Unmasking the Subconscious Fallacies Within Critical Infrastructure Protection

Marion Stephens
American Public University, Charles Town, WV, United States of America

marion.stephens@mycampus.apus.edu

Abstract: Cybersecurity, a vital challenge in today's ever-changing digital world, it has gained prominence with the global shift towards cyber-enabled critical infrastructures. Critical infrastructure protection efforts are fundamental for the continuation of essential services. Traditionally constituted as separate sectors, these infrastructures are increasingly interconnected, leading to potential domino effects during security breaches. For instance, failures within the power grid could have cascading effects on multiple sectors that depend on electricity for their operations, creating large-scale failures that affect functions on which society depends. The multidimensional nature of the infrastructures presents complex challenges for solutions, given their status as long-established legacy systems needing further development and enhancements to withstand the digital world. The lack of a concerted and focused infrastructure enhancement strategy has led to incremental approaches versus a comprehensive revamp to ensure a holistic cyber protection program. A lack of national focus has created inconsistencies that can lead to potentially catastrophic consequences. Understanding the decision-making processes within a complex environment is critical to the mission success. One significant risk is the cognitive roadblocks that have the potential to influence one's judgements as this often outweighs balanced decisions. This study aims to investigate the subconscious biases that arise from a perceived resolution of the problem which can lead to de-prioritization within the decision-making processes. The study employs a convergent parallel mixed methods design to collect and analyse the data. The study then will compare the results allowing for the exploration of various aspects of the research. This approach is aligned to provide a thorough understanding of the challenges associated with protecting the infrastructures and the underlying subconscious fallacies in the digital age, thereby devising effective mitigation strategies, and fostering a more sustainable and resilient critical infrastructure that is useful for a variety of stakeholders, including policymakers, infrastructure owners and operators, cybersecurity professionals, and researchers.

Keywords: Cybersecurity, Critical Infrastructure, Decision-Making, De-prioritization, Subconscious Bias, and Mitigation Strategies

1. Introduction

In the intricate web of modern society, there exist certain threads stronger and more vital than others. These threads are the underlying critical infrastructures that are universally recognized as systems or assets that are indispensable to the functioning of today's societies. However, the specifics of these infrastructures can vary based on each nation's unique needs and perceptions (De Felice et al, 2022). These requirements are governed by what each nation identifies as the fundamental pillars of its social functions. The designation of 'critical' for infrastructure is derived from its impact on the safety, health, and economic well-being of a nation (Mussington, 2021). The interconnected critical infrastructures form the backbone of a functioning society, providing essential services that society has become dependent upon. Given this dependency, it becomes evident that this emphasizes the importance of safeguarding the critical infrastructures. However, the condition of the critical infrastructure is deteriorating across the globe due to factors such as aging, environmental impacts, lack of adequate maintenance, budget constraints, limitations to legacy systems, and an inability to keep up with technological advancements (Zahidi, 2023). In addition to these ongoing challenges, the systems also face heightened risks from natural disasters to cyber-attacks. It is critical to ensure the nation's security and resilience against potential threats. In today's interconnected digital age, these critical infrastructures are not always isolated within national boundaries. They often have global implications. They are intertwined to such an extent that a threat to one can potentially trigger a domino effect of disruptions across multiple infrastructures (De Felice et al, 2022). Despite the variations in the definitions of critical infrastructures across different nations, there is a universal need to safeguard all critical infrastructures. Given the global interconnectedness, this is to prevent any debilitating impacts that could compromise not just a single nation's functioning, but potentially have far-reaching effects on a global scale. A single misguided decision could potentially trigger cascading failures, posing threats from national security to loss of life. The protection of critical infrastructures is thus not just a national concern, but a global one, emphasizing the shared responsibility of all nations in safeguarding the security and resilience of modern society's lifeline.

