DAFTAR PUSTAKA

A Review of Major Viewpoints on Cyber Sovereignty around the World. (2016). *Chinese Journal of Engineering Science*, *18*(6). https://doi.org/10.15302/j-sscae-2016.06.018

A Strategy for the Weaker Country in the Asymmetrical Military Alliance Alignment. (2020). 세계지역연구논총, *38*(1).

Abrams, S. S., & Merchant, G. (2013). The Digital Challenge. *International Handbook of Research on Children's Literacy, Learning, and Culture*, 319–332. https://doi.org/10.1002/9781118323342.ch23

Ahn, W., Chung, M., Min, B. G., & Seo, J. (2015). Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs. *International Journal of Distributed Sensor Networks*, *2015*. https://doi.org/10.1155/2015/836258

Al-Khurafi, O. B., & Al-Ahmad, M. A. (2016). Survey of Web Application Vulnerability Attacks. *Proceedings - 2015 4th International Conference on Advanced Computer Science Applications and Technologies, ACSAT 2015*. https://doi.org/10.1109/ACSAT.2015.46

Al-Shamisi, A. (2014). Active offensive cyber situational awareness: theory and practice. *PQDT - UK & Ireland*, *August*.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. In *Future Internet* (Vol. 12, Issue 10). https://doi.org/10.3390/fi12100168

Alford, L. D. J. (2001). Cyber Warfare: A New Doctrine and Taxonomy. *CrossTalk*, *April*.

Alieyan, K., Almomani, A., Manasrah, A., & Kadhum, M. M. (2017). A survey of botnet detection based on DNS. In *Neural Computing and Applications* (Vol. 28, Issue 7). https://doi.org/10.1007/s00521-015-2128-0

Allen, J. (2001). CERT System and Network Security Practices. *Carnegie Mellon University. Software Engineering Institute. CERT Coordination Center*.

Anderson, R. J. (1994). Liability and Computer Security: Nine Principles. *ESORICS '94: Proceedings of the Third European Symposium on Research in Computer Security*, *LNCS 875*, 231–245. https://doi.org/10.1007/3-540-

58618-0_67

Andone, D., & Vasiu, R. (1998). *13 Development of an ICT Open Learning Environment for Teaching Multimedia*. *McCormack*, 90–94.

Andress, J., & Winterfeld, S. (2011). Cyber Doctrine. In *Cyber Warfare*. https://doi.org/10.1016/b978-1-59749-637-7.00003-4

Andress, J., & Winterfeld, S. (2014a). Chapter 4 - Cyber Doctrine. *Cyber Warfare (Second Edition)*. https://doi.org/http://dx.doi.org/10.1016/B978-0-12-416672-1.00004-0

Andress, J., & Winterfeld, S. (2014b). Cyber Doctrine. In *Cyber Warfare*. https://doi.org/10.1016/b978-0-12-416672-1.00004-0

Anggoro, K. (2003). Keamanan Nasional, Pertahanan Negara, dan Ketertiban Umum. *Seminar Pembangunan Hukum Nasional VIII. Diselenggarakan Oleh Badan Pembinaan Hukum Nasional*.

Anwar, S. (2018). PENGUASAAN TEKNOLOGI PERTAHANAN OLEH SDM PERTAHANAN INDONESIA DALAM RANGKA MENGHADAPI PEPERANGAN MASA DEPAN. *Jurnal Pertahanan & Bela Negara*, *5*(1). https://doi.org/10.33172/jpbh.v5i1.346

Arganata, bayu faris. (2019). *Strategi Indonesia Dalam Menghadapi Konstelasi Siber Global*.

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia'S National Cyber Defense and Security To Face the Global Cyber Threats Through Indonesia Security Incident Response Team on Internet Infrastructure (Id-Sirtii). *Jurnal Pertahanan & Bela Negara*, *9*(1), 17. https://doi.org/10.33172/jpbh.v9i1.515

Arnold, A. (2013). Cyber "hostilities" and the war powers resolution. In *Military Law Review* (Vol. 217).

Arvianissa, Y. R., & Fitriani, E. (2018). Perkembangan Peninjauan Lingkungan Strategis Dalam Buku Putih Pertahanan Indonesia, 1995&2015. *Jurnal Hubungan Internasional*, *11*(1). https://doi.org/10.20473/jhi.v11i1.4760

Aslan, O., & Samet, R. (2020). A Comprehensive Review on Malware Detection Approaches. In *IEEE Access* (Vol. 8). https://doi.org/10.1109/ACCESS.2019.2963724

Aucsmith, D. (2017). Disintermediation, Counterinsurgency, and Cyber Defense. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2836100

Austin, G. (2020). Australia's Digital Skills for Peace and War. Journal of Telecommunications and the Digital Economy, 2(4). https://doi.org/10.18080/jtde.v2n4.266

Awan, I. (2017). Cyber-Extremism: Isis and the Power of Social Media. Society, 54(2). https://doi.org/10.1007/s12115-017-0114-0

Bajoghli, N. (2019). The Researcher as a National Security Threat. *Comparative Studies of South Asia, Africa and the Middle East*, *39*(3). https://doi.org/10.1215/1089201x-7885400

Bambenek, J. (2017). Nation-state attacks: the new normal. Network Security, 2017(10). https://doi.org/10.1016/S1353-4858(17)30102-2

Banks, W. (2017). Cyber espionage and electronic surveillance: Beyond the media coverage. *Emory L.J.*, *66*(513).

Barde, P. (2020). Cyber Terrorism- The Weapon Of Mass Destruction. Digital Forensics (4n6) Journal. https://doi.org/10.46293/4n6/2020.02.02.11

Barnard-Wills, D. (2011). "This is not a cyber war, it's a...?" *International Journal of Cyber Warfare and Terrorism*, *1*(1). https://doi.org/10.4018/ijcwt.2011010102

Barrett, E. T. (2013). Warfare In A New Domain: The Ethics Of Military Cyber-Operations. *Journal of Military Ethics*, *12*(1). https://doi.org/10.1080/15027570.2013.782633

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4–5). https://doi.org/10.1080/23340460.2017.1414924

Bawany, N. Z., Shamsi, J. A., & Salah, K. (2017). DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. In *Arabian Journal for Science and Engineering* (Vol. 42, Issue 2). https://doi.org/10.1007/s13369-017-2414-5

Beidleman, S. W. (2009). Defining and Deterring Cyber War. *Dept. Military Strategy Planning and Operations, U.S. Army War College*.

Bendrath, R. (2001). The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security: An International Journal*, *7*. https://doi.org/10.11610/isij.0705

Bhardwaj, A., Subrahmanyam, G. V. B., Avasthi, V., & Sastry, H. (2016). Design a resilient network infrastructure security policy framework. *Indian Journal of Science and Technology*, *9*(19). https://doi.org/10.17485/ijst/2016/v9i19/90133

Boeke, S. (2018). National cyber crisis management: Different European approaches. *Governance*, *31*(3). https://doi.org/10.1111/gove.12309

Bolla, R., Carrega, A., & Repetto, M. (2019). An abstraction layer for cybersecurity context. *2019 International Conference on Computing, Networking and Communications, ICNC 2019*. https://doi.org/10.1109/ICCNC.2019.8685665

Bolla, Raffaele, Comi, P. M., & Repetto, M. (2018). A distributed cyber-security framework for heterogeneous environments. *CEUR Workshop Proceedings*, *2058*.

Borah, C. K. (2015). Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake. *Strategic Analysis*, *39*(4). https://doi.org/10.1080/09700161.2015.1047221

Brantly, A. F. (2019). Conceptualizing cyber policy through complexity theory. *Journal of Cyber Policy*, *4*(2). https://doi.org/10.1080/23738871.2019.1583763

Burton, J. (2015). NATO's cyber defence: strategic challenges and institutional adaptation. Defence Studies, 15(4). https://doi.org/10.1080/14702436.2015.1108108

Bytheway, A. (2014). Investing in Information. Investing in Information: The Information Management Body of Knowledge, 9783319119, 1–280. https://doi.org/10.1007/978-3-319-11909-0

Cai, T. (2018). Energy Infrastructure Security in the Digital Age. *International Journal of Public Administration in the Digital Age*, *5*(2). https://doi.org/10.4018/ijpada.2018040102

Calder, A. (2013). Information Security Information Security. *Information Securiy*

& ISO 27001, *101v1.1*(February).

