Cyber attacks, self-defence and the problem of attribution

DOI: 10.1093/jcsl/krs019

Journal of Conflict and Security Law, 2012, 17, 229-244.

#	Paper	IF	Citations
77	Cyber Conflict Bibliography. *SSRN Electronic Journal*, **2013**,	1	1
76	The □riptych of cyber security□A classification of active cyber defence. **2014**,		5
75	The Tallinn Manual on the International Law Applicable to Cyber Warfare: A Commentary on Chapter II□The Use of Force. **2014**, 19-43		7
74	Cyber Conflict Bibliography, 2015 Update. *SSRN Electronic Journal*, **2015**,	1	2
73	Attributing Cyber Attacks. *Journal of Strategic Studies*, **2015**, 38, 4-37	1	215
72	Predicting the trajectory of the evolving international cyber regime: Simulating the growth of a social network. *Social Networks*, **2015**, 41, 72-84	3.9	1
71	How to Think About Cyber Conflicts Involving Non-state Actors. *Philosophy and Technology*, **2015**, 28, 427-448	3.6	3
70	Cyber Operations and International Law: An Interventionist Legal Thought. *SSRN Electronic Journal*, **2016**,	1	12
69	The Law of Self-Defence and the New Argumentative Landscape on the Expansionists□Side. *Leiden Journal of International Law*, **2016**, 29, 43-65	0.5	17
68	The Never-Ending Game of Cyberattack Attribution. *Advanced Sciences and Technologies for Security Applications*, **2016**, 175-192	0.6	2
67	From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, **2017**, 30, 877-899	0.5	27
66	Cyber Attacks in International Law: From Atomic War to Computer War. *SSRN Electronic Journal*, **2017**,	1	
65	Grey is the new black: covert action and implausible deniability. *International Affairs*, **2018**, 94, 477-494	0.8	40
64	A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual. *Computers and Security*, **2018**, 74, 371-383	4.9	12
63	Dilution of Self-Defence and its Discontents. **2019**, 1-13		
62	The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. **2019**,		4
61	Deterring Russian cyber warfare: the practical, legal and ethical constraints faced by the United Kingdom. *Journal of Cyber Policy*, **2019**, 4, 257-274	1	3

60	Reinterpretation or Contestation of International Law in Cyberspace?. *Israel Law Review*, **2019**, 52, 295-326	2.9	21
59	Use and Misuse of New Technologies. **2019**,		0
58	Attribution to State of Cyber Operations Conducted by Non-State Actors. **2019**, 233-255		
57	Attribution of Cyber Attacks. **2019**, 279-303		3
56	US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, **2020**, 43, 245-280	1	13
55	A practical application of game theory to optimize selection of hardware Trojan detection strategies. *Journal of Hardware and Systems Security*, **2020**, 4, 98-119	1.6	4
54	Cyber conflict or democracy hacked? How cyber operations enhance information warfare. *Translational Research in Oral Oncology*, **2020**, 6,	3.8	4
53	Under false flag: using technical artifacts for cyber attack attribution. *Cybersecurity*, **2020**, 3,	5	4
52	From secrecy to accountability: The politics of exposure in the Belgrano affair. *British Journal of Politics and International Relations*, **2020**, 22, 542-560	1.1	2
51	Cambridge Studies in International and Comparative Law. **2020**, 514-522		
50	The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios. *Journal of Military Ethics*, **2020**, 19, 20-39	0.3	0
49	Does International Law Matter in Cyberspace?. **2020**, 1-50		1
48	Attribution. **2020**, 51-190		0
47	Attribution to a Machine or a Human: A Technical Process. **2020**, 55-86		
46	The Question of Evidence: From Technical to Legal Attribution. **2020**, 87-110		
45	Attribution to a State. **2020**, 111-188		
44	Part I Conclusion. **2020**, 189-190		
43	The Lawfulness of Cyber Operations. **2020**, 191-378		

