Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
©2025 ESREL SRA-E 2025 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P6228-cd

Reviewing Game Theory and Risk and Reliability in Infrastructures and Networks

Kjell Hausken

Faculty of Science and Technology, University of Stavanger, Norway. E-mail: kjell.hausken@uis.no

Jonathan W. Welburn

Pardee RAND Graduate School, USA. E-mail: jwelburn@rand.org

Jun Zhuang

Department of Industrial and Systems Engineering, University of Buffalo, USA. E-mail: jzhuang@buffalo.edu

Abstract
Game theory and risk and reliability analysis are reviewed in the context of infrastructures and networks. Players maximize utilities in static or repeated games, determining equilibria or min-max solutions under complete or incomplete information. This review examines attacker-defender dynamics, resource allocation, and network interdependencies. It identifies gaps in earlier reviews, which insufficiently focused on risk analysis within infrastructure systems. The study synthesizes methodologies, highlighting game-theoretic advancements in defense strategies, system survivability, and network resilience. It further evaluates interdiction strategies in power grids and transportation networks, outlining future research needs.

Keywords: Game theory, risk analysis, reliability, infrastructure protection, infrastructure, network.

1 Introduction

Risk analysis and strategic decision-making have long shaped infrastructure security. Early risk considerations can be traced back to hunter-gatherer societies assessing predatory threats. Deisler and Schwing (2000) describe how Phoenician shipowners pooled insurance against maritime risks as early as 1500 BC, an early form of collective risk management.

Modern risk analysis integrates probability theory and decision science to anticipate system failures and external threats (O'Connor & Kleyner, 2012). Reliability, a key aspect of risk analysis, is defined as the probability that a component or system will function as intended for a specified period under given conditions.

Game theory, first formalized by Von Neumann (1944), models strategic interactions between rational players. A game requires at least two players, each with a set of strategies that influence the resulting payoffs. Cox (2009) highlights how risk analysis and game theory reinforce each other: while risk analysis assesses probabilities of different outcomes in attacker-defender scenarios, game theory directly models adversarial decision-making. Bier et al. (2009) demonstrate that game theory enhances reliability theory by accounting for adaptive threats, allowing defenders to optimize their strategies in response to intelligent adversaries.

The primary purpose of the review is both to fill gaps in the literature and provide a structured overview of game-theoretic applications in risk and reliability analysis, particularly in infrastructure security. The reviewed articles have been included using the search terms game theory, risk analysis, infrastructure and networks in Web of Science. The key themes emerging are those in this review's section headings.

2 Comparing with earlier reviews

Previous reviews have explored attacker-defender models in security contexts, but few have examined infrastructure interdependencies. Bier and Tas (2012) assess game theory in infrastructure security, while Hausken and Levitin (2012) focus on defense strategies in reliability systems. However, these studies lack an in-depth analysis of cascading failures and network resilience. More recent reviews (Hunt & Zhuang, 2024; Seaberg et al., 2017) discuss attacker-defender dynamics but overlook strategic risk modeling for critical infrastructure. This review integrates these perspectives while extending the focus to interconnected systems.

3 Reliability systems involving defense and attack

Reliability systems are critical for infrastructure security, balancing defensive investments against attack strategies. Hausken and Levitin (2012) classify these systems into structures, defense measures, and attack tactics, highlighting redundancy and adaptive protection as key strategies.

Cox et al. (1996) model reliability as a two-player game, optimizing inspections and repairs under uncertainty. Azaiez and Bier (2007) extend this by incorporating strategic adversaries, showing how economic constraints shape resource allocation. Ben Yaghlane and Azaiez (2017) expand this perspective by defining system survivability as the probability that a system continues functioning under attack, contrasting it with conventional reliability measures that assume passive failure rather than adversarial threats.

Defensive strategies depend on system architecture. Bier et al. (2005) and Hausken (2008, 2010) analyze series and parallel systems, revealing that redundancy improves system survivability. Levitin and Hausken (2009a, 2009b) and Peng et al. (2016) further explore how target separation and false targets enhance resilience. Ben Yaghlane et al. (2019) and Suryahatmaja et al. (2023) analyze survivability in attacker-defender models, incorporating factors such as cost minimization, critical path identification, and maximizing minimum survival probability.