Campbell, P. (2018). Generals in Cyberspace: Military Insights for Defending Cyberspace. *Orbis*, *62*(2). https://doi.org/10.1016/j.orbis.2018.02.006

Canan, M., & Akil, A. (2020). A warfare domain approach to the disinformation problem. *Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020*. https://doi.org/10.34190/ICCWS.20.023

Carayannis, E. G., Campbell, D. F. J., & Efthymiopoulos, M. P. (2014). Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, opportunities and implications for theory, policy and practice. In *Cyber-Development, Cyber-Democracy and Cyber-Defense: Challenges, Opportunities and Implications for Theory*. https://doi.org/10.1007/978-1-4939-1028-1

Carías, J. F., Arrizabalaga, S., Labaka, L., & Hernantes, J. (2020). Cyber resilience progression model. *Applied Sciences (Switzerland)*, *10*(21). https://doi.org/10.3390/app10217393

Carlin, D., Burgess, J., O'Kane, P., & Sezer, S. (2020). You Could Be Mine(d): The Rise of Cryptojacking. *IEEE Security and Privacy*, *18*(2). https://doi.org/10.1109/MSEC.2019.2920585

Cartin, J. (2014). Don't Forget the Humans: Toward a 21st Century Offensive Cyber Strategy. *Global Security Studies*, *5*(2).

Carvalho, M. (2015). *Resilient Command and Control Infrastructures for Cyber Operations*. https://doi.org/10.1109/seams.2015.17

Caywood, C., Heath, R., Nelson, R. A., Coates, J., & Ewing, R. (1988). Issues Management. Corporate Public Policymaking in an Information Society. *Journal of Marketing*, *52*(2). https://doi.org/10.2307/1251270

Cempaka Timur, F. G. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. KnE Social Sciences, 2(4). https://doi.org/10.18502/kss.v2i4.893

Cebula, J. J., & Young, L. R. (2010). A Taxonomy of Operational Cyber Security Risks. Carnegie-Mellon Univ Pittsburgh Pa Software Engineering Inst, December.

Cha, S., Baek, S., Kang, S., & Kim, S. (2018). Security Evaluation Framework for Military IoT Devices. *Security and Communication Networks*, *2018*. https://doi.org/10.1155/2018/6135845

Chandler, D. (2012). Resilience and human security: The post-interventionist paradigm. *Security Dialogue*, *43*(3). https://doi.org/10.1177/0967010612444151

Chappelow, J. (2019). *Conflict Theory Definition*. Investopedia.

Chayes, A. (2015). Rethinking Warfare: The Ambiguity of Cyber Attacks. Harvard National Security Journal, 6(2).

Cheung, K. S. (2006). A comparison of webct, blackboard and moodle for the teaching and learning of continuing education courses. In Enhancing Learning through Technology. https://doi.org/10.1142/9789812772725_0018

Chiluwa, I. E. [Ed], & Samoilenko, S. A. [Ed]. (2019). Handbook of Research on Deception, Fake News, and Misinformation Online. In *IGI Global book series Advances in Media, Entertainment, and the Arts (AMEA)*.

Cho, O. H., & Kim, E. K. (2015). Design of flight stabilization system for acquisition of UAV based monitoring image. In *Lecture Notes in Electrical Engineering* (Vol. 352). https://doi.org/10.1007/978-3-662-47487-7_42

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. *Politica Vol. 10 No. 2 November 2019*, *10*(2), 113–128. https://doi.org/https://doi.org/10.22212/ jp.v10i1.1447

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. (2019). Penerapan Military Confi dence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. *Jurnal Ketahanan Nasional*, *25*(3). https://doi.org/10.22146/jkn.50344

Christian, C. (2015). Intersubjectivity and modern conflict theory. *Psychoanalytic Psychology*, *32*(4). https://doi.org/10.1037/pap0000011

Colarik, A., & Janczewski, L. (2012). Establishing Cyber Warfare Doctrine. Journal of Strategic Security, 5(1). https://doi.org/10.5038/1944-0472.5.1.3

Corn, G. P., & Taylor, R. (2017). Sovereignty in the Age of Cyber. *AJIL Unbound*, *111*. https://doi.org/10.1017/aju.2017.57

Crow, G. (2015). Race, Community and Conflict as a methodological classic. *Ethnic and Racial Studies*, *38*(3). https://doi.org/10.1080/01419870.2015.975260

Cuihong, C. (2018). Global cyber governance: China's contribution and approach. China Quarterly of International Strategic Studies, 4(1). https://doi.org/10.1142/S2377740018500069

Cybersecurity Risks: Are They Inflated? (2016). *Salus Journal*, *4*(2).

Czosseck, C., Ottis, R., & Talihärm, A.-M. (2011). Estonia after the 2007 Cyber Attacks. *International Journal of Cyber Warfare and Terrorism*, *1*(1). https://doi.org/10.4018/ijcwt.2011010103

Dada, E. G., Bassi, J. S., Chiroma, H., Abdulhamid, S. M., Adetunmbi, A. O., & Ajibuwa, O. E. (2019). Machine learning for email spam filtering: review, approaches and open research problems. *Heliyon*, *5*(6). https://doi.org/10.1016/j.heliyon.2019.e01802

Damodaran, S. K., & Mittal, S. (2017). Modeling cyber effects in cyber-physical systems with DEVS. Simulation Series, 49(4). https://doi.org/10.22360/springsim.2017.tmsdevs.039

Dawson, M. (2020). National Cybersecurity Education: Bridging Defense to Offense. *Land Forces Academy Review*, *25*(1). https://doi.org/10.2478/raft-2020-0009

Denning, D. E. (2015). Rethinking the Cyber Domain and Deterrence. *Joint Force Quarterly*, *77*(April).

De Souza, P. (2013). National cyber defense strategy. In Strategic Intelligence Management: National Security Imperatives and Information and Communications Technologies. Copyright © 2013 Elsevier Inc. All rights reserved. https://doi.org/10.1016/b978-0-12-407191-9.00018-1

Dewar, R. S. (2014). The "triptych of cyber security": A classifi cation of active

cyber defence. *International Conference on Cyber Conflict, CYCON*, *2014*. https://doi.org/10.1109/CYCON.2014.6916392

Dilisen, M. M. (2018). Sovereignty over cyber territories. *International Journal of Interdisciplinary Civic and Political Studies*, *13*(3–4). https://doi.org/10.18848/2327-0071/CGP/v13i02/1-11

Dinstein, Y. (2012). The principle of distinction and Cyber war in international armed conflicts. *Journal of Conflict and Security Law*, *17*(2). https://doi.org/10.1093/jcsl/krs015

Domingo, A., & Parmar, M. (2019). Functional Analysis of Cyberspace Operations. *Proceedings - IEEE Military Communications Conference MILCOM*, *2019-Octob*. https://doi.org/10.1109/MILCOM.2018.8599844

Dorsey, M. E., & Diaz-Barriga, M. (2010). Beyond surveillance and moonscapes: An alternative imaginary of the U.S.-Mexico border wall. In *Visual Anthropology Review* (Vol. 26, Issue 2). https://doi.org/10.1111/j.1548-7458.2010.01073.x

Dube, D. P., & Mohanty, R. P. (2020). Towards development of a cyber security capability maturity model. *International Journal of Business Information Systems*, *34*(1). https://doi.org/10.1504/IJBIS.2020.106800

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. In Journal of Cybersecurity (Vol. 5, Issue 1). https://doi.org/10.1093/cybsec/tyz013

Durante, M. (2015). Violence, Just Cyber War and Information. Philosophy and Technology, 28(3). https://doi.org/10.1007/s13347-014-0176-5

Dwicahyo, S. (2019). Dark Territory: The Secret History of Cyber War. *Lembaran Sejarah*, *14*(2). https://doi.org/10.22146/lembaran-sejarah.45440

Edwards, B., Furnas, A., Forrest, S., & Axelrod, R. (2017). Strategic aspects of cyberattack, attribution, and blame. *Proceedings of the National Academy of Sciences of the United States of America*, *114*(11). https://doi.org/10.1073/pnas.1700442114

Edwards, B., Hofmeyr, S., & Forrest, S. (2016). Hype and heavy tails: A closer look at data breaches. *Journal of Cybersecurity*, *2*(1). https://doi.org/10.1093/cybsec/tyw003