42	Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law. **2020**, 193-272		
41	The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack. **2020**, 273-342		1
40	Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations. **2020**, 343-352		
39	Cyber Operations and the Principle of Due Diligence. **2020**, 353-376		
38	Part II Conclusion. **2020**, 377-378		
37	Remedies against State-Sponsored Cyber Operations. **2020**, 379-492		
36	State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation. **2020**, 381-422		
35	Measures of Self-Help against State-Sponsored Cyber Operations. **2020**, 423-490		0
34	Part III Conclusion. **2020**, 491-492		
33	Table Assessing the Lawfulness of Cyber Operations and Potential Responses. **2020**, 499-501		
32	Select Bibliography. **2020**, 502-508		
31	Index. **2020**, 509-513		
30	Conclusion. **2020**, 493-498		
29	Attribution Across Cyber Attack Types: Network Intrusions and Information Operations. *IEEE Open Journal of the Communications Society*, **2021**, 2, 1082-1093	6.7	2
28	Digital force majeure: The Mondelez case, insurance, and the (un)certainty of attribution in cyberattacks. *Business Horizons*, **2021**,	10.1	2
27	Scalable Algorithms for Identifying Stealthy Attackers in a Game-Theoretic Framework Using Deception. **2021**, 47-61		
26	International Law As We Know It: Cyberwar Discourse and the Construction of Knowledge in International Legal Scholarship. **2021**,		0
25	Bibliography. **2021**, 213-237		

24	Appendix Chapter 5. **2021**, 179-212		
23	Index. **2021**, 238-240		
22	“The Greater Part of Jurisconsults”. **2021**, 97-126		
21	“Call Me Again If You’re Ever Ready to Begin Answering the Questions”. **2021**, 127-169		
20	Knowing International Law. **2021**, 1-25		
19	“Legal Problem-Solution” and the Cyberwar Discourse. **2021**, 26-62		
18	“Not ‘Armed Force’ in the Literal Sense”. **2021**, 63-96		
17	In Conclusion: International Law As We Know It. **2021**, 170-178		
16	Introduction: Conundrum of New Technologies in the Law of Armed Conflict. **2014**, 1-17		1
15	Cyber Operations and International Law. **2020**,		39
14	Macht im Cyberspace: Eine Übersicht der bisherigen Forschung und künftiger Perspektiven anhand des Proxy-Konzepts. *Zeitschrift Für Friedens- Und Konfliktforschung*, 1	0.2	1
13	Cyber Attacks Under the United Nations Charter. Critical Reflections on Consequentialist Reasoning.. *SSRN Electronic Journal*,	1	
12	NATO AND CYBER DETERRENCE. *Contemporary Military Challenges*, **2016**, 29-50	0.1	
11	The Use of Force to Prevent Recurrence of Conflict: Where are the Limits of Self-Defense?. *SSRN Electronic Journal*,	1	
10	Identifying Stealthy Attackers in a Game Theoretic Framework Using Deception. *Lecture Notes in Computer Science*, **2019**, 21-32	0.9	5
9	Demystifying the Cyber Attribution: An Exploratory Study. **2020**,		0
8	Malicious Cyber Operations, “Hackbacks” and International Law: An Austrian Example as a Basis for Discussion on Permissible Responses. *Masaryk University Journal of Law and Technology*, **2020**, 14, 227-258	0.6	
7	NATO IN THE NEW STRATEGIC ENVIRONMENT: CYBER ATTACKS NOW COVERED BY ARTICLE 5 OF THE NORTH ATLANTIC TREATY. *Studia Bezpieczeństwa Narodowego*, **2014**, 6, 397-418	0	2

6	Cyber-attacks an unlawful use of digital technologies. **2022**, 40-50	0.3
5	Democracy and cyberconflict: how regime type affects state-sponsored cyberattacks. *Journal of Cyber Policy*, 1-23	1
4	Contributing to Cyber Peace by Maximizing the Potential for Deterrence. **2022**, 131-153	
3	Positioning Diplomacy Within a Strategic Response to the Cyber Conflict Threat. *Lecture Notes in Computer Science*, **2022**, 131-152	0.9
2	Skepticism, Self-Defense/Help and Global Justice. **2023**, 37-82	0
1	A sliding scale of secrecy: toward a better understanding of the role of publicity in offensive cyber operations. 1-19	0