

Secure. Innovative. Successful.



*Success Stories
from the Austrian
Safety Pin*



KIRAS
Civil Security Research

FORTE
Security and Defense Research

K-PASS
Cybersecurity Research



From Research to Market:
10 Projects from the Austrian Safety Pin

EXPERT INTERVIEW

Dr. Ralph HAMMER***Why is security research more important than ever, and what role does it play in Austria's economy and innovation ecosystem?***

Security research has always been of fundamental importance, as it can only be effective if it is supported well in advance of crises and other security-related events. It generally takes five to seven years to progress from an initial idea to an operational solution. Stakeholders such as emergency response organisations, the armed forces and operators of critical infrastructure must therefore identify future challenges at an early stage so that relevant solutions can be supported through the research funding programmes of the Austrian Federal Ministry of Finance (BMF). This ensures that "Made in Austria" products and services are available when needed, while also generating economic value.

How important are the research programmes under the Austrian Safety Pin for Austria as a centre of innovation?

Through their strategic focus and dedicated budgets, the programmes under the Austrian Safety Pin specifically target an area of innovation that cuts across multiple sectors and would be difficult to develop in a structured and successful manner without dedicated funding measures. Most European countries have no government-level instruments comparable to KIRAS, FORTE or K-PASS. This gives Austria an important competitive advantage in terms of both security policy and economic development.

What sets Austrian security research and the Austrian Safety Pin apart internationally?

With the launch of the civilian security research programme KIRAS in 2006, Austria became the first European country to establish a programme of its kind. Its mandatory involvement of end users, research institutions, businesses and the humanities, social sciences



Ministerial Councillor

Dr. Ralph HAMMER

Director of the Staff Department for Security Research and Technology Transfer

Federal Ministry of Finance

Directorate-General VI – Mining

Staff Department for Security Research and Technology Transfer

ralph.hammer@bmf.gv.at

+43 1 514 335 061 30

www.kiras.at

and cultural studies created a pioneering innovation model that has since been widely adopted at EU level. Another distinguishing feature is the funding coordination framework provided by the Austrian Safety Pin. The Austrian Federal Ministry of Finance coordinates and finances both civilian (cyber)security research and national defence research, while also aligning their thematic priorities. This bundles existing strengths and effectively coordinates the diverse expectations of the stakeholders involved.

IMPRESSUM

Publisher and Media Owner: Media Guide

Editor: Jonas Buchegger, jbuchegger@myguides.at

Photography: AdobeStock, Freepik, Vertragspartner

Layout: Agentur be-design, Karin Schön, office@be-design.at, www.be-design.at

The publication „Success Stories from the Austrian Safety Pin“ is published in cooperation with the Austrian Federal Ministry of Finance. The content of this publication has been reviewed by subject-matter experts. While every effort has been made to ensure the accuracy of the information provided, all content is supplied without guarantee. Neither the authors, the reviewers, nor the publisher accept any liability for any loss or damage arising from the use of the information contained in this publication. No part of this publication may be reproduced or republished, in whole or in part, without the prior written permission of the publisher.

Advertising and Partnerships: For information about advertising or partnership opportunities, please contact: Media Guide Publishing, Tel. 0664/5271172, E-Mail: jbuchegger@myguides.at.

We would like to express our sincere thanks to everyone whose expertise, support, and collaboration contributed to the successful completion of this publication.

TABLE OF CONTENTS

Infographic Austrian Safety Pin	3
Fact Sheet Security Research	4
HiProtect®	6
Backbone	8
Deiser Bakery	10
Fake-Shop Detector	12
DeFiTrace	14
CESARE	16
Minerva	18
AIT - AttackBed and Cyber Range	20
KI-SecAssist	22
Desinfact	24

Austrian Safety Pin Impact Level – Measuring Research Impact

How does a promising idea become a successful real-world solution? The Austrian Safety Pin Impact Level provides a clear overview of a project's development journey. Using seven development stages, ranging from a validated research concept to successful market deployment and scaling, it illustrates how far a project has progressed on its path toward practical impact.

Project coordinators assess their projects both overall and across four key impact dimensions: security, societal benefit, export potential, and economic potential. This self-assessment is carried out on a scale from 1 to 7, creating a consistent basis for comparing the projects presented in this publication.

The Austrian Safety Pin Impact Level is not intended as a scientific evaluation. Instead, it serves as a practical framework for transparently communicating a project's level of maturity and its potential impact. It enables readers to quickly understand how far a project has advanced and what potential it holds for industry, society, and security research.

AUSTRIAN SAFETY PIN IMPACT LEVEL

From Idea to Impact. MEASURABLE. FUTURE ORIENTED. INNOVATIVE.



	1	2	3	4	5	6	7
SECURITY	☐	☐	☐	☐	☐	☐	☐
SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☐	☐
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☐
ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☐	☐

Fact Sheet

Security Research

THE THREE RESEARCH PROGRAMMES:

What is the Austrian Safety Pin („Sicherheitsklammer“)?

The Austrian Safety Pin

- > The civil security research programme KIRAS, which was founded in 2006 the defence research programme FORTE, which has been running since 2018, and the digital (cyber) security research programme Kybernet Pass (K-PASS), introduced in 2023, together form Austrian Safety Pin („Sicherheitsklammer“), under which all federal security related research funding is consolidated.
- > Funding instruments: Collaborative R&D projects and R&D services.
- > More than 540 projects have been funded to date, representing a total investment of approximately €196 million.
- > The Austrian Research Promotion Agency (FFG) has been entrusted with programme management.

	1 KIRAS	2 FORTE	3 K-PASS
Number of Calls for Proposals 2006-2024	49	7	2
Number of Project Proposals Submitted	1.013	204	46
Number of Approved Projects	415	82	24
Approval to Rejection Ratio	~ 1 : 2.43	~ 1 : 1.49	~ 1 : 2
Total Project Costs	~ € 230 million	~ € 75.9 million	~ € 26.3 million
Funding Awarded	~ € 148.2 million	~ € 35.4 million	~ € 11.3 million
Total Funding Requested to Date	~ € 349.4 million	~ € 97.6 million	~ € 23.7 million

General Figures on Austria's Security Industry (Excluding the Defence Sector) Gross value added: approximately €2.8 billion Employment: approximately 41,500 people Production multiplier: approximately 1.53, comparable to the construction industry**).

*) Includes funded Innovation AKUT projects from the 2023/24 and 2024/25 calls for proposals.
 **) Based on the results of the 2022 Austrian Security Satellite Account.

HiProtect®

Development of a Novel Lightweight Composite Material with Ballistic and Self-Healing Protective Properties



The image on the right shows the assembled structure consisting of four individual modules arranged side by side.



Ballistic protection systems for military units must be easy to transport and quick to deploy. Fibre-reinforced high-performance composite materials are ideally suited for lightweight protection applications, although achieving the required level of ballistic resistance depends on the development of advanced material and structural designs.

The project resulted in a fully functional prototype of a modular, ultra-lightweight protection system capable of absorbing projectile energies of at least 1,600 joules while weighing only 4.9 kg/m². This corresponds approximately to protection against assault rifle fire from a distance of 50 to 100 metres. The individual modules are delivered as flat, space-saving stacked panels and can be rapidly assembled on site into large-area protective structures. The image on the left shows such a configuration consisting of four individual elements, with the bullet impact visible on the white front panel.

In addition to protecting equipment and critical infrastructure, the modular system's underlying protection concept can also be applied to vehicles. In cooperation with Liebherr in Telfs, a telescopic handler was converted into a demonstration vehicle to showcase this application.



