# Cyber Security without Cyber War

DOI: 10.1093/jcsl/krs017
Journal of Conflict and Security Law, 2012, 17, 187-209.

| # | Paper | IF | Citations |
|---|---|---|---|
| 95 | Toward criteria for international cyber weapons bans. **2013**, | | 1 |
| 94 | Cyber Conflict Bibliography. *SSRN Electronic Journal*, **2013**, | 1 | 1 |
| 93 | Cyberspace and International Relations. **2014**, | | 9 |
| 92 | US Policy on Active Cyber Defense. *Journal of Homeland Security and Emergency Management*, **2014**, 11, | 1.2 | 8 |
| 91 | Legal challenges tocyber security institutions. 308-322 | | |
| 90 | Cyber Conflict Bibliography, 2015 Update. *SSRN Electronic Journal*, **2015**, | 1 | 2 |
| 89 | References. 219-281 | | |
| 88 | NATO's cyber defence: strategic challenges and institutional adaptation. *Defence Studies*, **2015**, 15, 297-319 | 0.7 | 12 |
| 87 | 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 |
| 86 | How to Think About Cyber Conflicts Involving Non-state Actors. *Philosophy and Technology*, **2015**, 28, 427-448 | 3.6 | 3 |
| 85 | Cyber warfare: Issues and challenges. *Computers and Security*, **2015**, 49, 70-94 | 4.9 | 46 |
| 84 | Developing Norms for Cyber Conflict. *SSRN Electronic Journal*, **2016**, | 1 | |
| 83 | The EU, Strategy and Security Policy. **2016**, | | 13 |
| 82 | On the Risks of Relying on Analogies to Understand Cyber Conflicts. *Minds and Machines*, **2016**, 26, 317-321 | 1.9 | 17 |
| 81 | The ethics of hacking back. **2016**, | | 2 |
| 80 | Review on information security, laws and ethical issues with online financial system. **2016**, | | 0 |
| 79 | Cyberoperations and international humanitarian law. *Information and Computer Security*, **2016**, 24, 38-52 | 1.4 | 3 |

| | | | |
|---|---|---|---|
| 78 | Situation awareness in the Internet of Things. **2017**, | | 5 |
| 77 | One year after Warsaw: The growing need for a NATO cyber command. **2017**, | | |
| 76 | From the vanishing point back to the core: The impact of the development of the cyber law of war on general international law. **2017**, | | 0 |
| 75 | Cyber Attacks, Information Attacks, and Postmodern Warfare. *Baltic Journal of Law and Politics*, **2017**, 10, 63-89 | 0.1 | 8 |
| 74 | Circumscribing Cyberbullying. **2017**, 321-342 | | |
| 73 | Cyber Hygiene: The Big Picture. *Lecture Notes in Computer Science*, **2018**, 291-305 | 0.9 | 4 |
| 72 | Simplistic Approach to Detect Cybercrimes and Deter Cyber Criminals. **2018**, | | 3 |
| 71 | The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective. *Journal of Chinese Political Science*, **2019**, 24, 225-247 | 1.8 | 1 |
| 70 | Self-Defence, Pernicious Doctrines, Peremptory Norms. **2019**, 174-257 | | |
| 69 | Reinterpretation or Contestation of International Law in Cyberspace?. *Israel Law Review*, **2019**, 52, 295-326 | 2.6 | 21 |
| 68 | The Limited Exception for Self-Defence. **2019**, 152-205 | | |
| 67 | Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management*, **2019**, 24, 215-240 | 10 | 35 |
| 66 | Cambridge Studies in International and Comparative Law. **2020**, 514-522 | | |
| 65 | Does International Law Matter in Cyberspace?. **2020**, 1-50 | | 1 |
| 64 | Attribution. **2020**, 51-190 | | 0 |
| 63 | Attribution to a Machine or a Human: A Technical Process. **2020**, 55-86 | | |
| 62 | The Question of Evidence: From Technical to Legal Attribution. **2020**, 87-110 | | |
| 61 | Attribution to a State. **2020**, 111-188 | | |

