next generation

cyber security

Bringing research-driven cybersecurity and innovation **closer to SMEs in Denmark**

Next Generation Cyber Security is a partnership between Digital Research Centre Denmark (DIREC), the National Defence Technology Center, Security Tech Space, and the Danish Industry Foundation. It aims to bring research-driven cybersecurity and innovation closer to small and medium-sized enterprises (SMEs) in Denmark.

This paper presents 11 Next Generation projects shaping the future of cybersecurity.

DIREC Digital Research Centre Denmark
National Defence Technology Centre
Security Tech Space NATIONAL TRYGHED - MED SIKKERHED
INDUSTRIENS FOND

NEXT GENERATION CYBER SECURITY PROJECT

DIPS IN SPACE

CYBERSECURITY FOR SATELLITES

Project partners: Technical University of Denmark, Alexandra Institute, FORCE Technology, GomSpace

A NEW DIGITAL FRONTLINE

Right now, a satellite race is underway. Global powers are investing heavily in satellite technology, and the market is booming. Yet satellites remain highly vulnerable to cyberattacks. They are deeply interconnected with ground-based systems and are often developed by smaller companies with limited cybersecurity resources. The DIPS in Space project addresses this new reality where satellites form part of the digital frontline, and sophisticated cyberattacks must be detected and mitigated.

A SPACE FOR STRONGER COLLABORATION

At the core of the project lies data collected from GomSpace's satellite platform. In close collaboration with DTU, a DIPS (Detection, Intrusion and Prevention System) will be integrated to detect cyberattacks directly onboard the satellite. FORCE Technology develops threat models that help identify critical vulnerabilities and guide cybersecurity efforts, forming an important foundation for the project's security and AI work. The collected datasets are transferred to the Alexandra Institute, which develops and trains AI and machine learning models for detecting potential cyberattacks.

DTU · ALEXANDRA INSTITUTTET · FORCE TECHNOLOGY · GOMSPACE

NEXT GENERATION CYBER SECURITY PROJECT

SECURE AM

CYBERSECURITY IN 3D PRINTING

Project partners: University of Southern Denmark, Danish Technological Institute, Partisia, Create it REAL

CAN YOUR PRINTER BE HACKED?

It's no longer just a game of printing playful plastic figures. 3D printing, also known as Additive Manufacturing (AM), is now a central component in the production of everything from aircraft to medical equipment. However, because 3D printing systems are inherently digital, they carry significant security risks. The SECUREAM project develops a methodology to strengthen security in additive manufacturing.

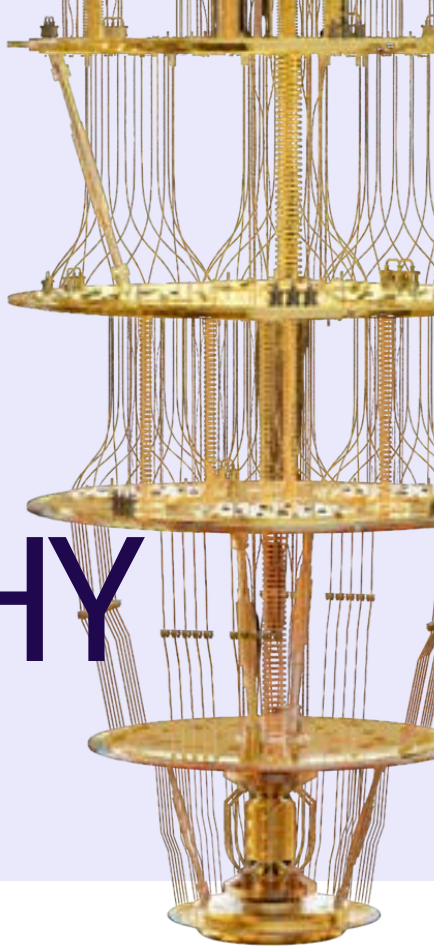
MEETING THE DEMANDS

SECUREAM enhances cyber resilience across digital AM workflows by combining blockchain-based security and Multi-Party Computation (MPC) technologies. This approach ensures confidentiality and integrity, supports regulatory compliance, and ultimately meets the demand for certified, secure AM solutions.

SDU University of Southern Denmark · TEKNOLOGISK INSTITUT · Partisia · Create it REAL

NEXT GENERATION CYBER SECURITY PROJECT

QUANTUM-SECURE CRYPTOGRAPHY



Project partners: Aarhus University, BlockDaemon

THE QUANTUM THREAT

Classical cryptography depends on keeping secret keys secure, but the rise of quantum computers threatens to undermine the foundations that protect today's systems. To prepare for future advances in quantum computing, there is increasing focus on post-quantum cryptography that combines strong security with practical deployment. This project is a collaboration between Aarhus University and Blockdaemon and addresses that challenge by adapting threshold-based key management - where control of cryptographic keys is distributed among multiple parties.