2. Methodology

This study employed a convergent parallel mixed methods design approach to allow simultaneous collection of qualitative and quantitative data to enhance the understanding of the research problem. The empirical data, constituting as the foundation of the study, was obtained through surveys, focus groups, and observation to generate a comprehensive dataset. The data analysis was conducted through rigorous methodologies such as meta-analysis for quantitative data and thematic analysis for qualitative data, supporting the validity and reliability of the results. Descriptive and inferential statistics were used to interpret the quantitative data, while themes and patterns were identified in the qualitative data. These results were then used to produce the mitigations within this study.

3. Challenges Protecting the Critical Infrastructures

Critical infrastructures are vital to a fully functioning society and economy. Protecting them requires a comprehensive understanding of potential threats, vulnerabilities, and impacts. As the world collaborates to protect the critical infrastructures, various reports have identified national emerging threats and high-risk factors. The Executive Opinion Survey (EOS) by the World Economic Forum (2023) surveyed 121 economies to identify the top emerging risks to critical infrastructures. The most significant potential impacts were identified as the energy supply crisis, cost-of-living crisis, rising inflation, food supply crisis, and cyberattacks (World Economic Forum 2023). However, some risks may not be immediately apparent. KPGM International (2023) adds additional insight into the risks of territorialism, digital transformation, and supply chain disruptions. Upon reflection of recent developments, it becomes evident that the spectrum of risks has broadened. For instance, the 2024 Global Risks Report highlighted the increasing concern over environmental risks due to the more recent extreme weather changes (World Economic Forum 2024). In today's digital world, the threat of cyberattacks is escalating. While certain attacks can be predicted and defended against, others, such as zero-day attacks, necessitate a comprehensive set of protective measures and a robust emergency plan to ensure resilience. The Homeland Threat Assessment by the United States Homeland Security (2024) predicts that both domestic and foreign adversaries will likely target critical infrastructures in the coming year. The resilience of these aging systems is a matter of concern, especially with the increasing focus on the critical infrastructures. A Gartner survey indicated a 38% increase in funds allocated for operational technology protection for critical infrastructures in 2022, with an expected annual increment of 5% (Moore 2021). However, even with this increased investment, the survey also predicted that by 2025, around 30% of critical infrastructures worldwide will have fallen victim to successful cyber breaches (Moore 2021). Analysis suggests that the existing strategies are inadequate to meet the requirements and overcome the challenges posed by the digital era. These figures consider over 14,000 infrastructure projects worldwide, costing more than $14.8 trillion USD (Global Data, 2023). Thus, adding budgetary constraints as another layer of risk. Moreover, Raina (2023) highlights the global shortage of skilled cyber professionals mixed with high rates of employee attrition as another threat to businesses which then adds another layer to the risks. It is estimated globally by 93% of cyber professionals and 86% of business leaders that a catastrophic cyberattack will occur within the next couple of years that will cause global geopolitical instability (Raina 2023). Given these threats, it becomes crucial for the decision-making process to have a comprehensive understanding of the issues at hand. This 360-degree view is essential for making better-informed decisions.

4. Decision Making

Effective decision-making plays a pivotal role in managing risks associated with cybersecurity, a field marked by its complexity and need for specialized knowledge. However, not all decision-makers possess cyber expertise, leading them to rely on simplified explanations or visible security indicators. These indicators are tangible, measurable aspects of a system's security that can be easily understood and monitored such as, the frequency of security patches applied or the status of networked devices. Yet, the simplicity of these metrics does not show the full complexity of the situation. These tendencies, as noted by Villadiego (2020), leads to a preference for more conspicuous solutions, which are typically influenced by the rapid pace of technological change, communication gaps, resource constraints, and the pressure for immediate results. Collectively, these factors shape the decision-making process in cybersecurity. To delve deeper into these factors, it is important to note that the constant evolution of cybersecurity—with new threats and solutions emerging regularly—poses significant challenges for decision-makers occupied with multiple responsibilities. Villadiego (2020) provides further insight into the challenges that decision-makers face due to their lack of cyber expertise by explaining how technical experts, with their deep understanding of the field, often face challenges in conveying complex

cybersecurity issues in a manner that decision-makers, who may lack such specialized knowledge, can understand and act upon. This gap can lead to misinterpretations and potentially flawed decision-making. Moreover, implementing a comprehensive approach to cybersecurity can be resource intensive. Decision-makers are tasked with balancing cybersecurity needs with other organizational priorities, which may lead them to opt for less comprehensive, but also less resource-intensive solutions. These solutions often yield immediate, tangible results, making them appear "shiny" or noticeable. In contrast, a holistic approach to cybersecurity is a long-term investment that may not produce immediate visible results, as highlighted by Villadiego (2020).

