# Cybersecurity & Critical Infrastructure Protection (CCIP) Research Group

**Objectives and Scope**: **Kadir Has University's Center for Cybersecurity & Critical Infrastructure Protection (CCIP)**, established in 2018, is one of the first centres focusing on Critical Infrastructure Protection (CIP) research, such as security of Industrial Control Systems (ICS), detection of advanced cyber threats (malware, anomalies etc.) and leveraging AI technologies for cybersecurity in Turkey. CCIP aims to become a hub for the researchers on cybersecurity and CIP both in Turkey and its close region.

CCIP's research capacity relies on the axis of two aspects: *Technical Aspects* (Computer Engineering, Management & Information Systems etc.), and *Human Aspects* (Computational Social Sciences, International Relations, Psychology etc.) of cybersecurity. Based on its multidisciplinary team, CCIP does research on different angles of cybersecurity including resilience, innovative cyber threat detection methods, management of cyber threats etc.

Research Center's R&D activities are divided into three main areas: **Developing solutions towards industry and scientific community**, **providing trainings for researchers and professionals**, **capacity building** and **networking**. Therefore, **the main objective of CCIP** is to develop methods, tools, and strategies to detect, identify, and prevent all types of cyber-attacks through state of art research; to educate researchers and society; to collaborate with private sector, research organizations, non-for-profit organizations and local/national authorities and policy makers depending on CCIP's in-depth knowledge and expertise on cybersecurity and its various applications both in Pan-European and Global context.

**Skills and Expertise**:
**1) Advanced Malware Detection Methods: Malware Classification using Ensemble Models**: Traditional deep learning architectures' components, such as batch normalization and max pooling, cause architecture to be more complex and the models to be more sensitive to data. The capsule network architectures, on the other hand, reduce the aforementioned complexities by eliminating these components. Therefore, our study focuses on creating a new ensemble of capsule networks-based malware type classification task. For this purpose, we have created random capsule forest model (inspired by Random Forest) for predicting malware types.
**2) Anomaly Detection in Critical Infrastructures and Federated Anomaly Detection from Logs:** Critical infrastructures (CI) refer to systems which are essential to the health, safety, security and well-being of country. Emergence of Industry 4.0 and Internet of Things (IoT) technologies extends CI systems to become more decentralized and interconnected. It also enhances edge devices' computing powers and ability to create vast amount of data. Despite that, these advancements motivate Information Technologies (IT) - Operational Technologies (OT) convergence which increases vulnerabilities in CIS. Cyber-attacks can cause disruptions in CI which may result in catastrophic consequences. Our team studies on building decentralized learning mechanism to detect anomalies leveraging NLP-based log analysis. It aims to enhance detection speed and perception of anomalies.
**3) Machine Learning and Deep Learning Applications on Cyber Security Data.**
**4) Deep Learning for Anomaly Detection in Critical Infrastructures.**

**Recent Successful National and International Projects**:
**1) TUBITAK-QNRF-WARNNING** (***A Defense-in-depth Cyber Intelligence Platform to Defend against Emerging Cyber Attacks***) (Partner)**:** In 2018, KHAS CCIP was awarded with a prestigious grant by TUBITAK (The Scientific and Technological Research Council of Turkey) and QNRF (Qatar National Research Fund) Joint Call (Academia-Industry Cooperation on Cybersecurity) and completed WARNNING (A Defense-in-depth Cyber Intelligence Platform to Defend against Emerging Cyber Attacks) Project. This project was established for developing a defense-in-depth Cyber Threat Intelligence platform capable of analysing big security data and produces actionable intelligence in an efficient and timely manner. The main goal of the developed platform was to help individual organisations and the nation as a whole to better defend against the most common and severe external threats, as well as the sophisticated ones such as zero-days, APTs, and the targeted attacks.

**2) MSCA-RISE-2020-AI4LABOUR** (Coordinator): Research regarding the future of work suggests that 30 % of the hours worked globally could be automated by 2030. Focussing on the impact this will have on jobs and skills, the EU-funded AI4LABOUR project aims to predict the types of occupations that will appear in the future and the skills these will require as well as the training needed to gain these skills. To achieve this, the project will design a novel artificial intelligence skill-based model and a skill development methodology. The project's work will create the foundation for a web portal that links role, skill and learning recommendations for all actors.

**3) TUBITAK 2244-Industrial PhD programme for Developing Novel Industry 4.0 based Production Techniques with Big Data Analytics** (Coordinator): The primary purpose of this research project is to train PhD students who will then be able to combine the theoretical aspects of the field with the practices at the market and actively perform R&D activities. This project also aims to develop new scientific methods capable of optimizing the production process of smart industrial automation systems as a whole based on sensor technologies that have come into prominence in recent years. The PhD students are expected to convey what they will experience during this process through working in the R&D department of the company and thus combine the scientific working techniques with the production processes. Besides these successfully funded projects, CCIP group has been applying to several EU-funded, international, and national projects since 2018 (e.g., WIDENING-Twinning, MSCA-ITN/DN, MSCA-RISE, H2020 IA, etc.).

