Karlsruhe Institute of Technology

# Position Paper: Security-Relevant Research @ KIT

We are living in a period of increasing global instability, shaped by multiple crises and conflicts across the world. Geopolitical dynamics and balances of power are changing while political tensions are rising. These developments pose direct threats to our core values such as democracy, freedom, and security.

At KIT, we are committed to protect these core values and, in light of today's uncertainties, determined to stand up for and defend them. We take responsibility for societal and global challenges by developing innovative solutions that safeguard internal and external security and reinforce resilience of democracy, be it in our digital or physical society. By clearly positioning ourselves on security-relevant research, we accept our obligation as a public research institution to contribute to the common good and societal needs and, at the same time, prepare for Baden Württemberg's Innovation Campus Security and Defense. While remaining mindful of the risks and ethical questions inherent in security-relevant research, we emphasize the need for responsible research and innovation that strengthen Germany's and Europe's security and sovereignty.
As an institution combining the strengths of a university and a Helmholtz Center, we are uniquely positioned to pursue security relevant research responsibly for peacekeeping purposes and with substantial impact – particularly in the following fields:

The development of **resilient** internal **structures** is a central factor in ensuring security and sovereignty. This includes the protection and reliable operation of **critical infrastructure**, as well as crisis-resistant production and distribution of **goods** and **public services**. To identify vulnerabilities and weaknesses, e.g., critical dependencies across entire value chains or key bottlenecks and risk nodes, systematic analyses are required as a first critical step. In this regard, KIT can draw on its broad expertise in adaptable production and supply chains, critical raw materials, recycling, energy systems, and **cybersecurity**, to develop implementable and scalable measures in the short term and strengthen **supply security** in the longer term.

The evolving threat landscape has a significant impact on **IT security** and underscores the importance of **digital sovereignty**, reflected in (state-sponsored) attacks, sabotage and kill-switch incidents, and the explosive growth of disinformation. Combined physical-digital attacks require deeper analysis, along with coherent security models, digital twins, and a level of system resilience that ensures operational continuity even under successful attacks. With the KASTEL Security Labs, KIT provides extensive expertise in **cybersecurity** research, in particular, for the sectors of energy, mobility, and production. The Energy Lab simulates future energy systems to prevent information-level attacks. The Mobility Lab tests methods for detecting cyberattacks in autonomous driving. The Production Lab (Karlsruhe Research Factory for AI-integrated Production) examines resilience and develops cybersecurity and trustworthy assistance systems for industrial enterprises.

**Robotics** plays an increasingly important role in security-relevant research, as advanced **autonomous technologies** are being developed to protect people and **critical infrastructures**. At KIT, one of the leading robotics hubs in Germany, we have strong expertise across robot design and system integration, perception, control, machine learning, motion planning and navigation, human–robot interaction, decision-making, and multi-robot system. Until now, our robotics research has primarily focused on applications in everyday life, mobility, health care, production, and logistics. Looking ahead, we will expand our activities in security-related robotics and to stimulate innovation both within and beyond security-related domains to enhance European technological sovereignty.

Moreover, **sensing** and **communication** represent fundamental key technologies for security and defense. Sensors detect, classify, and analyze threats on land, in the air, on and under water, as well as in space. In this context, new camera and radar systems, combined with powerful data-processing algorithms, play a central role. For communication, fiber-op-

tic technologies are essential, as are robust, flexible and secured wireless connections. KIT develops the hardware, systems, and algorithms required for these purposes – ranging from innovative sensing technologies and high-performance radar and communication solutions to specialized microelectronics and software that are indispensable for the functioning of modern security technologies, including quantum encrypted communication systems.

Modern security and defense technologies require an integrated perspective on their evolving individual components – a need we address through **systems engineering**. High power density and robust **drive systems** are essential for highly reliable mobile platforms, robotics, and safety-critical applications; **simulation** and **digital twins** enable the realistic assessments of risks, system reliability, and human–machine interactions; **virtual validation** supports the development, assurance and optimization of defense-relevant technologies under realistic conditions. With expertise in AI-based decision support, secure information and operational technologies, advanced systems-engineering approaches and human-centered safety, KIT develops security-relevant systems holistically – from architecture through simulation and testing to full validation.

We place another strategic focus on the **development**, **production** and **deployment** of **drones**, as well as **drone defense technologies**. Together with the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation and the Fraunhofer Institute for Chemical Technology we advance this topic in the planned **Karlsruhe Innovation Centre for Drone and Counter-Drone Technologies**. Here, we pursue a distinctly holistic approach grounded in our broad scientific and technological competencies. These range from supply-chain logistics, **systems engineering** and modular production technologies to propulsion systems, batteries, avionics, **sensing**, AI-based signal and image processing, **autonomy** functions, communication technologies, software, **IT security**, as well as laser and high-frequency technologies for detection, tracking, classification and defense.

Grounding security- and defense-relevant research in democratic values and critical reflection at both the institutional and individual levels is crucial for KIT. This requires the careful assessment of project and collaboration risks to identify potential abuse, while balancing core scientific principles such as academic freedom, the pursuit of knowledge, and open science. Researchers will be supported in making informed decisions about protecting and sharing their results. As KIT is a place of academic freedom and plurality, direct participation in defense- and security-related research remains in all organizational units in principle voluntary.

To enable the engagement with security-relevant research, KIT will put the necessary institutional framework in place. This may include the required infrastructure, IT security, principles for collaborating with science, industry, and policy partners, as well as training and support services for ethical reflection. This is to foster awareness of ethical issues, help to identify potential value and goal conflicts at an early stage, and ensure that these are addressed in a structured manner. Taken together, we provide a framework of standards and guidelines that reflect our commitment to scientific integrity and ethical accountability, seeking to ensure that security-relevant research can be carried out responsibly. Given the diversity and complexity of such research, these measures will be tailored to the specific requirements of the respective research fields and may range from project-specific documentation and short advisory consultation to more comprehensive reviews. For requirements that we, as an internationally oriented university dedicated to societal openness, scientific transparency, and exchange, cannot fulfill (e.g. confidentiality requirements), we rely on our well-established collaborations with recognized partners from academia, government, and industry.