

Review of Systems Defense and Attack Models

KJELL HAUSKEN^{*1} and GREGORY LEVITIN²

¹*Faculty of Social Sciences, University of Stavanger, Norway*

²*The Israel Electric Corporation Ltd, Israel.*

(Received on September 14, 2011 and revised on May 19, 2012)

Abstract: This review paper classifies 129 published papers according to the system structure, defense measures, and attack tactics and circumstances. System structure is further divided into single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Defense measures are divided into separation of system elements, redundancy, protection, multilevel defense, false targets deployment and preventive strike. Attack tactics and circumstances are divided into attack against single element, attack against multiple elements, consecutive attacks, random attack, combination of intentional and unintentional impacts, incomplete information, and variable resources. The classification is intended to give an overview of the field and implicitly suggest future areas of research.

Keywords: System, defense, attack, classification, performability, game theory.

1. Introduction

The literature on the defense and attack of systems has grown steadily. This paper classifies some recent contributions. We categorize according to system structure, defense measures, and attack tactics and circumstances. System structure is further divided into single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Defense measures are divided into separation of system elements, redundancy, protection, multilevel defense, deployment of false targets and preventive strike. Attack tactics and circumstances are divided into attack against single element, attack against multiple elements, consecutive attacks, random attack, combination of intentional and unintentional impacts, incomplete information, and variable resources.

The research classified in this paper does not exist in a vacuum and has strong linkages to related research. For tractability, we have proceeded as follows. First, we have confined attention to systems where the defender prefers reliable performability, functioning and continued existence, and the attacker has an opposite preference. Systems may have from simple to complex structure, and we have included single elements to the extent the research is otherwise connected. Second, we focus on a strategic attacker excluding work where the attack is exogenously given or specified as a probability. Third, we exclude information technology security which is a huge topic deserving a separate classification. Fourth, we have partially included terrorism to the extent the research is otherwise connected to the topic, though terrorism is also a huge topic deserving a separate classification.

Section 2 defines and elaborates the classification categories. Section 3 classifies ### papers. Section 4 suggests future research developments. Section 5 concludes.

* Corresponding author's email: kjell.hausken@uis.no

2. Classification categories

2.1. System structure

1 *Single element*

The defender goal may be to prevent the destruction of a single element (facility, object of value) by applying different defense measures.

2 *Series systems*

In the series system destruction of any one of elements inevitably causes destruction of the entire system.

3 *Parallel systems*

In parallel systems the entire system is destroyed only when all its elements are destroyed.

4 *Series-parallel systems*

These systems constitute a combination of parallel and series system

5 *Networks*

Networks are defined by a set of nodes and a set of links. The destruction/interdiction of some links can result in elimination of paths between certain nodes or in reduction of possible flow between nodes.

6 *Multiple elements*

Systems or infrastructures can consist of multiple elements which are not linked in any particular way. For example, the September 11, 2001 attack was directed towards four elements, *i.e.*, the North and South towers of the World Trade Center, the Pentagon, and either the Capitol Building or the White House.

7 *Interdependent systems*

Systems where an impact on one element gets transferred further to one or several other elements due to linkages.

8 *Other types of systems*

Other types of systems include consecutively connected systems, interdependent systems, sliding window systems that fail if certain combinations of their elements are destroyed.

2.2. Defense Measures

1 *False targets*

False targets are cheap inoperative elements which look genuine to the attacker. Incorporating false targets into one's system design can cause the attacker to dilute its resources across more targets than the number of genuine elements the defender actually has at its disposal.

2 *Separation of system elements*

Separation of elements removes coupling factors (common power supply, close location *etc.*) that can cause common cause failures caused by any single attacks. If the collection of elements is divided into several separated groups, no more than one group can be destroyed by any attack.

3 *Redundancy*

Introducing redundancy makes systems tolerant to destruction of some elements. Indeed, any subsystem of redundant elements can be considered as a parallel system because it can be destroyed only if all of the redundant elements are destroyed.

Introducing redundancy without separation can be non effective because all redundant elements having coupling factors can be destroyed by a single attack.

4 *Protection*

Protection is a complex of technical and/or organizational measures aimed at reducing the conditional probability of target destruction given it is attacked. The increase of protection effort decreases destruction probability of the protected object.

5 *Multilevel defense*

Multilevel defense (defense in depth) presumes construction of layered protections such that any inner protection can be destroyed only when the outer protection is destroyed. Any outer protection can protect several protected groups such that the protections compose an hierarchical structure.

6 *Preventive strike*

Preventive strike is the defender's attempt to destroy the attacker's ability to strike before the attack. If the preventive strike fails the probability of the revenge attack is usually greater than the probability of the unprovoked attack in the case of no preventive strike.

