

Active learning-based mobile malware detection utilizing auto-labeling and data drift detection

Deng, Zhe; Hubert, Arthur; **Ben Yahia, Sadok**; **Bahsi, Hayret** Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience, CSR 2024 2024 / p. 146 - 151 <https://doi.org/10.1109/CSR61664.2024.10679343> [Article at Scopus](#) [Article at WOS](#)

Analysis of national cyber situational awareness practices

Bahsi, Hayret Strategic cyber defense : a multidisciplinary perspective 2017 / p. 31-41 <https://doi.org/10.3233/978-1-61499-771-9-31>

Android malware concept drift using system calls : detection, characterization and challenges

Guerra Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayret** Expert systems with applications 2022 / art. 117200, 19 p. : ill <https://doi.org/10.1016/j.eswa.2022.117200> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Anomalous File System Activity detection through Temporal Association rule mining

Reza, M.; Iman, H.; **Chikul, Pavel**; **Jervan, Gert**; **Bahsi, Hayret**; **Ghasempouri, Tara** Proceedings of the 9th International Conference on Information Systems Security and Privacy ICISSP. Vol. 1 2023 / p. 733-740 <https://doi.org/10.5220/0000168400003405>

Capability detection and evaluation metrics for cyber security lab exercises

Caliskan, Emin; Tatar, Unal; **Bahsi, Hayret**; **Ottis, Rain**; **Vaarandi, Risto** Proceedings of the 12th International Conference on Cyber Warfare and Security, ICCWS 2017 2017 / p. 407-414 : ill <https://www.scopus.com/record/display.uri?eid=2-s2.0-85018944652&origin=inward&txId=dad813d957372581ca0932bf6e4fb5d8>

A case study about the use and evaluation of cyber deceptive methods against highly targeted attacks

Farar, Alexandria Elaine; **Bahsi, Hayret**; Blumbergs, Bernhards 2017 International Conference On Cyber Incident Response, Coordination, Containment and Control, Cyber Incident 2017 : London, United Kingdom, 19 June 2017 through 20 June 2017 2017 / [7] p. : ill <https://doi.org/10.1109/CYBERINCIDENT.2017.8054640>

A comparative framework for cyber threat modelling : case of healthcare and industrial control systems

Balogun, Taofeek Mobolarinwa; **Bahsi, Hayret**; Keskin, Omer F.; Tatar, Unal International Journal of Critical Infrastructures 2021 / 1 p <https://doi.org/10.1504/IJCIS.2024.10046187>

A comparative framework for cyber threat modelling: case of healthcare and industrial control systems

Balogun, Taofeek Mobolarinwa; **Bahsi, Hayret**; Keskin, Omer F.; Tatar, Unal International Journal of Critical Infrastructures 2023 / p. 405-431 <https://doi.org/10.1504/IJCIS.2023.133282> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Concept drift and cross-device behavior : challenges and implications for effective android malware detection

Guerra Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayret** Computers & Security 2022 / art. 102757, 20 p. : ill <https://doi.org/10.1016/j.cose.2022.102757> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

A conceptual nationwide cyber situational awareness framework for critical infrastructures

Bahsi, Hayret; **Maennel, Olaf Manuel** Secure IT systems : 20th Nordic Conference, NordSec 2015, Stockholm, Sweden, October 19-21, 2015 : proceedings 2015 / p. 3-10 : ill https://doi.org/10.1007/978-3-319-26502-5_1 [Conference Proceedings at Scopus](#) [Article at Scopus](#) [Conference Proceedings at WOS](#) [Article at WOS](#)

Corrigendum to Concept drift and cross-device behavior: Challenges and implications for effective android malware detection Computers & Security, Volume 120, 102757 (Computers & Security (2022) 120, (S0167404822001523), (10.1016/j.cose.2022.102757))

Guerra-Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayret** Computers and Security 2023 / art. 102998 <https://doi.org/10.1016/j.cose.2022.102998> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

A cyber attack taxonomy for microgrid systems

Bahsi, Hayret; **Dola, Henry Ochieng**; **Khalil, Shaymaa Mamdouh**; **Korötko, Tarmo** 2022 17th Annual System of Systems Engineering Conference (SOSE) 2022 / p. 324-331 <https://doi.org/10.1109/SOSE55472.2022.9812642>