NO ONE SHOULD HAVE THE KEYS TO THE WHOLE HOUSE

The project develops post-quantum methods that let several parties jointly manage and use cryptographic keys, so no single participant ever holds the full secret. It relies on lattice-based cryptography, which is widely seen as resistant to quantum attacks, and tests whether these techniques are efficient enough for real-world use. The resulting designs are implemented as prototypes and integrated into Blockdaemon's systems, enabling organizations to adopt quantum-secure, shared key management with minimal disruption.

AARHUS UNIVERSITY

BLOCKDAEMON

NEXT GENERATION CYBER SECURITY PROJECT

SECURITY IN HYBRID APPS

Project partners: Aarhus University, University of Southern Denmark, Airofit

CAN MY HEALTH APP BE RISKY BUSINESS?

A health app can show something as immediate as your breathing in real time. To make this possible, data moves constantly between different technologies and programming languages. These complex data flows are difficult for many traditional security tools to analyze, creating blind spots where sensitive information may unintentionally leak. This challenge exists far beyond health apps, affecting areas like banking and defense as well. Hybrid applications are efficient, but they often introduce insecure data paths that attackers can exploit.

TEACHING APPS ABOUT BOUNDARIES

Led by researchers from SDU and Aarhus University, and validated by the company AiroFit, the project is developing an analysis tool that helps developers identify and fix such vulnerabilities. By combining static and dynamic code analysis across multiple languages, the project aims to turn research into a practical tool that strengthens privacy and security in everyday apps.

AARHUS UNIVERSITY SDU AIROFIT

NEXT GENERATION CYBER SECURITY - EXPLORE PROJECT

SECURITY BY DESIGN

FOR AI STARTUPS

Project partners: Alexandra Institute, PrivacyMate

MOVING FAST AND NOT BREAKING THINGS

Many AI startups build advanced agents quickly, but security and compliance are often addressed too late in the process. This creates risks around data protection, trust, and long-term scalability. This project tackles that challenge by helping startups embed security into AI agents from the very beginning. Led by the Alexandra Institute, the project focuses on identifying practical tools and frameworks that make “security by design” achievable for young AI companies.

A FIELD GUIDE TO AI SECURITY

The project results are consolidated in a whitepaper that presents a practical, research-based approach to AI security. It builds on a concrete case from the Danish startup Hipako, which uses AI to automate compliance workflows. The whitepaper introduces AI threat modelling using the MAESTRO framework, tailored to agent-based AI architectures, and provides an overview of security testing techniques such as automated red teaming with tools like garak and promptfoo.

ALEXANDRA INSTITUTTET

NEXT GENERATION CYBER SECURITY PROJECT

CLEARSIGHT

PROTECTING DENMARK'S DIGITAL INFRASTRUCTURE

Project partners: Technical University of Denmark, CSIS Security Group, Kyiv Polytechnic Institute

SMALL FAULTS CAN BE BIG

Failures in critical infrastructure often start small: An outdated controller, an unpatched system, or a subtle fault that goes unnoticed. As Europe's essential supply systems increasingly rely on aging and digital equipment, even minor issues can escalate into major outages with serious societal impact. Clearsight addresses this risk by developing an intelligent monitoring system for Operational Technology (OT) networks.

AN EARLY-WARNING SYSTEM

Clearsight is creating a practical tool that helps organizations spot weaknesses in their control systems before they lead to serious incidents. The system safely "listens in" on network traffic without disrupting operations, continuously monitoring for unusual behavior and clear signs of risk. It is designed to be easy to understand and use - even for smaller companies without large security teams. The project is led by DTU, working closely with CSIS Security Group to ensure the solution meets real-world industry needs. Kyiv Polytechnic Institute will run pilot deployments and independent confirmations in Ukraine's industrial sector.

DTU Technical University of Denmark

CSIS

NEXT GENERATION CYBER SECURITY PROJECT

AN INTELLIGENT DEFENSE

AGAINST HACKERS

Project partners: IT University of Copenhagen, Technical University of Denmark, Aalborg University, TDC NET

IT LOOKS NORMAL, RIGHT?

Normally, data flows quietly and safely through a network. But a cyberattack can change everything - often without obvious signs. The most dangerous attacks are designed to look normal, differing only slightly in timing, order, or behavior. Traditional Network Intrusion Detection Systems (NIDS), especially those trained on synthetic data, often miss these subtle manipulations.

SCIENCE MEETS REAL-WORLD

The project brings a new approach. Researchers from ITU, DTU, and AAU, together with TDC NET, are developing a next-generation NIDS that combines learning to recognize attacks from network traffic data with a rule-based approach, where experts train the machine learning model to recognize known attacks. By testing the technology directly in TDC NET's real network environment, the team aims to move the solution beyond the lab. The goal is to turn research into a working tool that can improve cybersecurity in everyday networks across society.

IT UNIVERSITY OF CPH

DTU

AALBORG UNIVERSITY

tdc net

NEXT GENERATION CYBER SECURITY - EXPLORE PROJECT

FRAUD DETECTION IN PAYMENTS

Project partners: Kynapse, Vipps MobilePay, Aarhus University

SEEING THE BIGGER PICTURE

Financial fraud is becoming more organized and harder to detect using traditional methods that look at one transaction at a time. Criminal networks hide their activity by spreading small actions across many accounts so they appear harmless on their own. This project takes a different approach by looking at payments and logins as part of a connected network, making it possible to spot patterns that reveal coordinated fraud early. The result is faster, more proactive protection of Nordic payment systems and greater financial security for citizens.

