SECURITY & DEFENCE QUARTERLY
https://securityanddefence.pl/

Intelligent terrorism as a security threat to critical infrastructure

Ossi Heino

ossi.heino@tuni.fi

https://orcid.org/0000-0003-0818-3879

Faculty of Social Sciences, Tampere University, Arvo Ylpön katu 34, FI-33520, Tampere, Finland

Abstract

This paper considers terrorism as potentially 'intelligent', as a threat capable of abusing the critical infrastructures of societies and the related methods for knowledge production. Respectively, it sees critical infrastructures as attractive mediums for terrorist influence. The paper describes the contrast between the logic of providing security and certainty for critical infrastructures and the threat of terrorism, which is evolving in terms of its systemic capacities and intelligence. The way security is provided within critical infrastructures and the way intelligent terrorism could operate seem to separate from each other, thereby creating vulnerability. The paper seeks to enhance the conceptual understanding of this question by describing and closing the gap created by the intellectual separation. By doing so, the article will shed light on the conceptual dimension of the (in)security that has gone unnoticed in the interface between critical infrastructures and terrorism. It outlines the aforementioned dilemma and provides conceptual understanding that makes it easier to grasp and communicate further. The paper shows that the intellectual separation has weakened the possibilities for theoretically understanding and practically recognising terrorism as a phenomenon that is becoming systemically more conscious, more intelligent and potentially increasingly capable in a form of violence that exploits the basic structures of societies and the related knowledge methods for its own purposes. As a conclusion, the paper stresses the importance of profoundly critical tools. Such tools are often perceived as being undesirable or even counter-productive in figuring out the mechanism through the very means utilised in providing for security.

Keywords:

security, threat, critical infrastructures, intelligent terrorism, technical rationality

Article info
Received: 29 April 2022
Revised: 14 June 2022
Accepted: 26 July 2022
Available online: 27 August 2022

Citation: Heino, O. (2022) 'Intelligent Terrorism as a Security Threat to Critical Infrastructure', Security and Defence Quarterly, 39(3), pp. 33–44. doi: 10.35467/sdq/152422.

Introduction

Security has been, is, and continues to be an ever-present concern in societies. The way states, institutions and organisations provide security also affects how it is perceived. Perceived insecurity can be extensive, even when many indicators show that life is more peaceful and secure than before. The interpretation frameworks through which security is grasped therefore play a key role. States, institutions and organisations not only produce information about their operations and operating environment, but also create frameworks for interpretation that determine how reliable, functional and strategically up-to-date these operators are perceived to be. This is a particularly important theme for systems that have a special role to play in the functioning and continuity of societies. It therefore deserves critical conceptual research.

Critical infrastructures (CIs) are the cornerstone of societies' day-to-day functioning, safety and security (Bennett, 2018; Żaboklicka, 2020). CIs include, but are not limited to, sectors such as energy, water, transportation, information and communications technology, nuclear, financial services and government facilities.[1] As Hellström (2007) explains, '[c]ritical infrastructures are "critical", not because they are important in general, but because they are strategically connected in such a way that they focus society's total vulnerability to a few particular points in the system.' In this sense, CIs have the potential to cause adverse effects that go deep into societies' functional ability (Graham, 2010). They have become a security problem (Collier and Lakoff, 2007).

[1] *https://www.cisa.gov/critical-infrastructure-sectors*

Considering CIs as socio-technical systems, significant amounts of material and intellectual capital are tied to them, not to mention the professional capital needed to keep the systems safe to operate. This material and intellectual capital that has accumulated and cultivated over time has its well-established tracks and well-polished ways to focus on the essentials. It has enabled CIs to become more capable so that they can better serve changing needs. Moreover, it incorporates a knowledge structure that formulates the guidelines for development and frames how risks and threats should be managed, thereby assuring people about the reliability of CIs. Performing as expected, CIs become a set of self-evident structures upon which daily operations can be designed (Graham, 2010).

It is interesting to consider CIs as systems in which technological assemblies are intertwined with the social processes of knowledge production. This paper grasps this through the concept of the black box, introduced by Latour (1987, 1994, 1999). According to this theorisation, as the number of a system's components and their management become increasingly complex and hence more difficult to understand, it is reasonable to describe it as a black box from which only inputs and outputs need to be known. The historical bifurcation points of the systems, unselected development paths, controversial choices, conflicting mindsets, different interests of actors, etc. are locked in a box, so that only its main function remains visible (Latour, 1987, 1999; see also Shindell, 2020). Blackboxing 'obfuscates actions and inner workings due to stable and reliable functioning' as De Rosa (2018) explains.