2.3. Attack Tactics and Circumstances

1 *Attack against single element*

In this case the attacker chooses a single target among several system elements anticipating that destruction of this target will cause the greatest damage to the defender

2 *Attack against multiple elements*

In this case the attacker chooses a subset of elements to attack anticipating that destruction of these targets will cause the greatest damage to the defender

3 *Consecutive attacks*

The attacker launches a sequence of attacks, possibly changing elements of its strategy among the attacks.

4 *Random attack*

In this case the attacker either has no ability to direct the attack among specific set of targets or has no information to decide which set to attack. In some cases the attacker can determine how many targets to attack, but chooses the set of attacked targets at random. In other cases the attacker randomly chooses the number and the set of attacked targets and it may be assumed that any target can be attacked with equal probability.

5 *Combination of intentional and unintentional impacts*

The defender can consider possibility of both intentional and unintentional impacts (attacks and disasters) as well as their combination when it builds the system defense. The unintentional impacts can hit any system element with the same probability, whereas the strategic attacker usually chooses the set of targets that can cause the greatest damage. The magnitude of unintentional impacts (disasters) usually does not depend on the number of elements affected. On the contrary, the intentional attacker usually has a fixer resources which it distributes among the targets so that the greater the number of attacked targets the less per-target attack effort.

6 *Incomplete information*

Incomplete information can be caused by the lack of knowledge about the counterpart's goals, target valuation, plans or resources, by influence of chance on the attack outcome, by imperfect detection of intermediate outcomes in the case of consecutive actions

7 *Variable resources*

In some cases the resources of the attacker and the defender change with time, or they are not subject to constraints. For example they can be given on the base of annual budgets or can change among consecutive actions.

3. Classification

Table 1 classifies the listed references according to system structure, defense measures, attack tactics and circumstances.

Table 1: Classification of Papers

Reference No	System structure	Defense measures	Attack tactics and circumstances
1	4	4	2,3,6
2	4	4	2
3,47,75	1	4,6	1
5,10	6	4	1
6	2,3	4	2
8	6	4	1,6
9	2,3	4	1,2
4,11,12,14,19,100, 106,108,112	5	4	2
7,13,23,27,94,99, 101,102	6	4	2
16	6	4	1,6
17	6	4	3
18	6	4	4,6
20	6	5	2,7
21,113	6	4	2,5
15,22,56,97,115,116	6	4	2,6
24,25	5	3,4	2
26	6	5	1
28,29,30,33	4	4	2,7
31	4,5	4	2,7
32	4,5,7,8	3,4	2,3,7
34	4	4	2,3,7
35	4,5,7,8	4	2,7
36	2,3	4	2,7
37	1	4	1,7
38	1	4	1,5,7
39	3	2,4	2
40	4	2,4	2
41	2	1,4	2
42	3	4	2,3
43	2	1,4	1,2
44	3	2,4	2,7
45	3	4	2,3
46	3	3,4	2,3
48	3	4	2
49,51	1	4,6	1,3
50,52	1	4	1,3,7
53	1	4	1,6,7
54	5	4	2,3
55	5	4	1
57,60	4	1,2,4	1,2,6
58,61	4	2,4	1,2,6
59	1	5	1
62	5	3,4	2,6
63	3	3,4	2
64	3	4	2,3
65,67	3	1,3,4	2
66	1	1,4	2
68,95	1	1,4	2,6
69	3	1,3,4	2,6

70	3	4	2
71	3	3,4	2,5
72	3	2,4	2,6
73	3	1,2,3,4	2,6
74	3	2,3,4	2,6
76	1	4	1,3
77	1	4,6	1,3
78	3	3,4	2,3,4
79	2,3	5	2
80	3	3,4	2,3
81,82	1	1,4,6	2
83,114	1	4	1,3,6
84	1	4,6	1,3
85	5	4	2
86,98	5	4	2,6
87	5	3,4	5
88,89	5	4	5
90,107	1	4	1
91	6	4	2,3,5
92	8	4	2,6
93	6	4	2,3
96	2,3	1,4	2,6
112	6	4,6	2
104	6	4,6	2,3,6
105,110	8	4	2
109	5	3,4	2,4,6
111	6	4	2,3,6
117	5	4	2,3
118	1	4,6	1
119	6,7	4	2
120,121,122	6,7	4	2,7
123	1	4	3
124,125	7	4	4
126	6	4	2,6
127	5	4	2,3
128	6,7	4	2
129	6	4	4,6

4. Future Developments

Future developments can occur along many interesting trajectories. One can consider the cases of perfect and imperfect FTs (FTs that can be distinguished and ignored by the attacker). One can consider the dynamic of the FTs deployment when the attacker's and defender's resources are stockpiling (for constant resource increment rate).

