BIBLIOGRAPHY

[1] Y. Nugraha, I. Brown, and A. S. Sastrosubroto, "An adaptive wideband delphi method to study state cyber-defence requirements," *IEEE Transactions on Emerging Topics in Computing*, vol. 4, no. 1, pp. 47–59, 2016.

[2] A. Ubowska and T. Królikowski, "Building a cybersecurity culture of public administration system in poland," in *Procedia Computer Science*, vol. 207. Elsevier B.V., 2022, pp. 1242–1250.

[3] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb, and S. Mahmood, "Cyber security threats and vulnerabilities: A systematic mapping study," *Arabian Journal for Science and Engineering*, vol. 45, pp. 3171–3189, 4 2020.

[4] F. R. Bechara and S. B. Schuch, "Cybersecurity and global regulatory challenges," *Journal of Financial Crime*, vol. 28, pp. 359–374, 2020.

[5] M. Vielberth, F. Bohm, I. Fichtinger, and G. Pernul, "Security operations center: A systematic study and open challenges," *IEEE Access*, vol. 8, pp. 227 756–227 779, 2020.

[6] D. Shahjee and N. Ware, "Integrated network and security operation center: A systematic analysis," *IEEE Access*, vol. 10, pp. 27 881–27 898, 2022.

[7] M. A. Majid and K. A. Z. Ariffin, "Model for successful development and implementation of cyber security operations centre (soc)," *PLoS ONE*, vol. 16, 11 2021.

[8] C. Onwubiko and K. Ouazzane, "Challenges towards building an effective cyber security operations centre," Tech. Rep., 2019.

[9] Badan Siber dan Sandi Negara (BSSN), "Lanskap keamanan siber indonesia 2023," Badan Siber dan Sandi Negara Republik Indonesia, Jakarta, Indonesia, Tech. Rep., 2023, accessed: 2025-06-23. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf

[10] ——, "Lanskap keamanan siber indonesia 2024," Badan Siber dan Sandi Negara Republik Indonesia, Jakarta, Indonesia, Tech. Rep., 2024, accessed: 2025-06-23. [Online]. Available: https://www.bssn.go.id/wp-content/uploads/2025/02/LANSKAP-KEAMANAN-SIBER-2024-1.pdf

[11] N. I. of Standards and Technology, "Computer security incident handling guide," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-61 Revision 3, 2025. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r3

[12] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," 2025.

[13] D. P. Dube and R. P. Mohanty, "Application of grounded theory in construction of factors of internal efficiency and external effectiveness of cyber security and developing impact models," *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 3, pp. 41–70, 9 2023.

[14] European Union Agency for Cybersecurity (ENISA), "How to set up csirt and soc: A guide for member states," 2020, available: https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc.

[15] M. Saraiva and N. Mateus-Coelho, "Cybersoc framework a systematic review of the state-of-art," in *Procedia Computer Science*, vol. 204. Elsevier B.V., 2022, pp. 961–972.

[16] P. Johannesson and E. Perjons, *An Introduction to Design Science*. Cham: Springer, 2014.

[17] European Union Agency for Cybersecurity (ENISA), "Enisa threat landscape 2024," https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024, 2024, accessed May 21, 2025.

[18] I. Bongiovanni, K. Renaud, H. Brydon, R. Blignaut, and A. Cavallo, "A quantification mechanism for assessing adherence to information security governance guidelines," *Information and Computer Security*, vol. 30, pp. 517–548, 10 2022.

[19] A. M. Al-Hawamleh, "Investigating the multifaceted dynamics of cybersecurity practices and their impact on the quality of e-government services: evidence from the ksa," *Digital Policy, Regulation and Governance*, vol. 26, pp. 317–336, 4 2024.

[20] A. S. Muhammad and T. Kaya, "Factors affecting the citizen's intention to adopt e-government in nigeria," *Journal of Information, Communication and Ethics in Society*, vol. 21, pp. 271–289, 7 2023.

[21] M. Corporation, "Mitre att&ck framework," Available at https://attack.mitre.org/, 2023, accessed 2025.

[22] M. Dev and D. Saha, "Does e-government development moderate the impact of female labor participation on national cybersecurity maturity? an empirical investigation," *Information and Computer Security*, vol. 32, pp. 74–92, 1 2024.

[23] Pemerintah Republik Indonesia, "Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik," https:

//peraturan.bpk.go.id/Home/Details/123175/pp-no-71-tahun-2019, 2019, diakses pada 23 Juni 2025.

[24] Pemerintah Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi," https://peraturan.bpk.go.id/Home/Details/204267/uu-no-27-tahun-2022, 2022, diakses pada 23 Juni 2025.

[25] N. I. o. S. Joint Task Force and Technology, "Security and privacy controls for information systems and organizations," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST Special Publication 800-53 Revision 5, 2020. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-53r5

[26] R. van Os, "Soc-cmm: Designing and evaluating a tool for measurement of capability maturity in security operations centers," Master's thesis, Luleå University of Technology, Sweden, 2016, master's thesis.

[27] C. Pascoe, S. Quinn, and K. Scarfone, "The nist cybersecurity framework (csf) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep. NIST Cybersecurity White Paper 29, 2024. [Online]. Available: https://doi.org/10.6028/NIST.CSWP.29

[28] A. Perera, S. Rathnayaka, N. D. Perera, W. W. Madushanka, and A. N. Senarathne, "The next gen security operation center," in *2021 6th International Conference for Convergence in Technology, I2CT 2021.* Institute of Electrical and Electronics Engineers Inc., 4 2021.

[29] T. Y. Khaw, A. Amran, and A. P. Teoh, "Building a thematic framework of cybersecurity: a systematic literature review approach," pp. 234–256, 5 2024.

