference. Proceedings from the Critical Energy Infrastructure Protection Policy Research Series. Ottawa: The Norman Patterson School of International Affairs.

SINTEF Industrial Management. (2004). Organisational accidents and resilient organisations: Five perspectives. SINTEF Report: Research Council of Norway.

U.S.-Canada Power System Outage Task Force (2004). Final report on the August 14th blackout in the United States and Canada: causes and recommendations. Retrieved from https://reports.energy.gov/BlackoutFinal-Web.pdf

U.S. National Research Council (2002). Making the Nation Safer. Washington: National Academies Press.