Research and Development Center for Cybersecurity and Critical Infrastructure Protection
Team. The research capacity of the center has three disciplines. Engineering and Information Systems, International Relations as the Social Science part, and Law.

Engineering and Information Systems Team: Hasan Dağ, PhD; E. Fatih Yetkin, PhD, Tamer Dağ, PhD, Aykut Çayır, Zeeshan Rafi, and Uğur Ünal PhD Students, Abdülkadir Özçelik, undergraduate student.
Social Science Team: Akın Ünver, PhD; Mitat Çelikpala, PhD; Salih Bıçakçı, PhD; (Sinem Açıkmeşe, PhD; and Mustafa Aydın, PhD; as additional collaborators), 1 PhD student.
Law Team: Aslıhan Erbaş Açıkel, PhD.

Vision, Mission, and Objectives
***Vision*:** We advocate state of art research and development for the fast-and-never ending cybersecurity related issues (attacks, vulnerabilities, defense etc.) to safeguard the well-being of society in general, but institutions and companies in specific.

***Mission*:** Our mission is to develop methods, tools, and strategies to detect, identify, and mitigate all types of cybersecurity related threats for institutions, companies, and nationally important industrial control systems.

***Objective*:** Our objective is to develop methods, tools, and strategies to detect, identify, and prevent all types of cyber-attacks through state of art research, train personal and society, education students of all level while providing consultancy to relevant companies, institutions, organizations, and governments.

Our Expertise:
Our R&D and application efforts are divided into three sectors:
1) Development of innovative methodologies and tools for cybersecurity related issues. Most of those methodologies are aimed to be applicable to industrial control systems.
2) Cyber-physical protection of national and International (energy) systems.
3) Law implication of all research and application activities of cybersecurity, cyber-physical, and physical protection systems. For example, involvement in the legal working groups of Nabucco and Tanap Natural Gas Pipeline Projects and involvement in the negotiations of the related intergovernmental agreements and the host government agreements.

1) We provide Regular services

We are a comparatively a newly founded research center for Cybersecurity and Critical Infrastructure Protection. While conducting technical R&D we also look at the problem from social and law context as well. Thus, the research team of the center is composed of three disciplines. Thus, our regular services are covering a broad range.

A) Research, development, and application of cybersecurity related studies to industrial problems
B) Consultancies in a broad area of cybersecurity and digitalization such as:
- On conflict research, computational methods and digital crisis communication, 'Digital Agent-based Modelling of Civil Wars'.
- Machine and deep learning-based malware detection and prevention methods
- Training on cyber-thing (security, war, warfare, terrorism etc.)
- On cyber and cyber-physical protection (of Industrial Control Systems, ICs)
- wireless sensor networks, indoor positioning systems and software defined networks.

- Protection of current communication infrastructures (including 4G and SDN/NVF), analyse in depth potential cascading effects and impact on dependent critical infrastructures and mission critical services
- The project on the CI *Health Services* will focus on physical and cyber protection of health services and infrastructures. In particular, it will contribute to better protect health-sector related building management systems and IT infrastructures, but also medical devices.

2) Recent successful projects

A) We received prestigious project award for Turkish-Qatar bilateral relationships worth of 1,158,205 USD (Turkish Side only). The title of the project is: WARNING: A Defense-in-depth Cyber Intelligence Platform to Defend against Emerging Cyber Attacks

B) An Internally funded project on the development of Cybersecurity research lab and graduate program along with developing hybrid malware detection systems, the project budget is about 50,000 USD.

C) Two Research projects are submitted for funding to Turkish funding agency, Tübitak.

3) Topic of Interest

Our main H2020 interest – are to take part in the main call of SU-INFRA01-2018-2019-2020 "Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe" and/or some sub-projects under this main call. For example, **Security for smart and safe cities, including for public spaces.**

4) Our Role as a Partner

Fundamental research, applied research, development, design, testing, piloting, validation, dissemination, education, and training, etc. It will be adjusted for the specific call.

Contact :
Prof. Dr. Hasan Dag
hasan.dag@khas.edu.tr