THE RTO INNOVATION SUMMIT

THE 2ND RTO INNOVATION SUMMIT

Industrial technologies for the future

Cybersecurity in the Digital Age

RTOs and European-wide cooperation play a crucial role in fighting against global cyber threats

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY · cea · DANISH TECHNOLOGICAL INSTITUTE · Fraunhofer · imec · RISE · SINTEF · tecnalia · TNO innovation for life · VTT

Contributing organisations and authors

This discussion paper has been produced by the authors listed below and is supported by their organisations.

AIT Austrian Institute of Technology (AIT):
Helmut Leopold, Head of Center Digital Safety and Security, helmut.leopold@ait.ac.at
Markus Kommenda, Business Development, Center for Digital Safety and Security, markus.kommenda@ait.ac.at

RISE Research Institutes of Sweden (RISE):
Shahid Raza, Director of Cybersecurity, shahid.raza@ri.se
Anneli Petersson, Strategic Research Support, anneli.petersson@ri.se

Stiftelsen for industriell og teknisk forskning (SINTEF):
Karin Bernsmed, Senior Research Scientist, SINTEF Digital, Karin.Bernsmed@sintef.no

Tecnalia Research & Innovation Foundation (TECNALIA):
Ana Ayerbe, TRUSTECH Business Area Director, ana.ayerbe@tecnalia.com

Background and Motivation

The digitalisation of almost every area of our society has changed the rules of the economy and many mechanisms of our society at an impressive pace. This transformation has been enabled by modern Information and Communication Technologies (ICT) and advances in microelectronics in combination with the networking of billions of people. The digitalisation and transformation process is gaining further momentum through the networking of numerous physical objects that are becoming the Internet of Things (IoT) and what could be in the future the Internet of Everything, as objects are going to have more and more intelligence and people and objects will be constantly connected. Everything is becoming digital in one sense or another. These developments open a huge potential for creating new applications, businesses and value streams.

However, the threats to our digital systems have also radically changed and intensified. As more and more of our physical environment is becoming digital and connected, this not only threatens our IT systems, but also our physical world and our personal privacy. As our future industry, transport systems, smart cities, power plants, energy networks, etc. will depend entirely on safe and secure systems, cybersecurity will also become a critical safety issue for our digital control systems in many spheres of our life. Safety-critical control systems in industry 4.0, in the automotive, aviation and maritime area are already demanding new methodologies and tools for safe and secure system development and will therefore even define new regulations.

Cybersecurity will not only become a crucial issue for the safety of our new digital critical systems, but it will also be a prerequisite for creating trust in our digital economy. It will be a key factor for the resilience of products, systems and ubiquitous services and thus an important factor for their global competitiveness.

The current COVID-19 crisis has been accompanied by new cybercrime patterns, mostly due to more intense teleworking and e-commerce. Cyber-attacks around the world have shown how vulnerable our society and economy have become, and that even large companies and governments are struggling to cope with cyber threats. Given that the results of a cyberattack can destroy somehow the trust of people in digital systems, the functioning of our economy and society is becoming strongly dependent on cybersecurity.

Moreover, Europe's digital infrastructure today heavily depends on systems developed in Asia and in the US, and neither users nor public authorities have full control of the security level of these systems and of the data protection mechanisms in place. There are rising concerns that Europe's digital sovereignty is at stake and that cybersecurity and privacy protection evolve too slowly to cope with all these challenges.

Major challenges and needs

Cybersecurity is intrinsically tied to challenging requirements in a complex environment. On the one hand, cybersecurity is a growing market at international level, but Europe has a cybersecurity industry with few global players and a fragmented R&D landscape. On the other hand, public investment, including research in cybersecurity, is low compared with the investments being made in other parts of the world such as the US or China. If we add that threats are global and trans-national, that there are constantly emerging threats with threat patterns and associated technologies changing quickly, and new application areas entailing new vulnerabilities and additional attack surfaces, we must recognise that Europe is in a difficult situation in fighting against cyber threats.