Hausken and He (2016) emphasize dynamic countermeasures, advocating for deception tactics and real-time monitoring to strengthen defenses. By distinguishing between frequentist and Bayesian approaches, Ben Yaghlane and Azaiez (2019) highlight how defenders can adapt their strategies based on information availability. The integration of game theory into reliability and survivability systems helps optimize resource allocation, improving infrastructure resilience against intelligent adversaries.

4 Multiple-target attacker-defender games

In many security scenarios, defenders must allocate limited resources to protect multiple targets from strategic attackers. Traditional models often assume a single defender and a single attacker, optimizing resource distribution to minimize losses. However, some studies explore more complex scenarios, such as Insua et al. (2016), who analyze multiple uncoordinated attackers using adversarial risk analysis, considering cascading effects in rail security. A key challenge is optimizing resource allocation. Bier et al. (2008) and Nikoofal and Zhuang (2012) examine cases where defenders protect all targets while attackers select one to strike, contrasting with models where both players choose subsets of targets.

Temporal aspects are another critical factor. Shan and Zhuang (2018) investigate how defense strategies evolve in a multi-period game, distinguishing between myopic defenders, who focus on short-term gains, and long-sighted defenders, who allocate resources with future risks in mind. Their work highlights the importance of dynamic defense strategies that account for changing attack probabilities and cascading threats.

Defender-attacker interactions vary in their assumptions about timing, information, and rationality. While most models assume the defender moves first, simultaneous-move games also exist, particularly in high-speed decision environments such as cybersecurity and critical infrastructure protection. Some models integrate probabilistic reasoning to estimate detection and attack probabilities, enhancing predictive accuracy for real-world applications.

The literature also explores empirical validation, incorporating data from sectors such as transportation, energy, and counterterrorism. Zhuang and Bier (2007) analyze strategic attacker decisions in infrastructure settings, while Zhang et al. (2021) and Aziz et al. (2020) refine attacker-defender models using behavioral and stochastic factors. Such studies highlight the need for balancing theoretical rigor with practical applicability, ensuring that resource allocation models are adaptable to real-world security threats.

Overall, multiple-target attacker-defender games provide essential insights into optimizing defensive measures across interconnected systems. Future research should focus on incorporating uncertainty, dynamic threat evolution, and empirical validation to refine these models for broader practical use.

5 Multiple targets at multiple levels involving defense and attack

In many security scenarios, targets are structured into hierarchical levels, requiring defenders to allocate resources across multiple layers of protection. These layers can range from individual targets to groups and overarching networks. Traditional models often assume independent targets, with a single defender and attacker. However, Levitin and Hausken (2012) and Hausken (2013) extend this by considering targets arranged in series, parallel, and hybrid structures, influencing how vulnerabilities propagate through networks.

Strategic defense planning becomes increasingly complex when multiple levels of organization exist. Golalikhani and Zhuang (2011) and Levitin et al. (2014) introduce models where defenders can select from more than two levels of protection, allowing dynamic adjustments based on threat severity. This contrasts with conventional models that assume fixed resource allocation across two levels, overlooking the adaptive nature of real-world security measures.

Another key consideration is the sequencing of moves. Most studies assume the defender acts first, providing a structured framework for allocating defenses before attackers respond. However, simultaneous-move models introduce greater uncertainty, as both players must anticipate each other's strategies in real time. While early research treats these interactions deterministically, recent work has explored stochastic and dynamic approaches to better reflect real-world uncertainties.

Practical applications of multi-level defense strategies span various domains, including critical infrastructure, military defense systems, and cybersecurity. Yolmeh et al. (2023) examine layered protection in transportation networks, while Hausken (2017) and Peng et al. (2014) explore security investments in interconnected systems. These studies highlight the trade-offs between centralized and decentralized defense strategies, demonstrating how resource allocation priorities shift based on interdependencies within multi-tiered targets.