60 Part I Conclusion. **2020**, 189-190

59 The Lawfulness of Cyber Operations. **2020**, 191-378

58 Internationally Wrongful Cyber Acts: Cyber Operations Breaching Norms of International Law. **2020**, 193-272

57 The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack. **2020**, 273-342 1

56 Circumstances Precluding or Attenuating the Wrongfulness of Unlawful Cyber Operations. **2020**, 343-352

55 Cyber Operations and the Principle of Due Diligence. **2020**, 353-376

54 Part II Conclusion. **2020**, 377-378

53 Remedies against State-Sponsored Cyber Operations. **2020**, 379-492

52 State Responsibility and the Consequences of an Internationally Wrongful Cyber Operation. **2020**, 381-422

51 Measures of Self-Help against State-Sponsored Cyber Operations. **2020**, 423-490 0

50 Part III Conclusion. **2020**, 491-492

49 Table Assessing the Lawfulness of Cyber Operations and Potential Responses. **2020**, 499-501

48 Select Bibliography. **2020**, 502-508

47 Index. **2020**, 509-513

46 Conclusion. **2020**, 493-498

45 Preface. **2020**, ix-x

44 Cybersecurity Incidents and International Law. **2020**, 1-42

43 The Spectre of Cyberwar. **2020**, 3-16

42 Terminology. **2020**, 17-20

41 International Legal Framework. **2020**, 21-42

40 Unilateral Remedies to Cybersecurity Incidents. **2020**, 43-258

39 Self-Defence. **2020**, 47-112

38 Countermeasures. **2020**, 113-200

37 Necessity. **2020**, 201-258

36 Outlines of an Emergency Regime for Cyberspace. **2020**, 259-284

35 Transnational Cybersecurity, Unilateral Remedies, and the Rule of Law. **2020**, 261-266

34 Such Incidents Might Recur at Any Time. **2020**, 267-271

33 Possible Elements of the Cyber Emergency Regime. **2020**, 272-281

32 Concluding Remarks. **2020**, 282-284

31 Bibliography. **2020**, 285-318

30 Index. **2020**, 319-326

29 Ethical Principles for Designing Responsible Offensive Cyber Security Training. *IFIP Advances in Information and Communication Technology*, **2021**, 21-39 0.5

28 Cyber Security In Mobile Apps And User CIA. **2021**, 0

27 A New Way of Conducting War: Cyberwar, Is That Real?. **2014**, 125-139 1

26 Geography, Territory and Sovereignty in Cyber Warfare. **2014**, 75-93 6

25 Cyber Operations and International Law. **2020**, 39

| | | | |
|---|---|---|---|
| 24 | Problems of Qualifying Crimes Under Article 273 of the Criminal Code of the Russian Federation at the Stage of Initiating Criminal Proceedings. *Russian Journal of Criminology*, **2018**, 12, 590-600 | 0.5 | 1 |
| 23 | Digital Risk Society. *SSRN Electronic Journal*, | 1 | 0 |
| 22 | Cyber Warfare. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, **2015**, 13-36 | 0.2 | 0 |
| 21 | Cybersecurity, Cyberculture, and Africa. **2016**, 107-113 | | |
| 20 | Global Encyclopedia of Public Administration, Public Policy, and Governance. **2016**, 1-9 | | |
| 19 | Warfare of the Future. *Advanced Sciences and Technologies for Security Applications*, **2018**, 171-183 | 0.6 | |
| 18 | Global Encyclopedia of Public Administration, Public Policy, and Governance. **2018**, 1270-1278 | | |
| 17 | An overview of distributed denial of service and internet of things in healthcare devices. **2020**, | | 2 |
| 16 | Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution. **2020**, | | 1 |
| 15 | Contemplating a Cyber Weapons Convention: An Exploration of Good Practice and Necessary Preconditions. *Baltic Journal of Law and Politics*, **2020**, 13, 51-80 | 0.1 | |
| 14 | Norms and Strategies for Stability in Cyberspace. *Digital Ethics Lab Yearbook*, **2020**, 31-44 | 0.2 | |
| 13 | US□China Tech Wars: Shaping Africa□s Agency. *International Political Economy Series*, **2022**, 183-203 | 0.2 | |
| 12 | Droit international et cyber-propagande. *Etudes Internationales*, **2020**, 51, 313 | 0.1 | |
| 11 | 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 |
| 10 | Cyber-attacks □an unlawful use of digital technologies. **2022**, 40-50 | 0.3 | |
| 9 | The Dimensionality of the Cyber Warrior. *Lecture Notes in Computer Science*, **2022**, 326-339 | 0.9 | |
| 8 | Positioning Diplomacy Within a□Strategic Response to□the□Cyber Conflict Threat. *Lecture Notes in Computer Science*, **2022**, 131-152 | 0.9 | |
| 7 | Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning□A Review. *Journal of Cybersecurity and Privacy*, **2022**, 2, 527-555 | 4 | 2 |

| | | |
|---|---|---|
| 6 | Who in charge and how does it work? US cybersecurity of critical infrastructure. 1-20 | 0 |
| 5 | Research Pattern of Internet of Things and its Impact on Cyber Security. **2022**, | 0 |
| 4 | Differentially Distributed Private Intelligence Security in Cybersecurity Infrastructures. **2023**, | 0 |
| 3 | Cybersecurity as Social Policy. **2022**, 2872-2879 | 0 |
| 2 | A review of cyber vigilance tasks for network defense. 4, | 0 |
| 1 | Cybernetics and battle management system (BMS) in network soldier system application. 1-23 | 0 |