The Security of Critical Infrastructures: Introduction and Overview

Marcus Matthias Keupp

1 The Vulnerability of Critical Infrastructures

Human life and economic organization in urban areas must fundamentally rely on essential systems that provide water, health services, electricity, supply, mobility, and communication to the population. Any temporary or permanent disruption of these critical infrastructures has severe negative consequences that range from reduced economic productivity to the loss of human life.

Much work has described erratic failures of critical infrastructure as a result of weather-related incidents (e.g., [23, 46]). Severe natural disasters such as the 2005 hurricane *Katrina* can put complete critical infrastructure systems out of operation, and heatwaves as well as heavy snowfall can disrupt transportation and communication networks. Further, the urbanization of the human population increases. While as of 1950, only 30% of the world's population lived in cities, the United Nations expect that rate to grow to 68% by 2050 [53]. Since increased power demand induced by population growth already causes power outages [6], future generations of infrastructure will face an intensifying challenge to respond to this demand [26].

While this book does not dispute the relevance of such weather- and demand-related factors, it points to another, non-erratic risk which all critical infrastructure operators must face, namely, intentional attack. Three major reasons motivate this analytical focus.

First, the analysis of natural hazards and demand fluctuation fundamentally differs from the analysis of intentional attacks since probabilistic risk analysis is

M. M. Keupp (✉)
Department of Defense Economics, Military Academy at the Swiss Federal Institute of Technology Zurich, Birmensdorf, Switzerland
e-mail: mkeupp@ethz.ch

M. M. Keupp (ed.), *The Security of Critical Infrastructures*, International Series in Operations Research & Management Science 288,
https://doi.org/10.1007/978-3-030-41826-7_1

inappropriate if risk is induced by an intelligent adversary [7, 8, 11, 12, 20, 37, 40]. As a result, forecasting models that assume a random occurrence of disruptive events are not applicable to a scenario of intentional attack.

Second, any particular infrastructure can be thought of as a cyber-physical system in which three layers are intertwined: the physical infrastructure, i.e. mechanical and electric components, operating systems (OS) that steer and control these components, and information systems (IS) that connect and remote-control OS. Industrial control systems on the OS layer which control physical components are designed for failsafe and stable operations. Originally, these systems were relatively isolated and maintained locally, remote access being the exception rather than the norm. However, today they are linked and remote-controlled by software applications on the IS layer, many of which are connected to the internet and therefore exposed to the cybersphere [2, 59]. As a result, access paths to OS can be identified by specialized search engines such as `shodan.io`, and weaknesses in their protocols can be exploited [55]. It goes without saying that if this exploitation is done with an intention to disrupt or demolish system components, significant damage to the OS layer can be inflicted. The `dragonfly` attacks of 2014 and 2015 that targeted critical infrastructures in many countries exemplify this problem [18]. This exposure is intensified by an increasing integration of third-party supplier systems that interact with the operator's proprietary architecture. OS components such as metering devices or sensors often come without a graphical user interface, and they have weak or no password protection [26]. As services are outsourced to third-party suppliers, dependabilities and vulnerabilities are also created. For example, in the `dragonfly` case, infrastructure operators were lured to doppelganger update servers from which they downloaded the code, assuming it would be a regular vendor update [50]. Using the same method, an attacker could first infiltrate a supplier and then exploit links between supplier and infrastructure operator.

Third, such intentional damage is worst when it is inflicted by terrorist and state actors, and there is growing evidence that critical infrastructures have become a target for both groups. Terrorist attacks intend to physically demolish system components and therefore do not require technological knowledge about the system. As a result, the operative cost of such attacks is negligible. For example, the cost of the 2005 London attacks which targeted mass transit infrastructure is estimated at a mere eight thousand British pounds [52]. It is therefore not surprising that organized terrorism is targeting critical infrastructures. In particular, EIAD data suggest that energy infrastructures have become a significant target for terrorist attacks in many countries [30]. Ever since the Iraq War began in 2003, attacks on energy and oil transport infrastructure in the Middle East continue [51]. The universal feasibility of such attacks is exemplified by the recent drone attacks on oil refineries in Saudi Arabia [15].