Cyber incident management in low-income countries

Hountomey, Jean-Robert; **Bahsi, Hayret**; Tatar, Unal; Hashem, Sherif; Dubois, Elisabeth 2022 <https://cybilportal.org/wp-content/uploads/2022/01/CSIRTs-In-Low-Income-Countries-Final-Report-part-1-v16.pdf> <https://thegfce.org/working-groups/working-group-b/>

Cyber incident management in low-income countries

Hountomey, Jean-Robert; **Bahsi, Hayret**; Tatar, Unal; Hashem, Sherif; Dubois, Elisabeth 2022 <https://cybilportal.org/wp-content/uploads/2022/01/CSIRTs-In-Low-Income-Countries-Final-Report-part-2-v16.pdf> <https://thegfce.org/working-groups/working-group-b/>

The cyber-insurance market in Norway

Bahsi, Hayret; Franke, Ulrik; Langfeldt Friberg, Even Information and computer security 2020 / p. 54-67 <https://doi.org/10.1108/ICS-01-2019-0012> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Cybersecurity knowledge requirements for strategic level decision makers

Garcia-Granados, F.; **Bahsi, Hayret** Proceedings of the 15th International Conference on Cyber Warfare and Security (ICWS) : Old Dominion University (ODU), Norfolk, Virginia, USA, 12-13 March 2020 2020 / p. 559-568 <https://doi.org/>

Deep learning-based detection of cyberattacks in software-defined networks

Mirsadeghi, Seyed Mohammad Hadi; Bahsi, Hayret Digital forensics and cyber crime : 13th EAI international conference, ICDF2C 2022, Boston, MA, November 16-18, 2022 : proceedings 2023 / p. 341-354 https://doi.org/10.1007/978-3-031-36574-4_20

Differences in Android behavior between real device and emulator : a malware detection perspective

Guerra Manzanares, Alejandro; Bahsi, Hayret 6th International Conference on Internet of Things: Systems, Management and Security (IOTSMS), Granada, Spain, October 22-25, 2019 2019 / art. 8939268, p. 399-404 <https://doi.org/10.1109/IOTSMS48152.2019.8939268>

Digital forensic analysis of mobile automotive maintenance applications

Sumaila, Faisal; Bahsi, Hayret Forensic Science International : Digital Investigation 2022 / art. 301440 <https://doi.org/10.1016/j.fsi.2022.301440> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Dimensionality reduction for machine learning based IoT botnet detection

Bahsi, Hayret 15th International Conference on Control, Automation, Robotics and Vision (ICARCV 2018) : Singapore, November 18-21, 2018 2018 / p. 1857-1862 : ill <https://doi.org/10.1109/ICARCV.2018.8581205>

Elutähtsate teenuste ristsõltuvuse analüüs

Laud, Peeter; **Bahsi, Hayret**; **Lenin, Aleksandr**; Mändmaa, Kalev; **Priisalu, Jaan**; Tuuling, Reedik Sõjateadlane 2020 / lk. 207-237 https://www.ester.ee/record=b4555087*est

Enhancing IoT botnet attack detection in SOCs with an explainable active learning framework

Kalakoti, Rajesh; Nömm, Sven; Bahsi, Hayret 2024 IEEE World AI IoT Congress (AlloT) 2024 / p. 265 - 272 <https://doi.org/10.1109/AlloT61789.2024.10578957> [Article at Scopus](#) [Article at WOS](#)

Enhancing privacy risk modeling in practice: a case study of an e-justice system

Gakh, Valerii; **Bahsi, Hayret**; Hoffmann, Thomas; Boyarchuk, Artem; Khramov, Oleksii IEEE Access 2024 / p. 183851-183874 <https://doi.org/10.1109/ACCESS.2024.3509332>

Expert knowledge elicitation for skill level categorization of attack paths

Mezešova, Terezia; **Bahsi, Hayret** 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) 2019 / 8 p. : tab <https://doi.org/10.1109/CyberSecPODS.2019.8885192>

Expert knowledge elicitation for skill level categorization of attack paths

Mezešova, Terezia; **Bahsi, Hayret** Cyber science 2018 : conference programme 2018 / p. 29 <https://www.c-mric.com/wp-content/uploads/2018/04/20180611-Cyber-Science-2018-Event-Brochure-DRAFT-v0.6.pdf>

Experts still needed : boosting long-term android malware detection with active learning