Future work should enhance multi-level defense with probabilistic models. Addressing attacker learning mechanisms, cascading failures, and real-time decision-making will further refine these models, making them more applicable to modern security challenges.

6 Interdependence between targets and in networks and infrastructures

Interdependencies between targets significantly influence defense and attack strategies, as actions on one target can create cascading effects on others. This complexity arises in critical infrastructure systems, where nodes and links form interconnected networks. Attackers exploit these dependencies to maximize disruption, while defenders must allocate resources strategically to mitigate systemic risks.

Kunreuther and Heal (2003) analyze interdependent security across various domains, including the airline industry, fire protection, and cybersecurity, demonstrating how risk mitigation in one sector influences others. This notion extends to financial systems, where systemic risk propagates through bankruptcy and contagion models. Ignoring interdependencies leads to suboptimal security investments.

Several studies examine resource substitution across interdependent targets. Lakdawalla and Zanjani (2002) and Enders and Sandler (2004), investigate how strategic actors redistribute efforts when one target becomes more resilient, highlighting adversarial adaptation in dynamic security environments. Hausken (2006) extends these concepts by modeling competitive security investments across sectors, illustrating trade-offs between concentrated and distributed defense strategies.

A critical concern in interdependent security is cascading failures, where initial attacks trigger chain reactions. Bier and Tas (2014) and Li et al.

(2015) analyze models of sequential breakdowns in infrastructure systems, showing how attack strategies evolve based on defender responses. Wu et al. (2016) and Wang et al. (2015) develop probabilistic frameworks to predict the likelihood of secondary failures, emphasizing the need for preemptive mitigation strategies.

Empirical studies further validate these models. Alderson et al. (2015) assess the vulnerability of transportation networks, demonstrating how disruptions in one node affect overall connectivity. Rao et al. (2016) and He et al. (2020) analyze resilience strategies in energy grids, revealing the effectiveness of decentralized risk management. Shan and Zhuang (2020) examine multi-sector dependencies, emphasizing the role of coordination between independent entities in maintaining system stability.

Future research should enhance these models by integrating real-time monitoring, adaptive resource allocation, and behavioral game theory to better capture decision-making under uncertainty. Addressing multi-agent coordination and refining probabilistic assessments will further improve the applicability of interdependence modeling in security contexts.

7 Preserving the operation of networks through interdiction strategies

Networks commonly conceptualize nodes and arcs with one-way or two-way flows, in contrast to the previous sections conceptualizing targets with or without interdependence. Players may exert efforts into both nodes and arcs, which again contrasts with the focus on targets in the previous sections. Examples of arcs are railway tracks, roads, and channels for information, telecommunication, water, gas, and electric power. The stronger focus on arcs implies different solution methods. For example, Mrad et al. (2021) identify the most vital disjoint and non-disjoint cut-sets of a network, to determine the least costly attack. Carlyle et al. (2007) calculate resource constrained-shortest path optimal routes for manned or unmanned aircrafts encountering various threats. Gharbi et al. (2010) apply dynamic programming to optimize an attack to disconnect a network. Oh et al. (2018) present a decomposition algorithm to optimize the route and speed of a ground convoy moving through a network subject to attack. Garnaev et al. (2014) evaluate Bayesian network defense where the attacker's motivation us unknown to the defender. Yolmeh and Baykal-Gürsoy (2021) consider a damage-maximizing attacker hiding objects within a network. Alderson et al. (2013) identify critical components in a network subject to multiple simultaneous attacks.

8 Disrupting the operation of networks through interdiction strategies

A defender may prefer to disrupt networks, e.g. for flows of illegal material, drugs, enemy troops, and communication between adversaries. Wood (1993) applies integer programming to determine how a defender interdicts the flow of drugs and chemicals through river and road networks. Washburn and Wood (1995) develop two-person zero-sum games where an evader minimizes its detection probability, and the interdictor applies probabilistic arc inspection, generalized to multiple evaders or interdictors, and unknown origins and destinations. Cormican et al. (1998) utilize stochastic integer programming where the interdiction successes are binary random variables. Israeli and Wood (2002) apply Benders decomposition and a mixed-integer program for resource constrained interdiction. Royset and Wood (2007) use Lagrangian relaxation involving max-flow min-cut problems to minimize the maximum flow through a network. Akgün et al. (2011) consider the interdiction of maximum network flow by converting an NP hard bilevel minmax problem into a mixed integer problem.