KEY ADVANTAGES:

- > No chassis reinforcement required
- > High design flexibility with no need for rigid plate construction
- > Existing vehicle certification can be maintained
- > Rapid field installation and upgrade capability
- > Low additional weight without negatively affecting vehicle handling or centre of gravity
- > The vehicle remains fully operational for everyday use and can be quickly adapted for crisis response
- > Damaged protective modules can be replaced individually, quickly, and without heavy equipment

EXPERT INTERVIEW WITH

Dr.-Ing. Jochen Schmidt

What economic potential do you see for HiProtect and its successor, Hi2Protect, in the international security and lightweight materials market?

The economic potential of HiProtect and Hi2Protect lies in their unique combination of high-performance ballistic protection and lightweight construction. This combination is in growing demand worldwide, both in the defence sector and in civilian safety-critical applications. Lightweight composite solutions offer particular advantages for critical infrastructure by reducing installation effort, structural load requirements, and operating costs. We also see significant opportunities in the mobility sector, including specialised vehicles, maritime applications, and personal protective equipment.

How could the combination of ballistic protection and self-healing properties reduce costs over the long term?

The combination of ballistic protection and self-healing capabilities offers substantial economic benefits throughout the entire lifecycle of a protection system. The Hi2Protect system is able to seal impact damage automatically, making it no longer visible from the outside while continuing to protect the underlying material from environmental influences. As a result, maintenance requirements, inspection intervals, and replacement costs can be significantly reduced. This is particularly valuable for critical infrastructure, where downtime often results in costs that exceed the value of the damaged component itself.

What opportunities does this technology, developed in Austria, create for the country's economy?

The technology developed in Austria through the FORTE research funding programme offers significant technological, economic, and strategic opportunities. In particular, Austria has the potential to establish a leading international position in the field of intelligent



Dr.-Ing. Jochen Schmidt
Hintsteiner Group

j.schmidt@hintsteiner.at
+43 3864 23 36 - 54
www.hintsteiner-group.com

DEVELOPER STATEMENT:

Liebherr / Michael Hagner
Key Account Manager Defense/
Product Manager Telescopic handler
Michael.Hagner@liebherr.com



For the Liebherr plant in Telfs, as a manufacturer of telescopic handlers and bulldozers, the Hi2Protect system offers significant advantages. Thanks to its lightweight design, we can provide customers with a standard production vehicle that does not require extensive modifications, such as reinforced axles or other structural components, to accommodate a protected cabin. This allows customers to benefit not only from the cost advantages of a series-production machine but also from the excellent availability of spare parts for a platform that has already proven itself in thousands of vehicles in operation.

lightweight protection systems. Technologies such as HiProtect and Hi2Protect strengthen Europe's technological independence in security-critical high-performance materials while reducing dependencies on external suppliers. At the same time, the rapidly growing global market for security, infrastructure, and mobility solutions offers considerable export opportunities. In the long term, Austria can further establish itself as a leading European centre for the development and production of advanced protective and composite technologies. ♦

AUSTRIAN SAFETY PIN

IMPACT LEVEL

7

	1	2	3	4	5	6	7
 SECURITY	☐	☐	☐	☐	☐	☒	☐
 SOCIETAL BENEFITS	☐	☐	☐	☐	☒	☐	☐
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
 ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☒	☐

BACKBONE

ULTRA-SECURE END-USER-DEVICE

EXPERT INTERVIEW with **PHILIPP LECHNER**, CEO of MUSE Electronics

Which specific use cases of your BACKBONE tablet have proven to be particularly effective in real world operations, and what sets it apart from comparable products?

Let me illustrate this with two military scenarios that demonstrate why BACKBONE is far more than a conventional tablet. In fact, the term single device describes it more accurately: one device that enables users to operate across multiple security domains through strict physical data separation.

Imagine an intelligence officer deployed on a multinational NATO mission. They need to work simultaneously with Mission Secret data from the joint command structure and National Confidential information belonging to their home country, data that must never be mixed under any circumstances. With BACKBONE, they carry a single device that can process and store data from both security domains while keeping them physically separated. This is not a software based solution. It is true hardware enforced separation, representing a fundamental shift in secure mobile computing.

The second scenario involves a special operations mission in challenging terrain. Here, the priority is not only data security but also absolute reliability under extreme physical conditions. The device must continue to perform at temperatures as low as minus 20 degrees Celsius, in heavy rain, after a fall. It must also



Mag. Philipp Lechner
CEO of MUSE Electronics

contact@backbone.io
www.backbone.io

guarantee that, even in the event of a compromise, no mission critical data can be extracted. BACKBONE automatically detects tampering attempts and immediately initiates security protocols.

What sets us apart from other products is our approach to security. Comparable devices rely primarily on software to protect sensitive information, an approach that remains structurally vulnerable. We solve this challenge at the hardware level. This is not an incremental improvement. It is a fundamental one. As Mag. Wolfgang Hacker, CTO of Directorate 6 ICT and Cyber, aptly puts it: „A hardened end user device that supports multiple communication channels, can operate across different security domains, and remains compatible with existing infrastructure offers enormous potential for the future ICT architecture of operational deployments.“

From your perspective, where does your solution hold the greatest commercial potential: in scaling existing markets or in opening entirely new application areas?

Both, but on different time horizons. In the short term, the greatest opportunity clearly lies in scaling existing markets. Europe is strengthening its defence capabilities, NATO member states are significantly increasing their defence spending, and the demand for trusted European technology has never been greater. As consortium lead within the European Defence Fund, we are well positioned to capitalize on this momentum. In the medium term, however, I see enormous potential in entirely new application areas. The driving force is clear: cyber threats are not becoming fewer, they are

broader, more targeted and increasingly sophisticated. Critical infrastructure, energy providers, the judiciary and public authorities have long been targets of both state sponsored and non state actors. As a result, the demand for hardware based security solutions is expanding far beyond the defence sector.

Wherever multiple devices have traditionally been required, or where sensitive information has been processed on insufficiently secured end user devices, BACKBONE can serve as a unified, trusted platform. It is not limited to soldiers in the field. It is a response to a challenge that affects society as a whole.

This brings me to a point that is particularly important to me: Europe needs an autonomous hardware industry. We cannot call for digital sovereignty while continuing to rely on devices manufactured outside Europe to process our most sensitive data. System critical industries, and the hardware industry is undoubtedly one of them, must be built and strengthened within Europe. BACKBONE is a tangible example of this vision: developed and manufactured in Austria, with the ambition of becoming the European standard for secure mobile computing.

What are the next key steps in establishing BACKBONE on a large scale, and what role do partnerships and international expansion play in this process?

The most important step is the commercial launch that is currently underway, together with the delivery of our first customer systems. This marks the foundation for everything that follows. At the same time, building a strong network of specialized system integration partners is essential. BACKBONE must integrate seamlessly into existing security architectures, and that can only be achieved through close collaboration with experienced, long term partners.

As for international expansion, our primary focus is on Europe, NATO member states and partner countries. These are the regions that are actively strengthening their defence capabilities while reducing their technological dependence on non European suppliers.



This is a pivotal moment. The procurement decisions made today will shape the security architecture of the next decade.

Wherever armed forces, government agencies and public authorities depend on interoperable, highly secure end user devices, BACKBONE provides a compelling solution. Not despite its European origin, but precisely because of it. Trust begins with knowing where a device is developed and manufactured, and by whom.