Guerra-Manzanares, Alejandro; Bahsi, Hayret Journal of Computer Virology and Hacking Techniques 2024 / p. 901 - 918 <https://doi.org/10.1007/s11416-024-00536-y> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Explainable federated learning for Botnet Detection in IoT networks

Kalakoti, Rajesh; Bahsi, Hayret Proceedings of the 2024 IEEE International Conference on Cyber Security and Resilience (CSR), September 2-4, 2024, London, UK 2024 / p. 22-29 <https://doi.org/10.1109/CSR61664.2024.10679348> [Article at Scopus](#) [Article at WOS](#)

Forensics analysis of an on-line game over Steam Platform

Tabuyo-Benito, Raquel; **Bahsi, Hayret**; Peris-Lopez, Pedro Digital Forensics and Cyber Crime : 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10-12, 2018, Proceedings 2019 / p. 106-127 https://doi.org/10.1007/978-3-030-05487-8_6 [Conference proceeding at Scopus](#) [Article at Scopus](#)

Hybrid cybersecurity research and education environment for maritime sector

Visky, Gabor; Šiganov, Aleksei; Rehman, Muaan ur; Vaarandi, Risto; Bahsi, Hayret 2024 IEEE International Conference on Cyber Security and Resilience (CSR) : proceedings 2024 / p. 644-651 <https://doi.org/10.1109/CSR61664.2024.10679392>

Hybrid feature selection models for machine learning based botnet detection in IoT networks

Guerra Manzanares, Alejandro; Bahsi, Hayret 2019 International Conference on Cyberworlds : CW 2019 : 2-4 October 2019, Kyoto, Japan : proceedings 2019 / p. 324-327 : ill <https://doi.org/10.1109/CW.2019.00059>

Impact assessment of cyber actions on missions or business processes : a systematic literature review

Bahsi, Hayrettdin; Udokwu, Chibuzor; Tatar, Unal; **Norta, Alexander** Proceedings of the 13th International Conference on Cyber Warfare and Security, ICCWS 2018 : National Defence University, Washington DC, USA, 6-9 March 2018 2018 / p. 11-20 : ill <http://toc.proceedings.com/38822webtoc.pdf>

Improving IoT security with explainable AI : quantitative evaluation of explainability for IoT botnet detection

Kalakoti, Rajesh; Bahsi, Hayrettdin; Nömm, Sven IEEE Internet of Things Journal 2024 / p. 18237 - 18254
<https://doi.org/10.1109/IJOT.2024.3360626> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Improving transparency and explainability of deep learning based IoT botnet detection using explainable artificial intelligence (XAI)

Kalakoti, Rajesh; Nömm, Sven; Bahsi, Hayrettdin 22nd IEEE International Conference on Machine Learning and Applications : ICMLA 2023 : 15-17 December 2023, Jacksonville Riverfront, Florida : proceedings (2023) 2023 / p. 595 - 601
<https://doi.org/10.1109/ICMLA58977.2023.00088>

In-depth feature selection and ranking for automated detection of mobile malware

Guerra Manzanares, Alejandro; Nömm, Sven; Bahsi, Hayrettdin Proceedings of the 5th International Conference on Information Systems Security and Privacy : ICISSP 2019 : February 23-25, 2019, Prague, Czech Republic. Vol. 1 2019 / p. 274-283 : ill
<https://doi.org/10.5220/0007349602740283>

In-depth feature selection for the statistical machine learning-based botnet detection in IoT networks

Kalakoti, Rajesh; Nömm, Sven; Bahsi, Hayrettdin IEEE Access 2022 / p. 94518-94535
<https://doi.org/10.1109/ACCESS.2022.3204001> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

KronoDroid : time-based hybrid-featured dataset for effective android malware detection and characterization

Guerra Manzanares, Alejandro; Bahsi, Hayrettdin; Nömm, Sven Computers & Security 2021 / art. 102399, 32 p
<https://doi.org/10.1016/j.cose.2021.102399> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Learning from few cyber-attacks : addressing the class imbalance problem in machine learning-based intrusion detection in software-defined networking

Mirsadeghi, Seyed Mohammad Hadi; Bahsi, Hayrettdin; Vaarandi, Risto; Inoubli, Wissem IEEE Access 2023 / p. 140428 - 140442 <https://doi.org/10.1109/ACCESS.2023.3341755> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Leveraging the first line of defense : a study on the evolution and usage of android security permissions for enhanced android malware detection