**Awards:** Kaggle Microsoft Malware Prediction Competition – Microsoft has sponsored for two data science competitions in cybersecurity domain at Kaggle platform. In 2019 competition, Kadir Has CCIP team is placed at 5th among 2,426 teams. Our work is presented as 'Use Case Study: Data Science Application for Microsoft Malware Prediction Competition on Kaggle' at International conference on Data Science, Machine Learning and Statistics (2019). This paper, as a use case of a data science application in cybersecurity domain, aims to show that a general data science pipeline might be more useful than many complex models.

**Research Team:**

**Prof. Dr. Hasan Dağ:** Dr. Dağ is a full Prof. in Kadir Has University and director of CCIP. His current research interests can be divided into four main areas: power systems, data science, computational science, and management information systems.

**Dr. E. Fatih Yetkin:** Dr. Yetkin's main research interests are numerical linear algebra, high performance computing and machine learning. In his early studies, he focused on soft-error problem in high-performance systems and applied linear algebra. His active research areas is machine learning in industrial control systems.

**Assoc. Prof. Salih Bıçakcı:** Dr. Bicakci is an associate Prof. in Kadir Has University, International Relations Department. He gave lectures on the Middle East in International Politics, International Security, International Relations Theory, and Turkish Foreign Policy at various universities. In recent years, he has focused his work on cyber security and protection of critical infrastructures.

**Dr. Aykut Çayır:** Dr. Çayır's research areas are statistical, machine and deep learning and their applications on cybersecurity.

**Uğur Ünal:** Ünal is enrolled in the PhD Program in Management Information Systems at Kadir Has University. His study focused on text mining and natural language processing methods for cybersecurity making use of log analysis.

**Ayhan Gücüyener:** Gücüyener is enrolled in PhD Kadir Has University, International Relations Program. Her research areas are focusing on energy security, cyber security policies in international relations and cyber security dimension of energy security.

**Ferhat Demirkıran:** Demirkıran is enrolled in cybersecurity masters program in Kadir Has University and dealing with machine learning and deep learning applications on cyber security data.

**Berkant Düzgün:** Düzgün is currently doing his master's degree in Management Information Systems at Kadir Has University. He works on natural language processing algorithms based on deep learning for anomaly detection in critical infrastructures.

**Recent Publications:**

**(1)** S Cools, E.F Yetkin, E Agullo, L Giraud, W Vanroose, "Analysing the effect of local rounding error propagation on the maximal attainable accuracy of the pipelined conjugate gradient method", SIAM Journal on Matrix Analysis and Applications, 39 (1), pp.426-450
**(2)** E. Agullo, S. Cools, E. F. Yetkin, L. Giraud, N. Schenkels, and W. Vanroose, "On Soft Errors in the Conjugate Gradient Method: Sensitivity and Robust Numerical Detection," SIAM Journal on Scientific Computing 2020 42:6, C335-C358
**(3)** I.S. Lamprianidou, T.A. Papadopoulos, G.C. Kryonidis, E. Fatih Yetkin, K.D. Pippi, A.I. Chrysochos, "Assessment of load and generation modelling on the quasi-static analysis of distribution networks", Sustainable Energy, Grids and Networks, Volume 27, 2021.
**(4)** A. Çayır, U. Ünal, H. Dağ, "Random CapsNet forest model for imbalanced malware type classification task", Computers and Security,102133, 2021

**We are interested in** the Secure societies – Protecting freedom and security of Europe and its citizens calls including but not limited to HORIZON-CL3-2021-INFRA-01-01; HORIZON-CL3-2021-CS-01-01; HORIZON-CL3-2021-CS-01-04

**Role as a Partner**: We have expertise on advanced security and privacy management approaches including the following:

(i) AI-based static, dynamic and behaviour-based attack detection, information-hiding, deceptive, self-healing, and scalable techniques;
(ii) Threat detection frameworks (e.g., collaborative, open, and dynamic repositories of information on threats and vulnerabilities; build on and update existing ontologies, taxonomies and models; dynamic tools for automated detection with advanced analytic capabilities, and where possible response and recovery; and synchronised real time self- encryption/decryption schemes with recovery capabilities.);
(iii) Immersive and highly realistic, pattern-driven modelling and automated tools for checking the security and privacy of data, and supporting computer-aided security design (e.g., automatic code generation);
(iv) Real-time, dynamic, accountable and secure trust, identity and access management in order to ensure secure, privacy-enabled, interoperable and scalable devices, systems, online products and businesses.

Our contribution to a possible consortium will be the provision of comprehensive, resource-efficient, and flexible security analytics and threat intelligence, keeping pace with new vulnerabilities and threats in order to enable EU industry better prepared for the threats to IoT, ICS, AI and other systems. We also would like to have the responsibility on the standardisation and automated assessment frameworks for secure networks and systems, allowing better-informed investment decisions related to security and privacy.

**Contacts : h2020@khas.edu.tr ; ayhan.gucuyener@khas.edu.tr**