Nineteen national cyber security strategies

DOI: 10.1504/ijcis.2013.051608
International Journal of Critical Infrastructures, 2013, 9, 3.

#	Paper	IF	Citations
57	Current cyber security threats and challenges in critical infrastructures protection. **2013**,		8
56	Cyber Conflict Bibliography. *SSRN Electronic Journal*, **2013**,	1	1
55	Adaptive Responses to Cyberterrorism. **2014**, 175-195		
54	An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications*, **2015**, 9, 13-20	2	9
53	Cyber Conflict Bibliography, 2015 Update. *SSRN Electronic Journal*, **2015**,	1	2
52	Adaptation of the JDL Model for Multi-Sensor National Cyber Security Data Fusion. *International Journal of Cyber Warfare and Terrorism*, **2016**, 6, 17-30	0.3	2
51	Was macht Cyber? Epistemologie und Funktionslogik von Cyber. *Zeitschrift F Auen- Und Sicherheitspolitik*, **2016**, 9, 213-222	0.1	2
50	A cybersecurity culture research philosophy and approach to develop a valid and reliable measuring instrument. **2016**,		15
49	A Second Order Cybernetic Model for Governance of Cyber Security in Enterprises. **2016**,		2
48	Mitigating Emergent Vulnerabilities in Oil and Gas Assets via Resilience. *IFIP Advances in Information and Communication Technology*, **2016**, 43-61	0.5	
47	A Strategy for a Cybersecurity Culture: A South African Perspective. *Electronic Journal of Information Systems in Developing Countries*, **2017**, 80, 1-17	1.3	13
46	Cyber Attacks, Contributing Factors, and Tackling Strategies. *International Journal of Cyber Behavior, Psychology and Learning*, **2017**, 7, 68-82	0.5	3
45	The European Network and Information Security Directive a Cornerstone of the Digital Single Market. **2018**, 287-295		2
44	A comparative study of smartphone-user security perception and preference towards redesigned security notifications. **2018**,		1
43	Cybersecurity Breach and Crisis Response: An Analysis of Organizations Official Statements in the United States and South Korea. *International Journal of Business Communication*, **2018**, 232948841877703	1.5	5
42	The Evolution of German Cybersecurity Strategy. *SpringerBriefs in Cybersecurity*, **2018**, 15-29	0.2	1
41	Is the responsibilization of the cyber security risk reasonable and judicious?. *Computers and Security*, **2018**, 78, 198-211	4.9	19

40	Interoperability for Disaster Relief Operations in Smart City Environments. **2019**,		3
39	Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human Computer Studies*, **2019**, 131, 169-187	4.6	25
38	Dynamics of State Modernization in Colombia: The Virtuous Cycle of Military Transformation. *Democracy and Security*, **2019**, 15, 75-104	0.4	6
37	Managing cyber risk in supply chains: a review and research agenda. *Supply Chain Management*, **2019**, 25, 223-240	10	39
36	Chapter 1. **2019**, 1-31		
35	Design principles for national cyber security sensor networks: Lessons learned from small-scale demonstrators. **2019**,		1
34	Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management*, **2019**, 24, 215-240	10	35
33	Cyber Security Responsibilization: An Evaluation of the Intervention Approaches Adopted by the Five Eyes Countries and China. *Public Administration Review*, **2020**, 80, 577-589	5.8	4
32	Lean Six Sigma and Industry 4.0 integration for Operational Excellence: evidence from Italian manufacturing companies. *Production Planning and Control*, **2020**, 1-18	4.3	46
31	Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation. *Risk Analysis*, **2021**,	3.9	5
30	Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, **2021**, 8,	2.8	2
29	Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Management*, **2021**, ahead-of-print,	10	5
28	Examining the relationship between e-government development, nations' cyber-security commitment, business usage and economic prosperity: a cross-country analysis. *Information and Computer Security*, **2021**, ahead-of-print,	1.4	2
27	Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures. *ACM Transactions on Management Information Systems*, **2021**, 12, 1-29	2	2
26	Achieving a Security Culture. **2022**, 233-261		
25	National Cybersecurity Strategies. **2022**, 500-513		
24	National Cybersecurity Strategies. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, **2021**, 84-102	0.2	
23	Twenty-five years of cyber threats in the news: a study of Swedish newspaper coverage (1995–2019). *Translational Research in Oral Oncology*, **2021**, 7,	3.8	0

22	Achieving a Security Culture. *Advances in Information Security, Privacy, and Ethics Book Series*, **2019**, 72-100	0.3	8
21	Cybersecurity Culture: An Ill-Defined Problem. *IFIP Advances in Information and Communication Technology*, **2017**, 98-109	0.5	6
20	A Social Cyber Contract Theory Model for Understanding National Cyber Strategies. *Lecture Notes in Computer Science*, **2017**, 166-176	0.9	
19	SAME THREAT, DIFFERENT ANSWERS? COMPARING AND ASSESSING NATIONAL CYBER DEFENCE STRATEGIES IN CENTRAL-EASTERN EUROPE. *Security and Defence Quarterly*, **2017**, 16, 52-74	0.2	
18	Das Konzept von Situationsbewusstsein und Cyber-Lagebildern. **2018**, 1-41		1
17	Organisations□bergreifender Austausch sicherheitsrelevanter Informationen als Grundlage f□ Cyber-Lagebilder. **2018**, 43-80		
16	Cyber Attacks, Contributing Factors, and Tackling Strategies. **2019**, 407-424		
15	Adaptation of the JDL Model for Multi-Sensor National Cyber Security Data Fusion. **2019**, 92-107		
14	Managing Cyber Risk in Supply Chains: A Review and Research Agenda. *SSRN Electronic Journal*,	1	2
13	Cyber Attacks, Contributing Factors, and Tackling Strategies. **2019**, 20-37		0
12	Adaptation of the JDL Model for Multi-Sensor National Cyber Security Data Fusion. **2019**, 311-326		
11	Cyber Attacks, Contributing Factors, and Tackling Strategies. **2019**, 60-77		
10	Using Datasets from Industrial Control Systems for Cyber Security Research and Education. *Lecture Notes in Computer Science*, **2020**, 122-133	0.9	
9	Analytical Framework for National Cyber-security and Corresponding Critical Infrastructure: A Pragmatistic Approach. **2020**,		
8	Revisiting □Cyber□ Definition. *Advances in Information Security, Privacy, and Ethics Book Series*, **2020**, 1-17	0.3	
7	A holonic architecture for the supply chain performance in industry 4.0 context. *International Journal of Logistics Research and Applications*, 1-28	3.8	0
6	The United States, States and the False Claims of the End of the Global Internet. **2021**, 1-42		
5	G7 □KELERN□N S□BER G□VENL□K PERFORMANSLARININ ANAL□□ ENTROP□ TABANLI MABAC Y□NTEM□□E B□R UYGULAMA. *G□venlik Bilimleri Dergisi*, 263-286	0	

4	Attributes impacting cybersecurity policy development: An evidence from seven nations. *Computers and Security*, **2022**, 120, 102820	4.9	0
3	Estrategias de ciberseguridad en los paises latinoamericanos un an sis comparativo. **2022**, 89-104		0
2	Building cybersecurity capacity: a framework of analysis for national cybersecurity strategies. 1-24		0
1	Conceptual Mapping of the Cybersecurity Culture to Human Factor Domain Framework. **2023**, 729-742		0