Using the fact that FTs can be destroyed with much less effort than the GOs, the attacker can apply a double attack strategy in which it tries first to eliminate with optimal effort as many FTs as possible in the first attack and then distributes its entire remaining resource among all surviving targets in the second attack. The defender's counter-measures (protection of all or part of FTs) can be analyzed in the case of the double attack assuming perfect and imperfect attacker's detection of the targets destroyed in the first attack.

One research agenda is to explore all the combinations of false targets, separation, redundancy, and number of attacks in Table 1, combined further with 1-out-of-N versus k-out-of-N of system, production of elements, preventive versus reactive strikes, disaster, *etc.*

More generally, future research possibilities follow from determining combinations of characteristics in the classification of earlier works that have hitherto not been analyzed.

5. Conclusion

The literature on the defense and attack of system has grown steadily. This paper provides a review. We develop a table which categorizes the literature according to system structure, defense measures, and attack tactics and circumstances. System structure is further divided into single element, series systems, parallel systems, series-parallel systems, networks, multiple elements, interdependent systems, and other types of systems. Defense measures are divided into separation of system elements, redundancy, protection, multilevel defense, false targets deployment and preventive strike. Attack tactics and circumstances are divided into attack against single element, attack against multiple elements, consecutive attacks, random attack, combination of intentional and unintentional impacts, incomplete information, and variable resources. The classification is intended to give an overview of the field and implicitly suggest future research trajectories. false targets, separation, redundancy, and number of attacks. We discuss other characteristics, and suggest future research trajectories.

References

- [1]. Azaiez, M.N. *A Bayesian Model for a Game of Information in Optimal Attack/Defense Strategies*. In: Bier, V.M. and Azaiez, M.N. (eds.), *Game Theoretic Risk Analysis of Security Threats*, Springer, New York, 2009; 99-123.
- [2]. Azaiez, M.N. and Bier, V.M. *Optimal Resource Allocation for Security in Reliability Systems*. *European Journal of Operational Research*, 2007; 181(2): 773-786.
- [3]. Bandyopadhyay, S., and Sandler, T. *The interplay between preemptive and defensive counterterrorism measures: A two-stage game*. *Economica*, 2011; 78(311): 546-564.
- [4]. Bell, M.G.H., Kanturska, U., Schmocker, J.-D., and Fonzone, A. *Attacker-defender models and road network vulnerability*. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2008; 366(1872): 1893-1906.
- [5]. Bier, V.M. *Choosing what to protect*. *Risk Analysis*, 2007; 27(3): 607-620.
- [6]. Bier, V.M. and Abhichandani, V. *Optimal Allocation of Resources for Defence of Simple Series and Parallel Systems from Determined Adversaries*. *Proceedings of the Engineering Foundation Conference on Risk-Based Decision Making in Water Resources X*, Santa Barbara, CA: American Society of Civil Engineers, 2002: 59-76.
- [7]. Bier, V.M. and Haphuriwat, N. *Analytical method to identify the number of containers to inspect at US ports to deter terrorist attacks*. *Annals of Operations Research*, 2011; 187(1): 137-158.
- [8]. Bier, V.M., Haphuriwat, N., Menoyo, J., Zimmerman, R., and Culpén, A.M. *Optimal Resource Allocation for Defense of Targets Based on Differing Measures of Attractiveness*. *Risk Analysis*, 2008; 28(3): 763-770.
- [9]. Bier, V.M., Nagaraj, A. and Abhichandani, V. *Protection of Simple Series and Parallel Systems with Components of Different Values*. *Reliability Engineering and System Safety*, 2005; 87(3): 315-323.
- [10]. Bier, V.M., Oliveros, S., and L. Samuelson. *Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker*. *Journal of Public Economic Theory*, 2007; 9(4): 563-587.
- [11]. Brown, G., Carlyle, M., Salmerón, J. and Wood, K. *Defending Critical Infrastructure*. *Interfaces*, 2006; 36(6): 530-544.
- [12]. Cohen, F. *Managing Network Security: Attack and Defence Strategies*. *Network Security*, 1997(4): 7-11, 1997