[30] Y. Jiang and Y. Atif, "A selective ensemble model for cognitive cybersecurity analysis," *Journal of Network and Computer Applications*, vol. 193, 11 2021.

[31] S. Paul, "A survey of technologies supporting design of a multimodal interactive robot for military communication," pp. 156–193, 11 2023.

[32] M. Malatji, A. L. Marnewick, and S. V. Solms, "Cybersecurity capabilities for critical infrastructure resilience," *Information and Computer Security*, vol. 30, pp. 255–279, 3 2022.

[33] R. van Os, "Soc-cmm: Measuring capability maturity in security operations centers," Available at https://soc-cmm.com/, 2018, retrieved from SOC-CMM Official Website.

[34] V. E. Kulugh, U. M. Mbanaso, and G. Chukwudebe, "Cybersecurity resilience maturity assessment model for critical national information infrastructure," *SN Computer Science*, vol. 3, 5 2022.

[35] International Organization for Standardization and International Electrotechnical Commission, *ISO/IEC 27001:2022 - Information Technology – Security Techniques – Information Security Management Systems – Requirements*, Geneva, Switzerland, 2022.

[36] ISACA, "Cobit 2019 framework: Governance and management objectives," Information Systems Audit and Control Association (ISACA), Rolling Meadows, IL, USA, Tech. Rep., 2018, accessed: 2025-06-23. [Online]. Available: https://www.isaca.org/resources/cobit

[37] ISACA, "Cobit 5 for information security," Information Systems Audit and Control Association (ISACA), Rolling Meadows, IL, USA, Tech. Rep., 2012, accessed: 2025-06-23. [Online]. Available: https://www.isaca.org/bookstore/cobit/whlc5is

[38] B. Abazi, "Establishing the national cybersecurity (resilience) ecosystem," in *IFAC-PapersOnLine*, vol. 55. Elsevier B.V., 10 2022, pp. 42–47.

[39] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design science in information systems research," *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[40] A. AlHogail, "Design and validation of information security culture framework," *Computers in Human Behavior*, vol. 49, pp. 567–575, 2015.

[41] A. Adel, D. Sarwar, and A. Hosseinian-Far, "Transformation of cybersecurity posture in it telecommunication: A case study of a telecom operator," Tech. Rep., 1 2021. [Online]. Available: http://www.springer.com/series/5540

[42] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan, R. Chou, J. Glanville, J. M. Grimshaw, A. Hróbjartsson, M. M. Lalu, T. Li, E. W. Loder, E. Mayo-Wilson, S. McDonald, L. A. McGuinness, L. A. Stewart, J. Thomas, A. C. Tricco, V. A. Welch, P. Whiting, and D. Moher, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," 3 2021.

[43] J. E. Van Aken, "Design science in the field of management: Development of design knowledge and methodology," *British Journal of Management*, vol. 16, no. 1, pp. 19–36, 2005.

[44] N. K. Denzin, *The Research Act: A Theoretical Introduction to Sociological Methods*. New York: McGraw-Hill, 1978.

[45] N. Carter, D. Bryant-Lukosius, A. DiCenso, J. Blythe, and A. J. Neville, "The use of triangulation in qualitative research," *Oncology Nursing Forum*, vol. 41, no. 5, pp. 545–547, 2014.

[46] S. T. Ali, K. Petersen, and C. Wohlin, "A comparative study of criteria for evaluating slr quality in software engineering," in *Proceedings of the 2010 ACM-IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*. IEEE, 2010, pp. 1–10.

[47] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, 2006.

[48] F. Skopik and T. Pahi, "Under false flag: using technical artifacts for cyber attack attribution," *Cybersecurity*, vol. 3, 12 2020.

[49] Organisation for Economic Co-operation and Development (OECD), "Oecd recommendation on digital security of critical activities," https://www.oecd.org/sti/oecd-recommendation-on-digital-security-of-critical-activities.htm, 2021, accessed May 21, 2025.

[50] International Organization for Standardization, "Iso/iec 27035-1:2023 — information security incident management — part 1: Principles of incident management," https://www.iso.org/standard/81904.html, 2023, accessed May 21, 2025.

[51] T. Nagasako, "A consideration of the case study of disinformation and its legal problems," in *Human-Centric Computing in a Data-Driven Society*, ser. IFIP Advances in Information and Communication Technology, D. Kreps, T. Komukai, T. V. Gopal, and K. Ishii, Eds., vol. 590, pp. 262–272.

[52] U. J. Butt, W. Richardson, A. Nouman, H.-M. Agbo, C. Eghan, and F. Hashmi, "Cloud and its security impacts on managing a workforce remotely: A reflection to cover remote working challenges," in *Cybersecurity, Privacy and Freedom Protection in the Connected World*, ser. Lecture Notes in Computer Science, H. Jahankhani, A. Jamal, and S. Lawson, Eds. Springer, 2021, pp. 285–295.

[53] D. Huang and L. Wang, *MCF-CSA: AMulti-level Collaboration Framework for Cyber Situation Awareness and Information Sharing*, X. Sun, X. Zhang, Z. Xia, and E. Bertino, Eds. Springer International Publishing, 7 2021, vol. 1424. [Online]. Available: https://link.springer.com/10.1007/978-3-030-78621-2

[54] M. N. Alraja, U. J. Butt, and M. Abbod, "Information security policies compliance in a global setting: An employee's perspective," *Computers and Security*, vol. 129, 6 2023.