Infrastructure systems can quite obviously be considered black boxes, as they are taken for granted and their internal mechanisms are not assumed to be understood by outsiders (Graham, 2010; Latour, 1994). Only their failure—when, for example, they become 'transformed into weapons of mass disruption, destruction and often death' (Graham, 2005)—may reveal something about the functioning of the inner world of black boxes, whereas in ordinary times when they operate as expected, the underlying assumptions of their operations and security become blackboxed, faded out of the critical sight.

However, trust in CIs requires that they can show that they are aware of their operational security environment and that they can manage risks. It must be demonstrated in an evidence-based manner that CIs are in competent hands—the reliability of operations must be credibly reported (Bennett, 2018). But what is classified as evidence and how conclusions about the reliability of CIs are drawn stay out of reach (Aven and Guikema, 2011). In addition, what also remains hidden is the process in which non-knowledge is worn in the form of expert knowledge.[2] This is essential since knowledge and non-knowledge are both constitutive in the decision-making processes (Beck, 2002; Daase and Kessler, 2007). In line with Rydin *et al.* (2018), it can be argued that the question is how knowledge-claims are constructed in response to the uncertainty of the security environment. In fact, from the outside of a black box, it is impossible to see beyond the knowledge-claims presented from inside the box and assess their limitations and validity. That is, one only needs to trust CIs' reliability and be interested only in inputs and outputs.

[2]For instance, what are the unknown knowns, 'knowledge that is not known because it is not supposed to be known' described by Daase and Kessler (2007).

In this context, terrorism constitutes a particularly interesting security threat for CIs in its capacity for creativity, learning and intelligence[3] (Gill *et al.*, 2013). How the development potential of terrorism is interpreted—what is perceived as being possible for it—affects the interests of terrorism research, the counter-terrorism practices, and risk assessment work regarding vital functions of societies. New types of terrorist acts keep pushing the boundaries of seeing that potential, but that sight tends to come only after the effect. It can be said that the events of 9/11 caused long-term impacts precisely because they undermined the then-established ideas and assumptions of terrorism prevention: something happened that had been thought impossible, or not properly thought of or deemed as being beyond comprehension (The 9/11 Commission Report, 2004).

[3]In this article, intelligence is defined in line with the Merriam Webster dictionary as 'the ability to learn or understand or to deal with new or trying situations' and as 'the ability to apply knowledge to manipulate one's environment or to think abstractly as measured by objective criteria'. In this sense, intelligence is not a normative or ethical statement.

Although a great deal has been learned from the 9/11 event, CIs as increasingly complex bundles of operations that extend into the daily functioning of societies continue to constitute a platform of opportunity for terrorism (Collier and Lakoff, 2007; Coward, 2009). Things that remain outside the established interpretative framework can become a reality in new and drastic ways, which may further shake the closely guarded contents of black boxes in addition to causing extensive and deep adverse impacts in other ways (Botha, 2020). In this regard, harnessing such systems that have developed into increasingly complex bundles of critical societal functions and their interdependencies over time (Cedergren *et al.*, 2018; Hempel *et al.*, 2018; Peerenboom and Fisher, 2010; Wang *et al.*, 2013) to serve terrorist purposes as a weapon would make 9/11 look like a short prelude.

Moreover, what is undoubtedly left unburied in black boxes concerns our understanding of the interconnections and dependencies in the CIs. Not only is our ability to manage complex systems limited, but also the ways in which security threats are examined and uncertainty is reduced are formulated and developed further in silos (Aradau and van Munster, 2011). Our vulnerability to terrorism thus reflects the very nature of our systems and the way they have been organised (Logan *et al.*, 2019). It is therefore important to understand the dynamics of such a threat and the provision of security in the context of CIs in more diverse and critical ways.

Aim and method

When terrorism is grasped as an active threat that proceeds intelligently in terms of its purpose and objectives, it appears to be capable of becoming aware of the vulnerabilities of CIs and adjusting its tactics to avoid the terrorism prevention measures (Hausken, 2017; Quijano *et al.*, 2018). In this sense, the way security is provided within CIs and the way intelligent terrorism could operate form an interesting tension for closer

examinations. They are separating from each other in a way that creates vulnerability, albeit it is not well understood how.