Cyberattacks are becoming more and more sophisticated, making use of the latest technologies, and cyber defenders are in a permanent race with them for innovation to perform their duties. Therefore, advanced cybersecurity-related technologies (Cryptography, AI/Machine Learning/Deep Learning, Quantum Technology, …) are crucial, as well as new methodologies for designing future systems with cybersecurity and privacy by design. The role of R&D is fundamental in this innovation race.

A comprehensive approach to ensure secure and safe systems

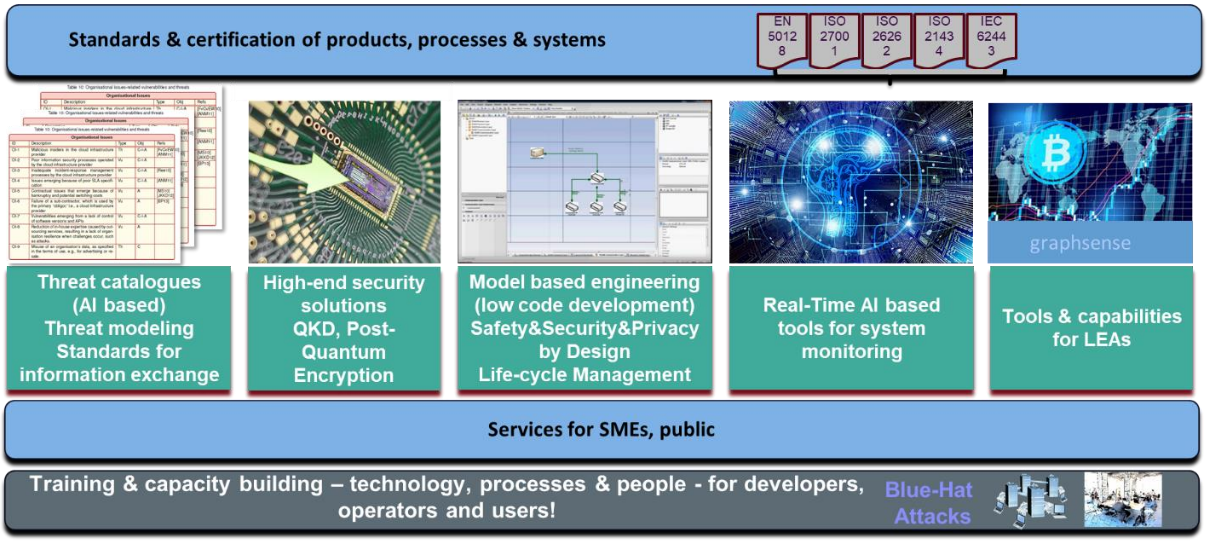
In order to ensure secure and safe digital ecosystems, a comprehensive approach, that not only covers technological developments, but also organisational and regulatory aspects is needed:

- A collaborative R&D ecosystem along the whole supply chain
- Broad adoption of proven methodologies and tools for safety and security system design and development as well as operation
- Legal frameworks, national/international policies
- Standards and certification procedures
- Awareness and capacity building for a broad spectrum of (industrial, private, governmental…) users
- Facilitating cybersecurity management for citizens

In this respect, R&D lays the ground for progress in the following key areas which complement each other to achieve safety and security in the Digital Age (cf. Fig.1 below):

- We need extensive threat catalogues for our digital systems which are continuously updated by scalable tools and methodologies by experts (from system developers to security researchers) or even Artificial Intelligence (AI)-based search tools which continuously analyse various information sources available at a global scale.
- The use of encryption should be extended to a much wider scope to ensure authenticity, integrity and confidentiality of data for highly secure information exchange and storage. Quantum Key Distribution (QKD) and other post-quantum encryption technologies are key drivers in this area.
- Safety&security&privacy-by-design methodologies and model-based low-code system development approaches will enable a new system generation and form the basis for effective testing and system certification, including cybersecurity&privacy by design of AI systems.
- New effective tools based on AI for real-time monitoring of digital as well as analogue systems are necessary to detect threats as early as possible, and to ensure safe and secure systems in operation.
- Law enforcement agencies (LEAs) and other governmental stakeholders will need new competences as well as tools to be able to effectively fight against cybercrime, espionage and terrorism in our future digital universe.