Eggenschwiler, J., & Silomon, J. (2018). Challenges and opportunities in cyber weapon norm construction. Computer Fraud and Security, 2018(12). https://doi.org/10.1016/S1361-3723(18)30120-9

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration*, *43*(5). https://doi.org/10.1080/01900692.2019.1680689

Elden, S. (2007). Governmentality, calculation, territory. *Environment and Planning D: Society and Space*, *25*(3). https://doi.org/10.1068/d428t

Eom, J. H., Kim, N. U., Kim, S. H., & Chung, T. M. (2012). Cyber military strategy for cyberspace superiority in cyber warfare. *Proceedings 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, CyberSec 2012*. https://doi.org/10.1109/CyberSec.2012.6246114

Erbel, M., & Kinsey, C. (2018). Think again–supplying war: reappraising military logistics and its centrality to strategy and war. *Journal of Strategic Studies*, *41*(4). https://doi.org/10.1080/01402390.2015.1104669

Ertl, B. (2008). E-Collaborative Knowledge Construction: Learning from Computer-Supported and Virtual Environments: Learning from Computer-Supported and Virtual Environments. https://doi.org/10.1002/9783527622771

Eszter Katalin, B. (2018). POSSIBILITIES AND SECURITY CHALLENGES OF USING IOT FOR MILITARY PURPOSES. In *Hadmérnök (XIII)*.

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. Journal of Innovation and Entrepreneurship, 8(1). https://doi.org/10.1186/s13731-019-0105-z

Fagan, C. (2013). Documenting Virtual War. InMedia. The French Journal of Media Studies, 4.

Fallon, T. (2015). The new silk road: Xi jinping's grand strategy for eurasia. *American Foreign Policy Interests*, *37*(3). https://doi.org/10.1080/10803920.2015.1056682

Farrell, H., & Glaser, C. (2016). The Role of Effects, Saliencies and Norms in

U.S. Cyberwar Doctrine. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2836066

Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, *53*(1). https://doi.org/10.1080/00396338.2011.555586

Fischer, F., & Miller, G. J. (2017). Handbook of public policy analysis: Theory, politics, and methods. In *Handbook of Public Policy Analysis: Theory, Politics, and Methods*. https://doi.org/10.4324/9781315093192

Fitri, A., & Sanur, D. (2019). Pemberdayaan Industri Pertahanan Nasional Dalam Pemenuhan Minimum Essential Forces (Mef). *Info Singkat : KAJIAN SINGKAT TERHADAP ISU AKTUAL DAN STRATEGIS*, *XI*(22).

FitzGerald, B., & Wright, P. (2014). Decentralizing Cyber Command and Control. *Disruptive Defense Papers*, *April*.

Flowers, A., & Zeadally, S. (2014). US policy on active cyber defense. *Journal of Homeland Security and Emergency Management*, *11*(2). https://doi.org/10.1515/jhsem-2014-0021

Fraga-Lamas, P., & Fernández-Caramés, T. M. (2019). Fake News, Disinformation, and Deepfakes: Leveraging Distributed Ledger Technologies and Blockchain to Combat Digital Deception and Counterfeit Reality. In *arXiv*.

Gawthorpe, A. J. (2016). A guide to national security: threats, responses and strategies. *Defence Studies*, *16*(1). https://doi.org/10.1080/14702436.2015.1092285

Geers, K. (2010). The challenge of cyber attack deterrence. *Computer Law and Security Review*, *26*(3), 298–303. https://doi.org/10.1016/j.clsr.2010.03.003

Geers, K. (2012). Strategic Cyber Defense: Which Way Forward? *Journal of Homeland Security and Emergency Management*, *9*(1). https://doi.org/10.1515/1547-7355.1868

Ghaffari, F., & Arabsorkhi, A. (2019). A New Adaptive Cyber-security Capability Maturity Model. *9th International Symposium on Telecommunication: With Emphasis on Information and Communication Technology, IST 2018*. https://doi.org/10.1109/ISTEL.2018.8661018

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: the human factor. *Journal of Supercomputing*, *74*(10). https://doi.org/10.1007/s11227-

018-2337-2

Giles. (2013). Sun Tzu On The Art Of War. In *Sun Tzu On The Art Of War*. https://doi.org/10.4324/9781315030081

Gisladottir, V., Ganin, A. A., Keisler, J. M., Kepner, J., & Linkov, I. (2017). Resilience of Cyber Systems with Over- and Underregulation. *Risk Analysis*, *37*(9). https://doi.org/10.1111/risa.12729

Goldsmith, M. (2015). Thomas R. Dye, "Politics, Economics and the Public: Policy Outcomes in the American States." *The Oxford Handbook of Classics in Public Policy and Administration*, *April 2018*. https://doi.org/10.1093/oxfordhb/9780199646135.013.21

Gomez, M. A. N. (2016). Arming Cyberspace: The Militarization of a Virtual Domain. *Global Security and Intelligence Studies*, *1*(2). https://doi.org/10.18278/gsis.1.2.4

Good, A. (2018). American Exception: Hegemony and the Dissimulation of the State. *Administration and Society*, *50*(1). https://doi.org/10.1177/0095399715581042

Goodin, R. E., Moran, M., & Rein, M. (2009). The Oxford Handbook of Public Policy. In *The Oxford Handbook of Public Policy*. https://doi.org/10.1093/oxfordhb/9780199548453.001.0001

Gordon, N., & Ram, M. (2016). Ethnic cleansing and the formation of settler colonial geographies. *Political Geography*, *53*. https://doi.org/10.1016/j.polgeo.2016.01.010

GREAVU-ŞERBAN, V., & ŞERBAN, O. (2014). Social Engineering a General Approach. Informatica Economica, 18(2), 5–14. https://doi.org/10.12948/issn14531305/18.2.2014.01

Griffioen, H., Booij, T., & Doerr, C. (2020). Quality Evaluation of Cyber Threat Intelligence Feeds. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *12147 LNCS*. https://doi.org/10.1007/978-3-030-57878-7_14

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer Networks*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Gupta, C. M., & Kumar, D. (2020). Identity theft: a small step towards big

financial crimes. In *Journal of Financial Crime* (Vol. 27, Issue 3). https://doi.org/10.1108/JFC-01-2020-0014

Haataja, S. (2017). The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology*, *9*(2). https://doi.org/10.1080/17579961.2017.1377914

Hägerdal, N. (2019). Ethnic Cleansing and the Politics of Restraint: Violence and Coexistence in the Lebanese Civil War. *Journal of Conflict Resolution*, *63*(1). https://doi.org/10.1177/0022002717721612

Hama, H. H. (2017). State Security, Societal Security, and Human Security. *Jadavpur Journal of International Relations*, *21*(1). https://doi.org/10.1177/0973598417706591

Hamonangan, I., & Assegaff, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Relations*, *1*(4). https://doi.org/10.24198/padjir.v1i4.26246

Handbook of Public Policy Analysis. (2017). In *Handbook of Public Policy Analysis*. https://doi.org/10.4324/9781315093192

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. Internet of Things, 11. https://doi.org/10.1016/j.iot.2020.100204

Hare, F. B. (2019). Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary Security Policy*, *40*(2). https://doi.org/10.1080/13523260.2018.1529369

H. Saini, D. (2016). Proactive Cyber Defense and Reconfigurable Framework for Cyber Security. International Journal on Information Technology (IREIT), 4(1). https://doi.org/10.15866/ireit.v4i1.9668

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. In *California Law Review* (Vol. 100, Issue 4). https://doi.org/10.15779/Z38CR6N

Healey, J., & Jenkins, N. (2019). Rough-And-Ready: A Policy Framework to Determine if Cyber Deterrence is Working or Failing. *International Conference on Cyber Conflict, CYCON*, *2019-May*. https://doi.org/10.23919/CYCON.2019.8756890

Hemanidhi, A., & Chimmanee, S. (2017). Military-based cyber risk assessment framework for supporting cyber warfare in Thailand. Journal of Information and Communication Technology, 16(2). https://doi.org/10.32890/jict2017.16.2.8229

Herbst, L., Konrad, K. A., & Morath, F. (2017). Balance of power and the propensity of conflict. *Games and Economic Behavior*, *103*. https://doi.org/10.1016/j.geb.2015.12.013

Hey, J. (2004). The data, information, knowledge, wisdom chain: the metaphorical link. Intergovernmental Oceanographic Commission. *2004*, *December*, 18. http://www.dataschemata.com/uploads/7/4/8/7/7487334/dikwchain.pdf

Hidayat, S., & Ridwan. (2017). Kebijakan Poros Maritim dan Keamanan Nasional Indonesia: Tantangan dan Harapan. *Jurnal Pertahanan & Bela Negara*, *7*(3).