This article seeks to enhance the conceptual understanding by analysing this intellectual separation using the lens from the black box theorisation (Latour 1994, 1987). By so doing, the article sheds light on the conceptual dimension of the (in)security that has gone unnoticed in the interface between CIs and terrorism (Ranstorp and Normark, 2009). It aims to outline the aforementioned dilemma and provide conceptual understanding that makes it easier to grasp and communicate further. It is conducted in the following way: First, the rationality of creating security within the context of Cis is outlined (i.e., the logic of blackboxing). After that, terrorism targeted at CIs as a method capable of opening black boxes is scrutinised. Then, the potential next level of terrorism that could shake the content hidden in the box is discussed. Finally, conclusions are drawn, whose intention is to open new paths in thinking in unforeseen—but when it comes to terrorism—relevant and insightful ways.

Results

Critical infrastructure and the logic of creating security

The security of CIs requires not only the effective assessment and management of threats and risks and proven reliability,[4] but also public trust in that reliability; the dependence of everyday activities on CI systems indicates and requires trust and certainty (Critical Five, 2014). The interpretation frameworks through which certainty assessments are made and trust maintained reflect the way threats are perceived, prepared for and managed.

Increased connections and the formation of dependencies within CIs are essential features that reflect the level of modern societies' development. However, the critical elements of the systems need to be protected, and external interference with the processes must be prevented—in terms of *target hardening*, for instance—to ensure the continuity of the respective operations, and also in exceptional times (Bennett, 2018; Botha, 2020; Kahan, 2017; Wang *et al.*, 2013; Wiśniewski, 2016). Such a solidification of protection is a way of making systems more robust and less susceptible to interference and harm (Aradau, 2010). However, it is concurrently a method for blackboxing CI systems in a way that supports their main functional objectives and draws attention to their essential aspects. That is, they encapsulate not only in a technical sense but also in terms of knowledge production (Moore *et al.*, 2019). But what does this capsulation mean more specifically?

In modern societies, CIs consist of sheltered systems of this type, together with connections and dependencies between them. Due to such complexity, even if an individual function or process can be sheltered and controlled, this capacity is unavailable at the system level; security, reliability and the related knowledge within separate systems do not translate into a broader system-level capacity (Hempel *et al.*, 2018). Despite this, CIs must deliver on their promise of certainty and prove their ability to provide for security. But how does the mechanism behind this 'providing for security' work? In other words, how is blackboxing conducted so that CIs present themselves as systems performing their functions in a fool-proof manner?

As socio-technological systems, CIs rely on a concept of rationality that is linked to technical and engineering expertise, with their characteristic action ideals (Delanty and Harris, 2021; Mitcham, 2015; see also Schön, 1983). As technical rationality aims to produce order and control capacity through data classification and calculation

[4] *Measuring the security of CIs is an extraordinary complex task. However, various measures for assessing it have been developed, such as approved CI protection plans, audit of CI protection status, structural and budgetary changes, and exercises (Piekarski and Wojtasik, 2022).*

(Gunderson *et al.*, 2018), the provision for security builds on the concepts of risks and threats identified from previous events, as well as their management mechanisms, criticality and vulnerability analysis, and scenario models, among others (Chen *et al.*, 2019; Reniers and Audenaert, 2014; Wang *et al.*, 2013; Zio, 2016). Technical rationality brings efficiency to interpreting reality and turning what has been learned from previous events into better capability. It seldom expresses its selectivity, but instead represents itself as the only reasonable indicator of reality and provider of solutions, as is typical for black boxes.

Technical rationality recognises errors and imperfection as part of activity, so errors made and deficiencies identified can be turned into an ability to close gaps in security, learn from failures and strengthen management capacity (Gómez, 2015). The internal logic of technical rationality determines what stands out as an error, an imperfect performance or a gap in security. The very idea that this logic could be defective or even harmful is absurd. It is impossible to scrutinise analytically within itself. Systems learn in a way that represents a stronger capacity to address an increasingly diverse range of security threats and an enhanced capability to manage them effectively. It builds trust in the capability of expertise to face uncertainty (Bieder, 2017; Runciman, 2006). In this way, technical rationality can ensure that the CIs are always the best possible ones considering the given situation, and that they are capable of evolving towards the next best possible condition.