Guerra Manzanares, Alejandro; Luckner, Marcin; **Bahsi, Hayrettdin** Journal of Computer Virology and Hacking Techniques 2022 / 32 p. : ill <https://doi.org/10.1007/s11416-022-00432-3> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Machine learning-based detection and characterization of evolving threats in mobile and IoT Systems = Masinõppepõhine arenevate ohtude tuvastamine ning kirjeldamine mobiilseadmete ja värkvõrkude jaoks

Guerra Manzanares, Alejandro 2022 <https://doi.org/10.23658/taltech.54/2022> <https://digikogu.taltech.ee/et/Item/f56ae778-e5a5-4147-a8e4-4833e08fa789> https://www.ester.ee/record=b5511898*est

A machine learning-based forensic tool for image classification - a design science approach

Del Mar-Raave, Joanna Rose; Bahsi, Hayrettdin; Mrcic, Leo; Hausknecht, Kresimir Forensic Science International : Digital Investigation 2021 / art. 301265, 13 p <https://doi.org/10.1016/j.fsidi.2021.301265> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Mapping cyber attacks on the internet of medical things : a taxonomic review

Kondeti, Venkatesh; Bahsi, Hayrettdin 2024 19th Annual System of Systems Engineering Conference (SoSE) 2024 / p. 84 - 91
<https://doi.org/10.1109/SOSE62659.2024.10620925> [Article at Scopus](#) [Article at WOS](#)

Mapping the information flows for the architecture of a nationwide situation awareness system : (Poster)

Bahsi, Hayrettdin; Dieves, Veiko; **Kangilaski, Taivo;** Laud, Peeter; **Mõtus, Leo;** Murumets, Jaan; Ploom, Illimar; **Priisalu, Jaan;** Seeba, Mari; **Täks, Ermo;** Tammel, Kaide; **Tamppuu, Piia;** **Taveter, Kuldar;** Trumm, Avo; Truusa, Tiia-Triin; Vihailemm, Triin Proceedings 2019 IEEE International Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA) : Las Vegas, NV, USA, 8-11 April 2019 2019 / p. 152-157 <https://doi.org/10.1109/COGSIMA.2019.8724167>

Maritime cyber-insurance : The Norwegian case : [abstract]

Franke, Ulrik; Langfeldt Friberg, Even; Bahsi, Hayrettdin International Journal of Critical Infrastructures 2022 / p. 267-286
<https://doi.org/10.1504/IJCS.2022.10046729>

MedBloT : generation of an IoT Botnet Dataset in a medium-sized IoT network

Guerra Manzanares, Alejandro; Medina-Galindo, Jorge; Bahsi, Hayrettdin; Nömm, Sven Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP : February 25-27, 2020, La Valletta, Malta. Vol. 1 2020 / p. 207-218 : ill <https://doi.org/10.5220/0009187802070218>

Model-based analysis of secure and patient-dependent pacemaker monitoring system

Tsiopoulos, Leonidas; Kuusik, Alar; Vain, Jüri; Bahsi, Hayrettdin Body Area Networks. Smart IoT and Big Data for Intelligent Health : 15th EAI International Conference, BODYNETS 2020, Tallinn, Estonia, October 21, 2020 : proceedings 2020 / p. 77-91
https://doi.org/10.1007/978-3-030-64991-3_6 [Journal metrics at scopus](#) [Article at Scopus](#)

On the application of active learning for efficient and effective IoT botnet detection

Guerra Manzanares, Alejandro; Bahsi, Hayrettdin Future Generation Computer Systems 2023 / p. 40-53 : ill
<https://doi.org/10.1016/j.future.2022.10.024> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

On the application of active learning to handle data evolution in Android malware detection

Guerra Manzanares, Alejandro; Bahsi, Hayrettdin Digital forensics and cyber crime : 13th EAI international conference, ICDF2C 2022, Boston, MA, November 16-18, 2022 : proceedings 2023 / p. 256-273 https://doi.org/10.1007/978-3-031-36574-4_15

On the relativity of time : implications and challenges of data drift on long-term effective android malware detection

Guerra Manzanares, Alejandro; Bahsi, Hayrettdin Computers & Security 2022 / art. 102835, 15 p. : ill
<https://doi.org/10.1016/j.cose.2022.102835> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