9 Electric power grids

Common networks are electric power grids involving generators, transformers, transmission lines, etc. Bier et al. (2007) consider optimal resource allocation for defense against interdiction of the power transmission line with the highest dynamically changing load in an iterative procedure. Brown et al. (2006) and Brown et al. (2005) develop trilevel models where the players move in different sequences, gather data from red-team exercises, and pinpoint vulnerabilities. Salmerón and Wood (2015) and Salmerón, Wood and Baldick (2009) apply and generalize Benders decomposition to single out critical components. Several of these models are also applicable for other systems involving communication, water flows, etc.

10 Transportation

The literature mostly considers general transportation networks of goods, humans, etc. Numerical methods are usually applied to handle the complexity. The arcs can be roads, railways, etc. on land; narrow straits such as the Suez Canal at sea; and air corridors, restricted air space, etc. for air transportation. Congestion, common in road networks, is analyzed by Alderson et al. (2011), Alderson et al. (2018), and Bier and Hausken (2013). They determine optimal travel routes subject to defense and attack. Salmerón, Wood and Morton (2009) apply a stochastic mixed integer model to minimize interference with ships carrying military cargo subject to attack. Further research examples are by Zhang et al. (2013), Baykal-Gürsoy et al. (2014), Zhang et al. (2018), and Kosanoglu and Bier (2020). Future research should address cyber security associated with wireless communication between driverless vehicles and data centers, see Hausken et al. (2024).

11 Conclusion

Game theory has emerged as a critical tool in risk and reliability analysis, particularly for understanding attacker-defender interactions, optimizing resource allocation, and enhancing infrastructure resilience. This review has highlighted how game-theoretic models complement traditional risk analysis by accounting for strategic behavior, adversarial adaptation, and interdependencies within critical systems.

By synthesizing findings from existing literature, this study has identified key research gaps. While previous reviews have examined defender-attacker dynamics and infrastructure security, limited attention has been given to cascading failures, evolving threats, and dynamic risk mitigation in interconnected networks. Furthermore, integrating empirical validation with theoretical models remains an ongoing challenge.

A key takeaway is that defensive strategies must evolve to address complex, multi-layered, and interdependent threats. Traditional reliability measures that assume passive failures are insufficient when facing intelligent adversaries. Instead, game-theoretic approaches provide a structured framework for optimizing security investments, balancing proactive and reactive measures, and anticipating adversarial behavior.

Future research should focus on multi-agent coordination, real-time decision-making, and hybrid modeling approaches that integrate game theory with probabilistic risk assessments and behavioral analysis. Expanding applications to emerging domains such as cyber-physical security, artificial intelligence-driven risk assessment, and adaptive infrastructure protection will further enhance resilience against strategic threats.

Ultimately, this review underscores the importance of bridging theoretical advancements with real-world applications. By refining attacker-defender models, incorporating empirical insights, and addressing uncertainty in strategic decision-making, game theory can significantly improve the protection and reliability of critical infrastructure systems.

References

Akgün, İ., Tansel, B. Ç., & Kevin Wood, R. (2011). The Multi-Terminal Maximum-Flow Network-Interdiction Problem. *European Journal of Operational Research*, *211*(2), 241-251. https://doi.org/10.1016/j.ejor.2010.12.011

Alderson, D. L., Brown, G. G., & Carlyle, W. M. (2015). Operational Models of Infrastructure Resilience. *Risk Analysis*, *35*(4), 562-586. https://doi.org/10.1111/risa.12333

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Cox, L. A. (2013). *Sometimes There Is No Most-Vital Arc: Assessing and Improving the Operational Resilience of Systems*. Naval Postgraduate School Monterey CA.

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Wood, R. K. (2011). Solving Defender-Attacker-Defender Models for Infrastructure Defense. 12th INFORMS Computing Society Conference, Monterey, CA.