Our vision is for BACKBONE to become the established standard for secure mobile operations in high risk environments. Developed and manufactured in Austria, designed for Europe and its partners. ♦

FACTS:

BACKBONE is developed and manufactured by MUSE Electronics in Vienna and Budapest. Led by CEO Philipp Lechner, the company is supported by Austria's FORTE Defence Research Programme and the European Defence Fund, and has further strengthened its growth through a Series A investment from Sparring Capital Partners.



AUSTRIAN SAFETY PIN

IMPACT LEVEL

6

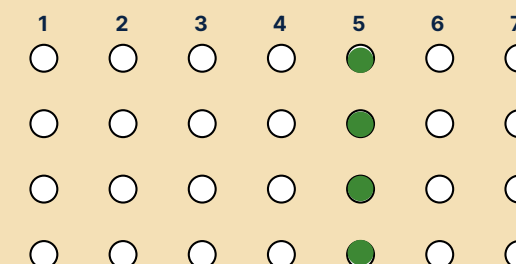


SECURITY

SOCIETAL BENEFITS

EXPORT POTENTIAL

ECONOMIC POTENTIAL



Deiser Bakery

Canned Bread for Emergency Supplies



BENEFITS:

- > The product range now includes five types of bread and two types of cake: wholegrain rye bread, mixed rye bread, wholegrain mixed bread with sunflower seeds, protein bread, hemp bread, chocolate cake with chocolate chips, and lemon cake.
- > Long shelf life of up to ten years from the date of production.
- > Made with high quality, natural ingredients. The breads are produced with sourdough, contain no added yeast, and are vegan. The wholegrain rye bread is also wheat free. The cakes are made without palm oil.
- > Ready to eat immediately with no preparation required
- > A reliable emergency food supply can provide psychological reassurance and strengthen self sufficiency during crises.
- > Packaged in a tin can with a BPA free internal coating
- > Convenient for travel, outdoor activities, and emergency preparedness.
- > Operated by a self sufficient production facility that is capable of continuing operations during crisis situations such as a blackout. In such a scenario, however, production would be focused on supplying the population with fresh bread.

Deiser Bakery was founded in 1964 as a traditional family owned bakery in Vienna, operating its own retail shop and offering a wide range of breads, pastries, and baked goods. In 1989, Christian Deiser took over the business and deliberately steered it in a new direction. Alongside specializing in sourdough bread, he focused on sourcing at least 90 percent of all raw ingredients from Austria.

At the same time, the company placed a strong emphasis on energy efficiency. An initial heat recovery system was implemented at the Vienna site before a new energy self sufficient production facility was opened in Baden near Vienna in 2017.

In early 2019, the Staff Department for Security Research and Technology Transfer, together with the Austrian Research Promotion Agency (FFG), the Austrian Federal Economic Chamber (WKÖ, Food Division), and the Austrian Bakers' Guild, began searching for an Austrian bakery with available production capacity to reestablish the domestic production of canned bread. Canned bread had previously been manufactured by a Viennese bakery until the mid-1970s with the objective to restore self-sufficiency in Austria.

This was not an Austrian Safety Pin research project but rather the fulfillment of individual customer orders. Since Deiser Bakery was already well known within the industry for its newly built production facility, its ability to generate and store its own electricity while feeding surplus energy into the grid, and its available production capacity, it proved to be the ideal crisis resilient partner for reintroducing canned bread production in Austria.



EXPERT INTERVIEW WITH MMST CHRISTIAN P. DEISER

What role can canned bread play in private emergency preparedness and in ensuring basic food supply during crises?

Canned bread can play an important role in private emergency preparedness because it is a shelf stable, ready to eat staple food that does not depend on electricity, refrigeration, or cooking.

While previous generations routinely maintained emergency food reserves, today's around the clock availability of goods has created a false sense of security. In situations such as power outages, supply chain disruptions, or natural disasters, however, the importance of personal preparedness quickly becomes evident.

Although canned bread is not intended to provide a complete diet on its own, it can help secure basic nutrition for days or even weeks when combined with water, spreads, and canned foods. It therefore serves as a practical solution for bridging temporary supply shortages.

Greater availability in retail stores would make emergency preparedness more accessible and encourage more households to build their own food reserves. Beyond emergency situations, canned bread is also a convenient and reliable option for everyday use and outdoor activities such as camping and hiking.

As part of Austria's critical infrastructure, how does your bakery ensure resilient and energy independent operations, particularly through the production of canned bread?

Since 2018, our bakery has operated as a fully energy autonomous production facility. We cover 100 percent of our electricity demand through our own 182 kWp photovoltaic system combined with energy storage. In addition, we operate a 400 kW biomass heating plant that supplies our thermal oil baking ovens with heat. The wood chips used as fuel are sourced from the im-



Team Deiser
Deiser Bakery

team@deisers.com
www.deisers.com

mediate surrounding region.

As part of Austria's critical infrastructure, we consistently rely on regional supply chains. At least 90 percent of our raw materials originate in Austria. Our grain is supplied by farmers in Lower Austria through a nearby mill. In the event of a crisis, we are able to collect the grain ourselves, mill it locally, and process it directly into bread. This enables us to maintain resilient, energy independent production and ensure a reliable food supply even under exceptional circumstances.

What opportunities does this create for Austrian producers such as Deiser to become international pioneers?

The increasing number of global crises and the growing importance of supply security create significant opportunities for Austrian producers, particularly if national and international visibility continues to grow. Our energy autonomous production model allows us to operate reliably and independently, even under challenging conditions. Combined with high quality standards and the strong reputation of products made in Austria as a credible alternative to fragile global supply chains, this creates the potential for Austrian producers to establish themselves as international pioneers in resilient food production. ♦

AUSTRIAN SAFETY PIN

IMPACT LEVEL

7

	1	2	3	4	5	6	7
SECURITY	☐	☐	☐	☐	☐	☒	☐
SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☐	☒
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☒	☐
ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☐	☒

Fake-Shop Detector

Fake-Shop Detector

No chance for online scams:
Detecting fake online shops with more
than 99 % accuracy

Cybercrime is an increasingly serious challenge for consumers in Austria. The Austrian reporting and information platform Watchlist Internet receives thousands of reports of online fraud every year. In 2025 alone, it recorded nearly 17,000 consumer reports, while as of June 2026 it listed around 25,000 fraudulent online shops. Once a payment has been made, the money is often impossible to recover, making prevention one of the most effective ways to combat online fraud.

To address this challenge, the Fake-Shop Detector was developed as an AI-powered tool that protects consumers while they shop online by providing real-time warnings. Installed as a browser extension, the tool evaluates online shops using a simple traffic light system, enabling users to assess a website's trustworthiness before making a purchase. Today, it is used daily by more than 10,000 users to help them shop safely online.

By identifying fraudulent websites before purchases are completed, the Fake-Shop Detector helps prevent financial losses, promotes safer e-commerce, and makes a significant contribution to fraud prevention by enabling fake online shops to be detected more quickly.

The AI-based research behind the Fake-Shop Detector was led by AIT Austrian Institute of Technology, the Austrian Institute for Applied Telecommunications (ÖIAT), and X-Net Services GmbH. The project received funding from the civil security research programme KIRAS, which is part of the Austrian Safety Pin.