Another key characteristic of technical rationality is its tendency to interpret reality as being composed of technical challenges calling for technical responses—since a black box is filled with technical content, engineering expertise represents the most advanced interpretation of the security of CIs (Gunderson *et al.*, 2018). It defines the most essential problems in the security environment, formulates them, and opens the vista to solutions deemed adequate, justified and sufficient (Hubbard, 2009). It is legitimised as the correct, commonly approved knowledge method (Aradau and van Munster 2011), which increases the distance between professionals and laypeople such as the ordinary users of infrastructure services, as it becomes increasingly sophisticated and strengthens its position (Gómez, 2015). Laypeople are expected to trust and believe that the security of the systems is in expert hands (Rodríguez, 2015).

However, it is worth asking whether these expert hands are tied to established habits of thinking (Aven and Guikema, 2011), and hence have become an instrument for solving the problems tailored to it more and more precisely and subtly. That is, on what basis can the capacity to design, operate and manage well-defined technical problems be extended to apply for providing for security to CIs on a larger scale? Such a question usually remains unasked, as the basic assumption regarding technical rationality standardises, moves aside from criticism, and thus allows argumentation and operation to be built on these assumptions (Mitcham, 2015). Paraphrasing Goldman (2018), it can be said that technical rationality gives an impression of the creation of security in a value-neutral, evidence-based manner, which is why it elicits trust and undermines sceptical arguments. However, why technical rationality is considered competent for determining the CIs' security environment, and what knowledge is being excluded or ignored by its interpretation framework, remains unexplored. Such taken-for-granted gaps provide for potential security hazards. Therefore, it is important to approach them as possible means and mediums intelligent terrorism could utilise by weaponising them.

Terrorism targeted at critical infrastructures

The unambiguous definition of the concept of terrorism has proved to be exceptionally challenging (Feyyaz, 2019), yet attempts to define it precisely may also have hampered

the grip of the phenomenon comprehensively (Ramsay, 2015). Despite the lack of consensus, the general features of terrorism include the desire to cause feelings of terror and insecurity through violence or the threat of violence within a group larger than the actual target of the very attacks (Horgan, 2005; Richards, 2014). According to Richards (2014), 'terrorism is best conceptualised as a particular method of political violence', which can be interpreted so that the very meaning of terrorism cannot be reduced to the immediate impacts of a limited attack, but the real impacts arise from the fundamental values, structures and assumptions terrorism threatens (e.g., Enders and Sandler, 2012). In other words, the core of the dynamics of terrorism consists of how terrorist activity is interpreted in the target society, and how these interpretations affect people's sense of security. By attacking a piece of critical infrastructure, as Bennett (2018) argues, terrorists may disrupt the standard of living and cause significant physical, psychological and financial damage. However, another question is how an attack would shake the joints of black boxes and undermine trust in CIs and their management in general.

Although CIs have been targets of terrorist attacks in recent history (on statistical analysis of this theme, see e.g. Miller, 2016), the extent to which they have succeeded in causing the long-term impacts in the larger scales is highly questionable (Abrahams and Gottfried, 2014; see also Muro, 2019). Roughly speaking, the CI systems have so far proved their ability to return to normal operation quickly after the attacks, and communities have regained their trust in the security of the systems. It seems that the attacks have generally failed to communicate in ways that would profoundly undermine people's trust in the technical systems and structures that underpin and maintain their daily lives. The acts have not disrupted the social fabric of societies by instilling distrust between people or caused them to question the basic assumptions on which everyday activities are built (Maras, 2013; see also Muro, 2019). In other words, people have sustained their sense that experts and administrations are capable of identifying and managing the respective threats as well as organising effective responses to attacks (cf., Van Der Does *et al.*, 2019). The knowledge strategy for maintaining the continuity and enhancing the security ex post facto of a CI has convinced the people of its capability and proven its reliability quite well (Hoffman and Shelby, 2017).

In the light of technical rationality, this would imply that even devastating terrorist attacks have been interpreted in the framework of the security of systems, and eventually, dissolved into black boxes' increased ability to recover from any incidents and to take necessary lessons from such experiences. It is possible to explain the attacks as external acts based on the sudden use of violence which, despite their unpredictability, have succeeded in remaining within the limits of security estimates, but which can be circumscribed even better in the future by learning from them. The acts are interpreted as having hit an area that can be explained in terms of limited resources, meaning that the identified gap can be closed through additional investments without the need for fundamental change in the scheme or its underpinning logic.