Alderson, D. L., Brown, G. G., Carlyle, W. M., & Wood, R. K. (2018). Assessing and Improving the Operational Resilience of a Large Highway Infrastructure System to Worst-Case Losses. *Transportation science*, *52*(4), 1012-1034. https://doi.org/10.1287/trsc.2017.0749

Azaiez, M. N., & Bier, V. M. (2007). Optimal Resource Allocation for Security in Reliability Systems. *European Journal of Operational Research*, *181*(2), 773-786. https://doi.org/10.1016/j.ejor.2006.03.057

Aziz, R., He, M., & Zhuang, J. (2020). An Attacker-Defender Resource Allocation Game with Substitution and Complementary Effects. *Risk Analysis*, *40*(7), 1481-1506.

Baykal-Gürsoy, M., Duan, Z., Poor, H. V., & Garnaev, A. (2014). Infrastructure Security Games. *European Journal of Operational Research*, *239*(2), 469-478. https://doi.org/10.1016/j.ejor.2014.04.033

Ben Yaghlane, A., & Azaiez, M. N. (2019). System Survivability to Continuous Attacks: A Game Theoretic Setting for Constant Attack Rate Processes. *The Journal of the Operational Research Society*, *70*(8), 1308-1320. https://doi.org/10.1080/01605682.2018.1489350

Ben Yaghlane, A., Azaiez, M. N., & Mrad, M. (2019). System Survivability in the Context of Interdiction Networks. *Reliability Engineering & System Safety*, *185*, 362-371. https://doi.org/10.1016/j.ress.2019.01.005

Bier, V. M., Cox, L. A., & Azaiez, M. N. (2009). Why Both Game Theory and Reliability Theory Are Important in Defending Infrastructure against Intelligent Attacks. In V. M. Bier & M. N. Azaiez (Eds.), *Game Theoretic Risk Analysis of Security Threats* (pp. 1-11). Springer US.

Bier, V. M., Gratz, E. R., Haphuriwat, N. J., Magua, W., & Wierzbicki, K. R. (2007). Methodology for Identifying near-Optimal Interdiction Strategies for a Power Transmission System. *Reliability Engineering & System Safety*, *92*(9), 1155-1161. https://doi.org/10.1016/j.ress.2006.08.007

Bier, V. M., Haphuriwat, N., Menoyo, J., Zimmerman, R., & Culpen, A. M. (2008). Optimal Resource Allocation for Defense of Targets Based on Differing Measures of Attractiveness. *Risk Analysis*, *28*(3), 763-770. https://doi.org/10.1111/j.1539-6924.2008.01053.x

Bier, V. M., & Hausken, K. (2013). Defending and Attacking a Network of Two Arcs Subject to Traffic Congestion. *Reliability Engineering & System Safety*, *112*, 214-224.

Bier, V. M., Nagaraj, A., & Abhichandani, V. (2005). Protection of Simple Series and Parallel Systems with Components of Different Values. *Reliability Engineering & System Safety*, *87*(3), 315-323. https://doi.org/10.1016/j.ress.2004.06.003

Bier, V. M., & Tas, S. (2012). Game Theory in Infrastructure Security. *WIT Transactions on State of the Art in Science and Engineering*, *54*, 91-104. https://doi.org/10.2495/978-1-84564-562-5/06

Bier, V. M., & Tas, S. (2014). Addressing Vulnerability to Cascading Failure against Intelligent Adversaries in Power Networks. *Energy Systems*, *7*, 193–213.

Brown, G., Carlyle, M., Salmerón, J., & Wood, R. K. (2006). Defending Critical Infrastructure. *Interfaces*, *36*(6), 530-544. https://doi.org/10.1287/inte.1060.0252

Brown, G., Carlyle, W. M., Salmerón, J., & Wood, R. K. (2005). Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses. *INFORMS TutORials in Operations Research*, 102-123, https://doi.org/110.1287/educ.1053.0018.

Carlyle, W. M., Royset, J. O., & Wood, R. K. (2007). *Routing Military Aircraft with a Constrained Shortest-Path Algorithm*. Naval Postgraduate School Monterey CA.