© Gregor Hofbauer



BENEFITS:

- > Over 99 % accuracy in detecting fake online shops
- > Awarded Most Effective Security Solution Against Fake Online Shops 2024 and recipient of the Austrian State Prize for Digitalisation 2023
- > Prevents fraud through proactive detection and prevention
- > Continuous AI re-learning to identify emerging fraud patterns
- > AI provides an additional analytical perspective for cybersecurity experts
- > Promotes users' digital literacy through a community-driven approach: „Protect yourself and others.“
- > Real-time AI analysis with instant traffic light warnings
- > Developed, operated, and hosted in Austria
- > Privacy by design with no storage of personal data

STATEMENT

Nikolaus Dürk
(Founder and CEO, X-Net)

The Fake-Shop Detector has become one of the world's leading AI systems for fraud prevention. If deployed nationwide across Austria, it could significantly reduce online fraud and prevent the loss of hundreds of millions of euros each year. AI-driven preventive technologies like this not only protect citizens but also reduce the burden on public authorities while keeping substantial economic value within Austria and the European economy instead of allowing it to flow to criminal networks abroad.

STATEMENT

Bernhard Jungwirth
(Managing Director, Austrian Institute for Applied Telecommunications (ÖIAT))

Every year, thousands of consumers report online fraud cases to Watchlist Internet. The Fake-Shop Detector was developed to protect exactly these people by providing real-time warnings directly within their browser. Newly identified fraudulent online shops are automatically incorporated into the Watchlist Internet warning database, allowing every user not only to protect themselves but also to help warn others more quickly. Effective consumer protection is created at the intersection of reliable information, easy-to-use technology, and a collaborative network that becomes stronger with every new report.

STATEMENT

Helmut Leopold
(Head of Center for Digital Safety & Security, AIT Austrian Institute of Technology)

The Fake-Shop Detector demonstrates how responsibly developed artificial intelligence can deliver tangible benefits for society. By combining AI-driven analysis with continuous quality assurance by experts, the system can identify online fraud at an early stage and protect consumers before financial damage occurs. Its multiple awards, including the Austrian State Prize for Digitalisation 2023, together with the latest independent evaluation by AV-Comparatives, which recognised the Fake-Shop Detector as Austria's highest-performing solution in an international comparison, reflect AIT's commitment to developing trustworthy technologies that create real impact for both society and the economy.

AUSTRIAN SAFETY PIN



	1	2	3	4	5	6	7
 SECURITY	☐	☐	☐	☐	☐	☐	☒
 SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☐	☒
 EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
 ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☒	☐

DeFiTrace

Tracing Illicit Financial Flows Through Decentralised Finance Systems

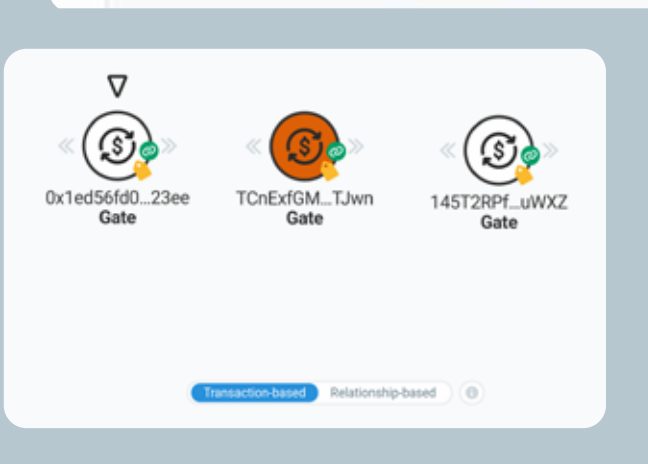
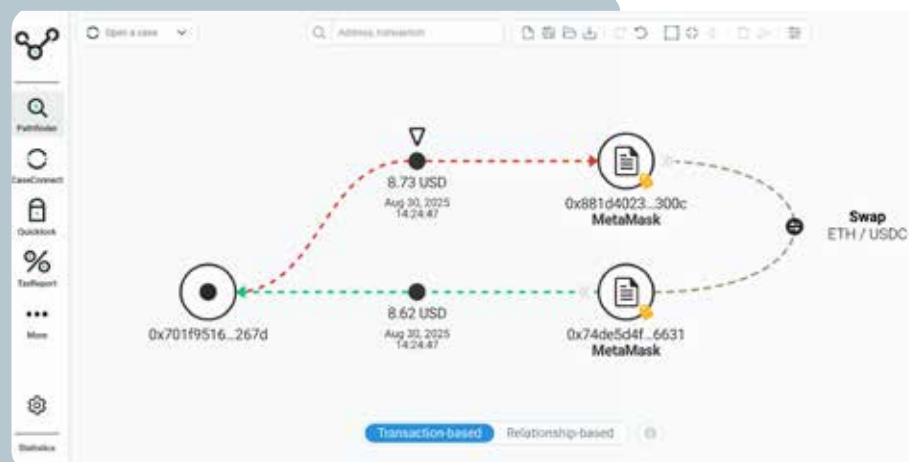
Decentralised Finance (DeFi) enables financial transactions to be carried out on blockchain networks without banks or other central intermediaries. While this creates new opportunities for digital finance, it also makes the tracing of illicit financial flows significantly more challenging. As part of the project, a baseline study documented more than 1,100 cybercrime cases involving losses exceeding USD 30 billion between 2017 and 2022.

The DeFiTrace project developed several data-driven analytical methods that have been integrated into the GraphSense investigation platform. A newly developed cross-chain analysis method identified more than 1.5 million cryptocurrency addresses connected across multiple blockchains. In addition, a quantitative governance analysis revealed that in more than 20% of DeFi projects, at least one key governance decision was made exclusively by centralised actors. The automated QuickLock system enables investigators to track suspicious financial transactions efficiently.

Developed in close cooperation with Austrian law enforcement authorities, these methods have been complemented by specialised training programmes for investigators. The project's findings have been permanently integrated into the curriculum of the Federal Finance Academy, helping to strengthen Austria's capabilities in combating financial crime.

KEY BENEFITS:

- > Cross-chain tracing across blockchain networks (UTXO and account models)
- > Automated large-scale analysis instead of time-consuming manual investigations (QuickLock)
- > Integrated into the production version of the GraphSense platform and ready for immediate use
- > General-purpose methods instead of protocol-specific solutions, making them adaptable to new DeFi protocols
- > Sustainably available as open source and as a prototype through Iknaio
- > Designed to meet the needs of law enforcement and financial supervisory authorities and validated with end users
- > Legal framework analysed, including MiCA, DAC8, and the Transfer of Funds Regulation, ensuring practical compliance



Number of criminal incidents (counts) related to Decentralised Finance and associated financial losses (in USD), 2017–2022.

EXPERT INTERVIEW WITH

Dipl.-Ing. Dr.techn. Stefan Kitzler

What economic and societal potential do you see for DeFiTrace in the international market for crypto forensics and compliance?

Demand is growing rapidly as more countries introduce comprehensive regulatory frameworks for digital assets, such as MiCA and DAC8 in Europe. These regulations significantly increase the need for transparent and traceable cryptocurrency transactions. Law enforcement agencies, financial regulators, and regulated crypto service providers therefore require advanced analytical tools based on sound scientific methods to understand and investigate financial flows.

From an economic perspective, financial innovation is a highly dynamic market. From a societal perspective, it is essential to keep pace with this rapid development, combat financial crime effectively, strengthen trust in digital financial markets, and better protect victims of fraud and illicit activity.

Which markets and application areas are most relevant for the solution, and how can it be scaled?

The solution is designed for organisations that need to analyse and understand financial transactions, particularly when dealing with very large volumes of data. This includes law enforcement agencies, financial intelligence units, tax authorities, financial supervisory bodies, banks, and cryptocurrency service providers.