5. The Subconscious Fallacies

Though it is important to note the reasoning behind every decision, the implementation of decisions is influenced by a myriad of factors, not all of which are easily discernible. To further analyse decision making one must address the psychological aspects of cognitive obstacles. According to cognitive theory, an individual's actions and decisions are influenced by their personality, environment, and thought processes (Erisen 2012). In essence, factors ranging from one's upbringing and accumulated experiences to their present circumstances influence their decision-making. Erisen (2012) further explains that these cognitive biases can lead to a form of heuristics, as shortcuts remain a consistent variable recurring within the decision-making process. This notion corroborates Freud's (1915) theory that human behaviour stems from the unconscious level within the mind. Even though some decisions appear to be well thought out this entails that there can be a biased judgment behind the decision, often unbeknownst to the decision-maker. Within the necessity of the decision processes exists a form of heuristics that often leads to a type of hyper fixation on achieving a goal, and rarely encompasses all potential outcomes causing de-prioritization (Gowda, 1999). In terms of critical infrastructures, this can lead to a subconscious bias that overemphasizes on physical security aspects. These biases can then potentially divert the decision-maker from making a logical choice considering all aspects of the problem. Utilizing cognitive theory allows for an analysis of each subject to understand the individual and the logic behind their decision-making process.

Personality significantly influences decision-making. While there are several frameworks to assess personalities one approach outlines that personality is comprised of six basic needs: certainty/comfort, variety, significance, connection, growth, and contribution (Ciccotti 2014). Certainty and comfort equate to security, variety is the necessary change needed so one does not become stagnate, significance is an actionable result the person requires, a connection is a sense of love, growth is a sense of maturing and expanding, and contribution is an effort that one is putting forth (Ciccotti 2014). These needs intertwine with personal biases and beliefs, which are ingrained as we grow and shape our reactions. Assumptions gathered during this process account for the normalcies within the era and environment. From the point humans are born, information is absorbed, establishing precedents for everything else in their life as biases develop and they independently condition to react in set patterns and mindsets. Schoen (2007) categorizes personality into five traits: neuroticism, extroversion, openness, conscientiousness, and agreeableness. As each person is individually different with a degree of like-mindedness then it is understood that this is true within the personality formed as each trait is varying by a spectrum where the individual would fall into a category. This spectrum within the big five personality traits then falls into the following: in neuroticism, which varies by controlling negative emotions, extraversion is a scale of socialness, openness varies by spontaneous pursuits, conscientiousness is self-disciplined, and agreeableness is trusting (Schoen 2007). Depending on which is the highest driving force of the personality would then depend on the categorization of the individual. This is where predictive behavioural analysis begins as it delves into the inner workings of the personality for then one can work to achieve a greater understanding of the reasoning within the decision formed (Erisen 2012). All decisions involve a choice. This is often based on Maslow's hierarchy of needs: physical needs, safety, love/belonging, self-esteem, and self-actualization (Davies 1963). On the basis of the basic human needs, one develops a type of necessity they want to achieve. By fulfilling these needs, consciously or subconsciously, individuals exert control over their feelings and actions, as explained by the Glasser Institute for Choice Theory (N.D.). In essence, humans exercise autonomy over their influences, making choices based on a complex interplay of personality traits, cognitive biases, and basic needs. Glasser Institute for Choice Theory (N.D.) explains that behaviour consists of feeling, acting, physiology, and thinking and by understanding the control within behaviours one can develop more of a rational mindset versus overreacting. Again, this falls in line with Mercer's (2005) theory that logical decisions are based on a form of emotion. This also gives the rationale that the individual can become empowered by realizing they do not have responsibility for other choices, just their own. However, whatever the choice Winter (2005) explains that the motive is based on one of three choices, achievement, affiliation, or power.