Cormican, K. J., Morton, D. P., & Wood, R. K. (1998). Stochastic Network Interdiction. *Operations Research*, *46*(2), 184-197. https://doi.org/10.1287/opre.46.2.184

Cox, L. A. (2009). Game Theory and Risk Analysis. *Risk Analysis*, *29*(8), 1062-1068. https://doi.org/10.1111/j.1539-6924.2009.01247.x

Cox, L. A., Chiu, S. Y., & Sun, X. (1996). Least-Cost Failure Diagnosis in Uncertain Reliability Systems. *Reliability Engineering & System Safety*, *54*(2), 203-216. https://doi.org/10.1016/S0951-8320(96)00076-2

Deisler, P. F., & Schwing, R. C. (2000). *History of the Society for Risk Analysis through the Year 2000*. https://www.sra.org/wp-content/uploads/2020/04/SRA20YearHistory.pdf

Enders, W., & Sandler, T. (2004). What Do We Know About the Substitution Effect in Transnational Terrorism? In A. Silke (Ed.), *Researching Terrorism: Trends, Achievements, Failures* (pp. 119-137). Frank Cass, http://dx.doi.org/10.4324/9780203500972.ch7

Garnaev, A., Baykal-Gursoy, M., & Poor, H. V. (2014). Incorporating Attack-Type Uncertainty into Network Protection. *IEEE Transactions on Information Forensics and Security*, *9*(8), 1278-1287. https://doi.org/10.1109/TIFS.2014.2329241

Gharbi, A., Azaiez, M. N., & Kharbeche, M. (2010). Minimizing Expected Attacking Cost in Networks. *Electronic Notes in Discrete Mathematics*, *36*, 947-954. https://doi.org/10.1016/j.endm.2010.05.120

Golalikhani, M., & Zhuang, J. (2011). Modeling Arbitrary Layers of Continuous-Level Defenses in Facing with Strategic Attackers [Article]. *Risk Analysis*, *31*(4), 533-547. https://doi.org/10.1111/j.1539-6924.2010.01531.x

Hausken, K. (2006). Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy*, *25*(6), 629-665. https://doi.org/10.1016/j.jaccpubpol.2006.09.001

Hausken, K. (2008). Strategic Defense and Attack for Series and Parallel Reliability Systems [Article]. *European Journal of Operational Research*, *186*(2), 856-881. https://doi.org/10.1016/j.ejor.2007.02.013

Hausken, K. (2010). Defense and Attack of Complex and Dependent Systems. *Reliability Engineering & System Safety*, *95*(1), 29-42. https://doi.org/10.1016/j.ress.2009.07.006

Hausken, K. (2013). Combined Series and Parallel Systems Subject to Individual Versus Overarching Defense and Attack. *Asia-Pacific Journal of Operational Research*, *30*(02), 1250056. https://doi.org/doi:10.1142/S021759591250056X

Hausken, K. (2017). Special Versus General Protection and Attack of Parallel and Series Components. *Reliability Engineering and System Safety*, *165*, 239-256. https://doi.org/10.1016/j.ress.2017.03.027

Hausken, K., & He, F. (2016). On the Effectiveness of Security Countermeasures for Critical Infrastructures. *Risk Analysis*. https://doi.org/10.1111/risa.12318

Hausken, K., & Levitin, G. (2012). Review of Systems Defense and Attack Models. *International Journal of Performability Engineering*, *8*(4), 355-366.

Hausken, K., Welburn, J. W., & Zhuang, J. (2024). A Review of Attacker-Defender Games and Cyber Security. *Games*, *15*(4), 1-27. https://www.mdpi.com/2073-4336/15/4/28

He, F., Zhuang, J., & Rao, N. (2020). Discrete Game-Theoretic Analysis of Attack and Defense in Correlated Cyber-Physical Systems. *Annals of Operations Research*, *294*, 741-767.

