Bibliography

Al-Mhiqani, M. N, Ahmad, R., Mohamed, W., Hassan, A., Abidin, Z. Z., Ali, N. S & Abdulkareem, K. H. (2018). *Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems. International Journal of Advanced Computer Science and Applications. 9. 499-508. 10.14569/IJACSA.2018.090169*. [on line]. Available at: https://www.researchgate.net/publication/322852405_Cyber-Security_Incidents_A_Review_Cases_in_Cyber-Physical_Systems [consulted 10/04/2021].

Aust Cyber. (2019). *Cyber Security Opportunities in the AESAN Region*. [on line]. Available at: https://www.austcyber.com/resource/cyber-security-opportunities-asean-region [consulted 10/04/2021].

Avi, S., Ameur, H., Kung, A., & Hervé, D. *The Impact of Artificial Intelligence on Security: A Dual Perspective.* [on line]. Available at: https://www.cesar-conference.org/wp-content/uploads/2018/11/articles/C&ESAR_2018_J1-03_A-SZYCHTER_Dual_perspective%20_AI_in_Cybersecurity.pdf [consulted 10/04/2021].

Bawack, R., Wamba, F. S., & Carillo, K. D. A. (2019). (PDF) Artificial Intelligence in Practice: Implications for Information Systems Research. *Americas Conference on Information Systems 2019At: Cancun, Mexico.* https://www.researchgate.net/publication/333853703_Artificial_Intelligence_in_Practice_Implications_for_Information_Systems_Research

Berryhill, J., Heang, K. K., Clogher, R. & McBride, K. (2019). *Artificial Intelligence and Its Use in The Public Sector*. [on line]. Available at: https://www.oecd-ilibrary.org/content/paper/726fd39d-en___ [consulted 10/04/2021]

Bhatele, K. R. & Shrivastava, H. (2019). *The Role of Artificial Intelligence in Cyber Security*. [on line]. Available at: https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security [consulted 10/04/2021].

Bhatele, K. R. & Shrivastava, H. (2019). *The Role of Artificial Intelligence in Cyber Security*. [on line]. Available at: https://www.researchgate.net/publication/330569376_The_Role_of_Artificial_Intelligence_in_Cyber_Security [consulted 10/04/2021].

BSI. (2018). *Information and Cyber Challenges in the Public Sector*. [on line]. Available at: https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-sector-cloud.pdf [consulted 10/04/2021].

Chakravarthy, D. (2020). *Cyber Security And Its Importance*. [on line]. Available at:
https://www.researchgate.net/publication/347439655_CYBER_SECURITY _AND_ITS_IMPORTANCE [consulted 10/04/2021].

Coventry, L. & Branley, D. *(2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward, Maturitas, vol. 113, Jul. 2018.* [on line] Available at: https://www.maturitas.org/article/S0378-5122(18)30165-8/fulltext [consulted 10/04/2021].

Deloitte. (2018). *Smart cyber: How Artificial Intelligence can Help Manage Cyber Risk*. [on line]. Available at: https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-en-smart-cyber-pov-aoda.pdf [consulted 10/04/2021].

Gochhait, G. S. (2020). *Cyber Security Trend Analysis using Web of Science: A Literature review Analysis.European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 7, Issue 06, 2020*. [on line]. Available at: https://ejmcm.com/article_4083_a8e8731dd5ab757b65ea243cb9af2a12.pdf [consulted 10/04/2021].

Herhalt, J. (2011). *Issues Monitor Cyber Crime –A Growing Challenge for Governments*. Zuritch: KPMG [on line]. Available at: https://info.kpmg.us/content/dam/institutes/en/government/pdfs/2011/cyber-crime-growing-challenge.pdf [consulted 10/04/2021].

Jahankhani, H., Al-Nemrat, A., Hosseinian-Far A. (2014). Cyber Crime and Cyber Terrorism Investigator's Handbook. Oxford: Syngress. P149-164

KPMG. (2016). *Five Ways for Governments to Tighten Up Cyber Security*. [on line] Available at: https://home.kpmg/xx/en/home/insights/2016/05/five-ways-for-governments-to-tighten-up-cyber-security.html [consulted 10/04/2021]

KMPG. (2018). *Building Cyber Resilience in Asset Management*. [on line]. Available at: https://assets.kpmg/content/dam/kpmg/uk/pdf/2018/04/building-cyber-resilience-in-asset-management.pdf [consulted 10/04/2021]

Kruse, C. S., Frederick, B., Jacobson, T., & Monticone, D. K. (2017). *Cybersecurity in healthcare: A systematic review of modern threats and trends, Technol. Health Care, vol. 25, no. 1, Feb. 2017*. [on line]. Available at: https://content.iospress.com/articles/technology-and-health-care/thc1263 [consulted 10/04/2021].

Lehto, M. (2013). *The Ways, Means and Ends in Cyber Security Strategies. In Proceedings of The 12th European Conference on Information Warfare and Security (Jyväskylä, 2013) Academic Publishing*. [on line]. Available at:

https://www.researchgate.net/publication/338197891_Lehto_The_Ways_M eans_and_Ends_in_Cyber_Security_Strategies [consulted 10/04/2021].

Leszczyna, R. (2018). *A review of standards with cybersecurity requirements for smart grid, Comput. Secur., vol. 77, Aug. 2018.* [on line]. Available at: https://www.sciencedirect.com/science/article/pii/S0167404818302803?via %3Dihub [consulted 10/04/2021].