In stark contrast to organized terrorism, state actors do not (or not yet) intend to demolish infrastructure, but rather to study and eventually control systems on the OS layer, such that they can credibly threaten to demolish or deactivate infrastructures. In principle, state actors attempt to obtain access to the OS layer by exploiting

weaknesses in the IS layer. Recent press coverage suggests that state actors are attempting to realize such access. Russia is purported to have infiltrated the national power grid of the USA [48, 49], Northern Ireland [44], and Ukraine [57], and the USA seem to have signaled that they are capable of attacking the Russian energy grid [45]. Such intentional attacks are unlikely to disappear soon. One might argue that Articles 22 and 23 of the 1907 Hague Convention should provide a backstop against critical infrastructure becoming a war target since they restrict belligerents' rights to choose methods or means of warfare, forbid action that causes suffering and destruction, and restrict the destruction of opponent property. However, the application of these articles requires attribution, and it is questionable whether or not a state actor who intentionally targets critical infrastructure would be willing to assume responsibility under international law. If an intentional attack is executed remotely by the cybersphere, attribution may be impossible to establish. Moreover, the convention only applies after a state of war has been explicitly declared, and hence it cannot consider de facto and hybrid warfare scenarios.

2 Contributions and Structure

This edited volume focuses on intentional attacks on critical infrastructure. It thus complements the vast contextual work that has studied quantitative analytical methods [39], sustainability and resiliency of operations [21, 42], interdependencies between infrastructures [24], engineering and industry-specific challenges [16, 43, 56], and technical standards [28].

However, the book also attempts to develop this literature by focusing on intentional attack as the very reason why sustainability, interdependency, and technical construction should be reconsidered in our time. Much of the above work has concentrated on static vulnerability analyses that identify weak spots in a network of system components (e.g., [29, 35]). In contrast, this book offers more complex attacker-defender scenarios, and it derives architectural implications for next-generation infrastructure. This choice is not only one of scope, but it also predisposes the methodological approach since the analysis of nonprobabilistic risk requires scenario-based setups, dynamic modeling, and numerical solution. The reader can reproduce the computation of these solutions since many authors share the original code they developed for this purpose.[1]

This scenario modeling unfolds in an interdisciplinary way. The authors in this volume have extensive backgrounds in economics, operations research, engineering, science, and computer science. Each author adds to the analysis from their disciplines' backgrounds, which yields a multifaceted, comprehensive work. The book therefore deploys a multi-method approach; it features graph analysis,

[1] Authorized readers can obtain the respective electronic supplementary material from the publisher's website.

linear programming, compartmentalized models, friction time analysis, and applied mathematical and statistical modeling.

All simulation and computation presented here was designed such as to maximize generalizability. While in many chapters, real supply and demand data from Switzerland is used to illustrate the analytical power of the models, their contribution is not limited to this context. Instead, the analytical procedures offered here can be globally applied to any infrastructure network in any country or economy. The book therefore addresses a global audience of both infrastructure operators, homeland security officials, and academic researchers.

The volume begins with the analysis of the risk implied by intentional attacks. This risk can be interpreted as a transitory or permanent imbalance between supply and demand once particular system components are demolished. As a result of such imbalances, the network may destabilize topologically. *Bürgy* explores such scenarios, using graph theory to formulate a generalizable operator model. He analyzes different attack strategies, the feasibility of which is contingent on the attacker's budget. Further, he calculates a complex illustration, using data from the Anytown model. His findings not only confirm that operator models can reveal vulnerabilities in the system. They also corroborate prior research that found that network elements cannot be prioritized by criticality [3].

Since such priority setting may be flawed, and since an all-hazard approach that would maximize the resilience of each and every element likely requires excessive investment, operators may choose to not invest at all and hedge the risk by buying insurance. Therefore, *Gillard* and *Anderhalden* analyze whether or not commercial insurers would be willing to offer such insurance. They estimate alphas required to calculate risk premiums, fitting a Pareto distribution to a sample of damages caused by terrorist attacks against critical infrastructure. Their analysis not only suggests that such risk premiums would be substantially larger than in the case of natural disaster. It also shows that the insurer would face an essentially unpredictable risk of bankruptcy. They conclude it is highly unlikely that any private firm would offer any insurance. They finally argue that substitutes such as the public sector or the capital market are unlikely to resolve this problem, confirming prior reserved assessments [54].

Both chapters demonstrate that any risk analysis of uncertain hazards, such as weather-related failure, is fundamentally different from a risk analysis of intelligent adversaries [40]. Still, industry groups and government officials worldwide continue to produce flawed probabilistic risk analysis and priority lists (e.g., [10, 13, 38, 47]). The contributions in the second part of this volume suggest that dynamic simulation and scenario evaluation is a much more productive approach when weaknesses and resilience are to be evaluated. Rather than debating the relevance of particular elements, these contributions look at the system as a whole, assuming that infrastructure operators are left to their own devices when it comes to protecting their systems. In particular, the analyses in this second section produce generalizable results that are applicable irrespective of the idiosyncratic setup of any particular network.