- [13]. Cox, T. *Some Limitations of "Risk = Threat x Vulnerability x Consequence" for Risk Analysis of Terrorist Attacks*. Risk Analysis, 2008; 28(6): 1749-1761.
- [14]. Cox, T. *Making Telecommunications Networks Resilient Against Terrorist Attacks*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 175-197.
- [15]. Cremonini, M. and Nizovtsev, D. *Risks and Benefits of Signaling Information System Characteristics to Strategic Attackers*. Journal of Management Information Systems, 2009–2010; 26(3): 241–274.
- [16]. Dighe, N., Zhuang J., and Bier V.M. *Secrecy in defensive allocations as a strategy for achieving more cost-effective attacker deterrence*, International Journal of Performability Engineering, 2009; 5(1): 31-43.
- [17]. Franqueira, V.N.L, van Eck, P., Wieringa, R., and Lopes, R.H.C. *A Mobile Ambients-Based Approach for Network Attack Modelling and Simulation*. International Conference on Availability, Reliability and Security, 2009; 546-553.
- [18]. Gaver, D.P., Glazebrook, K.D., Jacobs, P.A. *Search for a Malevolent Needle in a Benign Haystack*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 125-146.
- [19]. Gharbi, A., Azaiez, M.N., and Kharbeche, M. 2010. *Minimizing Expected Attacking Cost in Networks*. Electronic Notes in Discrete Mathematics, 2010; 36(August 1): 947-954.
- [20]. Golalikhani, M. and Zhuang, J. *Modeling Arbitrary Layers of Continuous Level Defenses in Facing with A Strategic Attacker*. Risk Analysis, 2011; 31(4): 533-547.
- [21]. Golany, B., Kaplan, E., Marmur, A., and Rothblum, U.G. *Nature Plays with Dice - Terrorists Do Not: Allocating Resources to Counter Probabilistic and Strategic Risks*. European Journal of Operational Research, 2009; 192(1): 198-208.
- [22]. Guikema, S.D. *Game Theory Models of Intelligent Actors in Reliability Analysis: A State of the Art Review*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 13-31.
- [23]. Guikema, S. and Aven, T. *Assessing Risk from Intelligent Attacks: A Perspective on approaches*. Reliability Engineering and System Safety, 2010; 95(5): 478–483.
- [24]. Haimes, Y.Y., Crowther, K, and Horowitz, B.M. *Homeland Security Preparedness: Balancing Protection with Resilience in Emergent Systems*. Systems Engineering, 2008; 11(4): 287-308.
- [25]. Haimes, Y.Y., Matalas, N.C., Lambert, J.H., Jackson, B.A., and Fellows, J.F.R. *Reducing vulnerability of water supply systems to attack*. Journal of infrastructure systems, 1998; 4(4): 164-177.
- [26]. Haphuriwat, N. and Bier, V.M. *Trade-offs between target hardening and overarching protection*. European Journal of Operational Research, 2011; 213(1): 320-328.
- [27]. Haphuriwat, N., Bier, V.M., and Willis, H.H. *Deterring the Smuggling of Nuclear Weapons in Container Freight Through Detection and Retaliation*. Decision Analysis, 2011; 8(2): 88-102.
- [28]. Hausken, K. *Probabilistic risk analysis and game theory*. Risk Analysis, 2002; 22 (1): 17-27.
- [29]. Hausken, K. *Strategic Defense and Attack for Series and Parallel Reliability Systems*. European Journal of Operational Research, 2008; 186(2): 856-881.
- [30]. Hausken, K. *Strategic Defense and Attack for Reliability Systems*. Reliability Engineering & System Safety, 2008; 93(11): 1740-1750.
- [31]. Hausken, K. *Strategic Defense and Attack of Complex Networks*. International Journal of Performability Engineering, 2009; 5(1): 13-30.
- [32]. Hausken, K. *Defense and Attack of Complex and Dependent Systems*. Reliability Engineering & System Safety, 2010; 95(1): 29-42.
- [33]. Hausken, K. *Defense and Attack of Two-Component Multi-State Systems*. International Journal of Performability Engineering, 2011; 7(3): 205-216.
- [34]. Hausken, K. *Game Theoretic Analysis of Two Period Dependent Degraded Multistate Reliability Systems*. International Game Theory Review, Forthcoming.
- [35]. Hausken, K. *Protecting Complex Infrastructures Against Multiple Strategic Attackers*.