Modern financial systems, particularly those based on blockchain and decentralised finance, generate transaction volumes that can no longer be analysed manually. Scalability has been considered from the very beginning of the project's development, resulting in transparent, scalable methods and tools that can be adapted to new DeFi protocols and additional blockchain networks.

What opportunities does this technology, developed in Austria, create for the country's economy and research landscape?



Dipl.-Ing. Dr.techn. Stefan Kitzler
Postdoctoral Researcher,
Complexity Science Hub.

kitzler@csh.ac.at
+43 1 423 010 21 00
<https://csh.ac.at>

Austria has the opportunity to establish itself as a leading European centre for crypto forensics, strengthening both Europe's technological independence in security-critical analytics and Austria's long-term competitiveness as a research and innovation hub. International conferences such as Advances in Financial Technologies (AFT 2024), held in Vienna during the DeFiTrace project, increase global visibility while attracting new talent and international collaborations. Awards such as the Houska Prize 2024 for DeFi research at the Complexity Science Hub further demonstrate the international quality of Austrian research. ♦

DEVELOPER STATEMENT:

Thomas Niedermayer
Developer, Iknaio Cryptoasset
Analytics GmbH



Why is DeFiTrace particularly exciting from a developer's perspective?

The DeFiTrace research project led to the development of new methods for cross-chain linking and automated transaction path analysis. These innovations enabled us to further enhance our GraphSense platform and solve challenges that conventional analytical tools cannot address. As a result, we can directly support investigators in their work. Being able to translate research results into a production-ready tool so quickly creates real value, both from a technological and a societal perspective.

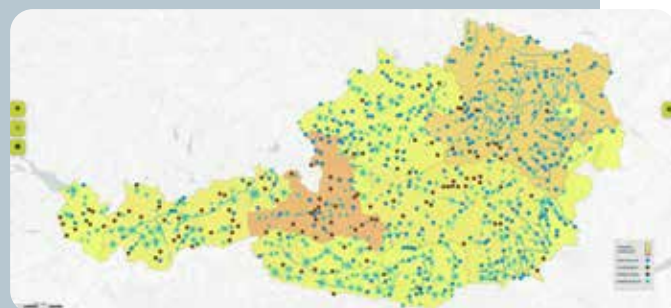
AUSTRIAN SAFETY PIN



	1	2	3	4	5	6	7
SECURITY	☐	☐	☐	☐	☐	☒	☐
SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☒	☐
EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
ECONOMIC POTENTIAL	☐	☐	☐	☐	☒	☐	☐

CESARE

Establishing a Nationwide Austrian Damage and Event Database



Interactive map view of the damage and events integrated into CESARE.



All key information at a glance in the web portal dashboard.

DEVELOPER STATEMENT:

Dipl.-Ing. (BA) Steffen Reichel and Matthias Laher, Software-Engineer and GIS-Expert
Spatial Services GmbH

Many organisations collect damage data to meet their own operational needs and responsibilities. Bringing these diverse datasets together into a coherent national picture is a complex challenge.

CESARE+PLUS addresses this task through modern technical solutions for data harmonisation and processing. For Spatial Services GmbH, the project has provided an exciting opportunity to develop a user-friendly platform that helps create a reliable and comprehensive national overview of disaster damage data.

Damage and event databases are a fundamental basis for effective disaster risk management. In Austria, natural hazards and their impacts are recorded by numerous institutions, but until now there has been no standardized, nationwide database for disaster events and damage.

The initial CESARE project (completed in February 2022), funded under the Austrian KIRAS security research programme, successfully harmonized damage and event data from a range of Austrian data sources for the first time and brought them together in a demonstration platform covering the federal states of Styria and Lower Austria. Since 2022, the system has been operated and continuously enhanced by GeoSphere Austria on behalf of the ASDR Platform.

Building on this success, the follow-up project CESARE+PLUS (funded under Innovation AKUT; completed in June 2025) expanded and updated the database, integrated additional hazard types, and transformed the original demonstration platform into a fully operational nationwide system. The new Web GIS portal, featuring interactive maps and dashboard modules, enables users to search, analyse, visualise, and export harmonised damage data.

Today, the platform supports disaster risk management at both regional and national levels, contributes to climate change adaptation, informs Austria's national risk assessment, and facilitates monitoring under the Sendai Framework for Disaster Risk Reduction. By providing harmonised damage data, meaningful indicators, and comprehensive statistics, it serves as a valuable decision-support tool for public authorities across all levels of government in Austria.



EXPERT INTERVIEW WITH Dr. Stefan Kienberger

What economic benefits does a national damage and event database like CESARE provide for Austria, particularly in terms of more efficient investment in prevention, infrastructure, and risk management?

A national damage and event database such as CESARE enables investments in prevention, infrastructure, and disaster risk management to be targeted far more effectively. By consolidating and harmonising data from multiple sources, it becomes possible to identify where the greatest risks and damage potential actually exist, allowing decision-makers to prioritise measures where they will have the greatest impact.

This leads to more efficient use of public resources, reduces the risk of misallocated investments, and increases the effectiveness of preventive measures. At the same time, infrastructure projects can be planned and adapted based on actual hazard exposure, helping to reduce long-term damage costs and improve overall resilience.

Do you see potential for the methods, standards, and technologies developed through CESARE to be applied internationally or exported as Austrian expertise?

CESARE is already attracting international attention and has been referenced in reports by the United Nations, the European Commission Joint Research Centre, and the World Bank. We are also receiving a growing number of enquiries from countries including Germany, Luxembourg, and Sweden that are interested in exchanging knowledge and experience.

We therefore see strong potential for transferring the approaches developed within CESARE internationally. This includes not only the process of establishing a national damage and event database and engaging the relevant stakeholders, but also the technical solutions developed by the project, such as data harmonisation methods and the implementation of the Web GIS platform together



Dr. Stefan Kienberger
Head of RiskLab – Weather,
Climate & Natural Hazards
GeoSphere Austria

stefan.kienberger@geosphere.at
+43 664 614 70 31
www.cesare.at

with its underlying database architecture.

With climate-related risks increasing and damage costs continuing to rise, the demand for reliable risk data is growing worldwide. What future do you see for CESARE, and what role could the project play over the next decade for business, research, and public administration?

As extreme weather events become more frequent and severe, creating a harmonised and comprehensive overview of damage and risk data will become increasingly important. Reliable, standardised data is essential for evidence-based disaster risk management and for developing effective climate change adaptation strategies. We see significant potential for CESARE in the years ahead, particularly by closing the remaining data gaps through the integration of additional stakeholders and data providers. This will enable a wide range of new applications, from continuous monitoring and risk assessment to evaluating the effectiveness of implemented measures. At the same time, advanced analytical capabilities will allow for deeper insights into damage patterns, long-term trends, and the relationships between hazards, exposure, and impacts.

