



## Special team from research institutes and universities

The 'AlgenCY' project, supported by the German Federal Ministry of Education and Research (BMBF), brings together specialists from CISA – Helmholtz Centre for Information Security, the Technical University of Berlin and the Free University of Berlin under the leadership of Fraunhofer AISEC. It also cooperates with Aleph Alpha, a pioneering AI company based in Heidelberg.



Project 'AlgenCY'



Department 'Cognitive Security Technologies'



### Contact

#### Dr. Philip Sperl

Head of Department  
Cognitive Security Technologies  
Phone: +49 89 3229986-141  
philip.sperl@aisec.fraunhofer.de



#### Prof. Dr.-Ing. habil. Gerhard Wunder

Head of Department  
Cognitive Security Technologies  
Phone: +49 89 3229986-1067  
gerhard.wunder@aisec.fraunhofer.de

# Generative AI in cyberspace – exploiting opportunities, averting dangers

How does generative AI affect cybersecurity – and how can we protect ourselves? The 'AlgenCY' research project is investigating the opportunities and risks of AI-generated content and developing defence strategies against new threats.

Led by Fraunhofer AISEC, leading research institutes and companies are working on solutions for a secure digital future.

With the research project 'AlgenCY – Opportunities and Risks of Generative AI in Cybersecurity,' leading experts from academia and industry are taking on the challenge of exploring the implications of generative artificial intelligence for cybersecurity.

Rapid advances in generative AI, particularly in neural networks, are revolutionising the creation of digital content. With generative AI, systems are able to generate and refine authentic texts, visual content and complex program codes. These capabilities open up new opportunities, but also pose significant risks. AlgenCY is therefore dedicated to identifying potential threats posed by AI-generated content and developing robust defence strategies to consolidate Germany's digital sovereignty and protect critical infrastructure – while at the same time strengthening Germany as a location for innovation.

As part of the project, an experimental laboratory will be set up to investigate the applicability of generative AI technologies in practical scenarios. Among other things, the laboratory will be used to investigate attack scenarios and concepts for increasing the robustness of systems against attacks in realistic scenarios.

'With the "AlgenCY" project, we have the opportunity to set the course for a secure digital future and drive forward AI innovations in the interests of a resilient society,' emphasises Prof. Dr. Claudia Eckert, Director of the Fraunhofer AISEC. 'With five million euros in funding from the BMBF over the next three

years, "AlgenCY" is well on its way to playing a key role in shaping this future-oriented field of research and innovation.'

### From anomaly detection to watermarking

The research team focuses on the following core topics:

- Malware control: Analysis of the generation of advanced malware by AI and development of appropriate countermeasures
- Prevention of social engineering, disinformation and fraudulent campaigns: increasing vigilance and improving detection of automated attacks
- Information gathering and processing: Understanding preventive attack strategies and how to defend against them
- Explainability and inference: Interpreting the decision-making of generative AI models and identifying systemic weaknesses
- Watermarking and anomaly detection: Tracing data origin and detecting unusual patterns that indicate possible attacks