- International Journal of Systems Science, 2011; 42(1): 11-29.
- [36]. Hausken, K. *Strategic Defense and Attack of Series Systems when Agents Move Sequentially*. IIE Transactions, 2011; 43(7): 483-504.
 - [37]. Hausken, K. and Bier, V. *Defending Against Multiple Different Attackers*. European Journal of Operational Research, 2011; 211(2): 370-384.
 - [38]. Hausken K, Bier V, Zhuang J. *Defending against Terrorism, Natural Disaster, and All Hazards*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 65-97.
 - [39]. Hausken, K. and Levitin, G. *Efficiency of Even Separation of Parallel Elements with Variable Contest Intensity*. Risk Analysis, 2008; 28(5): 1477-1486.
 - [40]. Hausken, K. and Levitin, G. *Minmax Defense Strategy for Complex Multi-state Systems*. Reliability Engineering & System Safety, 2009; 94(2): 577-587.
 - [41]. Hausken, K. and Levitin, G. *Protection vs. False Targets in Series Systems*. Reliability Engineering & System Safety, 2009; 94(5): 973-981.
 - [42]. Hausken, K. and Levitin, G. *Parallel Systems with Different Types of Defense Resource Expenditure under Two Sequential Attacks*. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2009; 223(1): 71-85.
 - [43]. Hausken, K. and Levitin, G. *Protection vs. False Targets in Series Systems*. Reliability Engineering & System Safety, 2009; 94(5): 973-981.
 - [44]. Hausken, K. and Levitin, G. *Protection vs. Separation in Parallel Non-Homogeneous Systems*. International Journal of Reliability and Quality Performance, 2009; 1(1): 11-28.
 - [45]. Hausken, K. and Levitin, G. *Two Sequential Attacks of a Parallel System when Defense and Attack Resources are Expendable*. International Journal of Performability Engineering, 2010; 6(4): 343-354.
 - [46]. Hausken, K. and Levitin, G. *Defence of Homogeneous Parallel Multi-State Systems Subject to Two Sequential Attacks*. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2010; 224(3): 171-183.
 - [47]. Hausken, K. and Levitin, G. *Active vs. Passive Defense against a Strategic Attacker*. International Game Theory Review, Forthcoming.
 - [48]. Hausken, K. and Levitin, G. *Optimizing Structure of Parallel Homogeneous Systems under Attack*. International Journal of Performability Engineering, 2012; 8(1): 21-33.
 - [49]. Hausken, K. and Levitin, G. *Shield vs. Sword Resource Distribution in K-round Duels*. Central European Journal of Operations Research, Forthcoming.
 - [50]. Hausken, K. and Zhuang, J. *Defending Against a Terrorist Who Accumulates Resources*. Military Operations Research, 2011; 16(1): 21-39.
 - [51]. Hausken, K. and Zhuang, J. *Governments' and Terrorists' Defense and Attack in a T-period Game*. Decision Analysis, 2011; 8(1): 46-70.
 - [52]. Hausken, K. and Zhuang, J. *The Timing and Deterrence of Terrorist Attacks due to Exogenous Dynamics*. Journal of the Operational Research Society, Forthcoming.
 - [53]. He, F. and Zhuang, J. *Modeling 'Contracts' between Terrorist Groups and Governments in a Sequential Game*. Journal of the Operational Research Society, Forthcoming.
 - [54]. Jiang L., Anantharam, V., and Walrand, J. *How Bad Are Selfish Investments in Network Security?* IEEE-ACM Transactions on Networking, 2011; 19(2): 549-560.
 - [55]. Kanturska, U., Schmöcker, J.D., Fonzone, A., Bell, M.G.H. *Improving Reliability through Multi-Path Routing and Link Defence: An Application of Game Theory to Transport*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 199-227.
 - [56]. Kaplan, E., Kress, M. and Szechtman, R. *Confronting Entrenched Insurgents*. Operations Research, 2010; 58(2): 329-341.
 - [57]. Levitin G. *Optimizing Defense Strategies for Complex Multi-State Systems*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 33-64.
 - [58]. Levitin, G. *Optimal Defense Strategy Against Intentional Attacks*. IEEE Transactions on Reliability, 2007; 56(1): 148-156.
 - [59]. Levitin, G. *Optimal distribution of constrained resources in bi-contest detection-impact*