Over the next decade, CESARE has the potential to become a key decision-support platform for Austria, providing valuable insights for businesses, researchers, and public authorities alike, while strengthening the country's resilience to future climate and disaster risks. ♦

AUSTRIAN SAFETY PIN

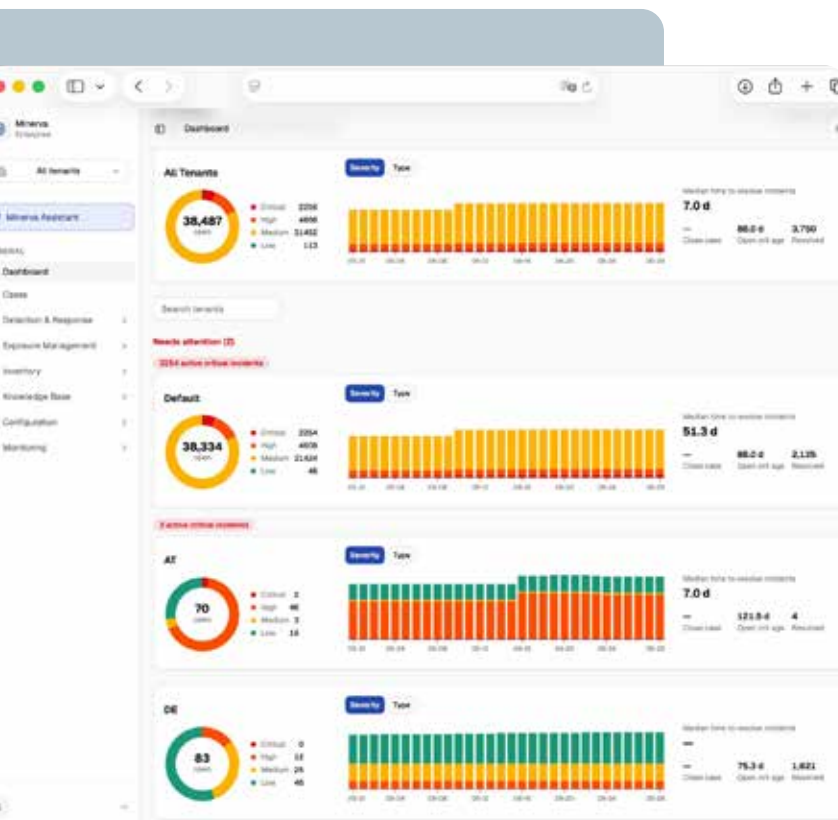
IMPACT LEVEL



	1	2	3	4	5	6	7
 SECURITY	☐	☐	☐	☐	☐	☐	☒
 SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☐	☒
 EXPORT POTENTIAL	☐	☐	☐	☐	☒	☐	☐
 ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☐	☒

Minerva

Sovereign AI-Powered Cyber Defence running entirely on your own infrastructure

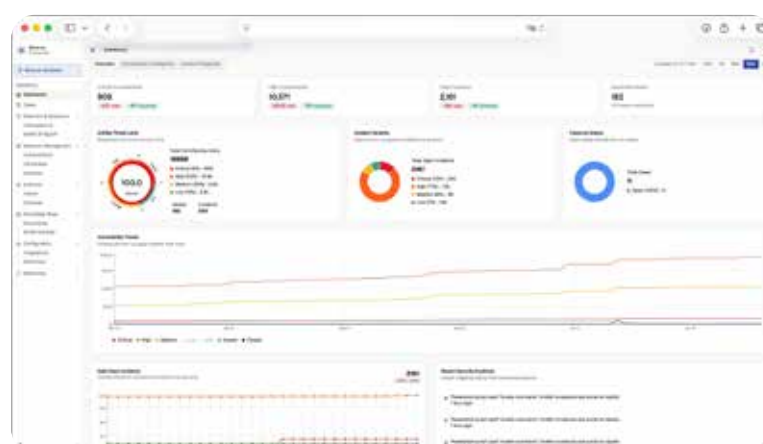


Cyberattacks targeting businesses, public authorities, and critical infrastructure such as energy, water, and financial services are increasing at an unprecedented pace. Attackers are now using artificial intelligence, enabling attacks that once took weeks to be carried out within minutes. Defending against these threats requires highly skilled cybersecurity professionals capable of distinguishing genuine threats from thousands of security alerts. Globally, there is a shortage of around 4.8 million cybersecurity professionals, while 71% of those currently working in the field report operating at or near burnout levels. This is where Minerva comes in. Supporting as the most experienced member of a security team, Minerva autonomously performs many of the tasks traditionally carried out manually by expert security analysts. Operating around the clock, it detects and responds to cyber threats while understanding the broader business context. Unlike cloud-based AI security solutions, Minerva runs entirely on an organisation's own infrastructure. Sensitive data never leaves the customer's environment and is never transferred to external cloud providers, which is essential wherever security-sensitive data must remain on-site.

Tasks that used to take days can now be completed in minutes. // No foreign provider can shut it down. Customers are already using Minerva.

KEY BENEFITS:

- > Runs entirely on the organisation's own infrastructure, with no sensitive data transferred to external cloud providers
- > Operates continuously, 24/7, even when cybersecurity specialists are unavailable
- > Identifies genuine threats within large volumes of security alerts, raises immediate warnings, and initiates response measures
- > Accelerates incident response while reducing the workload of security teams
- > Eliminates dependence on a single foreign provider that could restrict or disable access
- > Supports multiple customers simultaneously, making it ideal for managed IT security provider
- > Complies with European data protection and cybersecurity requirements



EXPERT INTERVIEW WITH

Asif Safdary

What economic potential and application areas do you see for Minerva?

Minerva combines autonomous cybersecurity with full control over sensitive data. Wherever organisations need to keep critical information on their own infrastructure, whether in energy and water utilities, banking, healthcare, public administration, or defence, Minerva performs security operations without sending data outside the organisation. Tasks that once took hours or even days are completed in less than five minutes.

Digital sovereignty is a highly relevant topic today. What role does it play for Minerva?

A central one. The European Union increasingly views dependence on non-European technology providers as a strategic risk for critical infrastructure. This became evident in June 2026, when a major US AI provider was required to disable its latest AI models (Fable 5 and Mythos 5) for international users overnight. Organisations that rely on externally controlled technology face



Asif Safdary
Founder & CEO,
CyberACI GmbH

asif.safdary@cyberaci.com
www.cyberaci.com

exactly this risk. Minerva operates independently on the customer's own infrastructure and cannot be switched off from the outside.

„AI against AI“ is becoming more common. How is it changing the threat landscape?

Attackers are increasingly using artificial intelligence to search for vulnerabilities around the clock, exploit them, adapt to defences, and automatically try again after every failed attempt. Human security teams alone can no longer keep pace, especially given the shortage of cybersecurity professionals. The only effective response to offensive AI is defensive AI, and that is precisely the role Minerva fulfils.

Which markets are most relevant for Minerva, and how do you plan to grow?

Minerva is particularly relevant for sectors with demanding cybersecurity and data protection requirements in Europe and beyond. Because these needs are universal, the solution is highly scalable and well suited for international markets. We plan to grow together with IT security service providers who can deploy Minerva across a broad customer base. At the same time, we are completing our first major funding round and expanding internationally with organisations that value digital sovereignty and want to avoid dependence on individual technology providers. ♦

CUSTOMER STATEMENT:

IT Manager at an International Staffing Company

Our security and IT operations teams were constantly stretched to their limits. Minerva has become the additional team member we were missing. It automatically analyses security alerts, identifies connections between incidents, and gives us back valuable time.

Keeping our data under our own control and on our own servers is essential for us. We were even able to cut our external security monitoring service because our team now has an experienced security analyst by its side 24 hours a day.