Ho, J. K.-K. (2014). Formulation of a Systemic PEST Analysis for Strategic Analysis. *European Academic Research*, *2*(5).

Hoang, X. D., & Nguyen, Q. C. (2018). Botnet detection based on machine learning techniques using DNS query data. *Future Internet*, *10*(5). https://doi.org/10.3390/FI10050043

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2018). Insight into insiders and it: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. In *arXiv*.

Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication*, *13*(1). https://doi.org/10.1080/17544750.2019.1687536

Hoofnagle, C. J. (2007). Identity theft: Making the known unknowns known. Harvard Journal of Law and Technology, 21(1).

Hu, H., Wu, J., Wang, Z., & Cheng, G. (2018). Mimic defense: A designed-in cybersecurity defense framework. *IET Information Security*, *12*(3). https://doi.org/10.1049/iet-ifs.2017.0086

Hu, X., & Wang, G. (2018). Maturity model of cyber ecosystem. *Xi Tong Gong Cheng Yu Dian Zi Ji Shu/Systems Engineering and Electronics*, *40*(10). https://doi.org/10.3969/j.issn.1001-506X.2018.10.30

Hughes, R. G., & Shaffer, R. (2020). Cyber war and lessons from history in the digital age. In *Intelligence and National Security* (Vol. 35, Issue 2). https://doi.org/10.1080/02684527.2018.1502002

Hull, G., John, H., & Arief, B. (2019). Ransomware deployment methods and analysis: views from a predictive model and human responses. *Crime Science*, *8*(1). https://doi.org/10.1186/s40163-019-0097-9

Hunker, J. (2010). Cyber war and cyber power - Issues for NATO doctrine. *Reseach Division. NATO Defense College*, *62*.

Hurst, W., Merabti, M., & Fergus, P. (2014). A survey of critical infrastructure security. *IFIP Advances in Information and Communication Technology*, *441*. https://doi.org/10.1007/978-3-662-45355-1_9

Hussain, N., Mirza, H. T., Rasool, G., Hussain, I., & Kaleem, M. (2019). Spam review detection techniques: A systematic literature review. In *Applied Sciences (Switzerland)* (Vol. 9, Issue 5). https://doi.org/10.3390/app9050987

Hutter, D. (2019). Information Security Reading Room Physical Security and Why It Is Important. *SANS Institute Information Security Reading Room*.

Indonesia, P. (2015). *Buku Putih Pertahanan*.

Indrajit, R. E. (2011). Forensik Komputer. Artikel, 1(C).

Irshad, S., & Soomro, T. R. (2018). Identity Theft and Social Media. *IJCSNS International Journal of Computer Science and Network Security*, *18*(1).

Islami, M. J. (2018). Tantangan Dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Masyarakat Telematika Dan Informasi : Jurnal Penelitian Teknologi Informasi Dan Komunikasi*, *8*(2), 137. https://doi.org/10.17933/mti.v8i2.108

Issa, I., Wagner, A. B., & Kamath, S. (2020). An Operational Approach to Information Leakage. *IEEE Transactions on Information Theory*, *66*(3). https://doi.org/10.1109/TIT.2019.2962804

Jackson Adams, & Mohamad Albakajai. (2016). Cyberspace: A New Threat to the Sovereignty of the State. *Management Studies*, *4*(6). https://doi.org/10.17265/2328-2185/2016.06.003

Janeliūnas, T., & Tumkevič, A. (2020). Avoiding a cyber world war: rational motives for negative cooperation among the United States, China and

Russia. Emerging Cyber Threats and Cognitive Vulnerabilities, 117–143. https://doi.org/10.1016/b978-0-12-816203-3.00006-x

Jazuli, A. (2016). Pembangunan Pertanahan Dan Keamanan Demi Penegakan Hukum Di Indonesia : Kewibawaan Suatu Negara. *Jurnal Penelitian Hukum De Jure*, *16*(2).

Jensen, Eric T. (2015). Cyber sovereignty: The way ahead. *Texas International Law Journal*, *50*(2).

Jensen, Eric Talbot. (2012). Sovereignty and Neutrality in Cyber Conflict. *Fordharm International Law Journal*, *35*(3).

Joiner, K. F. (2017). How Australia can catch up to U.S. cyber resilience by understanding that cyber survivability test and evaluation drives defense investment. In *Information Security Journal* (Vol. 26, Issue 2). https://doi.org/10.1080/19393555.2017.1293198

Jones, D. (2013). The dreadnought hoax and the theatres of war. *Literature and History*, *22*(1). https://doi.org/10.7227/LH.22.1.6

Jordán, J. (2020). An analysis of the Jewish-Roman War (66-73 AD) using contemporary insurgency theory. *Small Wars and Insurgencies*. https://doi.org/10.1080/09592318.2020.1775056

Joseph, R. C. (2018). Data Breaches: Public Sector Perspectives. IT Professional, 20(4). https://doi.org/10.1109/MITP.2017.265105441

Juma'h, A. H., & Alnsour, Y. (2020). The effect of data breaches on company performance. *International Journal of Accounting and Information Management*, *28*(2). https://doi.org/10.1108/IJAIM-01-2019-0006

Kalash, M., Rochan, M., Mohammed, N., Bruce, N. D. B., Wang, Y., & Iqbal, F. (2018). Malware Classification with Deep Convolutional Neural Networks. *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, *2018-January*. https://doi.org/10.1109/NTMS.2018.8328749

Kanniainen, V. (2019). Cyber Technology and the Arms Race. *German Economic Review*, *20*(4). https://doi.org/10.1111/geer.12181

Kanwal, G. (2009). China's Emerging Cyber War Doctrine. *Journal of Defence*

Studies, *3*(3).

Kapucu, N., & Demirhan, C. (2019). Managing collaboration in public security networks in the fight against terrorism and organized crime. *International Review of Administrative Sciences*, *85*(1). https://doi.org/10.1177/0020852316681859

Kassab, H. S. (2019). The Role of Cyber-attacks in 21st Century War. Revista de Estudos e Pesquisas Avançadas Do Terceiro Setor, 2(2). https://doi.org/10.31501/repats.v2i2.10404

Keim, Y., & Mohapatra, A. K. (2019). Cyber threat intelligence framework using advanced malware forensics. *International Journal of Information Technology (Singapore)*. https://doi.org/10.1007/s41870-019-00280-3

Kenway, J. E. (2019). The perfect weapon: war, sabotage, and fear in the cyber age. *Journal of Cyber Policy*, *4*(3). https://doi.org/10.1080/23738871.2019.1701694

Khalili, M. M., Liu, M., & Romanosky, S. (2019). Embracing and controlling risk dependency in cyber-insurance policy underwriting. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz010

Kim, S., Heo, G., Zio, E., Shin, J., & Song, J. gu. (2020). Cyber attack taxonomy for digital environment in nuclear power plants. *Nuclear Engineering and Technology*, *52*(5). https://doi.org/10.1016/j.net.2019.11.001

Klemas, T., Lively, R. K., & Choucri, N. (2019). Cyber Acquisition: Policy Changes To Drive Innovation In Response To Accelerating Threats In Cyberspace. *The Cyber Defense Review*. https://doi.org/10.2307/26846123

Kolton, M. (2017). Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence. *The Cyber Defense Review*, *2*(1). https://doi.org/10.1017/CBO9781107415324.004

Konsep Dan Sistem Keamanan Nasional Indonesia. (2016). *Konsep Dan Sistem Keamanan Nasional Indonesia*, *15*(1). https://doi.org/10.22146/jkn.22307

Kovács, L. (2019). National Cybersecurity Strategy Framework. Academic and Applied Research in Military and Public, 18(2). https://doi.org/10.32565/aarms.2019.2.9

Kovaitė, K., Šūmakaris, P., & Stankevičienė, J. (2020). Digital communication channels in industry 4.0 implementation: The role of internal communication. *Management (Croatia)*, *25*(1). https://doi.org/10.30924/mjcmi.25.1.10

Kruegel, C., & Vigna, G. (2003). Anomaly detection of Web-based attacks. *Proceedings of the ACM Conference on Computer and Communications Security*. https://doi.org/10.1145/948109.948144

Kruegel, C., Vigna, G., & Robertson, W. (2005). A multi-model approach to the detection of web-based attacks. *Computer Networks*, *48*(5). https://doi.org/10.1016/j.comnet.2005.01.009

Krueger, G. P., & Banderet, L. E. (2007). Implications for studying team cognition and team performance in network-centric warfare paradigms. In Aviation Space and Environmental Medicine (Vol. 78, Issue 5 II).