Liechti considers the fundamental requirement for human life: freshwater. He analyzes the consequences of a deliberate demolition of pipes that carry freshwater from reservoirs to urban areas as well as the utilization of such pipes to transmit organisms or substances which harm human health. He specifies a compartmentalized model that captures interactions between the attacker and the affected population, captures these interactions by a set of differential equations, and provides numerical solutions. His analysis clearly signals the benefits of dynamic scenario simulation that captures interactions instead of assigning static risk scores.

Human life is also at risk once intentional attacks on critical infrastructure have produced a mass casualty incident that strains the nation's medical treatment capacity. *Metzger* and *Keupp* consider such a case, using friction time analysis to estimate both recovery time and the capacity of the medical system to organize appropriate resources for timely treatment. Parametrizing their model with data from three model economies, they also show that a focus on restoring economic productivity may require preferential treatment and thus induce ethical dilemma.

Moreover, human life in urban areas must rely on a continuous and reliable supply of energy that not only provides heating and lighting but also powers all other critical infrastructure. Since that energy is typically transmitted from distant production sites to urban areas by the maximum voltage power grid, a disruption of this grid may cut off power supply. *Metzger*, *Paraď*, *Ravizza* and *Keupp* consider such a scenario. They use graph theory to specify a network interdiction model and apply this model to the case of Switzerland by using real topological, supply, and demand data. Specifying six different attack strategies by which nodes and edges are sequentially removed from the network, they analyze the resulting uncovered demand. They thus deepen prior approaches to dynamic analysis that recommend to delete nodes or arcs and reroute network flow over remaining network elements (e.g., [27, 34]). Their findings suggest that a blackout scenario is unlikely, whereas supply gaps are likely to persist for a long time, implying that power supply will have to be rationed. Their chapter does not only relativize populist and speculative scenarios by which the dire consequences of a total blackout are portrayed, but they also contribute to making networks more robust in a topological sense.

Human life in urban areas also depends on a continuous supply of goods required for food, consumption and production. Therefore, *Morstein* extends a network flow model designed by prior research, applying it to the level of a complex economy with multiple import routes and stockpiling. She then simulates the consequences of blocked import routes for both supply and stockpiling. Her results emphasize that significant cost savings can be achieved if disruption risk is assessed properly. The supply of such goods requires physical traffic, and in modern economies and urban areas, it is roads on which the majority of this traffic flows. Hence *Baumann* and *Keupp* provide a highly granular analysis of Switzerland's complete road network, using graph theory and supercomputing analysis to identify both topological weaknesses and consequences of traffic flow disruptions within and across urban areas. While the analysis of railway systems is beyond their scope, they nevertheless predict their model is transferable to such networks.

Finally, economic exchange and organization requires communication, and intentional attacks may target communication systems in order to disrupt or falsify any flow of information. *Strohmeier*, *Martinovic* and *Lender*s study such a scenario in the context of air traffic control. They provide a deep review of the extant literature, elaborating both an overview of extant technological vulnerabilities and an agenda of how future research should contribute to isolating communication systems against outside interference. This contribution can be extended to any type of information exchange once one considers that physical elements within critical infrastructures are controlled by OS that continuously exchange information with each other and interact with these physical elements (e.g., ETCS transponders control train movements, radio communication steers shipping traffic, etc.). Once such communication is distorted of falsified, physical damage may ensue, and hence there is a strong need for encryption whenever system elements exchange information.

The identification of vulnerabilities and topological weaknesses is useful when it comes to increasing the resilience of any critical infrastructure to intentional attack. However, the options available to operators are not limited to passive measures that focus on maximizing resilience. On the contrary, there are many ways by which infrastructure can be actively defended. Therefore, the three chapters in the third part of this volume discuss the extent to which such defense is feasible, and they show how systems can be designed to implement such defense.

Appropriate systems architecture is a prerequisite for effective defense. This is why *Kehrer*, *Tsigkanos*, and *Ghezzi* propose to conceive of critical infrastructures as cyber-physical systems that connect elements from the physical and the virtual world. Their formal and hence generalizable approach is rooted in bi-graph analysis. They develop a model that defines dependability requirements and proposes verification techniques which ensure that the system complies with the requirements, even in the presence of changes and unforeseen system evolution. This integrative approach is highly productive since it opens up a structured path to identifying integrative solutions.

Further, a crucial step to guarantee the security of a cyber-physical system is the detection and neutralization of unauthorized access, as well as the insulation of the system against future intrusions. *Casey* and *Nikkel* propose that digital forensics can realize these goals. Illustrating their approach with case vignettes from documented incidents, they explain how organizations can deploy forensic intelligence in order to improve their defense capabilities. They also provide counter-intuitive advice, indicating that it can be productive to quietly observe attackers that have infiltrated the infrastructure in order to study their behavior, rather than to eliminate the attack immediately. As organizations are attacked repeatedly and forensic insight from prior attacks accumulates over time, an iterative learning cycle is triggered whereby operators' responses to attacks become more and more effective.