AUSTRIAN SAFETY PIN



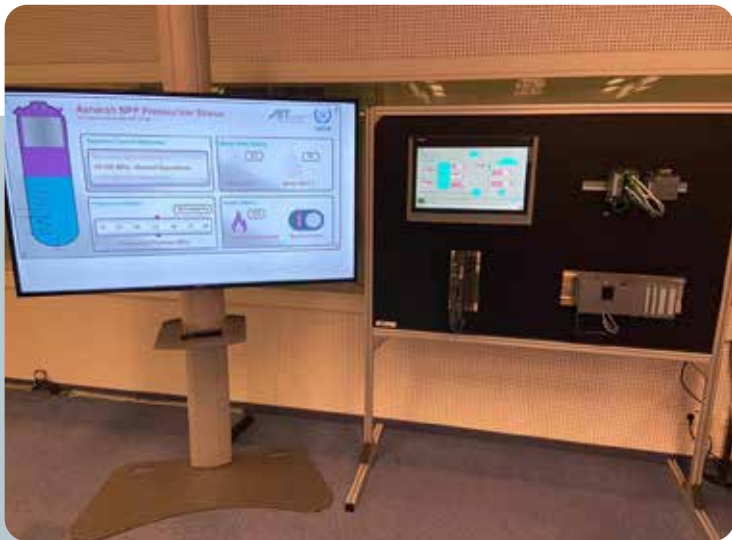
	1	2	3	4	5	6	7
SECURITY	☐	☐	☐	☐	☐	☐	☒
SOCIETAL BENEFITS	☐	☐	☐	☐	☐	☒	☐
EXPORT POTENTIAL	☐	☐	☐	☐	☐	☐	☒
ECONOMIC POTENTIAL	☐	☐	☐	☐	☐	☒	☐

AIT - AttackBed and Cyber Range

Technology portfolio for realistic cyber defence testing and training environments.

Cyberattacks pose one of today's greatest challenges to security and resilience. As part of hybrid threats, they target both civilian and military infrastructure and, as digitisation advances, increasingly affect all military domains. Due to professional, well-funded threat actors such as Advanced Persistent Threats (APTs), cyberattacks are becoming ever more targeted and sophisticated. Advances in AI make it possible to tailor attacks to specific targets, infrastructures and security mechanisms. Consequently, conventional and signature-based security solutions increasingly reach their limits.

To address this dynamic threat landscape, personnel and cybersecurity technologies must be tested, trained and improved under realistic conditions. AIT provides a comprehensive technology portfolio for this purpose: AttackMate supports analysing the impact of emerging threats on cyber-physical infrastructures, AttackBed enables the testing of security solutions, while FlowGin, Venjix and Learners enable hands-on training, for example, in cyber incident response. Playbooks and orchestration software enable automated deployment of these technologies, for example, on-premise on the AIT Cyber Range, or in public clouds.



ADVANTAGES:

> AttackMate orchestrates and automates complex attack scenarios that manifest themselves in log and network data just like real-world attacks.

> AttackBed simulates realistic cyber infrastructures and integrates hardware and digital twins of physical technologies, such as drones.

> FlowGin and Venjix automate scenarios and dynamically adapt them based on factors such as training progress.

> All technologies are continuously further developed through international and national research projects in collaboration with public authorities and industry stakeholders.



EXPERT INTERVIEW WITH Dr. Markus Wurzenberger

What sets AIT's AttackBed and Cyber Range technology portfolio apart from other solutions?
All presented technologies are open source. Therefore, they are transparent and verifiable. The same applies to generated data, which is published as open data. The tools are continuously further developed through security and defence research projects, ensuring that all functionalities remain state of the art. By working closely together with industry and public stakeholders, external input can be directly incorporated into the development process, which would not be possible with proprietary solutions.
As a non-profit organisation, AIT is not driven by profit pressures and can take greater risks in developing future technologies, creating greater potential for innovation.

What is the economic potential of the technology portfolio, and what impact does it create?
AIT uses these technologies to conduct national and international cybersecurity trainings and exercises. In addition to customised training programmes for companies, AIT has been running the KSÖ cyber exercise, one of the largest cyber exercises in the DACH region, for several years.
Industrial companies such as Rheinmetall also procure usage rights and trainings to use the technology portfolio for testing their own technologies and training their personnel. AIT's technologies are used in all ongoing projects of the European Defence Fund (EDF), related to the cyber domain with a particular focus on delivering realistic demonstrations for European armed forces using AttackBed and AttackMate.
A key priority is the generation of realistic, labelled datasets for the development of new cyber defence technologies. Particularly in military environments, the integration of cyber-physical systems, such as drones, is essential.

Dr. Markus Wurzenberger
AIT Austrian Institute of Technology GmbH

markus.wurzenberger@ait.ac.at
+43 664 815 79 37

What is needed to keep pace with the rapidly evolving cyber threat landscape?
As cyberattacks become increasingly sophisticated and networks and systems evolve at an ever faster pace, testing and training solutions must keep up with these developments. A high degree of automation is essential to meet these dynamic challenges. AI and agentic AI in particular offer new opportunities to respond rapidly to changing requirements and conditions. ♦

DEVELOPER STATEMENT:

Klaus Mayer, MSc
AIT Austrian Institute of Technology GmbH

Why is AIT's AttackBed and Cyber Range portfolio particularly exciting from an expert perspective?

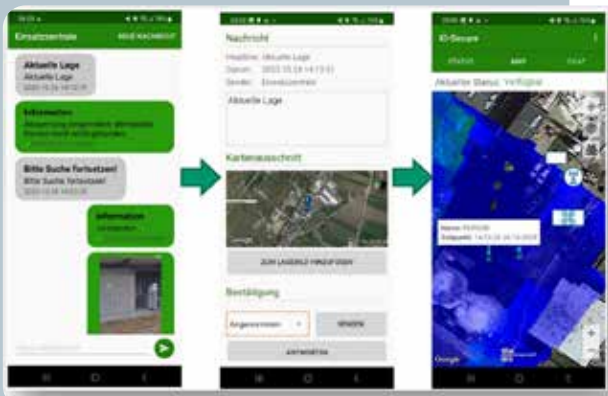
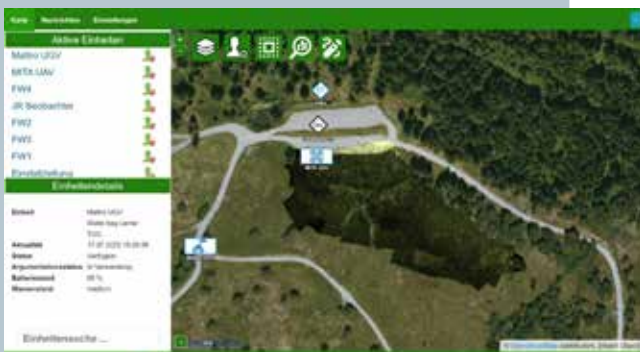
Unlike other solutions, AIT's technologies enable the individual adaptation and dynamic expansion of infrastructures and scenarios. Particular emphasis is put on implementing attack simulations in realistic environments, which is essential for gaining insights into real-world conditions. The research-driven, open-source approach promotes technological advancement and security.

KI-SecAssist

AI-Powered Support for Emergency Response in Crisis Situations



© JOANNEUM RESEARCH



A real-time situational picture makes a significant contribution to supporting emergency responders in making complex, data-driven decisions.

As part of the KIRAS project KI-SecAssist, researchers developed a demonstrator designed to provide AI-powered support for emergency responders in crisis and disaster situations. The aim was to connect unmanned aerial vehicles (UAVs) and unmanned ground vehicles (UGVs) equipped with AI-enabled sensor technology and cooperative task management capabilities, providing incident commanders with decision-relevant information in real time. The system autonomously collects and analyses sensor data and generates an up-to-date operational picture.

