Citation Report
List of articles citing

Cyber Threats

DOI: 10.1093/acprof:oso/9780195385014.001.0001
, 2009, , .

#	Paper	IF	Citations
55	Information security issues in higher education and institutional research. *New Directions for Institutional Research*, **2010**, 2010, 23-49	0.2	3
54	Combating cybercrime across the Taiwan Strait: investigation and prosecution issues. *Australian Journal of Forensic Sciences*, **2012**, 44, 5-14	1.1	1
53	Categorization and legality of autonomous and remote weapons systems. *International Review of the Red Cross*, **2012**, 94, 627-652	0.3	15
52	Patrol officersVperceived role in responding to cybercrime. *Policing*, **2012**, 35, 165-181	1.4	47
51	Introduction. 3-23		
50	Regulatory effectiveness IV: third-party interference and disruptive externalities. 342-368		
49	Identifying high-cardinality hosts from network-wide traffic measurements. **2013**,		2
48	Modelling and Simulation: Cyber War. *Procedia Technology*, **2013**, 10, 987-997		3
47	Assessing officer perceptions and support for online community policing. *Security Journal*, **2013**, 26, 349-366		12
46	The Role of Cloudlets in Hostile Environments. *IEEE Pervasive Computing*, **2013**, 12, 40-49	1.3	143
45	Formal and informal modalities for policing cybercrime across the Taiwan Strait. *Policing and Society*, **2013**, 23, 540-555	1.6	7
44	Legal challenges tocyber security institutions. 308-322		
43	Megatrends and Grand Challenges of Cybercrime and Cyberterrorism Policy and Research. *Advanced Sciences and Technologies for Security Applications*, **2016**, 3-15	0.6	2
42	Challenges Priorities and Policies: Mapping the Research Requirements of Cybercrime and Cyberterrorism Stakeholders. *Advanced Sciences and Technologies for Security Applications*, **2016**, 39-51	0.6	
41	Identifying High-Cardinality Hosts from Network-Wide Traffic Measurements. *IEEE Transactions on Dependable and Secure Computing*, **2016**, 13, 547-558	3.9	21
40	Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice*, **2017**, 33, 212-233	1.7	34
39	On the Value of Honeypots to Produce Policy Recommendations. *Criminology and Public Policy*, **2017**, 16, 739-747	3	11

38	The network structure of malware development, deployment and distribution. *Global Crime*, **2017**, 18, 49-69	1.4	13
37	Field, Frame and Focus. 112-172		2
36	From Simulations to Simulacra of War: Game Scenarios in Cyberwar Exercises. *Journal of War and Culture Studies*, **2018**, 11, 22-37	0.4	2
35	Assessing the Macro-Level Correlates of Malware Infections Using a Routine Activities Framework. *International Journal of Offender Therapy and Comparative Criminology*, **2018**, 62, 1720-1741	1.3	21
34	Corporate Social Responsibility in Times of Internet (In)security. **2019**, 237-250		1
33	Malicious Spam Distribution: A Routine Activities Approach. *Deviant Behavior*, **2020**, 1-17	1.1	7
32	Cambridge Studies in International and Comparative Law. **2020**, 514-522		
31	Does International Law Matter in Cyberspace?. **2020**, 1-50		1
30	Attribution. **2020**, 51-190		0
29	Attribution to a Machine or a Human: A Technical Process. **2020**, 55-86		
28	The Question of Evidence: From Technical to Legal Attribution. **2020**, 87-110		
27	Attribution to a State. **2020**, 111-188		
26	Part I Conclusion. **2020**, 189-190		
25	The Lawfulness of Cyber Operations. **2020**, 191-378		
24	Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law. **2020**, 193-272		
23	The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack. **2020**, 273-342		1
22	Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations. **2020**, 343-352		
21	Cyber Operations and the Principle of Due Diligence. **2020**, 353-376		

20	Part II Conclusion. **2020**, 377-378		
19	Remedies against State-Sponsored Cyber Operations. **2020**, 379-492		
18	State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation. **2020**, 381-422		
17	Measures of Self-Help against State-Sponsored Cyber Operations. **2020**, 423-490		0
16	Part III Conclusion. **2020**, 491-492		
15	Table Assessing the Lawfulness of Cyber Operations and Potential Responses. **2020**, 499-501		
14	Select Bibliography. **2020**, 502-508		
13	Index. **2020**, 509-513		
12	Conclusion. **2020**, 493-498		
11	Using Machine Learning to Examine Cyberattack Motivations on Web Defacement Data. *Social Science Computer Review*, 089443932199423	3.1	1
10	Examining the crime prevention claims of crime prevention through environmental design on system-trespassing behaviors: a randomized experiment. *Security Journal*, 1	1	1
9	Fog in the Fifth Dimension: The Ethics of Cyber-War. *Law, Governance and Technology Series*, **2014**, 3-23	0	1
8	Subcultural Theories of Crime. **2019**, 1-14		1
7	Cyber Operations and International Law. **2020**,		39
6	Cyber War: Do We Have the Right Mindset?. **2017**, 1-22		
5	Cyberwar and Cyberpeace. **2017**, 1-25		
4	Formal and informal modalities for policing cybercrime across the Taiwan Strait. **2017**, 132-147		
3	Cyberwar and Cyberpeace. **2018**, 885-909		

2	Cyber War: Do We Have the Right Mindset?. **2018**, 787-808	
1	Subcultural Theories of Crime. **2020**, 513-526	2