Gillard essentially pursues the same motive, arguing that the analysis of past attacks is crucial to develop defense options that can neutralize subsequent attacks. However, he discusses this idea in the context of machine learning and automated defense. Using prior research on recommender systems, he develops a generalizable

model that adapts its response function to past attackers' actions. He demonstrates that such attacker-defender interaction is comparable to a multi-period game during which the specification of the response function continuously adapts and becomes the more effective the more rounds are played. While such dynamic adaptation is superior to a static rule-based approach, it requires a high incidence rate of attacks if quick learning is desired.

3 Building Better Infrastructure

The physical and virtual topology of a critical infrastructure, the human beings intentionally attacking it, and other human beings defending it constitute an ecosystem in which all of these elements continuously co-evolve. This is why any critical infrastructure should be perceived as a dynamic system that requires continuous architectural adaptation as novel generations of infrastructures are to replace extant systems.

Most fundamentally, the construction of such novel generations should not be prejudiced by extant architectures. The contemporary topology and control of any system always constitutes an artifact that must be judged by its historical context. There is hence no coercing necessity that extant architectures should be replicated as next-generation systems are built. Today's physical infrastructures vital for human life and productivity, such as dams, water power plants and the national power grid, were constructed in the first three quarters of the twentieth century, i.e. at a time when deliberate attacks on this infrastructure by exploiting weak spots in the OS or IS layer were technologically infeasible or quite simply unimaginable. Hence, the planning of future generations of infrastructure should adopt a perspective of total analytical deconstruction.

Operators and researchers alike should confront themselves with the question how they would build a replacement infrastructure from scratch if the current system was rendered completely inoperative as a result of intentional attack. Thus, creative thought not prejudiced by the existence of today's physical structures would emerge. For example, when designing railway systems, operators often take the historically grown network of tracks as a given and try to optimize secure flow subject to this constraint. However, an efficient design should first consider which flow originates from where with which destination and then build tracks and security infrastructure that can satisfy this demand. This approach may entail deconstructing extant tracks and control systems as well as reconsidering geospatial planning.[2]

Until such novel generations of infrastructure are built, operators face the challenge of making extant infrastructures resilient not only to the weather, but also to intentional attack. Insulating infrastructure against the probabilistic risk

[2]The author thanks Thomas Süssli and Martin Ball for sharing these ideas and for some inspiring discussion.

of random failure is not equivalent to neutralizing the nonprobabilistic risk of intentional attack. Therefore, infrastructures designed to be resilient to weather-inflicted damage are not automatically protected from such attacks. There need not be any positive spillover effect whereby investments or insurance against random failure would also neutralize nonprobabilistic risk. In fact, investment models used to date might have to be reconsidered since the extant generation of physical infrastructure components was not designed to withstand intentional attacks. As a result, every architectural option which increases physical resilience to intentional attack requires significant investments.

The most radical way to produce such resilience is to minimize the exposure of physical infrastructure by moving it underground. Consider the case of alternating current power grids. While moving such grids underground is feasible for low- and medium-voltage local power lines, the case is different for high-voltage architectures, both because the air can no longer be used for insulation, and because high-voltage earth cables have lower transmission capacity due to reactive current and thermic loss. As a result, such cables require cooling and compensators every ten miles or so, moreover, they are difficult to inspect and maintain and more susceptible to failure than overhead lines. The only option would be a radical change of the complete grid architecture to a direct current design whose cables can span large distances underground even at high voltages (e.g., in underwater sea cables). However, in both cases, protecting power lines is not enough; transformer stations and rectifiers would have to be moved underground too. While the associated investment cost is probably excessive for a developed economy with a grown infrastructure, developing economies which build novel grids from scratch may consider such options.

However, rebuilding structures underground is not a panacea. Consider the sewage system, i.e. an infrastructure built underground by design. The structure is both critical for population health in urban areas and it is exposed to intentional attack. In contrast to the water supply system, sewage canals are not pressurized, hence they provide an open and easily accessible physical pathway to virtually every installation in an urban infrastructure. Since the system is designed to withstand extreme water flow caused by thunderstorms or flooding, the diameter of its pipes exceeds the diameter required for ordinary operation by a factor of 100. As a result, main sewage pipes have diameters of several yards but carry but a trickle of wastewater most of the time. This architecture makes the system eligible as a carrier structure for intentional attacks.[3] In this case, minimizing exposure requires sealing off all access points in streets and buildings, and introducing physical blocking, degassing, or purification devices. The associated investment cost is certainly significant.