While the theories of Glasser, Mercer, and Winter provide valuable insights into individual behaviour and decision-making based on emotions, achievement, affiliation, or power. However, it is important to consider these concepts in a broader context. As Rathbun (2009) suggests, the principle of realism is more relevant when the shift focuses on the state and international levels of analysis that has a pessimistic overview that leads to the primary concern of survival within the state on the basis of lack of trust or a strategic trust with the international relations. This perspective then emphasizes the imperative demand needed for the critical infrastructures to maintain a higher standard of reliability and security. At this level, the decision-making process considers key factors to the interconnectedness of the infrastructures, shared information and resources, potential threats, and global operations. Emotions, such as fear, could prompt the decision-maker to bolster security measures within their process, while simultaneously managing budgetary needs. Concurrently, one should bear in mind that security, akin to a picture, possesses multiple dimensions. In today's ever-changing environment, the heightened threat of a cyber-attack deepens the need for additional, yet-to-be-conceived strategies for cyber protection. This underscores the idea that unseen threats are still very real and must be accounted for in our security planning.

Transitioning from the discussion of security threats and the need for innovative strategies, another perspective to explore is liberalism. This school of thought offers a more optimistic viewpoint, advocating for a higher degree of trust (Rathbun, 2009). To understand how this concept fits into the decision-making process of critical infrastructures, one can draw parallels with the three levels of analysis in political psychology - individual, state, and international (Jervis, 1976). As each level is subject to the principle of bias, which can influence the decision-making process, the resulting analysis could provide the means to integrate the economic and social considerations into the decision-making process. Building onto this, it is important to note that one's approach can be influenced by both realism and liberalism, depending on the situation. For example, a person who typically leans towards realism might choose to operate based on trust when interacting with someone they feel a strong connection to. Within the context of critical infrastructures, decisions hinge more on overarching personality traits, as these processes frequently prioritize objects. These objects, in turn, impact the individual and serve as a motivational determinant. Nevertheless, is it of importance to state that if the threat is not immediately visible or one does not understand the full spectrum of the threat then this can incur a subconscious bias that leads to a lack of prioritization within the decision-making process. In any decision-making process, leadership is often perceived as the driving force to the most logical decisions (McDermott 2004). Within rational theory, the foundations of any decision are fundamentally based on logic. However, it was Mercer (2005) who established the general concept detailing the generation of logical decisions, suggesting these decisions are formed on top of an emotional response even if at a subconscious level. This idea gains further traction as McDermott (2004) rationalizes that thoughts and beliefs add crucial layers to the decision-making process. This method would be inherent to the decisions based on supply, price, and distribution of which could expand to a final decision built on realism.

While decisions are often tethered to sturdy foundations within the realm of logic and time-honoured principles, the incorporation of the human condition undermines their position with underlying bias (Nielson and Minda 2019). These biases, a natural flaw that intensifies as individuals mature and learn from past experiences, can influence future actions and shape behavioural patterns. These patterns can be a stem from both external influences like digitization and personal experiences like perception (Acciarini et al, 2020). The complexity of decision-making processes relies on roles with both conscious and unconscious thought. Newell and Shanks (2014) explain that judgment for decisions comes from multiple cues, deliberation without attention, and decisions relying on assumptions versus a type of certainty. As the human condition is in opposition to the innate significance of the decisions being selected, each component must be revised and calculated. Analysis suggests that this extra layer of protection would benefit the cyber realm as the act would retrace the decision process and generate a barrier in opposition to blatantly biased suggestions. These considerations must be held with multiple perspectives in mind, allowing the decision-makers to select the most profitable method. It could be theorized that cognitive bias leads to a form of prioritization, although it may not always be suited to deal with the present situation. An analysis might suggest that past events are considered preliminarily in response to the emergence of new threats in a modern era, providing clarity in unfamiliar situations. As the world evolves and unseen threats emerge, this issue may be predisposed based on the assumption that events and threats are judged by their past success. This theory could be further substantiated within the boundaries of positive and negative feedback, extending to the validation that behaviour becomes negotiated (Smith and Postmes 2011). In relation to visible outcomes, actions may be taken more swiftly to achieve immediate gratification. This holds true even for tasks that require more patience, emphasizing the propensity for immediate action. While this could pertain to a task that requires a touch more patience, this still yields true for immediate action. Individuals

