Active cyber defense with denial and deception: A cyber-wargame experiment

DOI: 10.1016/j.cose.2013.03.015
Computers and Security, 2013, 37, 72-77.

#	Paper	IF	Citations
29	The triptych of cyber security: A classification of active cyber defence. **2014**,		5
28	Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Translational Research in Oral Oncology*, **2015**, tyv003	3.8	13
27	Scientometric Analysis of Chinese Cyber-Denial and Deception Research. *International Journal of Cyber Warfare and Terrorism*, **2015**, 5, 15-58	0.3	
26	Proactive Damage Assessment of Cyber Attacks Using Mobile Observer Agents. **2017**,		2
25	Formally modeling deceptive patches using a game-based approach. *Computers and Security*, **2018**, 75, 182-190	4.9	4
24	Adaptive artificial immune networks for mitigating DoS flooding attacks. *Swarm and Evolutionary Computation*, **2018**, 38, 94-108	9.8	55
23	Deception Techniques in Computer Security. *ACM Computing Surveys*, **2018**, 51, 1-36	13.4	24
22	From Cyber-Security Deception to Manipulation and Gratification Through Gamification. *Lecture Notes in Computer Science*, **2019**, 99-114	0.9	1
21	Cyber Defence in Articles on WoK. **2019**,		
20	Hierarchical multistage Gaussian signaling games in noncooperative communication and control systems. *Automatica*, **2019**, 107, 9-20	5.7	14
19	A Markov Multi-Phase Transferable Belief Model for Cyber Situational Awareness. *IEEE Access*, **2019**, 7, 39305-39320	3.5	10
18	. **2019**,		0
17	Influence of Network Size on Adversarial Decisions in a Deception Game Involving Honeypots. *Frontiers in Psychology*, **2020**, 11, 535803	3.4	6
16	Adaptive Autonomous Secure Cyber Systems. **2020**,		0
15	A review of threat modelling approaches for APT-style attacks. *Heliyon*, **2021**, 7, e05969	3.6	11
14	HackIt: A Real-Time Simulation Tool for Studying Real-World Cyberattacks in the Laboratory. **2020**, 949-959		7
13	Improving cybersecurity hygiene through JIT patching. **2020**,		3

12	Cyber Counterdeception: How to Detect Denial & Deception (D&D). *Advances in Information Security*, **2015**, 103-140	0.7	1
11	Exercising Cyber-D&D. *Advances in Information Security*, **2015**, 83-92	0.7	
10	Software Engineering of Deceptive Software and Systems. **2016**, 189-213		
9	Strategic Learning for Active, Adaptive, and Autonomous Cyber Defense. **2020**, 205-230		1
8	The impact of attacks on urban services II: Reverberating effects of damage to water and wastewater systems on infectious disease. *International Review of the Red Cross*, 1-33	0.3	0
7	Influence of Probing Action Costs on Adversarial Decision-Making in a Deception Game. *Lecture Notes in Networks and Systems*, **2022**, 649-658	0.5	
6	Designing effective masking strategies for cyberdefense through human experimentation and cognitive models. *Computers and Security*, **2022**, 117, 102671	4.9	2
5	A-DEMO: ATT&CK Documentation, Emulation and Mitigation Operations. **2021**,		0
4	Table_1.DOCX. **2020**,		
3	Table_2.XLSX. **2020**,		
2	Shaping Attacker Behavior: Evaluation of an Enhanced Cyber Maneuver Framework. *Lecture Notes in Computer Science*, **2022**, 358-379	0.9	
1	Relativity Approach to the Strategic Cyber Conflict Management in Businesses.		0