The project developed and integrated methods for sensor fusion, semantic segmentation, and the detection of people, vehicles, and fire hotspots into a comprehensive system. These capabilities were complemented by cooperative task management, communication between systems, multimodal operational support, and interfaces to external applications.

The technologies were demonstrated in two realistic scenarios: an industrial accident at the premises of Messer involving a simulated gas leak, and a forest fire scenario conducted as part of the AART 2023 exercise at Seetaler Alpe. The demonstrations involved automated aerial surveys, AI-powered object detection, mobile operational pictures, and the coordinated deployment of UAVs, UGVs, and emergency responders. Participants included the Graz Professional Fire Brigade, the Gumpoldskirchen Volunteer Fire Brigade, and other project stakeholders and end users.

The project demonstrated the potential of AI-based assistance systems to reduce the workload of emergency responders and support decision-making in complex operational situations.



© TWINS

EXPERT INTERVIEW WITH DI Dr. Markus Bergen, BSc

What potential does KI-SecAssist have beyond the research project itself?

Meaningful decision support is already being provided by the technologies mentioned, although often through individual tools that enhance existing capabilities. Drones are already part of daily operations, but systematically combining the collected data into a digital operational picture is still far less common. At present, this operational picture is primarily built on the experience of incident commanders and their interaction with the response team.

In the future, it will be essential to combine this expert knowledge with AI-powered technologies as effectively as possible. Above all, new technologies should provide intuitive, easily accessible support without requiring additional resources. Further research is still needed, both at the technical level, particularly in automating and integrating different systems, and in optimising processes for effective collaboration between humans and AI.

How can the technology be successfully transferred into practice?

In 2026, a spin-off of JOANNEUM RESEARCH emerged partly as a result of this project. Backed by an international investor, the company lagebild.one will further develop key technologies that also played a central role in KI-SecAssist. This will enable the technology to reach TRL 7–8.

Which areas of application and end users can benefit from the project results?

Clearly, any field in which complex, challenging, or critical situations need to be managed by multiple actors. This includes the police, military, border protection



© JOANNEUM RESEARCH/ Bergmann

DI Dr. Markus Bergen, BSc
Coordinator, Security and Defence Business

Markus.Bergen@joanneum.at

Markus Bergen is Coordinator of the Security and Defence Business Unit and a specialist in photogrammetric image processing, geoinformation services, and multi-sensor systems. Since October 2023, he has been part of the Remote Sensing and Geoinformation research group at JOANNEUM RESEARCH DIGITAL. His current work focuses primarily on security and defence, providing comprehensive situational awareness through the use of mobile platforms (UxVs), wearable sensors, geospatial data analysis, and sensor fusion.

tion and coast guards, civil protection agencies, fire brigades, technical relief organisations, emergency services, agriculture and forestry, as well as training institutions.

The underlying goal is always the same: to support people in making complex decisions based on reliable data while enhancing the safety of everyone involved. ♦

AUSTRIAN SAFETY PIN



IMPACT LEVEL

	1	2	3	4	5	6	7
SECURITY	○	○	○	●	○	○	○
SOCIETAL BENEFITS	○	○	○	○	●	○	○
EXPORT POTENTIAL	○	○	○	○	○	●	○
ECONOMIC POTENTIAL	○	○	○	○	○	●	○

DesinFact

Early Detection of Emerging Disinformation Trends through Responsible Data-Driven Analysis



DesInfact Plugin



Disinformation can undermine critical infrastructure and democratic processes, particularly in the context of hybrid threats. Detecting emerging disinformation trends at an early stage can help institutions better understand evolving situations and prepare appropriate responses.

The KIRAS project DesinFact therefore explored scientific approaches to responsibly supporting the early detection of disinformation. The research focused on methods for analysing communication and network structures, as well as content-related characteristics, to identify indicators of coordinated dissemination patterns. Rather than attempting to automatically determine whether information is true or false, the project deliberately concentrated on transparent and explainable analytical methods whose results can support expert decision-making.

Another key area of research was the clear and transparent presentation of analytical findings, alongside legal, ethical, and data protection considerations. The project demonstrated that technical tools can make a valuable contribution to the structured analysis of potential disinformation campaigns, provided they meet high quality standards and complement rather than replace human judgement.

BENEFITS:

- > Early detection of emerging disinformation trends
- > Analysis of communication and network structures
- > Combined structural and content-based analytical approaches
- > Explainable and transparent analytical methods
- > Supporting human judgement rather than automated truth verification
- > Consideration of legal, ethical, and data protection requirements
- > Investigation of prototype concepts for public analytical tools
- > Research into transparent visualization of analytical results to support decision-making

EXPERT INTERVIEW WITH

Dr. Mina Schütz, B.Sc., M.Sc.

In which application areas do you see the approaches developed in the DesinFact project being used?

A key focus of DesinFact was exploring how technical analytical methods could support end users in assessing online content. The project investigated prototype approaches designed to provide users with structured insights without making automated judgements about whether information is true or false. Particular emphasis was placed on the clear presentation of results, transparency, anonymity, quality assurance, and safeguards against misuse. The project's findings provide a foundation for further research into these types of decision-support approaches.

Where do you see the greatest potential of the project's results?

From our perspective, the greatest potential lies in combining different analytical perspectives. DesinFact demonstrated that integrating network structures, communication patterns, and content-based analyses can provide a more comprehensive understanding of emerging disinformation trends than isolated analytical methods alone. At the same time, the project highlighted that transparency, explainability, and trustworthiness are essential prerequisites for the responsible use of such technologies. These findings provide an important foundation for future research and development in this field.

What opportunities do the project results create for research and practical applications?

DesinFact has shown that responsible technical support for analysing information environments is fundamentally feasible. At the same time, the project identified several open research challenges, including



Dr. Mina Schütz, B.Sc., M.Sc.
Data Science & Artificial Intelligence
Center for Digital Safety & Security
AIT Austrian Institute of
Technology GmbH

Mina.schuetz@ait.ac.at
www.ait.ac.at

multilingual analysis, the long-term monitoring of evolving narratives, and the effective communication of complex analytical results to different target audiences. The findings therefore provide a valuable basis for future research and can help shape the next generation of analytical tools to be more transparent, robust, and trustworthy. In the long term, such systems could support professionals such as journalists, fact-checkers, and public authorities in their daily work. ♦

SENIOR SCIENTIST STATEMENT:

Dr. Alexander Schindler
alexander.schindler@ait.ac.at



Disinformation is a complex societal phenomenon that cannot be reduced to simple technical solutions. DesinFact has shown that trustworthy support is only possible when technical performance, transparency, explainability, and legal and ethical requirements are considered together. Our goal was therefore not to automate judgement, but to develop transparent and understandable methods that can support experts in their analysis.

AUSTRIAN SAFETY PIN

IMPACT LEVEL

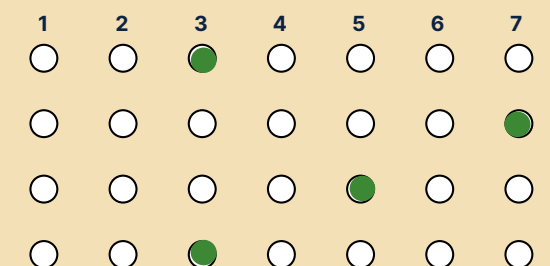


SECURITY

SOCIETAL BENEFITS

EXPORT POTENTIAL

ECONOMIC POTENTIAL



The Austrian Safety Pin



PLEASE TURN 

FOR THE GERMAN VERSION

FÜR DIE DEUTSCHE VERSION
BITTE WENDEN