are far less likely to act when placed within unfavourable conditions and will typically wait until an opportunity presents itself (Smith and Postmes 2011). This behaviour is predominant when information is partially obscured, and the potential threat is not immediately recognized. In this case, sight does not serve as the most effective identifier of information and should, therefore, be excluded from the conclusion.

6. Recommendations for Effective Mitigation

Effective mitigation in the critical infrastructure decision-making process requires a comprehensive strategy. There are various laws, defense-in-depth processes, and regular discussions to create protective measures, all appearing exemplary on paper, but that does not certify their significance in practice as learned from the analysis of the World Economic Forum (2024). Like in chess, where subtle moves can provide a powerful advantage, professional decisions require strategic thinking. Cyber initiatives tend to focus on hardening the infrastructure and security but often neglect the rationale behind decision-making processes Villadiego's (2020) insights, highlights the need to understand decision-making mindsets beyond defense and consider offensive measures. Until this is addressed, offensive measures will remain weak in practice despite appearing strong on paper. To make better, more informed decisions, it is essential to adopt a 360-degree view, considering various perspectives and evaluating potential solutions and their consequences. The demand for updating critical infrastructures and implementing additional protection measures to be implemented is unambiguous, highlighting the need for adaptability. To address these challenges, analysis suggests organizations should prioritize cybersecurity education for decision-makers and promote effective communication between technical experts and leadership. This point is derived from Raina's (2023) work, which highlights the shortage of skilled cyber professionals and high rates of employee attrition. Furthermore, decision-makers should be encouraged to adopt a long-term perspective on cybersecurity, acknowledging that a comprehensive approach can offer more robust protection against threats. Additionally noting that risk assessments are vital, requiring decision-makers to identify potential risks, emphasized by Mussington (2021). This involves fully understanding the nature of the threat, the vulnerability of the infrastructure to the threat, and the potential impact if the threat is realized. This is where the role of heuristics in decision-making and the need for a comprehensive view of decision-making should be acknowledged. While security is important, an overemphasis on it can lead to other aspects being neglected.

As the critical infrastructures span various domains and organizations, developing partnerships with private sectors can enhance efficiency, highlighted by KPGM International (2023). However, the gap between the theoretical strategies and their practical execution requires further discussion. This gap, or discrepancy, can be addressed by continuously monitoring and adjusting strategies based on practical experiences, promoting effective communication between different stakeholders, and fostering a culture of learning and adaptability. Enabling cybersecurity education for decision-makers can foster effective communication between technical experts and leadership. It is important to bridge the gap between technical experts who understand the nuances of the threats and decision-makers who determine the strategic response derived from Riana (2023). Bridging this gap ensures that decisions are informed by both theoretical knowledge and practical insights. Effectively communicating between multiple sectors can lead to efficiency and promote a mutual understanding between these two groups is essential for making informed and effective decisions in cybersecurity.

As these challenges are lessened by interdisciplinary collaboration. This collaborative practice brings together diverse perspectives and skill sets, providing a more comprehensive understanding of the situation and potential threats. Interdisciplinary collaboration is key, evolving into a bipartisan effort that delivers a unified message to all, from lawmakers to the general public advocated by Rathburn (2009). The duality of infrastructures ensures the consideration and cooperation of previously independent entities which could otherwise omit practices resulting in a negative impact on the now opposing counterpart. The key to an enhanced system that can outperform the current infrastructure array is to discover benefits within the public opinion, especially from those who have developed specialized skills within the respective fields necessary to maintain infrastructure. Construction workers pouring the concrete extending to the leaders who make the decisions would incorporate varying skill sets, perspectives, and influences which could better perpetuate an open forum type of conference, the message is well developed and supported. This type of decision would fall under the constructivism theory as it requires a form of knowledge gained and insight learned emphasized by Rathbun (2009). This would contrast with the current standing where a closed conference is held by the few for the many. Instead using constructivism theory there exists a role of learners from where the knowledge of each process is gained and the learning is an active process, that is both contextual and plays a role within the community of users observed by Rathbun (2009). Some examples of this include teams of construction workers that add the structure or