[55] A. A. . T. C. K. Renaud, *Positioning Diplomacy Within a Strategic Response to the Cyber Conflict Threat*, S. Parkin and L. Viganò, Eds. Springer International Publishing, 10 2022, vol. 13176. [Online]. Available: https://link.springer.com/10.1007/978-3-031-10183-0

[56] T. M. A. . E. C. A. A. M. Rita Zgheib, *Cyber Security Strategies While Safeguarding Information Systems in PublicPrivate Sectors*, F. Ortiz-Rodríguez, S. Tiwari, M.-A. Sicilia, and A. Nikiforova, Eds. Springer Nature Switzerland, 9 2022, vol. 1666. [Online]. Available: https://link.springer.com/10.1007/978-3-031-22950-3

[57] S. T. Jr, R. V. Heerden, S. C. Thakur, and A. Jordaan, "Cyber-security in the era of the covid-19 pandemic: a developing countries' perspective," *International Journal of Industrial Engineering and Operations Management*, vol. 5, pp. 77–85, 6 2023.

[58] E. O. Nwosu, C. C. Ajibo, U. Nwoke, and I. Okoli, "Legal and institutional frameworks for capital market regulation in nigeria: recasting the agendas beyond compliance-based regulation," *Journal of Financial Crime*, vol. 28, pp. 448–463, 2020.

[59] J. Pérez-Morón, "Eleven years of cyberattacks on chinese supply chains in an era of cyber warfare, a review and future research agenda," *Journal of Asia Business Studies*, vol. 16, no. 2, pp. 371–395, 2022.

[60] R. Saylam and A. Ozdemir, "Military acceptance of the internet of things: a research model," *Digital Policy, Regulation and Governance*, vol. 24, pp. 1–16, 2 2022.

[61] R. Gafni and T. Pavel, "Cyberattacks against the health-care sectors during the covid-19 pandemic," *Information and Computer Security*, vol. 30, pp. 137–150, 1 2022.

[62] P. N. Vasist and S. Krishnan, "Engaging with deepfakes: a meta-synthesis from the perspective of social shaping of technology theory," *Internet Research*, vol. 33, pp. 1670–1726, 11 2023.

[63] B. Krishna and S. M.P, "Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: a cross-country analysis," *Information and Computer Security*, vol. 29, pp. 737–760, 11 2021.

[64] A. B. Turner, S. McCombie, and A. J. Uhlmann, "Discerning payment patterns in bitcoin from ransomware attacks," *Journal of Money Laundering Control*, vol. 23, pp. 545–589, 10 2020.

[65] T. Gibbs, "Seeking economic cyber security: a middle eastern example," *Journal of Money Laundering Control*, vol. 23, pp. 493–507, 5 2020.

[66] A. Visvizi and M. D. Lytras, "Government at risk: between distributed risks and threats and effective policy-responses," *Transforming Government: People, Process and Policy*, vol. 14, pp. 333–336, 8 2020.

[67] H. S. M. Abbas, Z. H. Qaisar, X. Xu, and C. Sun, "Nexus of e-government, cybersecurity and corruption on public service (pss) sustainability in asian economies using fixed-effect and random forest algorithm," *Online Information Review*, vol. 46, pp. 754–770, 7 2022.

[68] L. Waller, S. C. Johnson, N. Satchell, D. Gordon, G. L. K. Daley, H. Reid, K. Fender, P. Llewellyn, L. Smyle, and P. Linton, "Woe is the dark web: the main challenges that governments of the commonwealth caribbean will face in combating dark web-facilitated criminal activities," *Transforming Government: People, Process and Policy*, vol. 17, pp. 87–100, 2 2023.

[69] S. Garibaldi and F. Deane, "Cyberspace as a fifth dimension of national security: trade measure exceptions," *Journal of International Trade Law and Policy*, vol. 22, pp. 67–88, 10 2023.

[70] H. Younies and T. N. el Al-Tawil, "Effect of cybercrime laws on protecting citizens and businesses in the united arab emirates (uae)," *Journal of Financial Crime*, vol. 27, pp. 1089–1105, 12 2020.

[71] N. Mugarura and E. Ssali, "Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system," *Journal of Money Laundering Control*, vol. 24, pp. 10–28, 2020.

[72] O. Oriola, A. B. Adeyemo, M. Papadaki, and E. Kotzé, "A collaborative approach for national cybersecurity incident management," *Information and Computer Security*, vol. 29, pp. 457–484, 2021.

[73] H. t.Allah Nabil Abd Al Ghaffar, "Government cloud computing and national security," *Review of Economics and Political Science*, vol. 9, pp. 116–133, 4 2024.

[74] B. Sule, U. Sambo, and M. Yusuf, "Countering cybercrimes as the strategy of enhancing sustainable digital economy in nigeria," *Journal of Financial Crime*, vol. 30, pp. 1557–1574, 12 2023.

[75] F. P. Duarte, "Non-kinetic hybrid threats in europe – the portuguese case study (2017-18)," *Transforming Government: People, Process and Policy*, vol. 14, pp. 433–451, 8 2020.

[76] A. Rabii, S. Assoul, K. O. Touhami, and O. Roudies, "Information and cyber security maturity models: a systematic literature review," pp. 627–644, 10 2020.

[77] T. N. Al-Tawil, "Ethical implications for teaching students to hack to combat cybercrime and money laundering," *Journal of Money Laundering Control*, vol. 27, pp. 21–33, 1 2024.

[78] N. H. Chowdhury, M. T. Adam, and T. Teubner, "Rushing for security: a document analysis on the sources and effects of time pressure on organizational cybersecurity," *Information and Computer Security*, vol. 31, pp. 504–526, 10 2023.

[79] A. Panda and A. Bower, "Cyber security and the disaster resilience framework," *International Journal of Disaster Resilience in the Built Environment*, vol. 11, pp. 507–518, 8 2020.