The acts have failed to put under question the form of expertise that provides for security and certainty and evolves around the related issues. Instead, the acts are grasped as isolated cases that mainly indicate the intellectual relevance and insufficient resources of the systems, but not fundamental deficiencies in the general framework. Thus accounted, terrorism operates appropriately for the technical rationality: although the attacks constitute a real, unpredictable and serious security threat in the short term, the longer-term capacity and reliability of CIs are not questioned. A terrorist attack comes as a surprise, reveals vulnerability, indicates a weak link and reveals the limitations of knowledge, but it

is eventually interpreted in a way that can be managed and effectively addressed by investing in stronger systems and broader up-to-date coverage.

Confidence in the logic of security creation is not undermined because the general framework appears fully capable in terms of making sense of attacks, providing for their prevention in the future, and thus not requiring deeper reflection or scrutiny. In other words, terrorist attacks fail to abuse the trust and confidence in the structures on which people rely (BaMaung *et al.*, 2018). However, the fact that the black boxes' internal logic has so far withstood them does not imply that it is free from vulnerabilities. To figure out the inherent vulnerability, it is necessary to delineate a trend in the development of terrorism that casts light on the need for alternative interpretation frameworks.

The potential next level of terrorism

In view of the above, one may ask, what forms of terrorism would call into question the framework utilised in making sense of terrorist acts? To begin with, it can be said that creating and maintaining trust and certainty—even their ability to be taken for granted and blackboxed—are at the core of the security and credibility of CIs. Undermining trust and certainty requires systematic abuse of the systems, a deliberate effort to change the operational logic of the system qualitatively. This would call for sustained action to integrate the threat into the very methods and means upon which the maintenance of security of operations have been established. Terrorism would sneak in through the very operating methods that are perceived as being critical, continuously updated, effective, benevolent, field-tested and confirmed apparatus for identifying and solving problems. Terrorism could infiltrate a black box, settle in its inner world, and exploit it for its own purposes.

Such terrorism would cause systemic damage to society by affecting the various stages of designing, building, operating and managing protected and sheltered CI systems. The consequences would not be limited to isolated shocks or cascaded disturbances. Instead, they would reveal an innate vulnerability in how CIs are becoming increasingly complex, more critical and hence more and more capable in causing harm (Hellström, 2007). This would question the assumptions about the method applied in the accumulation of knowledge, understanding and expertise on which the security of CI relies. Such an act would be reflected in the mechanisms through which people and societal functions have become and continuously are dependent on CI systems. Well-intentioned investments in system reliability would be questioned in a way that undermines the framework considered legitimate. It would destroy social trust by creating anticipatory fear about terrorism: As Godefroidt and Langer (2018) showed, fearing terrorism destroys social trust, and this threat of terrorism does not even have to be real.

Such terrorism targeted at CIs would be less about a new tool in the terrorists' toolbox, and more about a different logic of impact in which the vulnerability relates to intellectual foundations of certainty and security, not on the interruption or destruction of individual functions. When security and the ability to manage threats become thoroughly challenged, a shadow of doubt is also cast over systems operating with a similar logic. The essence and enormous size of black boxes would be revealed. It would be difficult for operators dependent on CIs to make informed decisions on the use of systems because the credibility of the information available would have been undermined. In this sense, the real impact of terrorism consists of the fact that the target group interprets the acts in ways that question the knowledge structure and the methods and means for strengthening it that have, in general, been sealed in a black box.

Conclusions

This paper discusses the contrast between the logic of providing for security and certainty for CIs and the intelligent development of terrorism as a major security threat to societies. The intellectual separation described above has weakened the possibilities for theoretically understanding and practically recognising terrorism as a phenomenon that is becoming systemically more conscious, more intelligent, and potentially increasingly capable in a form of violence that abuses the basic structures of societies and the related methods for knowledge production. The paper contributes to the research on terrorism by stressing the importance of profoundly critical tools that are often perceived as being undesirable or even counter-productive in figuring out the mechanism through the very means utilised in providing for security.