physical outreach to the critical infrastructures, the workers on ladders and in trenches spreading communication across the country, and even the teams in offices that demonstrate bureaucratic decision-making processes to ensure the safety of these communicational standards. Each member of each team implements specialized skills to create infrastructures. Together they provide a greater form of trust and communication incorporating a 360 view of the process.

7. Conclusion

While several studies on critical infrastructures focus on making the infrastructure being more sustainable and resilient by security measures, it is the mindset that drives the processes for achieving the innovations necessary to safeguard the critical infrastructures. Despite being meticulously designed, these powerful structures designed with great care from the ground up, have long since been established as obsolete, requiring further development and refinement to compete with the modern era. At the same time, it is the comprehension of such requirements that are not fully understood to properly mitigate the situation (Villadiego 2020). With the lack of awareness, the complexity of the situation, having other priorities, and even matters of cost considerations the decisions can overlook the issues. This situation can give rise to a phenomenon known as 'out of sight, out of mind,' where problems are disregarded because they are not immediately visible or causing pressing issues (Smith and Postumes 2011). It is human nature that is created via precedent, every decision, outcome, and outlier presented in life generating a mentality that guides not only the traditional thought processes that guide any coming decisions but also the outlook on life which generates biases and establishes powerful direction, such as a moral compass. While decision-makers are often entrusted with valuable information to determine pivotal actions, bias, and the human condition are inevitability something that cannot be easily avoided. Even when overcoming the bias for logical decisions, there is still the basis in emotional fundamentals, the human nature, that limits a single person to the quality of performance required in such a strategic decision (Mercer 2005). This mistaken belief in the effectiveness of independent decision-making is challenged when viewed within a team-based framework. In such a framework, a team, composed of different individuals selected independently from the previous panel each time, can offer a variety of perspectives towards each goal. This diversity of viewpoints can enhance the decision-making process, highlighting the limitations of relying solely on one individual's judgment. With a degree of randomization, the conflict of group mentality is minimized, while logic and perspective are quickly held at the forefront of the decision. This panel would provide the consideration and influence of numerous personalities while allowing for the consideration of realism, liberalism, and rational theory to meld in a culmination of logical decisions. This approach exemplifies the application of cognitive biases in decision-making for critical infrastructures.

References

Acciarini, Acciarini, C., Brunetta, F., and Boccardelli, P. (2020) "Cognitive biases and decision-making strategies in times of change: a systematic literature review", Management Decision, Vol 9, No. 4, pp 66–75. ISSN: 0025-1747.

Ciccotti, K. (2014) "The human factor in project management", PMI® Global Congress: Project Management Institute, Available online at: https://www.pmi.org/learning/library/human-factor-project-management-9276.

Davies, J.C. (1963) "You Can't Change Human Nature", John Wiley & Sons Inc, Hoboken, NJ., pp 1-30, Available online at: Doi: HTTP://dx.doi.org.ezproxy2.apus.edu/10.1037/14301-00.

De Felice, F., Baffo, I., and Petrillo, A. (2022) "Critical Infrastructures Overview: Past, Present and Future", Sustainability, Vol 14, No. 4, pp 11-13.

Erisen, E. (2012) "An Introduction to Political Psychology for International Relations Scholars", Perceptions, Vol. 17, No. 3, pp 9-28, Available online at: https://search-proquest-com.ezproxy2.apus.edu/scholarly-journals/introduction-political-psychology-international/docview/1196589032/se-2?accountid=8289.

Freud, S. (1915) "The unconscious", SE, Vol 14, pp 159-204. Available online at: http://dravni.co.il/wp-content/uploads/2014/01/Freud-S.-1915.-The-Unconscious.-.pdf.