Kuehn, A. (2018). New Paradigms in Securing Software Vulnerabilities An Institutional Analysis of Emerging Bug Bounty Programs and Their Implications for Cybersecurity. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2809862

Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. Journal of International Management, 11(4). https://doi.org/10.1016/j.intman.2005.09.009

Kumar, A., Chaudhary, M., & Kumar, N. (2015). *Social Engineering Threats and Awareness : A Survey*. *2*(11), 15–19.

Lampson, B. W. (2004). Computer security in the real world. *Computer*, *37*(6), 37–46. https://doi.org/10.1109/MC.2004.17

Landwehr, C. E. (2001). Computer security. *International Journal of Information Security*, *1*(1), 3–13. https://doi.org/10.1007/s102070100003

Lasiello, E. (2015). Are Cyber Weapons Effective Military Tools? *Military and Strategic Affairs*, *7*(1).

Laudrain, A. P. B. (2019). *France's New Offensive Cyber Doctrine*. Lawfare.

Leader Maynard, J. (2019). Ideology and armed conflict. *Journal of Peace Research*, *56*(5). https://doi.org/10.1177/0022343319826629

Lee, C. J. G. (2012). Reconsidering Constructivism in Qualitative Research.

Educational Philosophy and Theory, *44*(4). https://doi.org/10.1111/j.1469-5812.2010.00720.x

Lee, S. (2020). A basic principle of physical security and its link to cybersecurity. *International Journal of Cyber Criminology*, *14*(1). https://doi.org/10.5281/zenodo.3749780

Lehmann, E. E., & Menter, M. (2016). University–industry collaboration and regional wealth. Journal of Technology Transfer, 41(6). https://doi.org/10.1007/s10961-015-9445-4

Lehto, M. (2015). Phenomena in the cyber world. *Intelligent Systems, Control and Automation: Science and Engineering*, *78*. https://doi.org/10.1007/978-3-319-18302-2_1

Lendvay, R. (2016). Shadows of Stuxnet: Recommendaions for U.S. Policy on Critical Infrastructure Cyber Defense Derived from The Stuxnet Attack. *Homeland Security Affairs*.

Lewis, J. A. (2015). The Role of Offensive Cyber Operations in NATO's Collective Defence. *The Talliban Papers*, *8*.

Li, F., Li, Z., Han, W., Wu, T., Chen, L., Guo, Y., & Chen, J. (2019). Cyberspace-oriented access control: A cyberspace characteristics-based model and its policies. IEEE Internet of Things Journal, 6(2). https://doi.org/10.1109/JIOT.2018.2839065

Liaropoulos, A. (2013). Exercising state sovereignty in cyberspace: An international cyber-order under construction? *8th International Conference on Information Warfare and Security, ICIW 2013*.

Liff, A. P. (2013). The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio. *Journal of Strategic Studies*, *36*(1). https://doi.org/10.1080/01402390.2012.733312

Lilienthal, G., & Ahmad, N. (2015a). Cyber-attack as inevitable kinetic war. *Computer Law and Security Review*, *31*(3). https://doi.org/10.1016/j.clsr.2015.03.002

Lilienthal, G., & Ahmad, N. (2015b). Cyber-attack as inevitable kinetic war. *Computer Law and Security Review*, *31*(3), 390–400. https://doi.org/10.1016/j.clsr.2015.03.002

Lilli, E. (2020). President Obama and US cyber security policy. *Journal of Cyber Policy*. https://doi.org/10.1080/23738871.2020.1778759

Limnéll, J. (2016). The cyber arms race is accelerating – what are the consequences? Journal of Cyber Policy, 1(1), 50–60. https://doi.org/10.1080/23738871.2016.1158304

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3). https://doi.org/10.1080/09636412.2013.816122

Liu, L., De Vel, O., Han, Q. L., Zhang, J., & Xiang, Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. In *IEEE Communications Surveys and Tutorials* (Vol. 20, Issue 2). https://doi.org/10.1109/COMST.2018.2800740

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organisations. *Proceedings of the International Conference on Industrial Engineering and Operations Management*, *July*.

Lukasik, S. J. (2010). A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains. *Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy*.

Lundbohm, E. (2017). Understanding nation-state attacks. *Network Security*, *2017*(10). https://doi.org/10.1016/S1353-4858(17)30101-0

Lyu, X., Ding, Y., & Yang, S. H. (2019). Safety and security risk assessment in cyberphysical systems. In *IET Cyber-Physical Systems: Theory and Applications* (Vol. 4, Issue 3). https://doi.org/10.1049/iet-cps.2018.5068

Ma, J., Ning, H., Huang, R., Liu, H., Yang, L. T., Chen, J., & Min, G. (2015). Cybermatics: A Holistic Field for Systematic Study of Cyber-Enabled New Worlds. *IEEE Access*, *3*. https://doi.org/10.1109/ACCESS.2015.2498288

Maasberg, M., Zhang, X., Ko, M., Miller, S. R., & Beebe, N. L. (2020). An Analysis of Motive and Observable Behavioral Indicators Associated with Insider Cyber-Sabotage and Other Attacks. IEEE Engineering Management Review, 48(2). https://doi.org/10.1109/EMR.2020.2989108

Maathuis, C., Pieters, W., & Van Den Berg, J. (2017). Cyber weapons: A profiling framework. 2016 IEEE International Conference on Cyber Conflict, CyCon U.S. 2016. https://doi.org/10.1109/CYCONUS.2016.7836621

Macias, M. M., Pohorily, P., Morales Guerrero, J., & Karwat, D. M. A. (2020). When Mental Walls Lead to Physical Walls: The US-Mexico Border Wall, Art, and Public Conversations about the Social Responsibility of Engineering. *Engaging Science, Technology, and Society*, *6*. https://doi.org/10.17351/ests2020.379

Mandia, K., Prosise, C., & Pepe, M. (2003). Incident Response & Computer Forensics. In *Search*.

Mansor, W. N. A. B. W., Ahmad, A., Zainudin, W. S., Saudi, M. M., & Kama, M. N. (2020). Crytojacking Classification based on Machine Learning Algorithm. ACM International Conference Proceeding Series. https://doi.org/10.1145/3390525.3390537

Marshall, A. (2016). From civil war to proxy war: past history and current dilemmas. *Small Wars and Insurgencies*, *27*(2). https://doi.org/10.1080/09592318.2015.1129172

Maxwell, N. (2019). A New Task for Philosophy of Science. *Metaphilosophy*, *50*(3). https://doi.org/10.1111/meta.12355

McGarr, P. M. (2021). Fake News, Forgery, and Falsification: Western Responses to Soviet Disinformation in Cold War India. *International History Review*, *43*(1). https://doi.org/10.1080/07075332.2019.1662471

McGhee, J. E. (2016). Liberating Cyber Offense. *Strategic Studies Quarterly*, *4/2016*.

Michael, G. (2010). A Review of: “Richard A. Clarke and Robert K. Knake. Cyber War: The Next Threat to National Security and What To Do About It .” . Terrorism and Political Violence, 23(1). https://doi.org/10.1080/09546553.2011.533082

Mikolic-Torreira, I., Henry, R., Snyder, D., Beaghley, S., Pettyjohn, S., Harting, S., Westerman, E., Shlapak, D., Bishop, M., Oberholtzer, J., Skrabala, L., & Weinbaum, C. (2017). A Framework for Exploring Cybersecurity Policy

Options. In *A Framework for Exploring Cybersecurity Policy Options*. https://doi.org/10.7249/rr1700

Milevski, L. (2016). The nature of strategy versus the character of war. *Comparative Strategy*, *35*(5). https://doi.org/10.1080/01495933.2016.1241007

Miller, K., O'Halloran, B., Pollman, A., & Feeley, M. (2019). Securing the internet of battlefield things while maintaining value to the warfighter. *14th International Conference on Cyber Warfare and Security, ICCWS 2019*.