Since physical network elements cannot be prioritized by criticality, investment in the robustness of particular components is arbitrary and hence does not necessarily provide security. Still, operators are advised to build redundant

[3]The author is grateful to Jonas I. Liechti for developing and sharing these points.

architectures, i.e. to replicate several instances of components or subsystems (e.g., [5, 36]). Such blanket advice is questionable. For example, recommendations to always store at least one replica of complex components made to specification and difficult to replace at short notice (e.g., large transformers in power stations) comes at significant investment cost but ignores network topology and connectivity. Whenever the robustness of a complete network to intentional attack is to be maximized, its topological structure should be considered first. For example, scale-free networks are highly robust to random failure of elements, but not to intentional attack.

Inhomogeneous networks characterized by few but highly connected nodes have a significantly lower attack survivability; they break into many isolated fragments when the most connected nodes are targeted [1]. Since many critical infrastructures are scale-free networks (e.g., communication, power distribution), investments in redundancy must be subject to prior connectivity analysis. Such investments are also inversely related to the substitutability of any capacity between any two nodes. If a particular arc is intentionally attacked but network flow can be rerouted at low cost while the network stays connected, there is no need for additional redundancy, and vice versa. This relationship is nicely illustrated by the Rastatt incident. While not an intentional attack, it provides an ideal case study of what a lack of substitutability implies should such an attack occur.

In summer 2017, in the vicinity of the German city of Rastatt, tracks that route significant European north- and southbound railway freight traffic were disrupted for several weeks due to unintentional subsidence of the ground as a result of tunnel work (see [9] for extensive background documentation). Due to construction works, underutilization, and technical incompatibility on neighboring routes, this traffic could only be rerouted partially, and costly substitutes had to be improvised. Total loss to manufacturing, logistics, and operator companies is estimated at two billion Euros [25]. Since the European railway network is not a designed infrastructure, but rather an historically grown amalgam of very different technologies and standards, network redundancy is significantly limited as long as the interoperability of national subsystems is not improved or novel harmonized infrastructure built.

By contrast, the drone attacks on oil refineries in Saudi Arabia in September 2019 had no such long-term effect. Although global supply was reduced by 6% in a single day as a consequence of the attack, the network had both excess capacity and technological homogeneity that provided a high degree of substitutability. About 40% of the supply gap was compensated after 2 days, while full capacity was restored after several weeks [15].

Decentralization of network components does not only remove high-value targets such as power parks, thus raising both the transaction and the opportunity cost of terrorist attacks [17]. It also increases network reliability since centralized elements typically have greater connectivity. As future generations of physical infrastructures are built, decentralizing these by design may prove to be more effective than increasing the robustness of centralized networks. For example, today's power systems are essentially characterized by spatially separated supply (plants) and demand (urban areas) which are connected through a centralized maximum voltage

transfer network. This grid must therefore fulfil three tasks at the same time: equalize supply and demand network-wide to keep frequencies stable, trade energy internationally, and provide supply to urban areas.

The development of decentral microgrid architectures may reduce the importance of the latter task. Already today, energy-producing infrastructure can restart itself after an outage if kinetic energy from local primary reserves is available to power a black start and provide voltage stability [14]. As the efficiency of renewable energy sources, batteries and hydrogen tanks improves, urban areas may soon be able to provide a basic autonomous supply of power for themselves even in the case of main grid failure [32, 41]. Depending on the infrastructure in question and local geography, such autonomy could be designed at low cost. For example, if natural freshwater supplies are adjacent to urban areas, equipping the population with nanofiltration tubes that use physical membranes for universal water purification may provide an affordable, autonomous, individual-level fresh water supply if the main supply network is interrupted or contaminated.

While redundancy and decentralization may be effective, they only address the physical, but not virtual aspect of the architecture. Since cybersecurity is paramount to provide protection against intentional attacks on critical infrastructure [4, 33], measures on the OS and IS layers must complement efforts to strengthen the physical resilience of infrastructures. The challenge here is to shut off the system against unauthorized intrusion while maintaining connectedness with customers and suppliers. One way to address this challenge is the construction of ‘onion models’. In such a model, the IT landscape is partitioned by design into three security zones.

The inner zone comprises critical OS that control electrical or mechanical parts the mishandling of which carries significant security concern (e.g., machinery that controls the immersion of fuel rods in the cooling water in a nuclear power plant). Such OS must be fully isolated from any other IT system; ideally, any manipulation of the system should require the cooperation of at least two certified individuals. Suppliers and any other third parties should not be granted access to this zone.