FROM RESEARCH TO REAL-TIME PROTECTION

The project combines advanced graph analytics with the speed required in real payment systems. Researchers from Aarhus University work with Vipps MobilePay and Kynapse to develop software that can detect organized fraud in real time and uncover hidden fraud networks in historical data. By embedding this research directly into an industrial platform, the project turns cutting-edge science into a practical, low-latency defense that meets European standards for transparency, AI ethics, and data privacy.

AARHUS UNIVERSITY

Kynapse Technologies

Vipps MobilePay

NEXT GENERATION CYBER SECURITY - EXPLORE PROJECT

KEEPING TRACK OF ONLINE CONTENT

WITH THE RIGHT TO BE FORGOTTEN

Project partners: IT University of Copenhagen, InReality

IS THIS REAL OR AI?

AI-generated content and widespread misinformation are making it harder to know what we can trust online. The InReality platform helps solve this by registering digital content the moment it is created, so it can later be checked that the content comes from a trusted source and has not been changed.
To make this work at large scale, the system does not rely on everyone checking everything. Instead, a small, randomly chosen and anonymous group carries out the checks and produces a digital proof that anyone else can quickly and easily verify. This project tackles the challenge of how to scale these logs.

SCALABLE TRUST: PRIVACY-PRESERVING TECHNOLOGY

The project builds new technology that makes these transparency logs both scalable and privacy-friendly. It ensures that tampering can be detected and that content can be safely deleted, without revealing who was involved.
Developed jointly by InReality and the IT University of Copenhagen (ITU), the research combines strong scientific foundations with practical solutions designed for real-world deployment.

IT UNIVERSITY OF CPH

NEXT GENERATION CYBER SECURITY - EXPLORE PROJECT

HIGH-ASSURANCE GROUP MESSAGING

Project partners: Cryspen, Confiware, Aarhus University

CAN WE TRUST THE CHAT?

Secure digital communication is essential for society, public authorities, and national defense. While one-to-one messaging is already well protected, communication is increasingly happening in large groups used by governments, companies, and international organizations. This creates new security challenges: group communication must remain just as safe, trustworthy, and future-proof. The Messaging Layer Security (MLS) protocol is emerging as the global standard for secure group messaging, and strengthening it is key to ensuring open, reliable alternatives to closed Big Tech solutions.

FUTURE-PROOF SOLUTION BACKED BY SCIENCE

Researchers from Aarhus University work with industry partners Cryspen and Confiware to verify both the design and real-world implementations of MLS, including versions that can withstand future quantum computer attacks. By combining rigorous scientific methods with practical deployment and certification needs, the project helps ensure secure group communication for government, defense, and other critical systems.

AARHUS UNIVERSITY

CRYSPEN

Confiware

NEXT GENERATION CYBER SECURITY - EXPLORE PROJECT

SECMAS

SECURITY IN MULTI-AGENT SYSTEM COMMUNICATION

Project partners: ColleaiQ, Technical University of Denmark

SAFE AI TEAMWORK MAKES THE DREAM WORK

As AI systems increasingly work together as teams of agents, new security risks arise. The danger is no longer just what a single AI says, but how information and decisions move between agents. Untrusted input can silently spread through shared memory or delegated tasks and later influence sensitive actions. SecMAS addresses this by securing how AI agents communicate and share information, helping prevent mistakes, misuse of tools, and unintended escalation - especially in high-risk settings like automated cybersecurity testing.

TEACHING AI TO PLAY NICELY TOGETHER

The project SecMAS develops simple, enforceable security rules for how AI agents interact. Researchers from DTU and ColleaiQ work together to build a secure gateway that controls identity, access rights, delegation, and shared context. Low-risk inputs stay separated from high-impact actions, which require clear approval and leave an audit trail. By testing these protections in realistic scenarios, the project supports safer use of agent-based AI in critical environments.

DTU

ColleaiQ

next generation

cyber security

Next Generation Cyber Security is a partnership between Digital Research Centre Denmark (DIREC), the National Defence Technology Center, Security Tech Space, and the Danish Industry Foundation. It aims to bring research-driven cybersecurity and innovation closer to small and medium-sized enterprises (SMEs) in Denmark.

Launched as part of the Danish Industry Foundation's cybersecurity initiative, the project is backed by nearly DKK 12 million in funding to support the development of cutting-edge cybersecurity products. Additionally, both Digital Research Centre Denmark and the National Defence Technology Center are contributing DKK 3 million each.

CONTACT

Marie-Louise Wagner
Senior Project Manager
marielouise.wagner@direc.dk

Jeffrey Scott Saunders
Chief Technology Officer
jss@nfc.dk

DIREC Digital Research Centre Denmark · National Defence Technology Centre · Security Tech Space NATIONAL TRYGHED - MED SIKKERHED · INDUSTRIENS FOND