This article makes it clear that the threat of intelligent terrorism relates to perceptions of the capabilities in knowledge and control. Identifying threats, managing them and hardening the targets are essential functions that provide the desired certainty. Seeing the logic of producing certainty as blackboxing, this article shows how it can become a source of vulnerability and systematic blindness. Perhaps, therefore, the 'known' is less important than the means utilised in coming to know it. Perhaps the systems behind the identification of those who possess the very knowledge and the positions granted to them and the attached privileges in putting that knowledge into action deserve critical analysis. This paper concludes that the main practical challenge is to become aware of what threats are not being seen because of systematic blindfolds and blind spots. As can be seen, the formation of blind spots is linked to what is commonly seen as strength. However, threats beyond the field of vision will not cease to exist, even if the focus is increasingly on what is already in sight. The potential of the CIs' context to prepare for the coming of intelligent terrorism lies in this realisation. The ways by which terrorism can infiltrate into the black boxes and the ways in which preparedness can be developed accordingly are both interesting areas for further research.

Funding

This work was supported by the Academy of Finland under Grant 315074.

Data Availability Statement

Not applicable.

Disclosure statement

No potential conflict of interest was reported by the author. The author read and agreed to the published version of the manuscript.

References

Abrahams, M. and Gottfried, M.S. (2014) 'Does terrorism pay? An empirical analysis', *Terrorism and Political Violence*, 28, pp. 72–89. doi: 10.1080/09546553.2013.879057.

Aradau, C. (2010) 'Security that matters: critical infrastructure and objects of protection', *Security Dialogue*, 41, pp. 491–514. doi: 10.1177/0967010610382687.

Aradau, C. and van Munster, R. (2011) *Politics of catastrophe. Genealogies of the unknown*. Oxon: Routledge.

Aven, T. and Guikema, S. (2011) 'Whose uncertainty assessments (probability distributions) does a risk assessment report: the analysts' or the experts'?', *Reliability Engineering & System Safety*, 96, pp. 1257–1262. doi: 10.1016/j.ress.2011.05.001.

BaMaung, D., McIlhatton, D., MacDonald, M. and Beattie, R. (2018) 'The enemy within? The connection between insider threat and terrorism', *Studies in Conflict & Terrorism*, 41, pp. 133–150. doi: 10.1080/1057610X.2016.1249776.

Beck, U. (2002) 'The terrorist threat: world risk society revisited', *Theory, Culture and Society*, 19, pp. 39–55. doi: 10.1177/0263276402019004003.

Bennett, B.T. (2018) *Understanding, assessing and responding to terrorism: protecting critical infrastructure and personnel*. 2nd ed. Hoboken, NJ: Wiley.

Bieder, C. (2017) 'Conclusion', in G. Motet and C. Bieder (eds.), *The illusion of risk control: what does it take to live with uncertainty?* Cham: Springer, pp. 107–112.

Botha, A. (2020) 'Prevention of terrorist attacks on critical infrastructure', in A.P Schmid (ed.), *Handbook of terrorism prevention and preparedness*. The Hague: ICCT Press Publication, pp. 867–896.

Cedergren, A., Johansson, J. and Hassel, H. (2018) 'Challenges to critical infrastructure resilience in an institutionally fragmented setting', *Safety Science*, 110, pp. 51–58. doi: 10.1016/j.ssci.2017.12.025.

Chen, C., Reniers, G. and Khakzad, N. (2019) 'Integrating safety and security resources to protect chemical industrial parks from man-made domino effects: a dynamic graph approach', *Reliability Engineering & System Safety*, 191, 106470. doi: 10.1016/j.ress.2019.04.023.

Collier, S. and Lakoff, A. (2007) 'The vulnerability of vital systems: how "critical infrastructure" became a security problem', in M. Dunn and K.S. Kristensen (eds.), *Securing 'the homeland': critical infrastructure, risk, and (in)security*. Abingdon: Routledge, pp. 17–39.

Coward, M. (2009) 'Network-centric violence, critical infrastructure and the urbanization of security', *Security Dialogue*, 40, pp. 399–418. doi: 10.1177/0967010609342879.

Critical Five. (2014) *Forging a common understanding for critical infrastructure. Shared narrative*. Available at: https://www.cisa.gov/publication/critical-five-shared-narrative-2014 (Accessed: 10 June 2022).

Daase, C. and Kessler, O. (2007) 'Knowns and unknowns in the "war on terror": uncertainty and the political construction of danger', *Security Dialogue*, 38, pp. 411–434. doi: 10.1177/0967010607084994.

De Rosa, M. (2018) 'Land use and land-use changes in life cycle assessment: green modelling or black boxing?', *Ecological Economics*, 144, pp. 73–81. doi: 10.1016/j.ecolecon.2017.07.017.

Delanty, G. and Harris, N. (2021) 'Critical theory and the question of technology: the Frankfurt School revisited', *Thesis Eleven*, 166, pp. 88–108. doi: 10.1177/07255136211002055.