Lun, Y. Z., D'Innocenzo, A., Smarra, F., Malavolta, I. & Di Benedetto, M. D. (2019). *State of the art of cyber-physical systems security: An automatic control perspective. J. Syst. Softw., vol. 149. March 2019.* [on line]. Available at: https://www.sciencedirect.com/science/article/abs/pii/S0164121218302681? via%3Dihub [consulted 10/04/2021].

Mandiant, F. (2017). *How Government Agencies are Facing Cyber Security Challenges?*. [on line]. Available at: https://www.fireeye.com/content/dam/fireeye-www/solutions/pdfs/how-govt-agencies-are-facing-cyber-security-challenges.pdf [consulted 10/04/2021]

Mattioli, J., Perico, P., & Robic, P. O. (2020). *Artificial Intelligence based Asset Management. 151-156. 10.1109/SoSE50414.2020.9130505*. [on line] Available at: https://www.cesar-conference.org/wp-content/uploads/2018/11/articles/C&ESAR_2018_J1-03_A-SZYCHTER_Dual_perspective%20_AI_in_Cybersecurity.pdf [consulted 10/04/2021]

Miftahul, U. (2018). *Cyber Culture and Cyber Security Policy Of Indonesia: Combining Cyber Security Civic Discourse, Tenets and Copenhagen's Securitization Theory Analysis*. [on line]. Available at: https://www.researchgate.net/publication/322852237_CYBER_CULTURE_ AND_CYBER_SECURITY_POLICY_OF_INDONESIA_COMBINING_C YBER_SECURITY_CIVIC_DISCOURSE_TENETS_AND_COPENHAG EN'S_SECURITIZATION_THEORY_ANALYSIS_[consulted 10/04/2021]

Mulyadi, D. R. (2018). *Indonesia National Cybersecurity Review: Before and After Establishment National Cyber and Crypto Agency (BSSN)*. [on line]. Available at: https://www.researchgate.net/publication/332073891_Indonesia_National_ Cybersecurity_Review_Before_and_After_Establishment_National_Cyber_ and_Crypto_Agency_BSSN_[consulted 10/04/2021]

Noyons, E. & Moed, H. & Raan, T. (1999). *Integrating Research Performance Analysis and Science Mapping. Scientometrics. 46. 591-604. 10.1007/BF02459614*. [on line]. Available at: https://www.researchgate.net/publication/242916288_Integrating_research_ performance_analysis_and_science_mapping [consulted 10/04/2021].

Ramirez, R., & Choucri, N. (2016). *Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review. IEEE Access, 4, 2216-2243*. [on line]. Available at: https://doi.org/10.1109/access.2016.2544381 [consulted 10/04/2021]

Rizal, M. & Yani, Y. M. (2016). *Cybersecurity Policy and Its Implementation in Indonesia*. [on line]. Available at: https://media.neliti.com/media/publications/70606-EN-cybersecurity-policy-and-its-implementat.pdf [consulted 10/04/2021]

Robinson, S. (2020). *Why The Public Sector is an Increasing Target for Cyber Criminals* . [on line]. Available at: https://www.continuitycentral.com/index.php/news/technology/5731-why-the-public-sector-is-an-increasing-target-for-cyber-criminals [consulted 10/04/2021].

Saleh, Z. (2019). *Artificial Intelligence Definition, Ethics, and Standards*. [on line]. Available at: https://www.researchgate.net/publication/332548325_Artificial_Intelligence_Definition_Ethics_and_Standards [consulted 10/04/2021]

Scholl, M. (2018). *Information Security Awareness in Public Administrations (Provisional chapter) In: Ubaldo Comite, Public Management and Administration. Open Access: INTECH d.d.o. Rijeka (InTechOpen)*. [on line] Available at: https://www.intechopen.com [consulted 10/04/2021]

Smith, G. (2018). T*he Intelligent Solution: Automation, The Skills Shortage, and Cyber-Security. Computer Fraud & Security*. [on line] Available at: https://www.researchgate.net/publication/327027549_The_intelligent_solution_automation_the_skills_shortage_and_cyber-security/ [consulted 10/04/2021]

Sousa, W., Melo, E., Bermejo, P., Farias, R., & Gomes, A. (2019). *How and where is artificial intelligence in the public sector going? A literature review and research agenda. Government Information Quarterly, 36(4), 101392*. [on line]. Available at: https://doi.org/10.1016/j.giq.2019.07.004 [consulted 10/04/2021]

TRPC. (2015). *Public Data At Risk: Cyber Threats to the Networked Government*. [on line]. Available at: http://103.28.101.10/project51new/training/PublicDataAtRisk_Cybersecurity_Apr2015.pdf [consulted 10/04/2021]

United States Government Accountability Office, Report to Congressional Requesters. (2016). *Information Security: Agencies Need to Improve Controls Over Selected High Impact Systems*. [on line]. Available at: https://www.gao.gov/assets/gao-16-501.pdf [consulted 10/04/2021]

Von Solms, R. & Van Niekerk, J. (2013). *From Information Security to Cyber Security. Computers and Security*. [on line]. Available at: https://www.sciencedirect.com/science/article/pii/S0167404813000801 [consulted 10/04/2021].

Wirtz, B. W., Weyerer, J.C., & Geyer, C. (2018). *Artificial Intelligence and The Public Sector—Applications and Challenges*. [on line]. Available at: https://www.tandfonline.com/doi/abs/10.1080/01900692.2018.1498103 [consulted 10/04/2021]