Glasser Institute for Choice Theory (N.D.) "What is Choice Theory?" Glasser Institute for Choice Theory, Available online at: https://wglasser.com/what-is-choice-theory/.

Global Data. (2023) "Global Infrastructure Outlook to 2023" Global Data. Available online at: https://www.globaldata.com/store/report/global-infrastructure-outlook-to-2023/.

Gowda, R.M.V. (1999) "Heuristics, Biases, and the Regulation of Risk", Policy Sciences, Vol 32, No. 1, pp 59–78.

Jervis, R. (1976) "Perception and Misperception in International Relations", Princeton University Press.

KPGM International. (2023) "Emerging Trends in Infrastructure", KPGM International. Available online at https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2023/01/emerging-trends-in-infrastructure.pdf.

McDermott, R. (2004) "The Feeling of Rationality: The Meaning of Neuroscientific Advances for Political Science", Political Psychology Vol. 2 No. 4.

Mercer, J. (2005) "Rationality and Psychology in International Politics", International Organization, Vol 59, No. 1, pp 77-106.

Moore, S. (2021) “Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025”, Gartner, Available online at: https://www.gartner.com/en/newsroom/press-releases/2021-12-2-gartner-predicts-30–of-critical-infrastructure-organi.

Mussington, D. (2021) “Securing the Critical National Infrastructure” in Paul Cornish (ed.), The Oxford Handbook of Cyber Security, Oxford Handbooks (2021; online edn, Oxford Academic) Chapter 26, pp 429-446. Available online at: https://doi.org/10.1093/oxfordhb/9780198800682.013.26.

Nielsen, E.G., and Minda, J.P. (2019) “Problem Solving and Decision Making”, Psychology, DOI: 10.1093/OBO/9780199828340-0246.

Newell, B. and Shanks, D. (2014) “Unconscious influences on decision making: A critical review,” Behavioral and Brain Sciences, Cambridge University Press, Vol 37, No. 1, pp. 1–19. doi: 10.1017/S0140525X12003214.

Rathbun, B.C. (2009) “It Takes all Types: Social Psychology, Trust, and the International Relations Paradigm in our Minds: A Journal of International Politics, Law and Philosophy”, International Theory 1 Vol 3, No. 11, pp. 345-380 Available online at: https://search-proquest-com.ezproxy2.apus.edu/scholarly-journals/takes-all-types-social-psychology-trust/docview/217957605/se-2?accountid=8289.

Schoen, H. (2007) “Personality Traits and Foreign Policy Attitudes in German Public Opinion”, The Journal of Conflict Resolution Vol. 51, No. 3, pp. 408-430.

Smith, L.G.E., and Postmes, T. (2011) “The Power of Talk: Developing Discriminatory Group Norms through Discussion”, British Journal of Social Psychology Vol. 50 No.2, pp. 193–215 doi:10.1348/014466610X504805.

United States Department of Homeland Security (2024) “Homeland Threat Assessment”, Office of Intelligence and Analysis, Available online at: https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf.

Villadiego, R. (2020) “Decision Making in Cybersecurity”, Lumu Technologies, Available online at https://lumu.io/wp-content/uploads/2020/10/en_wp_decision-making-in-cybersecurity.pdf.

Winter, D.G. (2005) “Measuring the Motive of Political Actors at a Distance”, Psychological Assessment of Political Leaders pp. 153-177. Edited by Jerrold Post. Ann Arbor: University of Michigan Press.

World Economic Forum (2023) “Global Risks Report 2023”, World Economic Forum, 18th Edition, ISBN-13: 978-2-940631-36-0, Available online at: https://www.weforum.org/publications/global-risks-report-2023/.

World Economic Forum (2024) “Global Risks Report 2024”, World Economic Forum, 19th Edition, ISBN- 978-2-940631-64-3, Available online at: https://www.weforum.org/publications/global-risks-report-2024/digest/.

Zahidi, S. (2023) “Global Risks Report 2023”, World Economic Forum, 18th Edition, Available online at: https://www.weforum.org/publications/global-risks-report-2023504805