Enders, W. and Sandler, T. (2012) *The political economy of terrorism*. 2nd ed. Cambridge, MA: Cambridge University Press.

Feyyaz, M. (2019) 'Terrorism can and should be defined. But how?', *Strategic Analysis*, 43, pp. 310–327. doi: 10.1080/09700161.2019.1626581.

Gill, P., Horgan, J., Hunter, S.T. and Cushenbery, L.D. (2013) 'Malevolent creativity in terrorist organizations', *Journal of Creative Behavior*, 47, pp. 125–151. doi: 10.1002/jocb.28.

Godefroidt, A. and Langer, A. (2018) 'How fear drives us apart: explaining the relationship between terrorism and social trust', *Terrorism and Political Violence*, 32, pp. 1482–1505. doi: 10.1080/09546553.2018.1482829.

Goldman, S.L. (2018) 'Compromised exactness and the rationality of engineering', in C. García-Díaz and C. Olaya (eds.), *Social systems engineering: the design of complexity*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Gómez, A. (2015) 'Risk, uncertainty, and the dimensions of technological rationality', in W.J. Gonzalez (ed.), *New perspectives on technology, values, and ethics: theoretical and practical*. Cham: Springer, pp. 105–122.

Graham, S. (2005) 'Switching cities off', *City*, 9, pp. 169–194. doi: 10.1080/13604810500196956.

Graham, S. (2010) *Disrupted cities: when infrastructure fails*. New York, NY: Routledge.

Gunderson, R., Petersen, B. and Stuart, D. (2018) 'A critical examination of geoengineering: economic and technological rationality in social context', *Sustainability*, 10, p. 269. doi: 10.3390/su10010269.

Hausken, K. (2017) 'Special versus general protection and attack of parallel and series components', *Reliability Engineering & System Safety*, 165, pp. 239–256. doi: 10.1016/j.ress.2017.03.027.

Hellström, T. (2007) 'Critical infrastructure and systemic vulnerability: towards a planning framework', *Safety Science*, 45, pp. 415–430. doi: 10.1016/j.ssci.2006.07.007.

Hempel, L., Kraff, B.D. and Pelzer, R. (2018) 'Dynamic interdependencies: problematising criticality assessment in the light of cascading effects', *International Journal of Disaster Risk Reduction*, 30, pp. 257–268. doi: 10.1016/j.ijdrr.2018.04.011.

Hoffman, A.M. and Shelby, W. (2017) 'When the "laws of fear" do not apply: effective counterterrorism and the sense of security from terrorism', *Political Research Quarterly*, 70, pp. 618–631. doi: 10.1177/1065912917709354.

Horgan, J. (2005) *The psychology of terrorism*. London: Routledge.

Hubbard, G.W. (2009) *The failure of risk management: why it's broken and how to fix it*. Hoboken, New Jersey: John Wiley & Sons, Inc.

Kahan, J. (2017) 'Critical infrastructure protection: can we defend against terrorism?', *Homeland Security Affairs*, 13, pp. 1–41.

Latour, B. (1999) *Pandora's hope. Essays on the reality of science studies*. Cambridge, MA: Harvard University Press.

Latour, B. (1994) 'On technical mediation: philosophy, sociology, genealogy', *Common Knowledge*, 3, pp. 29–64.

Latour, B. (1987) *Science in action: how to follow scientists and engineers through society*. Cambridge, MA: Harvard University Press.

Logan, M.K., Ligon, G.S. and Derrick, D. (2019) 'Measuring tactical innovation in terrorist attacks', *Journal of Creative Behavior*, 54, pp. 926–939. doi: 10.1002/jocb.420.

Maras, M.-H. (2013) 'Risk perception, fear, and its consequences following the 2004 Madrid and 2005 London bombings', in S.J. Sinclair and D. Antonius (eds.), *The political psychology of terrorism fears*. New York, NY: Oxford University Press, pp. 227–245.

Miller, E. (2016) *Terrorist attacks targeting critical infrastructure in the United States, 1970–2015*. College Park, MD: START.

Mitcham, C. (2015) 'Rationality in technology and in ethics', in W.J. Gonzalez (ed.), *New perspectives on technology, values, and ethics: theoretical and practical*. Cham: Springer, pp. 63–88.

