**REFERENCES**

[1] National Cyber Security Centre. ” Example of Supply Chain Attacks.” NCSC. 2018. [Online] Available: https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-attack-examples. [2] A. Yeboah-Ofori, and S. Islam, “Cyber Security Threat Modelling for Supply Chain Organizational Environments.” MDPI. Future Internet. 11, (3), 63, March 2019. doi: 10.3390/611030063. [3] B. Woods, and A. Bochman, “Supply Chain in the Software Era” Scowcroft Center for Strategic and Security. Atlantic Council: Washington, DC, USA, May 2018. [4] ENISA “Exploring the Opportunities and Limitations of Current Threat Intelligence Platforms” Version 1. December 2017. [online] [5] C. Doerr, “Cyber Threat Intelligences Standards – A High Level Overview” TU Delft CTI Labs, 2018. [Online]. Available: https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018- presentations/cyber-threat-intelligence-standardization.pdf. [6] Microsoft Malware Prediction, Research Prediction. 2019. [Online] Available: https://www.kaggle.com/c/microsoft-malware-prediction/data. [7] A. Yeboah-Ofori, J. D. Abduli, F. Katsriku, “Cybercrime and Risks for Cyber Physical Systems” International Journal of Cyber Security and Digital Forensics. Vol.8 No1, pp 43-57. 2019. [8] CAPEC-437, Supply Chain. Common Attack Pattern Enumeration and Classification: Domain of Attack. October 2018. [Online] Available: https://capec.mitre.org/data/definitions/437.html. [9] Open Web Application Security Project (OWASP). The Ten Most Critical Application Security Risks. Creative Commons Attribution-Share Alike 4.0 International License. 2017. [Online] Available: https://owasp.org/www-pdf-archive/OWASP\_Top\_10- 2017\_%28en%29.pdf.pdf. [10] US-Cert. “Building Security in Software & Supply Chain Assurance.” 2020. [Online] Available: https://www.us-cert.gov/bsi/articles/knowledge/attack-patterns. [11] R. D. Labati, A. Genovese, V. Piuri and F. Scotti, "Towards the Prediction of Renewable Energy Unbalance in Smart Grids," 2018 IEEE 4th International Forum on Research and Technology for Society and Industry (RTSI), Palermo, Italy, 2018, pp. 1-5, doi: 10.1109/RTSI.2018.8548432. [12] J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”. NIST Computer. Sec. 2015, SP800, 1, doi:10.6028/NIST.SP.800. [13] NIST 2018 “Framework for Improving Critical Infrastructure Cybersecurity” National Institute of Standards and Technology. Ver. 1.1. https://doi.org/10.6028/NIST.CSWP.04162018. [14] J. F Miller, “Supply Chain Attack Framework and Attack Pattern”. MITRE Technical Report. MTR140021. 2013. [Online] Available: https://www.mitre.org/sites/default/files/publications/supply-chain-attack-framework-14-0228.pdf. [15] C. Ahlberg, C. Pace, “What Are the Phases of The Threat Intelligence Lifecycle?” The Threat Intelligence Handbook. A Practical Guide for Security Teams to Unlock the Power of Intelligence. CyberEdge Group. LLC. Annapolis MD. USA. 2018. [16] J, Freidman, and M Bouchard, “Definition Guode to Cyber Threat Intelligence. Using Knowledge About Adversary to Win The War Against Targeted Attacks.” iSightPartners.CyberEdge Group LLC. Annapolis, MD. USA 2018. [17] EY. Cyber Threat Intelligence: Designing, Building and Operating an Effective Program. 2016. [Online] Available: https://relayto.com/ey-france/cyber-threat-intelligence-report-js5wmwy7/pdf. [18] A. Yeboah-Ofori and C. Boachie, "Malware Attack Predictive Analytics in a Cyber Supply Chain Context Using Machine Learning," 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), 2019, pp. 66-73, doi: 10.1109/ICSIoT47925.2019.00019. [19] B. Gallagher and T. Eliassi-Rad. “Classification of HTTP Attacks: A Study on the ECML/PKDD 2007 Discovery Challenge”. Lawrence Liverpool National Laboratory (LLNL) Livermore, CA. 2009. doi.org/10.2172/1113394. [20] D. Bhamare, T. Salman, M. Samaka, A. Erba and R. Jain. “Feasibility of Supervised Machine Learning for Cloud Security” 3rd International Conference on Information Science and Security. IEEE Xplore. 2016. DOI: 10.1109/ICISSEC.2016.7885853. [21] A. L. Buczak, and E. Guven. “A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection”. IEEE Communications Surveys & Tutorials. Vol. 18. NO. 2, 2nd Quarter. 2016. DOI: 10.1109/COMST.2015.2494502 [22] O. Yavanoglu and M. Aydos. “A Review of Cyber Security Dataset for Machine Learning Algorithms” International Conference on Big Data, IEEE Xplore. Jan 2018. DOI: 10.1109//BigData.2007.8258167. [23] E. G. V. Villano. “Classification of Logs Using Machine Learning” M. S. Thesis. Norwegian University of Science and Technology. Norway. 2018 [24] R. C. Borges Hink, J. M. Beaver, M. A. Buckner, T. Morris, U. Adhikari and S. Pan, "Machine learning for power system disturbance and cyber-attack discrimination," 2014 7th International Symposium on Resilient Control Systems (ISRCS), Denver, CO, USA, 2014, pp. 1-8, doi: 10.1109/ISRCS.2014.6900095. [25] A. Gumaei, M. M. Hassan, S. Huda, Md. R. Hassan, D. Camacho, J. D. Ser, G. Fortino, "A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids.” Elsevier Science Direct. Applied Soft Computing, Vol. 96,106658, Nov. 2020, doi.org/10.1016/j.asoc.2020.106658.