[80] R. Goel, A. Kumar, and J. Haddow, "Prism: a strategic decision framework for cybersecurity risk assessment," *Information and Computer Security*, vol. 28, pp. 591–625, 10 2020.

[81] M. U. Rana, O. Ellahi, M. Alam, J. L. Webber, A. Mehbodniya, and S. Khan, "Offensive security: Cyber threat intelligence enrichment with counterintelligence and counterattack," *IEEE Access*, vol. 10, pp. 108 760–108 774, 2022.

[82] B. Al-Sada, A. Sadighian, and G. Oligeri, "Analysis and characterization of cyber threats leveraging the mitre attck database," *IEEE Access*, vol. 12, pp. 1217–1234, 2024.

[83] N. Afzaliseresht, Y. Miao, S. Michalska, Q. Liu, and H. Wang, "From logs to stories: Human-centred data mining for cyber threat intelligence," *IEEE Access*, vol. 8, pp. 19 089–19 099, 2020.

[84] E. U. Haque, W. Abbasi, S. Murugesan, M. S. Anwar, F. Khan, and Y. Lee, "Cyber forensic investigation infrastructure of pakistan: An analysis of the cyber threat landscape and readiness," *IEEE Access*, vol. 11, pp. 40 049–40 063, 2023.

[85] H. I. Kure, S. Islam, and H. Mouratidis, "An integrated cyber security risk management framework and risk predication for the critical infrastructure protection," *Neural Computing and Applications*, vol. 34, pp. 15 241–15 271, 9 2022.

[86] A. Pawlicka, M. Choraś, R. Kozik, and M. Pawlicki, "First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions," *Personal and Ubiquitous Computing*, vol. 27, pp. 193–202, 4 2023.

[87] J. Navajas-Adán, E. Badia-Gelabert, L. Jiménez-Saurina, M. J. Marijuán-Martín, and R. Mayo-García, "Perceptions and dilemmas around cyber-security in a spanish research center after a cyber-attack," *International Journal of Information Security*, vol. 23, pp. 2315–2331, 6 2024.

[88] S. K. Yadav, K. Sharma, C. Kumar, and A. Arora, "Blockchain-based synergistic solution to current cybersecurity frameworks," *Multimedia Tools and Applications*, vol. 81, pp. 36 623–36 644, 10 2022.

[89] G. González-Granadillo, M. Faiella, I. Medeiros, R. Azevedo, and S. González-Zarzosa, "Etip: An enriched threat intelligence platform for improving osint correlation, analysis, visualization and sharing capabilities," *Journal of Information Security and Applications*, vol. 58, 5 2021.

[90] N. Neshenko, C. Nader, E. Bou-Harb, and B. Furht, "A survey of methods supporting cyber situational awareness in the context of smart cities," *Journal of Big Data*, vol. 7, 12 2020.

[91] Z. Iqbal and Z. Anwar, "Scerm—a novel framework for automated management of cyber threat response activities," *Future Generation Computer Systems*, vol. 108, pp. 687–708, 7 2020.

[92] N. E. Park, Y. R. Lee, S. Joo, S. Y. Kim, S. H. Kim, J. Y. Park, S. Y. Kim, and I. G. Lee, "Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks," *Computers and Electrical Engineering*, vol. 105, 1 2023.

[93] M. M. Salim, S. K. Singh, and J. H. Park, "Securing smart cities using lstm algorithm and lightweight containers against botnet attacks," *Applied Soft Computing*, vol. 113, 12 2021.

[94] M. Allegretta, G. Siracusano, R. Gonzalez, and M. Gramaglia, "Are crowd-sourced cti datasets ready for supporting anti-cybercrime intelligence?" *Computer Networks*, vol. 234, 10 2023.

[95] N. Kshetri, "The evolution of cyber-insurance industry and market: An institutional analysis," *Telecommunications Policy*, vol. 44, 9 2020.

[96] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, "Attributes impacting cybersecurity policy development: An evidence from seven nations," *Computers and Security*, vol. 120, 9 2022.

[97] D. C. L. Nguyen and D. W. Golman, "Diffusion of the budapest convention on cybercrime and the development of cybercrime legislation in pacific island countries: 'law on the books' vs 'law in action'," *Computer Law and Security Review*, vol. 40, 4 2021.

[98] F. Sufi, "An innovative gpt-based open-source intelligence using historical cyber incident reports," *Natural Language Processing Journal*, vol. 7, p. 100074, 6 2024.

[99] S. Maesschalck, V. Giotsas, B. Green, and N. Race, "Don't get stung, cover your ics in honey: How do honeypots fit within industrial control system security," *Computers and Security*, vol. 114, 3 2022.

[100] X. Wang, W. W. Li, A. C. M. Leung, and W. T. Yue, "To alert or alleviate? a natural experiment on the effect of anti-phishing laws on corporate it and security investments," *Decision Support Systems*, vol. 179, 4 2024.

[101] A. M. del Rey, G. Hernández, A. B. Tabernero, and A. Q. Dios, "Advanced malware propagation on random complex networks," *Neurocomputing*, vol. 423, pp. 689–696, 1 2021.

[102] M. M. Yamin, B. Katt, and M. Nowostawski, "Serious games as a tool to model attack and defense scenarios for cyber-security exercises," *Computers and Security*, vol. 110, 11 2021.

[103] O. Gulyas and G. Kiss, "Impact of cyber-attacks on the financial institutions," in *Procedia Computer Science*, vol. 219. Elsevier B.V., 2023, pp. 84–90.

[104] W. Xu, F. Murphy, X. Xu, and W. Xing, "Dynamic communication and perception of cyber risk: Evidence from big data in media," *Computers in Human Behavior*, vol. 122, 9 2021.