Hunt, K., & Zhuang, J. (2024). A Review of Attacker-Defender Games: Current State and Paths Forward. *European Journal of Operational Research*, *313*(2), 401-417. https://doi.org/10.1016/j.ejor.2023.04.009

Insua, D. R., Cano, J., Pellot, M., & Ortega, R. (2016). Multithreat Multisite Protection: A Security Case Study [Article]. *European Journal of Operational Research*, *252*(3), 888-899. https://doi.org/10.1016/j.ejor.2016.01.041

Israeli, E., & Wood, R. K. (2002). Shortest-Path Network Interdiction. *Networks*, *40*(2), 97-111. https://doi.org/10.1002/net.10039

Kosanoglu, F., & Bier, V. M. (2020). Target-Oriented Utility for Interdiction of Transportation Networks. *Reliability Engineering & System Safety*, *197*, 106793.

Kunreuther, H., & Heal, G. (2003). Interdependent Security. *Journal of Risk and Uncertainty*, *26*(2-3), 231-249. https://doi.org/10.1023/a:1024119208153

[Record #5481 is using a reference type undefined in this output style.]

Levitin, G., & Hausken, K. (2009a). False Targets Efficiency in Defense Strategy. *European Journal of Operational Research*, *194*(1), 155-162.

Levitin, G., & Hausken, K. (2009b). Redundancy Vs. Protection Vs. False Targets for Systems under Attack. *Ieee Transactions on Reliability*, *58*(1), 58-68.

Levitin, G., & Hausken, K. (2012). Individual Versus Overarching Protection against Strategic Attacks. *Journal of the Operational Research Society*, *63*(7), 969-981. https://doi.org/10.1057/jors.2011.96

Levitin, G., Hausken, K., & Dai, Y. (2014). Optimal Defense with Variable Number of Overarching and Individual Protections. *Reliability Engineering & System Safety*, *123*, 81-90. https://doi.org/10.1016/j.ress.2013.11.001

Li, R.-q., Sun, S.-w., Ma, Y.-l., Wang, L., & Xia, C.-y. (2015). Effect of Clustering on Attack Vulnerability of Interdependent Scale-Free Networks. *Chaos Solitons & Fractals*, *80*, 109-116. https://doi.org/10.1016/j.chaos.2015.06.022

Mrad, M., Suryahatmaja, U. S., Ben Yaghlane, A., & Azaiez, M. N. (2021). Attack Strategies on Networks with a Budget Constraint. *IEEE Access*, *9*, 100530-100547. https://doi.org/10.1109/access.2021.3097039

Nikoofal, M. E., & Zhuang, J. (2012). Robust Allocation of a Defensive Budget Considering an Attackers Private Information. *Risk Analysis*, *32*(5), 930-943.

O'Connor, P. D. T., & Kleyner, A. (2012). *Practical Reliability Engineering* (5th ed.). Wiley.

Oh, D. H., Wood, R. K., & Lee, Y. H. (2018). Optimal Interdiction of a Ground Convoy. *Military Operations Research*, *23*(2), 5-18.

Peng, R., Guo, L., Levitin, G., Mo, H., & Wang, W. (2014). Maintenance Versus Individual and

Overarching Protections for Parallel Systems. *Quality Technology and Quantitative Management*, *11*(3), 353-362. <Go to ISI>://WOS:000341276100011

Peng, R., Zhai, Q. Q., & Levitin, G. (2016). Defending a Single Object against an Attacker Trying to Detect a Subset of False Targets. *Reliability Engineering and System Safety*, *149*, 137-147. https://doi.org/10.1016/j.ress.2016.01.002

Rao, N., Poole, S., Ma, C., He, F., Zhuang, J., & Yau, D. (2016). Defense of Cyber Infrastructures against Cyber-Physical Attacks Using Game-Theoretic Models. *Risk Analysis*, *36*(4), 694710.