Ministry of Defence. (2013). Cyber Primer. *Development Concepts and Doctrine Centre*.

Mitchell, N. J., & Zunnurhain, K. (2019). Vulnerability scanning with google cloud platform. *Proceedings - 6th Annual Conference on Computational Science and Computational Intelligence, CSCI 2019*. https://doi.org/10.1109/CSCI49370.2019.00269

Mohd Nizam, B., Zam Zuriyati, M., Awee, A., Farhana Hanim, M., & Suhaila, A. (2015). Cyber Entrepreneurship Ecosystem : Proposed Concept Paper . *Proceeding of IC-ITS 2015*, *June*.

Montalvan Castilla, J. E., & Pursiainen, C. (2019). Cyberspace Effects on Civil Society. The Ultimate Game-Changer or Not? *Journal of Civil Society*, *15*(4). https://doi.org/10.1080/17448689.2019.1672288

Mouton, F., Leenen, L., & Venter, H. S. (2016). Social engineering attack examples, templates and scenarios. *Computers and Security*, *59*. https://doi.org/10.1016/j.cose.2016.03.004

Mueller, M. L. (2019). Against Sovereignty in Cyberspace. *International Studies Review*. https://doi.org/10.1093/isr/viz044

Murphy, J., & Keane, A. (2019). Cyberpsychological threat intelligence. *European Conference on Information Warfare and Security, ECCWS*, *2019-July*.

Nagatsu, M., Davis, T., DesRoches, C. T., Koskinen, I., MacLeod, M., Stojanovic, M., & Thorén, H. (2020). Philosophy of science for sustainability science. *Sustainability Science*. https://doi.org/10.1007/s11625-020-00832-8

Nastiti, F. E., Prastyanti, R. A., Taruno, R. B., & Hariyadi, D. (2018). Social media warfare in Indonesia political campaign: A survey. *Proceedings - 2018 3rd International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2018*.

https://doi.org/10.1109/ICITISEE.2018.8720959

Nell, K. E. (2018). A Doctrine of Contingent Sovereignty. *Orbis*, *62*(2), 313–334. https://doi.org/10.1016/j.orbis.2018.02.009

Nopriono, & Suswanta. (2019). Pemberdayaan Masyarakat dalam Perspektif Kebijakan Publik. *JPK: Jurnal Pemerintahan Dan Kebijakan*, *1*(1).

Norman, M. D., & Koehler, M. T. K. (2017). Cyber defense as a complex adaptive system: A model-based approach to strategic policy design. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3145574.3145595

Norri–Sederholm, T., Norvanto, E., Talvitie–Lamberg, K., & Huhtinen, A. –M. (2020). Misinformation and Disinformation in Social Media as the Pulse of Finnish National Security. In *Advanced Sciences and Technologies for Security Applications*. https://doi.org/10.1007/978-3-030-47511-6_12

Nugraha, L. K., & Putri, D. A. (2016). Mapping the Cyber Policy Landscape: Indonesia. *No. November*, *November*.

Nye, J. S. (2014). The Regime Complex for Managing Global Cyber Activities. *CIGI Publications*, *1*.

Obama: Cyber-czar to be hand-picked. (2009). *Infosecurity*, *6*(4). https://doi.org/10.1016/s1754-4548(09)70070-1

Olofsson, A. D., & Lindberg, J. O. (2012). *Informed design of educational technologies in higher education : enhanced learning and teaching*. https://doi.org/10.4018/978-1-61350-080-4

Or-Meir, O., Nissim, N., Elovici, Y., & Rokach, L. (2019). Dynamic malware analysis in the modern era—A state of the art survey. ACM Computing Surveys, 52(5). https://doi.org/10.1145/3329786

Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies*, *16*(3). https://doi.org/10.1080/14702436.2016.1187568

Osho, O., & Onoja, A. D. (2015). National cyber security policy and strategy of nigeria: A qualitative analysis. *International Journal of Cyber Criminology*, *9*(1). https://doi.org/10.5281/zenodo.22390

Pande, M., & Bharathi, S. V. (2020). Theoretical foundations of design thinking –

A constructivism learning approach to design thinking. *Thinking Skills and Creativity*, *36*. https://doi.org/10.1016/j.tsc.2020.100637

Paquet-Clouston, M., Haslhofer, B., & Dupont, B. (2019). Ransomware payments in the Bitcoin ecosystem. *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz003

Park, D. W. (2016). Analysis and comparison of regulations for national cybersecurity. *International Journal of Security and Its Applications*, *10*(10). https://doi.org/10.14257/ijsia.2016.10.10.19

Peck, B., & Mummery, J. (2018). Hermeneutic Constructivism: An Ontology for Qualitative Research. *Qualitative Health Research*, *28*(3). https://doi.org/10.1177/1049732317706931

Pepping, C. A., Davis, P. J., & O'Donovan, A. (2015). The association between state attachment security and state mindfulness. *PLoS ONE*, *10*(3). https://doi.org/10.1371/journal.pone.0116779

Perloff-Giles, A. (2018). Transnational Cyber Offenses: Overcoming Jurisdictional Challenges. *Yale Journal of International Law*, *43*(1).

Pernik, P. (2020). National cyber commands. In *Routledge Handbook of International Cybersecurity*. https://doi.org/10.4324/9781351038904-17

Persson, M., & Rigas, G. (2014). Complexity: The dark side of network-centric warfare. Cognition, Technology and Work, 16(1). https://doi.org/10.1007/s10111-012-0248-1

Poirier, C. W. J., & Lotspeich, M. J. (2013). Air Force cyber warfare. *Air & Space Power Journal*, *October 2013*.

Poirier, W. J., & Lotspeich Maj, J. (2013). Air force cyber warfare now and the future. *Air and Space Power Journal*, *27*(5).

Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS attacks in software-defined networks through feature selection methods and machine learning models. *Sustainability (Switzerland)*, *12*(3). https://doi.org/10.3390/su12031035

Politik, R. J. (2017). Politik dan Kebijakan (Publik). *Jurnal Politik*, *3*(1). https://doi.org/10.7454/jp.v3i1.78

Prakasa, S. U. W., & Noviandi Nur, P. E. (2019). Analysist of cyber espionage in international law and indonesian law. Humanities and Social Sciences Reviews, 7(3). https://doi.org/10.18510/hssr.2019.736

Prinz, C., Kreggenfeld, N., & Kuhlenkötter, B. (2018). Lean meets Industrie 4.0 - A practical approach to interlink the method world and cyber-physical world. *Procedia Manufacturing*, *23*. https://doi.org/10.1016/j.promfg.2018.03.155

Rahman, F. (2018). Implementasi Doktrin Tridarma Ekakarma Melalui Teori Perimbangan Kekuatan. *JURNAL SOSIAL POLITIK*, *4*(1). https://doi.org/10.22219/sospol.v4i1.5125

Rahmawati, I. (2017). the Analysis Ofcyber Crime Threat Risk Management To Increase Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66. https://doi.org/10.33172/jpbh.v7i2.193

Ramdhani, A., & Ramdhani, M. A. (2017). Konsep Umum Pelaksanaan Kebijakan Publik. *Jurnal Publik*. https://doi.org/10.1109/ICMENS.2005.96

Reinhold, T., & Reuter, C. (2019). From Cyber War to Cyber Peace. In Information Technology for Peace and Security. https://doi.org/10.1007/978-3-658-25652-4_7

Riana Nugraha, M. H. (2017). Perencanaan Strategis Pertahanan Masa Depan Indonesia: Analisis Pada Lingkungan Strategis Asia Tenggara (Asean) Periode 2015-2020. *Jurnal Pertahanan & Bela Negara*, *7*(3). https://doi.org/10.33172/jpbh.v7i3.235

Riola, J. M., Fajardo-Toro, C. H., Reina, J. D., Torres, O. M., & López, M. A. G. (2020). Defense 4.0: Internet of battlefield things (IoBT) in naval defense. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2020(E29).