[105] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-forensic (iof): A blockchain based digital forensics framework for iot applications," *Future Generation Computer Systems*, vol. 120, pp. 13–25, 7 2021.

[106] R. Hoffmann, J. Napiórkowski, T. Protasowicki, and J. Stanik, "Risk based approach in scope of cybersecurity threats and requirements," in *Procedia Manufacturing*, vol. 44. Elsevier B.V., 2020, pp. 655–662.

[107] J. Zhao, Q. Yan, J. Li, M. Shao, Z. He, and B. Li, "Timiner: Automatically extracting and analyzing categorized cyber threat intelligence from social data," *Computers and Security*, vol. 95, 8 2020.

[108] B. Biswas, A. Mukhopadhyay, S. Bhattacharjee, A. Kumar, and D. Delen, "A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums," *Decision Support Systems*, vol. 152, 1 2022.

[109] H. Mouratidis, S. Islam, A. Santos-Olmo, L. E. Sanchez, and U. M. Ismail, "Modelling language for cyber security incident handling for critical infrastructures," *Computers and Security*, vol. 128, 5 2023.

[110] U. Noor, Z. Anwar, J. Altmann, and Z. Rashid, "Customer-oriented ranking of cyber threat intelligence service providers," *Electronic Commerce Research and Applications*, vol. 41, 5 2020.

[111] X. Zhang, M. Xu, G. Da, and P. Zhao, "Ensuring confidentiality and availability of sensitive data over a network system under cyber threats," *Reliability Engineering and System Safety*, vol. 214, 10 2021.

[112] L. A. Tawalbeh and F. Muheidat, "Factors that motivate defense against social engineering attacks across organizations," in *Procedia Computer Science*, vol. 224. Elsevier B.V., 2023, pp. 75–82.

[113] A. Seiler, "The use of playbooks in the incident response process," SANS Institute, GIAC (GCFA) Gold Certification Paper, 2022, accessed: 2025-05-29. [Online]. Available: https://www.sans.org/white-papers/the-use-of-playbooks-in-the-incident-response-process/

[114] International Organization for Standardization, *ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*, International Organization for Standardization Std., 2012, available: https://www.iso.org/standard/44381.html. [Online]. Available: https://www.iso.org/standard/44381.html

[115] W. P. Aung, H. H. Lwin, and K. K. Lin, "Developing and analysis of cyber security models for security operation center in myanmar," Tech. Rep., 2020.

[116] D. Weissman and A. Jayasumana, "Integrating iot monitoring for security operation center," in *GIoTS 2020 - Global Internet of Things Summit, Proceedings*. Institute of Electrical and Electronics Engineers Inc., 6 2020.

[117] F. Chen, Z. Yan, and L. Gu, *Towards Low-Latency Big Data Infrastructure at Sangfor*, J. Chen, D. He, and R. Lu, Eds. Springer Nature Switzerland, 10 2022, vol. 1641. [Online]. Available: https://link.springer.com/10.1007/978-3-031-23098-1

[118] A. Becue, M. Praddaude, E. Maia, N. Hogrel, I. Praca, and R. Yaich, *Digital Twins for Enhanced Resilience: Aerospace Manufacturing Scenario*, J. Horkoff, E. Serral, and J. Zdravkovic, Eds. Springer International Publishing, 6 2022, vol. 451. [Online]. Available: https://link.springer.com/10.1007/978-3-031-07478-3

[119] C. Daniel, M. Mullarkey, and M. Agrawal, *RQ Labs: A Cybersecurity Workforce Talent Program Design*, R. Krishnan, H. R. Rao, S. K. Sahay, S. Samtani, and Z. Zhao, Eds. Springer International Publishing, 10 2022, vol. 1549. [Online]. Available: https://link.springer.com/10.1007/978-3-030-97532-6

[120] R. Brisse, S. Boche, F. Majorczyk, and J.-F. Lalande, *KRAKEN: A Knowledge-Based Recommender System for Analysts, to Kick Exploration up a Notch*, P. Y. Ryan and C. Toma, Eds. Springer International Publishing, 11 2021, vol. 13195. [Online]. Available: https://link.springer.com/10.1007/978-3-031-17510-7

[121] C. Zhou, G. Wu, J. Li, and C. Zhang, "A dynamic processing algorithm for variable data in intranet security monitoring," Tech. Rep., 7 2021. [Online]. Available: http://www.springer.com/series/7409

[122] N. Cai, Z. Deng, and H. Wang, *An Intelligent Data Flow Security Strategy Model of Cloud-Network Integration*, W. Lu, Y. Zhang, W. Wen, H. Yan, and C. Li, Eds. Springer Nature Singapore, 8 2022, vol. 1699. [Online]. Available: https://link.springer.com/10.1007/978-981-19-8285-9

[123] W. Yang and K.-Y. Lam, *Automated Cyber Threat Intelligence Reports Classification for Early Warning of Cyber Attacks in Next Generation SOC*, J. Zhou, X. Luo, Q. Shen, and Z. Xu, Eds. Springer International Publishing, 12 2020, vol. 11999. [Online]. Available: http://link.springer.com/10.1007/978-3-030-41579-2

[124] A. Dey, E. Totel, and S. Navers, *Heterogeneous Security Events Prioritization Using Auto-encoders*, J. Garcia-Alfaro, J. Leneutre, N. Cuppens, and R. Yaich, Eds. Springer International Publishing, 11 2021, vol. 12528. [Online]. Available: https://link.springer.com/10.1007/978-3-030-68887-5

[125] T. F. Ask, R. G. Lugo, B. J. Knox, and S. Sütterlin, "Human-human communication in cyber threat situations a systematic review," Tech. Rep., 7 2021. [Online]. Available: http://www.springer.com/series/7409