Moore, S.A., Torrado, M. and Joslin, N. (2019) 'Knowledge production for interdependent critical infrastructures: constructing context-rich relationships across ecosociotechnical boundaries', *Environmental Science & Policy*, 99, pp. 97–104. doi: 10.1016/j.envsci.2019.05.018.

Muro, D. (ed.) (2019) *When does terrorism work?* London: Routledge.

Peerenboom, J.P. and Fisher, R.E. (2010) 'System and sector interdependencies: an overview', in J.G. Voeller (ed.), *Wiley handbook of science and technology for homeland security*. Hoboken, New Jersey: John Wiley & Sons, Inc, pp. 1161–1171.

Piekarski, M. and Wojtasik, K. (2022) 'Protection of polish critical infrastructure (CI) against air threats', *Security and Defence Quarterly*, 39, pp. 1–12. doi: 10.35467/sdq/14767.

Quijano, E., Insua, D.R. and Cano, J. (2018) 'Critical networked infrastructure protection from adversaries', *Reliability Engineering & System Safety*, 179, pp. 27–36. doi: 10.1016/j.ress.2016.10.015.

Ramsay, G. (2015) 'Why terrorism can, but should not be defined', *Critical Studies on Terrorism*, 8, pp. 211–228. doi: 10.1080/17539153.2014.988452.

Ranstorp, M. and Normark, M. (2009) 'Detecting CBRN terrorism signatures – challenges and new approaches', in M. Ranstorp and M. Normark (eds.), *Unconventional weapons and international terrorism. Challenges and new approaches*. New York, NY: Routledge, pp. 1–10.

Reniers, G.L.L. and Audenaert, A. (2014) 'Preparing for major terrorist attacks against chemical clusters: intelligently planning protection measures w.r.t. domino effects', *Process Safety and Environmental Protection*, 92, pp. 583–589. doi: 10.1016/j.psep.2013.04.002.

Richards, A. (2014) 'Conceptualizing terrorism', *Studies in Conflict & Terrorism*, 37, pp. 213–236. doi: 10.1080/1057610X.2014.872023.

Rodríguez, H. (2015) 'Risk and trust in institutions that regulate strategic technological innovations: challenges for a socially legitimate risk analysis', in W.J. Gonzalez (ed.), *New perspectives on technology, values, and ethics: theoretical and practical*. Cham: Springer, pp. 147–166.

Runciman, D. (2006) *The politics of good intentions. History, fear and hypocrisy in the new world order*. Princeton, NJ: Princeton University Press.

Rydin, Y., Natarajan, L., Lee, M. and Lock, S. (2018) 'Black-boxing the evidence: planning regulation and major renewable energy infrastructure projects in England and Wales', *Planning Theory & Practice*, 19, pp. 218–234. doi: 10.1080/14649357.2018.1456080.

Schön, D. (1983) *The reflective practitioner: how professionals think in action*. London: Temple Smith.

Shindell, M. (2020) 'Outlining the black box: an introduction to four papers', *Science, Technology, & Human Values*, 45, pp. 567–574. doi: 10.1177/0162243919883414.

The 9/11 Commission Report. (2004) *Final report of the national commission on terrorist attacks upon the United States*. Available at: https://www.govinfo.gov/app/details/GPO-911REPORT (Accessed: 1 September 2021).

Van Der Does, R., Kantorowicz, J., Kuipers, S. and Liem, M. (2019) 'Does terrorism dominate citizens' hearts or minds? The relationship between fear of terrorism and trust in government', *Terrorism and Political Violence*, 33, pp. 1276–1294. doi: 10.1080/09546553.2019.1608951.

Wang, S., Hong, L., Ouyang, M., Zhang, J. and Chen, X. (2013) 'Vulnerability analysis of interdependent infrastructure systems under edge attack strategies', *Safety Science*, 51, pp. 328–337. doi: 10.1016/j.ssci.2012.07.003.

Wiśniewski, M. (2016) 'Concept of situational management of safety critical infrastructure of state', *Foundations of Management*, 8, pp. 297–310. doi: 10.1515/fman-2016-0023.

Żaboklicka, E. (2020) 'Critical infrastructure in the shaping of national security', *Security and Defence Quarterly*, 28(1), pp. 70–81. doi: 10.35467/sdq/118585.

Zio, E. (2016) 'Critical infrastructures vulnerability and risk analysis', *European Journal for Security Research*, 1, pp. 97–114. doi: 10.1007/s41125-016-0004-2.