- game. *International Journal of Performability Engineering*, 2009; 5(1): 45-54.
- [60]. Levitin, G. *False targets in defense strategies against intentional attacks*. *International Journal of Performability Engineering*, 2009; 5(5): 433-446.
 - [61]. Levitin, G. and Ben Haim, H. *Importance of protections against intentional attacks*. *Reliability Engineering & System Safety*, 2008; 93(4): 639-646.
 - [62]. Levitin, G., Gertsbakh, I., and Shpungin, Y. *Evaluating the damage associated with the intentional network disintegration*. *Reliability Engineering & System Safety*, 2011; 96(4): 433-439.
 - [63]. Levitin, G. and Hausken, K. *Protection vs. Redundancy in Homogeneous Parallel Systems*. *Reliability Engineering & System Safety*, 2008; 93(10): 1444-1451.
 - [64]. Levitin, G. and Hausken, K. *Parallel Systems under Two Sequential Attacks*. *Reliability Engineering & System Safety*, 2009; 94(3): 763-772.
 - [65]. Levitin, G. and Hausken, K. *Redundancy vs. Protection vs. False Targets for Systems under Attack*. *IEEE Transactions on Reliability*, 2009; 58 (1): 58-68.
 - [66]. Levitin, G. and Hausken, K. *False Targets Efficiency in Defense Strategy*. *European Journal of Operational Research*, 2009; 194(1): 155-162.
 - [67]. Levitin, G. and Hausken, K. *False Targets vs. Redundancy in Homogeneous Parallel Systems*. *Reliability Engineering & System Safety*, 2009; 94(2): 588-595.
 - [68]. Levitin, G. and Hausken, K. *Intelligence and Impact Contests in Systems with Fake Targets*. *Defense and Security Analysis*, 2009; 25(2): 157-173.
 - [69]. Levitin, G. and Hausken, K. *Intelligence and Impact Contests in Systems with Redundancy, False Targets, and Partial Protection*. *Reliability Engineering & System Safety*, 2009; 94(12): 1927-1941.
 - [70]. Levitin, G. and Hausken, K. *Meeting a Demand vs. Enhancing Protections in Homogeneous Parallel Systems*. *Reliability Engineering & System Safety*, 2009; 94(11): 1711-1717.
 - [71]. Levitin, G. and Hausken, K. *Redundancy vs. Protection in Defending Parallel Systems Against Unintentional and Intentional Impacts*. *IEEE Transactions on Reliability*, 2009; 58(4): 679-690.
 - [72]. Levitin, G. and Hausken, K. *Separation in homogeneous systems with independent identical elements*. *European Journal of Operational Research*, 2010; 203: 625-634.
 - [73]. Levitin, G. and Hausken, K. *Defence and attack of systems with variable attacker system structure detection probability*. *Journal of the Operational Research Society*, 2010; 61(1): 124-133.
 - [74]. Levitin, G. and Hausken, K. *Influence of Attacker's Target Recognition Ability on Defense Strategy in Homogeneous Parallel Systems*. *Reliability Engineering & System Safety*, 2010; 95(5): 565-572.
 - [75]. Levitin, G. and Hausken, K. *Preventive Strike vs. Protection in Defense Strategy*. *Military Operations Research*, 2010; 15(3): 5-15.
 - [76]. Levitin, G. and Hausken, K. *Resource Distribution in Multiple Attacks against a Single Target*. *Risk Analysis*, 2010; 30(8): 1231-1239.
 - [77]. Levitin, G. and Hausken, K. *K-Round Duel with Uneven Resource Distribution*. *International Journal of Performability Engineering*, 2012; 8(1): 5-20.
 - [78]. Levitin, G. and Hausken, K. *Defense Resource Distribution between Protection and Redundancy for Constant Resource Stockpiling Pace*. *Risk Analysis*, Forthcoming.
 - [79]. Levitin, G. and Hausken, K. *Individual vs. Overarching Protection against Strategic Attacks*. *Journal of the Operational Research Society*, Forthcoming.
 - [80]. Levitin, G. and Hausken, K. *Parallel Systems under Two Sequential Attacks with Contest Intensity Variation*. *Central European Journal of Operations Research*, Forthcoming.
 - [81]. Levitin, G. and Hausken, K. *Preventive strike vs. false targets and protection in defense strategy*. *Reliability Engineering & System Safety*, 2011; 96(8): 912-924.
 - [82]. Levitin, G. and Hausken, K. *Preventive strike vs. false targets in defense strategy*. *International Journal of Performability Engineering*, Forthcoming.
 - [83]. Levitin, G. and Hausken, K. *Resource Distribution in Multiple Attacks with Imperfect Detection of the Attack Outcome*. *Risk Analysis*, Forthcoming.
 - [84]. Levitin, G., Hausken, K., and Ben Haim, H. *Active and Passive Defense Against Multiple*