[126] H. Kim, S. Choi, J.-H. Yun, B.-G. Min, and H. C. Kim, "Co-occurrence based security event analysis and visualization for cyber physical systems," Tech. Rep., 7 2020. [Online]. Available: http://www.springer.com/series/7899

[127] A. Kabil, T. Duval, and N. Cuppens, "Alert characterization by non-expert users in a cybersecurity virtual environment a usability study," Tech. Rep., 9 2020. [Online]. Available: http://www.springer.com/series/7412

[128] P. Dornheim and R. Zarnekow, "Factors shaping information security culture in an internal it department," Tech. Rep., 7 2020. [Online]. Available: http://www.springer.com/series/7409

[129] M. Glas, M. Vielberth, T. Reittinger, F. Böhm, and G. Pernul, "Improving cybersecurity skill development through visual programming," *Information and Computer Security*, vol. 31, pp. 316–330, 6 2023.

[130] J. A. Paul and M. Zhang, "Decision support model for cybersecurity risk planning: A two-stage stochastic programming framework featuring firms, government, and attacker," *European Journal of Operational Research*, vol. 291, pp. 349–364, 5 2021.

[131] C. Chedrawi and Y. Atallah, "Artificial intelligence in the defense sector: an rbv and isomorphism perspectives to the case of the lebanese armed forces," *Journal of Asia Business Studies*, vol. 16, pp. 279–293, 3 2022.

[132] J. Han, Z. Ju, X. Chen, M. Yang, H. Zhang, and R. Huai, "Secure operations of connected and autonomous vehicles," *IEEE Transactions on Intelligent Vehicles*, vol. 8, pp. 4484–4497, 11 2023.

[133] S. Galantucci, D. Impedovo, and G. Pirlo, "One time user key: A user-based secret sharing xor-ed model for multiple user cryptography in distributed systems," *IEEE Access*, vol. 9, pp. 148 521–148 534, 2021.

[134] S. Neupane, J. Ables, W. Anderson, S. Mittal, S. Rahimi, I. Banicescu, and M. Seale, "Explainable intrusion detection systems (x-ids): A survey of current methods, challenges, and opportunities," *IEEE Access*, vol. 10, pp. 112 392–112 415, 2022.

[135] S. Y. Cho, J. Happa, and S. Creese, "Capturing tacit knowledge in security operation centers," *IEEE Access*, vol. 8, pp. 42 021–42 041, 2020.

[136] M. Zago, M. G. Pérez, and G. M. Pérez, "Early dga-based botnet identification: pushing detection to the edges," *Cluster Computing*, vol. 24, pp. 1695–1710, 9 2021.

[137] K. Demertzis, L. Iliadis, N. Tziritas, and P. Kikiras, "Anomaly detection via blockchained deep learning smart contracts in industry 4.0," *Neural Computing and Applications*, vol. 32, pp. 17 361–17 378, 12 2020.

[138] H. Al-Mohannadi, I. Awan, and J. A. Hamar, "Analysis of adversary activities using cloud-based web services to enhance cyber threat intelligence," *Service Oriented Computing and Applications*, vol. 14, pp. 175–187, 9 2020.

[139] A. P. Psathas, L. Iliadis, A. Papaleonidas, and D. Bountas, "Corem2 project: a beginning to end approach for cyber intrusion detection," *Neural Computing and Applications*, vol. 34, pp. 19 565–19 584, 11 2022.

[140] J. Liu, J. Yan, J. Jiang, Y. He, X. Wang, Z. Jiang, P. Yang, and N. Li, "Tricti: an actionable cyber threat intelligence discovery system via trigger-enhanced neural network," *Cybersecurity*, vol. 5, 12 2022.

[141] G. Aivatoglou, M. Anastasiadis, G. Spanos, A. Voulgaridis, K. Votis, D. Tzovaras, and L. Angelis, "A rakel-based methodology to estimate software vulnerability characteristics score - an application to eu project echo," *Multimedia Tools and Applications*, vol. 81, pp. 9459–9479, 3 2022.

[142] J. Forsberg and T. Frantti, "Technical performance metrics of a security operations center," *Computers and Security*, vol. 135, 12 2023.

[143] C. M. Patterson, J. R. Nurse, and V. N. Franqueira, ""i don't think we're there yet": The practices and challenges of organisational learning from cyber security incidents," *Computers and Security*, vol. 139, 4 2024.

[144] S. Sicari, A. Rizzardi, and A. Coen-Porisini, "5g in the internet of things era: An overview on security and privacy challenges," *Computer Networks*, vol. 179, 10 2020.

[145] B. Dupont, C. Shearing, M. Bernier, and R. Leukfeldt, "The tensions of cyber-resilience: From sensemaking to practice," *Computers and Security*, vol. 132, 9 2023.

[146] E. Philippou, S. Frey, and A. Rashid, "Contextualising and aligning security metrics and business objectives: A gqm-based methodology," *Computers and Security*, vol. 88, 1 2020.

[147] N. Feng, S. Zhang, M. Li, and D. Li, "Contracting managed security service: Double moral hazard and risk interdependency," *Electronic Commerce Research and Applications*, vol. 50, 11 2021.

[148] S. Varga, J. Brynielsson, and U. Franke, "Cyber-threat perception and risk management in the swedish financial sector," *Computers and Security*, vol. 105, 6 2021.

[149] B. Green, R. Derbyshire, M. Krotofil, W. Knowles, D. Prince, and N. Suri, "Pcaad: Towards automated determination and exploitation of industrial systems," *Computers and Security*, vol. 110, 11 2021.

[150] A. Annarelli, F. Nonino, and G. Palombi, "Understanding the management of cyber resilient systems," *Computers and Industrial Engineering*, vol. 149, 11 2020.