The medium zone comprises less critical local OS that is to be remote-controlled by higher-level OS. All such intra-OS layer communication should be strongly encrypted, and all communication should be logged and monitored in real time. Ideally, the controlling OS application could be programmed as a closed system with firmware authentication procedures, such that it would refuse to execute non-proprietary code. Operators should also welcome novel point-to-point communication architectures that raise the technological barrier for outside intrusion. For example, the SCION architecture strives to remains highly available even in the presence of distributed adversaries that attempt to reroute traffic through self-created corrupted paths [58].

Finally, the outer zone isolates supplier and customer interaction on the IS layer, hence, there must be strong barriers to the medium zone. Suppliers should not be allowed to interact with or maintain OS systems unless they are closely surveilled in real time. This may both entail deconstructing remote-controlled and supplier-controlled architectures to some extent as well as reintroducing personalized control of equipment which is currently operated remotely.

Lastly, these protective measures should not deter operators from planning more proactive measures of defense. Besides strengthening the resilience of the physical, OS and IS layers, the system may also defend itself autonomously once intrusions are detected. Threat reconnaissance systems should continuously scan the environment for intentional attacks on both the OS, the IS, and the physical layer. Such systems may then launch a tailored response (e.g., erect magnetic fields to restrict drone operability once flight movements are detected) and learn from the attack, improving such response over time. The contributions by *Casey* and *Nikkel* and *Gillard* in this volume have demonstrated that such iterative learning cycles are productive, and automating such learning processes in machine learning procedures or AI algorithms seems a promising step. While such measures can require human authorization on the physical level, they can be fully automated on the IS and OS level, in order to shorten the cyber kill chain as much as possible, ideally, to zero days.

As such solutions and architectural changes are implemented in the context of national security, there are significant policy issues both within and beyond the organization that operates critical infrastructure. For the operator organization, appropriate investment planning does not only entail confronting the problem that systems and software on the IS layer obsolesces fast, whereas OS applications are operative for years and the physical infrastructure for decades until replacement investments are made. Given the disruptive effect of intentional attacks for the operation of critical infrastructure, operators should revise static investment models, such as [22]. Further, behavioral operations research postulates that human behavior is associated with the efficiency of systems operation and hence defense [19]. Since formal analytical models—including those deployed in this volume—explicitly or implicitly assume that human agents behave rationally, relaxing this assumption may lead to a better understanding of both intentional attacks and their defense. Further, operators should understand the contingencies that govern other operators' willingness to share or not share information about intentional attacks they have experienced [31].

National security policies may also have to be revised as novel generations of critical infrastructure are built. As long as government officials continue to produce probabilistic risk analysis and priority checklists, their work is of little use to operators who face intentional attacks. 'Spending down' such flawed priority lists until budgets are exhausted will do little, if anything, to improve security. Instead, governments should promote institutional innovation that can motivate operators to provide for the necessary security measures themselves. Since the architectural options discussed in this chapter require significant investment, operators might face the moral hazard of not investing enough in security measures since such investments reduce profitability. To alleviate this problem, the government should create a national supervisory authority that supervises operators and demands proof of effective security measures, but leaves the implementation of such measures and the associated investment planning to them.

Moreover, government should consider how to prepare its armed forces for a scenario of intentional attacks on critical infrastructure. In the absence of a highly

qualified engineer corps, the armed forces could probably help to mitigate the consequences of such attacks (e.g., public unrest, looting, mass casualty treatment), but they could not prevent the attack from happening in the first place. Therefore, cooperation between the armed forces and critical infrastructure operators, with the goal of developing effective defense capabilities, is certainly desirable.

The authors in this volume have used publicly available data to simulate intentional attacks on critical infrastructure, and there is no reason to believe that attackers could not do the same. Critical infrastructure operators cannot prevent intentional attacks from happening, but they can do much to strengthen the resilience of their infrastructures, and they can equip them with measures and procedures for automated defense. The contributions in this volume provide much useful material that helps to simulate and implement such solutions. The high degree of generalizability of these contributions makes them applicable on a global scale. Operators can and should use them to build defensible architectures that provide secure supply to future generations of urban populations.