- Attack Facilities*. Asia-Pacific Journal of Operational Research, 2011; 28(4): 431-444.
- [85]. Lin, F.Y.-S., Tsang, P.H. and Lin, Y.L. *Near Optimal Protection Strategies against Targeted Attacks on the Core Node of a Network*. Proc. ARES'07, 2007.
 - [86]. Lin, F.Y.-S., Wang, Y.-S., and Tsang, P.-H. *Efficient defense strategies to minimize attackers' success probabilities in honeynet*. Sixth International Conference on Information Assurance and Security (IAS), Atlanta, USA, 2010; 80-85.
 - [87]. Lin, F.Y.-S., Wang, Y.-S., and Tsang, P.-H., and Lo, J.-P. *Redundancy and Defense Resource Allocation Algorithms to Assure Service Continuity against Natural Disasters and Intelligent Attacks*. International Conference on Broadband, Wireless Computing, Communication and Applications, 2010; 206-213.
 - [88]. Michaud, D. and Apostolakis, G. *Methodology for Ranking the Elements of Water-Supply Networks*. Journal of Infrastructure Systems, 2006; 12(4): 230-242.
 - [89]. Murray, A.T., Matisziw, T.C., and Grubestic, T.H. *Critical network infrastructure analysis: interdiction and system flow*. Journal of Geographical Systems, 2007; 9(2): 103-117.
 - [90]. Okpara, U. and Bier, V.M. *Securing Passenger Aircraft from the Threat of Man-Portable Air Defense Systems (MANPADS)*. Risk Analysis, 2008; 28(6): 1583-1599.
 - [91]. Pate-Cornell, M.E. *Probabilistic Risk Analysis Versus Decision Analysis: Similarities, Differences and Illustrations*. Uncertainty and Risk: Mental, Formal, Experimental Representations: Book Series: Theory and Decision Series C Game Theory Mathematical Programming and Operations Research, 2007; 41, 223-242.
 - [92]. Paté-Cornell, M.E., Garber, R., Guikema, S., Kucik, P. *Games and Risk Analysis: Three Examples of Single and Alternate Moves*. In: Bier, V.M. and Azaiez, M.N. (eds.), Game Theoretic Risk Analysis of Security Threats, Springer, New York, 2009; 147-173.
 - [93]. Paté-Cornell, M.E. and Guikema, S.D. *Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures*. Military Operations Research, 2002; 7(4): 5-23.
 - [94]. Patterson, S. and Apostolakis, G. *Identification of Critical Locations Across Multiple Infrastructures for Terrorist Actions*. Reliability Engineering & System Safety, 2007; 92(9): 1183-1203.
 - [95]. Peng, R, Levitin, G., Xie, M., and Ng, S.H. *Defending simple series and parallel systems with imperfect false targets*. Reliability Engineering & System Safety, 2010; 95(6): 679-688.
 - [96]. Peng, R, Levitin, G., Xie, M., and Ng, S.H. *Optimal defense of single object with imperfect false targets*. Journal of the Operational Research Society, 2010; 62(1): 134-141.
 - [97]. Powell, R. *Allocating defensive resources with private information about vulnerability*. American Political Science Review 2007; 101(4): 799-809.
 - [98]. Ramirez-Marquez, J.E. Rocco, C.M., and Levitin, G. *Optimal Network Protection Against Diverse Interdictor Strategies*. Reliability Engineering & System Safety, 2011; 96(3): 374-382.
 - [99]. Rosoff, H. and von Winterfeldt, D. *A risk and economic analysis of dirty bomb attacks on the ports of Los Angeles and long beach*. Risk Analysis, 2007; 27(3), 533-546.
 - [100]. Salazar, D., Rocco, C.M., and Zio, E. *Optimal protection of complex networks exposed to a terrorist hazard: a multi-objective evolutionary approach*. Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2008; 222(3): 327-335.
 - [101]. Sandler, T. *What Do Transnational Terrorists Target? Has It Changed? Are We Safer?* Journal of Conflict Resolution, 2010; 54(2): 214-236.
 - [102]. Sandler, T. *New frontiers of terrorism research: An introduction*. Journal of Peace Research, 2011; 48(3); 279-286.
 - [103]. Sandler, T. and Siqueira, K. *Global terrorism: Deterrence versus pre-emption*. Canadian Journal of Economics, 2006; 39(4): 1370-1387.
 - [104]. Sandler, T. and Siqueira, K. *Games and Terrorism*. Simulation & Gaming, 2009; 40(2): 164-192.
 - [105]. Siqueira, K. and Sandler, T. *Terrorist networks, support, and delegation*. Public Choice, 2010; 142(1-2): 237-253.