[151] R. Derbyshire, B. Green, and D. Hutchison, ""talking a different language": Anticipating adversary attack cost for cyber risk assessment," *Computers and Security*, vol. 103, 4 2021.

[152] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Robotics cyber security: vulnerabilities, attacks, countermeasures, and recommendations," *International Journal of Information Security*, vol. 21, pp. 115–158, 2 2022.

[153] M. Repetto, A. Carrega, and R. Rapuzzi, "An architecture to manage security operations for digital service chains," *Future Generation Computer Systems*, vol. 115, pp. 251–266, 2 2021.

[154] B. Valkenburg and I. Bongiovanni, "Unravelling the three lines model in cybersecurity: a systematic literature review," *Computers and Security*, vol. 139, 4 2024.

[155] M. Chemmakha, O. Habibi, and M. Lazaar, "Improving machine learning models for malware detection using embedded feature selection method," in *IFAC-PapersOnLine*, vol. 55. Elsevier B.V., 2022, pp. 771–776.

[156] N. Miloslavskaya, "Network protection tools for network security intelligence centers," in *Procedia Computer Science*, vol. 190. Elsevier B.V., 7 2021, pp. 597–603.

[157] B. D. Bryant and H. Saiedian, "Improving siem alert metadata aggregation with a novel kill-chain based classification model," *Computers and Security*, vol. 94, 7 2020.

[158] M. Husák, L. Sadlek, S. Špaček, M. Laštovička, M. Javorník, and J. Komárková, "Crusoe: A toolset for cyber situational awareness and decision support in incident handling," *Computers and Security*, vol. 115, 4 2022.

[159] K. Hughes, K. McLaughlin, and S. Sezer, "A model-free approach to intrusion response systems," *Journal of Information Security and Applications*, vol. 66, 5 2022.

[160] A. Zibak, C. Sauerwein, and A. Simpson, "A success model for cyber threat intelligence management platforms," *Computers and Security*, vol. 111, 12 2021.

[161] E. Agyepong, Y. Cherdantseva, P. Reinecke, and P. Burnap, "A systematic method for measuring the performance of a cyber security operations centre analyst," *Computers and Security*, vol. 124, 1 2023.

[162] T. Savunen, H. Hämmäinen, K. Kilkki, and P. Kekolahti, "The role of mobile network operators in next-generation public safety services," *Telecommunications Policy*, vol. 47, 4 2023.

[163] S. M. AlHidaifi, M. R. Asghar, and I. S. Ansari, "Towards a cyber resilience quantification framework (crqf) for it infrastructure," *Computer Networks*, vol. 247, 6 2024.

[164] G. Angafor, I. Yevseyeva, and L. Maglaras, "Malaware: A tabletop exercise for malware security awareness education and incident response training," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 280–292, 1 2024.

[165] H. J. Ofte and S. Katsikas, "Understanding situation awareness in socs, a systematic literature review," *Computers and Security*, vol. 126, 3 2023.

[166] A. J. G. de Azambuja, T. Giese, K. Schützer, R. Anderl, B. Schleich, and V. R. Almeida, "Digital twins in industry 4.0 – opportunities and challenges related to cyber security," in *Procedia CIRP*, vol. 121. Elsevier B.V., 2024, pp. 25–30.

[167] S. Rass, S. König, J. Wachter, V. Mayoral-Vilches, and E. Panaousis, "Game-theoretic apt defense: An experimental study on robotics," *Computers and Security*, vol. 132, 9 2023.

[168] S. Yuan, M. Yang, and G. Reniers, "Integrated process safety and process security risk assessment of industrial cyber-physical systems in chemical plants," *Computers in Industry*, vol. 155, 2 2024.

[169] A. Galli, V. L. Gatta, V. Moscato, M. Postiglione, and G. Sperlì, "Explainability in ai-based behavioral malware detection systems," *Computers and Security*, vol. 141, 6 2024.

[170] H. Naseer, S. B. Maynard, and K. C. Desouza, "Demystifying analytical information processing capability: The case of cybersecurity incident response," *Decision Support Systems*, vol. 143, 4 2021.

[171] J. Suomalainen, J. Julku, A. Heikkinen, S. J. Rantala, and A. Yastrebova, "Security-driven prioritization for tactical mobile networks," *Journal of Information Security and Applications*, vol. 67, 6 2022.

[172] C. Engel, S. Mencke, R. Heumüller, R. Hormann, H. Aedtner, and F. Ortmeier, "Customizable operation center for smart security management," in *Procedia CIRP*, vol. 104. Elsevier B.V., 2021, pp. 1930–1935.

[173] M. D. Iannacone and R. A. Bridges, "Quantifiable comparable evaluations of cyber defensive capabilities: A survey novel, unified approach," *Computers and Security*, vol. 96, 9 2020.

[174] Y. Mirsky, T. Golomb, and Y. Elovici, "Lightweight collaborative anomaly detection for the iot using blockchain," *Journal of Parallel and Distributed Computing*, vol. 145, pp. 75–97, 11 2020.

[175] V. O. Kayhan, M. Agrawal, and S. Shivendu, "Cyber threat detection: Unsupervised hunting of anomalous commands (uhac)," *Decision Support Systems*, vol. 168, 5 2023.

[176] M. I. Rojo-Rivas, D. Díaz-Sánchez, F. Almenarez, and A. Marín-Lopez, "Kriper: A blockchain network with permissioned storage," *Future Generation Computer Systems*, vol. 138, pp. 160–171, 1 2023.

[177] J. C. Sancho, A. Caro, M. Ávila, and A. Bravo, "New approach for threat classification and security risk estimations based on security event management," *Future Generation Computer Systems*, vol. 113, pp. 488–505, 12 2020.