References

1. Albert, R., Jeong, H., Barabasi, A.L.: Error and attack tolerance of complex networks. Nature **406**, 378–382 (2000)
2. Alcaraz, C., Zeadally, S.: Critical infrastructure protection: requirements and challenges for the 21st century. Int. J. Crit. Infrastruct. Prot. **8**, 53–66 (2015)
3. Alderson, D., Brown, G., Carlyle, M., Cox, L.: Sometimes there is no 'most-vital' arc: assessing and improving the operational resilience of systems. Mil. Oper. Res. **18**(1), 21–37 (2013)
4. Anderson, R., Fuloria, S.: Security economics and critical national infrastructure. In: Moore, T., Pym, D., Ioannidis, C. (eds.) Economics of Information Security and Privacy, pp. 55–66. Springer, Boston (2010)
5. Bauer, E., Adams, R., Eustace, D.: Beyond Redundancy: How Geographic Redundancy Can Improve Service Availability and Reliability of Computer-Based Systems. John Wiley & Sons, Hoboken (2011)
6. Benna, U., Benna, I. (eds.): Urbanization and Its Impact on Socio-Economic Growth in Developing Regions. IGI Global, Hershey (2018)
7. Brown, G., Cox, L.: How probabilistic risk assessment can mislead terrorism risk analysts. Risk Anal. **31**, 196–204 (2011)
8. Brown, G., Cox, L.: Making terrorism risk analysis less harmful and more useful: another try. Risk Anal. **31**(2), 193–195 (2011)
9. Büchel, B., Partl, T., Corman, F.: The disruption at Rastatt and its effects on the Swiss railway system. In: Proceedings of the 8th International Conference on Railway Operations Modelling and Analysis (ICROMA), Norrköping, pp. 201–218 (2019)
10. Council of the European Union: Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council of the European Union, Brussels (2008)
11. Cox, L.: Some limitations of "Risk = Threat *x* Vulnerability *x* Consequence" for risk analysis of terrorist attacks. Risk Anal. **28**, 1749–1761 (2008)
12. Cox, L.: Improving risk-based decision making for terrorism applications. Risk Anal. **29**, 336–341 (2009)

13. Department of Homeland Security: National infrastructure protection plan. Washington DC (2013)
14. Ekman, C., Jensen, S.: Prospects for large scale electricity storage in Denmark. Energy Convers. Manag. **51**(6), 1140–1147 (2010)
15. Energy Intelligence Group: Market forces: Saudi recovery. Report. Energy Compass (2019). http://www.energyintel.com/pages/login.aspx?fid=art&DocId=1051919
16. Ericsson, G.: Cyber security and power system communication-essential parts of a smart grid infrastructure. IEEE Trans. Power Delivery **25**(3), 1501–1507 (2010)
17. Frey, B., Luechinger, S.: Decentralization as a disincentive for terror. Eur. J. Polit. Econ. **20**, 509–515 (2004)
18. Genge, B., Kiss, I., Piroska, H.: A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. Int. J. Crit. Infrastruct. Prot. **10**, 3–17 (2015)
19. Gino, F., Pisano, G.: Toward a theory of behavioral operations. Manuf. Serv. Oper. Manag. **10**(4), 676–691 (2008)
20. Golany, B., Kaplan, E., Marmur, A., Rothblum, U.: Nature plays with dice-Terrorists do not: allocating resources to counter strategic versus probabilistic risks. Eur. J. Oper. Res. **192**, 198–208 (2009)
21. Gopalakrishnan, K., Peeta, S. (eds.): Sustainable and Resilient Critical Infrastructure Systems. Springer, Berlin (2010)
22. Gordon, L., Loeb, M.: The economics of information security investment. ACM Trans. Inf. Syst. Secur. **5**, 438–457 (2002)
23. Guikema, S.D.: Natural disaster risk analysis for critical infrastructure systems: an approach based on statistical learning theory. Reliab. Eng. Syst. Saf. **94**(4), 855–860 (2009)
24. Hall, J., et al. (eds.): The Future of National Infrastructure: A System-of-Systems Approach. Cambridge University Press, Cambridge (2016)
25. Hanseatic Transport Consultancy: Estimation of the economic damage of the Rastatt interruption from a rail logistics perspective. Hamburg (2018). http://www.hupac.ch/EN/Study-Rastatt-disruption-b26dcc00
26. Huq, N., Hilt, S., Hellberg, N.: US cities exposed: industries and ICS. A shodan-based security study of exposed systems and infrastructure in the US (2017)
27. Kinney, R., Crucitti, P., Albert, R., Latora, V.: Modeling cascading failures in the North American power grid. Eur. Phys. J. B **46**(1), 101–107 (2005)
28. Knapp, E., Langill, J.: Industrial Network Security, 2nd edn. Elsevier, Amsterdam (2014)
29. Lopez, J., Setola, R., Wolthusen, S. (eds.): Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense. Springer, Berlin (2012)
30. Melkunaite, L., Giroux, J., Burgherr, P.: Research note on the energy infrastructure attack database (EIAD). Perspect. Terrorism **7**(6), 113–125 (2013)
31. Mermoud, A., Keupp, M., Huguenin, K., Palmié, M., Percia David, D.: To share or not to share: a behavioral perspective on human participation in security information sharing. J. Cybersecurity **5**(1), tyz006 (2019)
32. Mohammed, O., Youssef, T., Cintuglu, M., Elsayed, A.T.: Design and simulation issues for secure power networks as resilient smart grid infrastructure. Smart Energy Grid Engineering, pp. 245–342. Academic Press, Cambridge (2017)
33. Moore, T.: The economics of cybersecurity: principles and policy options. Int. J. Crit. Infrastruct. Prot. **3**, 103–117 (2010)
34. Motter, A., Lai, Y.C.: Cascade-based attacks on complex networks. Phys. Rev. E Stat. Nonlinear Soft Matter Phys. **66**(6), 065102 (2002)
35. Murray, A., Grubesic, T.: Critical Infrastructure: Reliability and Vulnerability. Springer Advances in Spatial Science, Berlin (2007)
36. National Infrastructure Advisory Council: A Framework for Establishing Critical Infrastructure Resilience Goals. Department of Homeland Security, Washington DC (2010)
37. National Research Council: Review of the Department of Homeland Security's Approach to Risk Analysis. The National Academy of Sciences, Washington, DC (2010)
38. Olsson, S. (ed.): Crisis Management in the European Union. Springer, Berlin (2009)

