NITECH

NATO Innovation and Technology

ISSUE 8 | DECEMBER 2022

Emerging and Disruptive Technologies	Supporting NATO and the Nations	Partnerships and Collaboration	Adopting an Innovative Culture

Focus on Technology

NATO OTAN
NATO Communications and Information Agency

MEET OUR NATO INNOVATION CHALLENGE WINNERS

Chris Aaron asks **Kai Rehnelt**, CEO of SECLOUS GmbH, what winning the NATO Innovation Challenge means for him and his company, and how non-visible data is gaining awareness

››› SECLOUS GmbH, in partnership with BWI innoX, recently won the 10th edition of NATO's Innovation Challenge, which focused on data security and management in the context of reconstruction operations – a topic that has immediate relevance to the situation in Ukraine.

Kai Rehnelt, SECLOUS founder and CEO, is confident that the win will bring important visibility for his company's technology. Although SECLOUS has trialled its software with the German armed forces, Rehnelt says, "It has been challenging for me to make NATO partners aware of this new technology." Winning the Innovation Challenge is a big step forward on that path.

Rehnelt has worked for most of his career in Enterprise Architecture, where he realized the need for providing enhanced data security and data control through a data protection layer added on top of any infrastructure. According to Rehnelt, "That layer provides a massive simplification of the required security measures and segmentation needs, and eases the protected and controlled access to any kind of data source. It can enable access to information from military multi-domain operations, even integrating civilian systems, whilst ensuring resilience, control, integrity, confidentiality and availability of the systems involved."

The security aspect involves taking any kind of digital data as it is 'created', chopping it up into chunks, extracting information from those chunks to autonomously encrypt and obfuscate each one, and then distributing the protected segments across the network without any meta-information surrounding it, essentially hiding the data. It is for this reason that Rehnelt uses the term non-visible data (NVD) to describe the approach.

When a user wishes to access some data, the necessary information is calculated on the user's device, so the relevant invisible chunks are retrieved from across the network, assembled and presented to the user on screen. This process is entirely transparent to the user, who simply uses the usual data-viewing applications as normal. However, under the surface, no visible information will ever leave the device again – just invisible data. The data-control aspect of the new technology has particular importance for organizations such as NATO that need to keep strict control over who can see particular data.

NO LOGIN, NO DATA MANIPULATION, NO LOSS OF PRIVACY

The typical login procedure and rights management has been replaced by crypto. So instead of first proving that you are the correct user and getting certain rights granted to access the data, the system calculates an ephemeral number that enables the local system to collect the required chunks, decrypt and make them usable for the defined purpose. There is no login, no data manipulation, no loss of privacy, but more control and the ability to fully revoke shared information (as the revoked users won't be able to find the chunks anymore).

In this way, the creator or owner of the data retains permanent control over who can view the data. Rehnelt explains, "All devices or servers (endpoints) would have the NVD software running on them. As the protection is part of the data, it has to happen where the data is generated or used. Keys for accessing data are calculated at these endpoints based on user and device identifiers, so there is no keystore to hack, and keys never leave the device. It doesn't matter what kind of network it is – a secure NATO network or an unsecured local civilian network – as long as the inputs to the algorithm are correct, then everyone can trust the reliability of the data, and the owner has full control of the distributed data."

Rehnelt recalls a high-ranking NATO officer at the NATO EDGE conference in Mons asking him why the big IT companies had not shown more interest in NVD. Rehnelt explains that the major IT corporates tend to have a different philosophy regarding data control and ownership – so providing clear ownership and control to the users could have a negative impact on data-driven business models. This is not because the access to data sources is harder, but rather because the cryptographic access control only allows use of the data for the agreed purposes.

THE ROAD TO BUCHAREST

SECLOUS started working with BWI, a German IT house that supports much of the non-military IT functions of the German armed forces, back in 2020. After SECLOUS had won a German forces Innovation Challenge in 2019, the military asked BWI to assess the SECLOUS NVD solution, and carry out penetration testing over a three-month period. When Markus Zobel at BWI received a newsletter announcing the NATO Innovation Challenge, he and Rehnelt agreed they should pitch the solution at the finale in Bucharest with the aim of spreading awareness and understanding of the technology across NATO.

Following the win in Bucharest, Rehnelt is exploring possible involvement with the newly formed DIANA (Defence Innovation Accelerator for the North Atlantic), which was agreed by NATO members in April 2022. In addition to the network of innovation hubs linked through DIANA, a $1 billion fund has been proposed for direct investment in innovative projects.

As Rehnelt observes, "There are other non-military organizations out there that have similar needs to NATO to achieve resilience and data control – needs that are not necessarily being met by mainstream IT providers. Schemes such as the NATO Innovation Challenge and DIANA can therefore act not only directly as drivers of innovation to meet NATO needs, but also indirectly as incubators for technologies with wider civilian and commercial applications. ❮

WHAT IS THE NATO INNOVATION CHALLENGE?

The NATO Innovation Challenge, initiated in 2017, is an ideas-generating process aimed at resolving common Alliance and NATO Nations operational problems efficiently and cost-effectively.

Co-organized by the NATO Innovation Hub at Allied Command Transformation, NATO and the Nations, the challenge gives priority access to non-traditional innovators (academia, individuals and startups) and expands NATO networks and collaboration with industry and academia.

The Innovation Challenge provides visibility to participants and their solutions and, for the winners, offers prize money and the opportunity to develop their products.

The NATO Innovation challenge is organized twice a year by Allied Command Transformation – NATO Innovation Hub. The 10th edition was co-organized with the NATO Communications and Information Agency (NCI Agency) and the Romanian Ministry of National Defence, which hosted the finale.

NATO INNOVATION CHALLENGE 2022

- 10th edition in 2022
- Location: Bucharest, Romania
- Hosts: NATO ACT Innovation Hub, NCI Agency, Romanian MoD
- Theme: Resilience
- Participants: 800+
- A network of 4,000 members

NATO INNOVATION CHALLENGE 2022 WINNERS

Team BWI innoX + SECLOUS NVD from Germany:

Resilient infrastructures and protected data management on unsecure components

Team Kinnami-University of Nebraska from the United States:

Smart resilient data fabric for real-time data collection, monitoring and analysis of critical infrastructure

Team WilNor from Norway:

Fusion of civilian and military data for improved situational awareness and management.