[178] L. Gallo, A. Maiello, A. Botta, and G. Ventre, "2 years in the anti-phishing group of a large company," *Computers and Security*, vol. 105, 6 2021.

[179] H. Hettema, "Rationality constraints in cyber defense: Incident handling, attribution and cyber threat intelligence," *Computers and Security*, vol. 109, 10 2021.

[180] O. Yurekten and M. Demirci, "Citadel: Cyber threat intelligence assisted defense system for software-defined networks," *Computer Networks*, vol. 191, 5 2021.

[181] M. Thangavelu, V. Krishnaswamy, and M. Sharma, "Impact of comprehensive information security awareness and cognitive characteristics on security incident management – an empirical study," *Computers and Security*, vol. 109, 10 2021.

[182] J. McGahagan, D. Bhansali, C. Pinto-Coelho, and M. Cukier, "Discovering features for detecting malicious websites: An empirical study," *Computers and Security*, vol. 109, 10 2021.

[183] L. Wawrowski, M. Michalak, A. Białas, R. Kurianowicz, M. Sikora, M. Uchronski, and A. Kajzer, "Detecting anomalies and attacks in network traffic monitoring with classification methods and xai-based explainability," in *Procedia Computer Science*, vol. 192. Elsevier B.V., 2021, pp. 2259–2268.

[184] S. Ainslie, D. Thompson, S. Maynard, and A. Ahmad, "Cyber-threat intelligence for security decision-making: A review and research agenda for practice," *Computers and Security*, vol. 132, 9 2023.

[185] H. Sedjelmaci, "Cooperative attacks detection based on artificial intelligence system for 5g networks," *Computers and Electrical Engineering*, vol. 91, 5 2021.

[186] R. Colelli, C. Foglietta, S. Panzieri, and F. Pascucci, "The smart extension approach for securing industrial control systems," in *IFAC-PapersOnLine*, vol. 53. Elsevier B.V., 2020, pp. 11 207–11 212.

[187] S. M. Ho and M. Gross, "Consciousness of cyber defense: A collective activity system for developing organizational cyber awareness," *Computers and Security*, vol. 108, 9 2021.

[188] Y. Chekhovskoy, K. Plaksiy, A. Nikiforov, and N. Miloslavskaya, "The use of virtual reality technologies in the specialists' training in the field of information security," in *Procedia Computer Science*, vol. 213. Elsevier B.V., 2022, pp. 223–231.

[189] C. Grajeda, J. Berrios, S. Benzo, E. Ogunwobi, and I. Baggili, "Expanding digital forensics education with artifact curation and scalable, accessible exercises via the artifact genome project," *Forensic Science International: Digital Investigation*, vol. 45, 7 2023.

[190] M. Pawlicki, R. Kozik, and M. Choraś, "A survey on neural networks for (cyber-) security and (cyber-) security of neural networks," *Neurocomputing*, vol. 500, pp. 1075–1087, 8 2022.

[191] F. Alves, A. Bettini, P. M. Ferreira, and A. Bessani, "Processing tweets for cybersecurity threat awareness," *Information Systems*, vol. 95, 1 2021.

[192] M. Cinque, R. D. Corte, and A. Pecchia, "Contextual filtering and prioritization of computer application logs for security situational awareness," *Future Generation Computer Systems*, vol. 111, pp. 668–680, 10 2020.

[193] J. Ramos, J. L. García-Dorado, and J. Aracil, "Workforce capacity planning for proactive troubleshooting in the network operations center," *Computer Networks*, vol. 221, 2 2023.

[194] R. Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions," *Information Fusion*, vol. 97, 9 2023.

[195] S. Suhail, S. U. R. Malik, R. Jurdak, R. Hussain, R. Matulevičius, and D. Svetinovic, "Towards situational aware cyber-physical systems: A security-enhancing use case of blockchain-based digital twins," *Computers in Industry*, vol. 141, 10 2022.

[196] O. Alshaikh, S. Parkinson, and S. Khan, "Exploring perceptions of decision-makers and specialists in defensive machine learning cybersecurity applications: The need for a standardised approach," *Computers and Security*, vol. 139, 4 2024.

[197] M. Wurzenberger, G. Höld, M. Landauer, and F. Skopik, "Analysis of statistical properties of variables in log data for advanced anomaly detection in cyber security," *Computers and Security*, vol. 137, 2 2024.

[198] P. H. Meland, D. A. Nesheim, K. Bernsmed, and G. Sindre, "Assessing cyber threats for storyless systems," *Journal of Information Security and Applications*, vol. 64, 2 2022.

[199] S. R. Zahra, M. A. Chishti, A. I. Baba, and F. Wu, "Detecting covid-19 chaos driven phishing/malicious url attacks by a fuzzy logic and data mining based intelligence system," *Egyptian Informatics Journal*, vol. 23, pp. 197–214, 7 2022.

[200] N. Miloslavskaya and S. Tolstaya, "Information security management maturity models," in *Procedia Computer Science*, vol. 213. Elsevier B.V., 2022, pp. 49–57.

[201] C. Acartürk, M. Ulubay, and E. Erdur, "Continuous improvement on maturity and capability of security operation centres," *IET Information Security*, vol. 15, pp. 59–75, 1 2021.

[202] M. El-Hajj, T. Itäpelto, and T. Gebremariam, "Systematic literature review: Digital twins' role in enhancing security for industry 4.0 applications," *SECURITY AND PRIVACY*, vol. 7, 9 2024.

[203] Industry Expert at Google Cloud Security, "External commentary on government soc model v1.0," 2025, private correspondence reviewed as part of post-evaluation feedback. Document archived in Appendix F of this thesis.