39. Ouyang, M.: Review on modeling and simulation of interdependent critical infrastructure systems. Reliab. Eng. Syst. Saf. **121**, 43–60 (2014)
40. Parnell, G., Smith, C., Moxley, F.: Intelligent adversary risk analysis: a bioterrorism risk management model. Risk Anal. **30**(1), 32–48 (2009)
41. Patrao, I., Figueres, E., Garcera, G., González-Medina, R.: Microgrid architectures for low voltage distributed generation. Renew. Sust. Energ. Rev. **43**, 415–424 (2015)
42. Petit, F., et al.: Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience. Argonne National Lab. (ANL), Argonne (2013)
43. Rinaldi, S.: Modeling and simulating critical infrastructures and their interdependencies. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences (HICSS'04) (2004)
44. Rogan, A., Bridge, M.: Russia-Backed Hackers Try to Hijack Britain's Power Supply. The Times, London (2017)
45. Sanger, D., Perlroth, N.: U.S. Escalates Online Attacks on Russia's Power Grid. The New York Times (2019)
46. Sarker, P., Lester, H.D.: Post-disaster recovery associations of power systems dependent critical infrastructures. Infrastructures **4**(2), 30 (2019)
47. Singh, A., Gupta, M., Ojha, A.: Identifying critical infrastructure sectors and their dependencies: an Indian scenario. Int. J. Crit. Infrastruct. Prot. **7**, 71–85 (2014)
48. Smith, R.: Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say. The Wall Street Journal (2018)
49. Smith, R., Barry, R.: America's Electric Grid has a Vulnerable Back Door-and Russia Walked Through It. The Wall Street Journal (2019)
50. Symantec Corporation: Dragonfly: Western energy sector targeted by sophisticated attack group. Outlook Series (2017). https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks
51. Tichý, L.: Energy infrastructure as a target of terrorist attacks from the Islamic State in Iraq and Syria. Int. J. Crit. Infrastruct. Prot. **25**, 1–13 (2019)
52. United Kingdom Home Office : Report of the Official Account of the Bombings in London on 7th July 2005. United Kingdom Home Office, London (2006)
53. United Nations: World Urbanization Prospects: The 2018 Revision. United Nations: Department of Economics and Social Affairs, Population Division (2018)
54. United States Department of Energy: Insurance as a risk management instrument for energy infrastructure security and resilience. U.S. Department of Energy, Washington DC (2013)
55. Xu, W., Tao, Y., Guan, X.: The landscape of industrial control systems (ICS) devices on the internet. International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Glasgow (2018)
56. Yusta, J., Correa-Henao, G., Lacal Arantegui, R.: Methodologies and applications for critical infrastructure protection: state-of-the-art. Energy Policy **39**, 6100–6119 (2011)
57. Zetter, K.: Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired (2016)
58. Zhang, X., Hsiao, H.C., Hasker, G., Chan, H., Perrig, A., Andersen, D.: SCION: Scalability, control, and isolation on next-generation networks. In: Proceedings – IEEE Symposium on Security and Privacy, pp. 212–227 (2011)
59. Zhu, B., Joseph, A., Sastry, S.: A taxonomy of cyber attacks on SCADA systems. In: Proceedings of the 2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, pp. 380–388. IEEE Computer Society, Washington (2011)