- [106]. Tsang, P.H., Lin, F.Y.S., and Chen, C.W. *Maximization of Network Survival Time in the Event of Intelligent and Malicious Attacks*. IEEE International Conference on Communications (ICC 2008), Beijing, China, May 19-23, 2008.
- [107]. von Winterfeldt, D. and O'Sullivan, T. *Should we protect commercial airplanes against surface-to-air missile attacks by terrorists?* Decision Analysis, 2006; 3(2): 63-75.
- [108]. Wang, X., Guan, S., and Heng Lai, C. *Protecting infrastructure networks from cost-based attacks*. New Journal of Physics, 2009; 11(3): 033006.
- [109]. Wang, L., Ren, S., Yue, K., and Kwiat, K. *Optimal resource allocation for protecting system availability against random cyber attacks*. 3rd International Conference on Computer Research and Development (ICCRD), Shanghai, 2011; 477 – 482.
- [110]. Wang, X. and Zhuang, J. *Balancing Congestion and Security in the Presence of Strategic Applicants with Private Information*. European Journal of Operational Research, 2011; 212(1): 100-111.
- [111]. Zhang, J., Shen, S., and Yang, R. *The impacts of adaptive attacking and defending strategies on mitigation of intentional threats*. Kybernetes, 2010; 39(5): 825 – 837.
- [112]. Zhang, L.J., Wang, W., Guo, L., Yang, W. and Yang, Y.T. *A Survivability Quantitative Analysis Model for Network System Based on Attack Graph*. International Conference on Machine Learning and Cybernetics, 2007; 6(issue): 3211-3216.
- [113]. Zhuang, J. and Bier, V.M. *Balancing Terrorism and Natural Disasters—Defensive Strategy with Endogenous Attacker Effort*. Operations Research, 2007; 55(5): 976-991.
- [114]. Zhuang, J., Bier, V.M. and Alagoz, O. *Modeling Secrecy and Deception in a Multiple-period Attacker-Defender Signaling Game*. European Journal of Operational Research, 2010; 203(2): 409-418.
- [115]. Zhuang, J. and Bier, V.M. *Reasons for Secrecy and Deception in Homeland-Security Resource Allocation*. Risk Analysis, 2010; 30(12): 1737-1743.
- [116]. Zhuang, J. and Bier, V.M. *Secrecy and Deception at Equilibrium, with Applications to Anti-Terrorism Resource Allocation*. Defence and Peace Economics, 2011; 22(1): 43-61.
- [117]. Bier, V.M., Gratz, E.R., Haphuriwat, N., Magua, W. and Wierzbicki, K.R. *Methodology for Identifying Near-optimal Interdiction Strategies for a Power Transmission System*. Reliability Engineering and System Safety, 2007; 92(9): 1155-1161.
- [118]. Bier, V.M. and Hausken, K. *Endogenizing the Sticks and Carrots: Modeling Perverse Effects of Counterterrorism Measures*. Annals of Operations Research, 2011; 186(1): 39-59.
- [119]. Nganje, W., Bier, V.M., Lin, H.-H., and Zach, L. *Models of Interdependent Security along the Milk Supply Chain*. American Journal of Agricultural Economics, 2008; 90(5): 1265-1271.
- [120]. Hausken, K. *Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment*. Journal of Accounting and Public Policy, 2006; 25(6): 629-665.
- [121]. Hausken, K. *Information Sharing among Firms and Cyber Attacks*. Journal of Accounting and Public Policy, 2007; 26(6): 639-688.
- [122]. Hausken, K. *Security Investment and Information Sharing for Defenders and Attackers of Information Assets and Networks*, in Rao, H.R. and Upadhyaya, S.J. (eds.), Information Assurance, Security and Privacy Services, Handbooks in Information Systems, Volume 4, Emerald Group Pub Ltd, United Kingdom, 2009; 503-534.
- [123]. Hausken, K. *Whether to Attack a Terrorist's Resource Stock Today or Tomorrow*. Games and Economic Behavior, 2008; 64(2): 548–564.
- [124]. Zhuang, J. *Impacts of Subsidized Security on Stability and Total Social Costs of Equilibrium Solutions in an N-Player Game with Errors*. The Engineering Economist, 2010; 55(2): 131-149.
- [125]. Zhuang, J., Bier, V.M. and Gupta, A. *Subsidies in Interdependent Security with Heterogeneous Discount Rates*. The Engineering Economist, 2007; 52(1):1-19.
- [126]. Nikoofal, M. and Zhuang, J. *Robust Allocation of a Defensive Budget Considering an Attacker's Private Information*. Risk Analysis, forthcoming.
- [127]. Golany, B., Kress, M., Penn, M., and Rothblum, U.G. *Network optimization models for resource allocation in developing military counter measures*. Operations Research, forthcoming.

- [128]. Kunreuther, H. and Heal, G. *Interdependent security*. The Journal of Risk and Uncertainty, 2003; 26(2/3): 231-249.
- [129]. Reniers, G. and Soudan, K. *A game-theoretical approach for reciprocal security-related prevention investment decisions*. Reliability Engineering and System Safety, 2010; 95(1): 1-9.

Authors' biographies are given at the end of previous paper (on p.354) of this issue.