An ontology engineering case study for advanced digital forensic analysis

Chikul, Pavel; Bahsi, Hayrettdin; Maennel, Olaf Manuel Model and Data Engineering : 10th International Conference, MEDI 2021, Tallinn, Estonia, June 21–23, 2021 : proceedings 2021 / p. 67–74 https://doi.org/10.1007/978-3-030-78428-7_6 [Conference Proceedings at Scopus](#) [Article at Scopus](#)

Preliminary analysis of cyberterrorism threats to internet of things (IoT) applications

Balogun, Taofeek Mobolarinwa; Bahsi, Hayrettdin; Karabacak, Bilge Terrorists' use of the Internet 2017 / p. 49-58
<http://doi.org/10.3233/978-1-61499-765-8-49>

Preliminary analysis of cyberterrorism threats to internet of things (IoT) applications [Online resource]

Bahsi, Hayrettdin Advanced Research Workshop supported by the NATO Science for Peace and Security Programme, Terrorists' Use of the Internet : assessment and response 2016 / p. 8 <http://www.cyberterrorism-project.org/wp-content/uploads/2016/11/Terrorists%E2%80%99-Use-of-the-Internet-Assessment-and-Response.pdf>

A systematic literature review of cyber security monitoring in maritime

Vaarandi, Risto; Tsiopoulos, Leonidas; Visky, Gabor; Rehman, Muan Ur; Bahsi, Hayrettdin IEEE Access 2025 / p. 85307-85329 <https://doi.org/10.1109/ACCESS.2025.3567385>

The invisible front : a cyber resilience perspective

Bahsi, Hayrettdin The geopolitics of power grids : political and security aspects of Baltic electricity synchronization : March 2018 2018 / p. 53–68 : ill https://www.ester.ee/record=b5053315*est

Threat modeling of cyber-physical systems - a case study of a microgrid system

Khalil, Shaymaa Mamdouh; Bahsi, Hayrettdin; Dola, Henry Ochieng; Korötko, Tarmo; McLaughlin, Kieran; **Kotkas, Vahur** Computers & Security 2023 / art. 102950, 16 p. : ill <https://doi.org/10.1016/j.cose.2022.102950> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Threat modeling of industrial control systems: A systematic literature review

Khalil, Shaymaa Mamdouh; Bahsi, Hayrettdin; Korötko, Tarmo Computers and security 2024 / art. 103543, 19 p. : ill
<https://doi.org/10.1016/j.cose.2023.103543> [Journal metrics at Scopus](#) [Article at Scopus](#) [Journal metrics at WOS](#) [Article at WOS](#)

Time-frame analysis of system calls behavior in machine learning-based mobile malware detection

Guerra Manzanares, Alejandro; Nömm, Sven; Bahsi, Hayrettdin 2019 International Conference on Cyber Security for Emerging Technologies : CSET 2019, Doha, Qatar, 27 October 2019 through 29 October 2019 2019 / art. 89049088 ; 8 p. : ill
<https://doi.org/10.1109/CSET.2019.8904908>

Towards the integration of a post-hoc interpretation step into the machine learning workflow for IoT botnet detection

Guerra Manzanares, Alejandro; Nömm, Sven; Bahsi, Hayrettdin 18th IEEE International Conference on Machine Learning and Applications : ICMLA 2019, 16–19 December 2019, Boca Raton, Florida, USA : proceedings 2019 / p. 1162-1169 : ill
<https://doi.org/10.1109/ICMLA.2019.00193>

Unsupervised anomaly based botnet detection in IoT networks

Nömm, Sven; Bahsi, Hayrettdin 17th IEEE International Conference on Machine Learning and Applications : ICMLA 2018, 17–20 December 2018, Orlando, Florida, USA : proceedings 2018 / p. 1048-1053 <https://doi.org/10.1109/ICMLA.2018.00171>

Using MedBloT dataset to build effective machine learning-based IoT botnet detection systems

Guerra Manzanares, Alejandro; Medina-Galindo, Jorge; Bahsi, Hayrettdin; Nömm, Sven Information Systems Security and Privacy : 6th International Conference, ICISP 2020, Valletta, Malta, February 25–27, 2020 : revised selected papers 2022 / p. 222–243 https://doi.org/10.1007/978-3-030-94900-6_11 [Conference proceedings at Scopus](#) [Article at Scopus](#) [Article at WOS](#)