Finally, advanced training services and platforms for various industries, service operators, critical infrastructure operators, citizens and governmental stakeholders are essential support measures which will strengthen the capacities required to build, operate and use our future digital systems in a highly secure way.



Standards & certification of products, processes & systems

EN 50128 ISO 27001 ISO 26262 ISO 21434 IEC 62443

Threat catalogues (AI based) Threat modeling Standards for information exchange

High-end security solutions QKD, Post-Quantum Encryption

Model based engineering (low code development) Safety&Security&Privacy by Design Life-cycle Management

Real-Time AI based tools for system monitoring

Tools & capabilities for LEAs

Services for SMEs, public

Training & capacity building – technology, processes & people - for developers, operators and users!

Blue-Hat Attacks

Fig.1: A comprehensive approach to ensure secure and safe systems

The role of collaborative research and RTOs in Europe

The challenges and needs described above overwhelm a single enterprise and call for Europe-wide cooperation, involving various actors: universities and research organisations, industry, infrastructure operators, public authorities and other users. Joint efforts are needed to strengthen the scientific base, to develop advanced technologies, tools and methodologies, and to support capacity building, standardisation and certification.

The European Framework Programme H2020 has stimulated significant R&D efforts in the area of cybersecurity and it is important that HORIZON EUROPE will continue in this direction. RTOs play a key role in this context as they have a wealth of experience and track record in initiating and leading joint research projects that bring together relevant players from academia and industry along with public stakeholders and target end users. Moreover, RTOs are in close contact with the local industry and thus able to detect their needs and to translate them into cybersecurity R&D objectives. At the same time, RTOs are experienced in putting research results into practice through various means such as the creation of start-ups and IPR transfer to industry. In this context, the four recently established pilot networks of cybersecurity competence centres[1] are particularly noteworthy initiatives: They will not only serve to pool the existing expertise, but also help to align R&D roadmaps, to build a common agenda for investments into cybersecurity, and to set priorities for research, development and roll-out of cybersecurity solutions.

[1] Cf. https://ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-prepare-european-cybersecurity-competence-network-infographic

Recommendations and conclusions

Europe should establish capabilities, tools, and framework conditions to be ready for the Digital Age and to achieve digital sovereignty as much as possible.

- Since practically every digitisation project, regardless of the sector, involves a network connection and may therefore be confronted with a cybersecurity problem, security and privacy aspects must be taken into account right from the project design stage. Developers should widely adopt new methodologies for building digital systems, in particular by following a safety&security&privacy-by-design approach.
- New encryption concepts should be implemented as a key part of privacy-by-design in our global digital service landscape.
- Infrastructure operators should ensure a technology management capability, especially to minimize the dependence on single technology providers in a global context by multi-vendor architectures and federated services structures.
- Infrastructure and service operators should extend and enhance training and capacity building for their staff.
- Last, but not least, we need to further intensify the links between academic knowledge, industrial capacities, infrastructure and service operators as well as public and private users. RTOs play a key role in strengthening the required cooperation across organisational and national boundaries and along the entire value chain.

Any new technology can either be used ethically for the purpose for which it was developed or for other, unethical purposes. Considering that cyber-attackers are usually early adopters of technologies such as AI, the Internet of Things and quantum computers, and use them in a clearly unethical way, RTOs and industry need to work together and address this with appropriate research efforts.

Cybersecurity is key for Europe's society and economy to become resilient and to recover quickly from a crisis such as the one caused by the current COVID-19 pandemic. Cybersecurity is a prerequisite for exploiting the huge potential which digitalisation opens for new applications, businesses and value streams. There is an evolving market for cybersecurity products and services, and Europe has a golden opportunity to position itself as a global leader in cybersecurity, and RTOs have an important role to play.