Royset, J. O., & Wood, R. K. (2007). Solving the Bi-Objective Maximum-Flow Network-Interdiction Problem. *INFORMS journal on computing*, *19*(2), 175-184. https://doi.org/10.1287/ijoc.1060.0191

Salmerón, J., & Wood, R. K. (2015). The Value of Recovery Transformers in Protecting an Electric Transmission Grid against Attack. *IEEE transactions on power systems*, *30*(5), 2396-2403. https://doi.org/10.1109/TPWRS.2014.2360401

Salmerón, J., Wood, R. K., & Baldick, R. (2009). Worst-Case Interdiction Analysis of Large-Scale Electric Power Grids. *IEEE transactions on power systems*, *24*(1), 96-104. https://doi.org/10.1109/TPWRS.2008.2004825

Salmerón, J., Wood, R. K., & Morton, D. P. (2009). A Stochastic Program for Optimizing Military Sealift Subject to Attack. *Military Operations Research*, *14*(2), 19-39.

Seaberg, D., Devine, L., & Zhuang, J. (2017). A Review of Game Theory Applications in Natural Disaster Management Research. *Natural Hazards*, *89*(3), 1461-1483.

Shan, X., & Zhuang, J. (2018). Modeling Cumulative Defensive Resource Allocation against a Strategic Attacker in a Multi-Period Multi-Target Sequential Game. *Reliability Engineering and System Safety*, *179*, 12-26. https://doi.org/10.1016/j.ress.2017.03.022

Shan, X. G., & Zhuang, J. (2020). A Game-Theoretic Approach to Modeling Attacks and Defenses of Smart Grids at Three Levels. *Reliability Engineering & System Safety*, *195*, 106683.

Suryahatmaja, U. S., Mrad, M., Azaiez, M. N., Yaghlane, A. B., & Gharbi, A. (2023). The K Critical Path Sets to Protect in Interdiction Networks under Limited Defensive Resources. *IEEE eTransactions on network and service management*, *20*(4), 1-1. https://doi.org/10.1109/TNSM.2023.3282709

Von Neumann, J. (1944). *Theory of Games and Economic Behavior*. Princeton University Press.

Wang, J., Wu, Y., & Li, Y. (2015). Attack Robustness of Cascading Load Model in Interdependent Networks. *International Journal of Modern Physics C*, *26*(3), Article 1550030. https://doi.org/10.1142/s0129183115500308

Washburn, A., & Wood, R. K. (1995). Two-Person Zero-Sum Games for Network Interdiction. *Operations Research*, *43*(2), 243-251. https://doi.org/10.1287/opre.43.2.243

Wood, R. K. (1993). *Deterministic Network Interdiction*.

Wu, B., Tang, A., & Wu, J. (2016). Modeling Cascading Failures in Interdependent Infrastructures under Terrorist Attacks. *Reliability Engineering & System Safety*, *147*, 1-8. https://doi.org/10.1016/j.ress.2015.10.019

Yolmeh, A., & Baykal-Gürsoy, M. (2021). Weighted Network Search Games with Multiple Hidden Objects and Multiple Search Teams. *European Journal of Operational Research*, *289*(1), 338-349. https://doi.org/10.1016/j.ejor.2020.06.046

Yolmeh, A., Baykal-Gürsoy, M., & Bier, V. (2023). A Decomposable Resource Allocation Model with Generalized Overarching Protections. *Annals of Operations Research*, *320*(1), 493-507. https://doi.org/10.1007/s10479-022-05064-w

Zhang, J., Wang, Y., & Zhuang, J. (2021). Modeling Multi-Target Defender-Attacker Games with Quantal Response Attack Strategies. *Reliability Engineering & System Safety*, *205*, 107165.

Zhang, J., Zhuang, J., & Behlendorf, B. (2018). Stochastic Shortest Path Network Interdiction with a Case Study of Arizona-Mexico Border. *Reliability Engineering & System Safety*, *179*, 62-73.

Zhang, P., Cheng, B., Zhao, Z., Li, D., Lu, G., Wang, Y., & Xiao, J. (2013). The Robustness of Interdependent Transportation Networks under Targeted Attack. *Epl*, *103*(6), Article 68005. https://doi.org/10.1209/0295-5075/103/68005

Zhuang, J., & Bier, V. M. (2007). Balancing Terrorism and Natural Disasters: Defensive Strategy with Endogenous Attacker Effort. *Operations Research*, *55*(5), 976-991. https://doi.org/10.1287/opre.1070.0434