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *JAS (Journal of ASEAN Studies)*, *4*(1). https://doi.org/10.21512/jas.v4i1.967

Robert Kehler, C., Lin, H., & Sulmeyer, M. (2017). Rules of engagement for cyberspace operations: A view from the USA. *Journal of Cybersecurity*, *3*(1). https://doi.org/10.1093/cybsec/tyx003

Robinson, M., Jones, K., Janicke, H., & Maglaras, L. (2018). An introduction to cyber peacekeeping. Journal of Network and Computer Applications, 114. https://doi.org/10.1016/j.jnca.2018.04.010

Rofiq, M. N. (2018). Peranan Filsafat Ilmu Bagi Perkembangan Ilmu Pengetahuan. *FALASIFA : Jurnal Studi Keislaman*, *9*(1). https://doi.org/10.36835/falasifa.v9i1.112

Romanosky, S., Ablon, L., Kuehn, A., & Jones, T. (2019). Content analysis of cyber insurance policies: How do carriers price cyber risk? *Journal of Cybersecurity*, *5*(1). https://doi.org/10.1093/cybsec/tyz002

Rose-Redwood, R. (2012). With numbers in place: Security, territory, and the production of calculable space. *Annals of the Association of American Geographers*, *102*(2). https://doi.org/10.1080/00045608.2011.620503

Rosenfield, D. K. (2009). Rethinking cyber war. *Critical Review*, *21*(1). https://doi.org/10.1080/08913810902812156

Rosner, E. (2017). Cyber Federalism: Defining Cyber's Jurisdictional Boundaries. *Homeland Security Affairs*.

Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection*, *7*(1). https://doi.org/10.1016/j.ijcip.2014.01.001

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense Sebagai Upaya Mempertahankan Kedaulatan Negara. *Perspektif*, *21*(3), 168. https://doi.org/10.30742/perspektif.v21i3.587

Sabillon, R., Cavaller, V., & Cano, J. (2016). National Cyber Security Strategies: Global Trends in Cyberspace. *International Journal of Computer Science and Software Engineering*, *5*(5).

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. In *Future Internet* (Vol. 11, Issue 4). https://doi.org/10.3390/FI11040089

Saltzman, I. (2013). Cyber posturing and the offense-defense balance. *Contemporary Security Policy*, *34*(1). https://doi.org/10.1080/13523260.2013.771031

Samaan, J. L. (2010). Cyber command the rift in us Military Cyber-Strategy. *RUSI Journal*, *155*(6). https://doi.org/10.1080/03071847.2010.542664

Samaras, H., Giouvanakis, T., Bousiou, D., & Tarabanis, K. (2006). Towards a New Generation of Multimedia Learning Research. *Assessment*, *14*, 3–30.

Sargent, J. F. (2018). Defense science and technology funding. In Science Policies and Programs: History, Funding and Issues.

Schläger, C., Ebert, A., Mattausch, A., & Beck, M. (2017). Enabling cyber sovereignty: With knowledge, not with national products. In *Digital Marketplaces Unleashed*. https://doi.org/10.1007/978-3-662-49275-8_79

Schmitt, M. N., & Vihul, L. (2017). Respect for sovereignty in cyberspace. *Texas Law Review*, *95*(7).

Schulze, M. (2020). *Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations*. 183–197. https://doi.org/10.23919/cycon49761.2020.9131733

Sebastian, E. (2018). PENINGKATAN PERANAN SDM PERTAHANAN NASIONAL GUNA MENGHADAPI PERANG GENERASI KEEMPAT. *Jurnal Pertahanan & Bela Negara*, *5*(1). https://doi.org/10.33172/jpbh.v5i1.351

Security in a Small Nation: Scotland, Democracy, Politics. (2017). In *Security in a Small Nation: Scotland, Democracy, Politics*. https://doi.org/10.11647/obp.0078

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2). https://doi.org/10.1080/07421222.2015.1063315

Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. Computers and Security, 97, 101996. https://doi.org/10.1016/j.cose.2020.101996

Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. J. (2019). Actionable threat intelligence for digital forensics readiness. Information and Computer Security, 27(2). https://doi.org/10.1108/ICS-09-2018-0110

Setiawan, R. (2018). Indonesia Cyber Security : Urgency To Establish Cyber Army In The Middle Of Global Terrorist Threat. *Journal of Islamic World and Politics*, *2*(1). https://doi.org/10.18196/jiwp.2109

Setiyawan, A. (2019). The Urgency of Defining Indonesia's National Critical Infrastructure. *UNIFIKASI : Jurnal Ilmu Hukum*, *6*(2). https://doi.org/10.25134/unifikasi.v6i2.1673

Shackelford, S. J., Charoen, D., Waite, T., & Zhang, N. (2019). RETHINKING ACTIVE DEFENSE: A COMPARATIVE ANALYSIS of PROACTIVE CYBERSECURITY POLICYMAKING. *University of Pennsylvania Journal of International Law*, *41*(2).

Shaji, R. S., Sachin Dev, V., & Brindha, T. (2019). A methodological review on attack and defense strategies in cyber warfare. Wireless Networks, 25(6). https://doi.org/10.1007/s11276-018-1724-1

Shani, G. (2017). Human security as ontological security: A post-colonial approach. *Postcolonial Studies*, *20*(3). https://doi.org/10.1080/13688790.2017.1378062

Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1). https://doi.org/10.1007/s41111-016-0002-6

Shvindina, H. (2019). Coopetition as an emerging trend in research: Perspectives for safety & security. *Safety*, *5*(3). https://doi.org/10.3390/safety5030061

Sigholm, J. (2016). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1). https://doi.org/10.1515/jms-2016-0184

Sirajuddin, M., Kamil, S. U. R., & Fachruddin, S. (2017). War 3.0: The Indonesia Challenge Against Hoax, Hate Speech and Social Media Abuse. https://doi.org/10.2991/uicosp-17.2017.25

Skyttner, L. (2005). Systems theory and the science of military command and control. In Kybernetes (Vol. 34, Issues 7–8). https://doi.org/10.1108/03684920510606000

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly ♦ Fall*, *12*(3). https://doi.org/10.2307/26481911

Soares, M. (2020). To catch a spy: the art of counterintelligence. Intelligence and National Security. https://doi.org/10.1080/02684527.2020.1746125

Sobiesk, E., Blair, J., Conti, G., Lanham, M., & Taylor, H. (2015). Cyber Education : A Multi-Level , Multi-Discipline Approach. Acm Sigite '15, 43–47. https://doi.org/10.1145/2808006.2808038

Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia. Potensi Pertahanan, 31–35.

Song, D., Brumley, D., Yin, H., Caballero, J., Jager, I., Kang, M. G., Liang, Z., Newsome, J., Poosankam, P., & Saxena, P. (2008). BitBlaze: A new approach to computer security via binary analysis. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 5352 LNCS, 1–25. https://doi.org/10.1007/978-3-540-89862-7_1

Soo Hoo, K. J. (2000). How much is enough? A risk management approach to computer security. Ph.D. Dissertation, Stanford University, USA, June, 99. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.16.4127&rep=rep1&type=pdf

Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. Jurnal Pertahanan & Bela Negara, 5(1), 89-108. https://doi.org/10.33172/jpbh.v5i1.350

Sultana, Z. (2017). Napoleon Bonaparte: His Successes and Failures. *European Journal of Multidisciplinary Studies*, *6*(2). https://doi.org/10.26417/ejms.v6i2.p189-197

Sun, C. C., Hahn, A., & Liu, C. C. (2018). Cyber security of a power grid: State-of-the-art. In *International Journal of Electrical Power and Energy Systems* (Vol. 99). https://doi.org/10.1016/j.ijepes.2017.12.020

Suratman, Y. P. (2017). PENGGUNAAN STRATEGI OPERASI KONTRA INTELIJEN DALAM RANGKA MENGHADAPI ANCAMAN SIBER NASIONAL. *Jurnal Pertahanan & Bela Negara*, *7*(2). https://doi.org/10.33172/jpbh.v7i2.176

Sutrisno, B. T. (2016). Urgensi Komando Pertahanan Siber (Cyber Defense Command) Dalam Menghadapi Peperangan Asimetris. *Defendonesia*, *1*(2).

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, *90*. https://doi.org/10.1016/j.cose.2019.101709

Tatar, U., Karabacak, B., Katina, P. F., & Igonor, A. (2019). A complex structure representation of the US critical infrastructure protection program based on the Zachman framework. *International Journal of System of Systems Engineering*, *9*(3). https://doi.org/10.1504/IJSSE.2019.102869

Tekerek, A. (2021). A novel architecture for web-based attack detection using convolutional neural network. *Computers and Security*, *100*. https://doi.org/10.1016/j.cose.2020.102096

The Effect of Cyberwar Technologies on Force Buildup: The Israeli Case. (2013). *Military and Strategic Affairs*, *5*(1).

The National Institute of Standards and Technology. (2013). Improving Critical Infrastructure Cybersecurity Executive Order 13636: Preliminary Cybersecurity Framework. *Nist Standards*, 1–47.

Theohary, C. A., & Harrington, A. I. (2015). Cyber operations in dod policy and plans: Issues for congress. In *Cyberspace Threat Landscape: Overview, Response Authorities, and Capabilities*.

Toprak, N. G. (2019). From Embargo to Blockade: An Evaluation of the United States Sanctions against Iran in the Context of the Use of Economic Impact Tools in Foreign Poli. *International Conference on Eurasian Economies 2019*. https://doi.org/10.36880/c11.02219

Truong, T. C., Diep, Q. B., & Zelinka, I. (2020). Artificial intelligence in the cyber domain: Offense and defense. *Symmetry*, *12*(3). https://doi.org/10.3390/sym12030410

Turunen, M., & Kari, M. J. (2020). Cyber deterrence and Russia's active cyber defense. European Conference on Information Warfare and Security, ECCWS, 2020-June. https://doi.org/10.34190/EWS.20.038

Tuttle, H. (2018). Cryptojacking. *Risk Management*, *65*(7).

Tuukkanen, T. (2013). Adapting the Current National Defence Doctrine to Cyber Domain. *International Journal of Cyber Warfare and Terrorism*, *1*(4).

https://doi.org/10.4018/ijcwt.2011100103

Urgessa, W. G. (2020). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. Computer Law and Security Review, 36(xxxx). https://doi.org/10.1016/j.clsr.2019.105368

Van der Kleij, R., Kleinhuis, G., & Young, H. (2017). Computer security incident response team effectiveness: A needs assessment. *Frontiers in Psychology*, *8*(DEC). https://doi.org/10.3389/fpsyg.2017.02179

Van Horenbeeck, M. (2018). The future of Internet governance and cyber-security. *Computer Fraud and Security*, *2018*(5), 6–8. https://doi.org/10.1016/S1361-3723(18)30042-3

Vaseashta, A., Susmann, P., & Braman, E. (2014). Cyber Security – Threat Scenarios , Policy Framework and Cyber Wargames. *Cyber Security and Resilency Policy Framework*. https://doi.org/10.3233/978-1-61499-446-6-1

von Billerbeck, S. B. K., & Gippert, B. J. (2017). Legitimacy in Conflict: Concepts, Practices, Challenges. In *Journal of Intervention and Statebuilding* (Vol. 11, Issue 3). https://doi.org/10.1080/17502977.2017.1357701

Wagner, T. D., Mahbub, K., Palomar, E., & Abdallah, A. E. (2019). Cyber threat intelligence sharing: Survey and research directions. *Computers and Security*, *87*. https://doi.org/10.1016/j.cose.2019.101589

Wang, D., Huang, L., Liu, J., Lü, L., Ruan, Z., & Lü, L. (2019). Cyber-physical system defense strategy considering loaded false data injection attacks. *Dianli Xitong Baohu Yu Kongzhi/Power System Protection and Control*, *47*(1). https://doi.org/10.7667/PSPC180003

Warner, J. (1998). Borders in cyberspace: Information policy and the global information infrastructure. *Journal of the American Society for Information Science*, *49*(4). https://doi.org/10.1002/(sici)1097-4571(19980401)49:4<387::aid-asi15>3.3.co;2-6

Waxman, M. C. (2013). Self-defensive Force against Cyber Attacks: Legal, Strategic and Political Dimensions. *U.S. Naval War College International Law Studies*, *89*.

Weed, S. A. C. N.-Q. 9. A. W. 2017. (2017). US policy response to cyber attack on SCADA systems supporting critical national infrastructure. In *Air Force Research Institute perspectives on cyber power*.

Weismann, M. F. (2010). Regulating unlawful behavior in the global business environment: The functional integration of sovereignty and multilateralism. *Journal of World Business*, *45*(3), 312–321. https://doi.org/10.1016/j.jwb.2009.12.002

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (2003). Handbook for Computer Security Incident Response Teams (CSIRTs). *SEI Digital Library*, *April*, 223. https://doi.org/CMU/SEI-2003-HB-002

Willett, M. (2019). Assessing cyber power. *Survival*, *61*(1). https://doi.org/10.1080/00396338.2019.1569895

Williams, E. J., Hinds, J., & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, *120*. https://doi.org/10.1016/j.ijhcs.2018.06.004

Williams, E. J., & Joinson, A. N. (2020). Developing a measure of information seeking about phishing. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa001

Wilner, A. S. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies*, *43*(2). https://doi.org/10.1080/01402390.2018.1563779

Wiśniewski, M. (2020). Methodology of Situational Management of Critical Infrastructure Security. *Foundations of Management*, *12*(1). https://doi.org/10.2478/fman-2020-0004

Wohlforth, W. C., Little, R., Kaufman, S. J., Kang, D., Jones, C. A., Hui, V. B., Eckstein, A., Deudney, D., & Brenner, W. L. (2007). Testing balance-of-power theory in world history. *European Journal of International Relations*, *13*(2). https://doi.org/10.1177/1354066107076951

Wong, W. P., Tan, H. C., Tan, K. H., & Tseng, M. L. (2019). Human factors in information leakage: mitigation strategies for information sharing integrity. *Industrial Management and Data Systems*, *119*(6). https://doi.org/10.1108/IMDS-12-2018-0546

Wu, Z. (2018). Classical geopolitics, realism and the balance of power theory. *Journal of Strategic Studies*, *41*(6). https://doi.org/10.1080/01402390.2017.1379398

Xu, W. (2020). Challenges to cyber sovereignty and response measures. *World Economy and International Relations*, *64*(2). https://doi.org/10.20542/0131-2227-2020-64-2-89-99

Yaacoub, J.-P., Noura, H., Salman, O., & Chehab, A. (2020). Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things*, *11*. https://doi.org/10.1016/j.iot.2020.100218

Yannakogeorgos, P. A. (2012). Internet governance and national security. *Strategic Studies Quarterly*, *6*(3).

Y. Connolly, L., & Wall, D. S. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers and Security, 87. https://doi.org/10.1016/j.cose.2019.101568

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *Prism*, *7*(2).

Yin, Y. (2020). Characteristics of social governing organizations and governance of emergent public security events from the perspective of public safety. *Revista de Cercetare Si Interventie Sociala*, *69*. https://doi.org/10.33788/rcis.69.15

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDOS) flooding attacks. *IEEE Communications Surveys and Tutorials*, *15*(4). https://doi.org/10.1109/SURV.2013.031413.00127

Zaytsev, A., Malyuk, A., & Miloslavskaya, N. (2017). Critical analysis in the research area of insider threats. *Proceedings - 2017 IEEE 5th International Conference on Future Internet of Things and Cloud, FiCloud 2017*, *2017-January*. https://doi.org/10.1109/FiCloud.2017.16

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics and Policy*, *45*(3). https://doi.org/10.1111/polp.12202

Zhang, J., & Pezeshkan, A. (2016). Host country network, industry experience, and international alliance formation: Evidence from the venture capital industry. *Journal of World Business*, *51*(2). https://doi.org/10.1016/j.jwb.2015.10.008

Zhang, Z., Chen, X., Ma, J., & Shen, J. (2020). SLDS: Secure and location-sensitive data sharing scheme for cloud-assisted Cyber-Physical Systems. *Future Generation Computer Systems*, *108*, 1338–1349. https://doi.org/10.1016/j.future.2018.01.025

Zhong, C., Lin, T., Liu, P., Yen, J., & Chen, K. (2018). A cyber security data triage operation retrieval system. *Computers and Security*, *76*.

https://doi.org/10.1016/j.cose.2018.02.011

Zotti, A. (2011). Inside cyber warfare. Global Change, Peace & Security, 23(3). https://doi.org/10.1080/14781158.2011.605638

Zou, B., Choobchian, P., & Rozenberg, J. (2021). Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies. *Journal of Transportation Security*. https://doi.org/10.1007/s12198-021-00230-w

Zrahia, A. (2018). Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views. Journal of Cybersecurity, 4(1). https://doi.org/10.1093/cybsec/tyy008