CYBER SECURITY & ROBUSTNESS

The Cyber Security and Robustness (CSR) department consists of approximately 50 enthusiastic, mostly academic professionals with in-depth knowledge on (technical) cyber security and quantitative models and algorithms.

Society is increasingly depending on reliable information systems

Our experts ensure that organisations can rely on secure and robust ICT networks and services today and in the future. We accomplish this through the development of innovative solutions and methods for the design, assessment and optimisation of complex ICT infrastructures with respect to cyber security, performance and resilience to failures and cyber threats. In our work we collaborate intensively with partners such as universities, other knowledge institutes and product vendors, both in the Netherlands and abroad. Our main customers are in the field of defence, banking, telecommunications and mobility/logistics. Amongst our customers are several international operators operation for whom secure and robust ICT is a critical success factor for their business.

Our work is focused around the four R&D areas below.

Transaction security: In the coming years transaction handling is expected to change radically with associated challenges in transaction security (e.g. blockchain, impact of quantum computing on cryptography, new identity and access management technology). This focus area deals with secure transaction design in this changing transaction world.

Security monitoring and detection: This focus area deals with innovative solutions for security monitoring and detection. We have a strong track record developing anomaly-based technology for targeted cyber attacks. By analysing network traffic for anomalies, we are able to identify yet unknown attacks. Our strong knowledge base in developing anomaly detection solutions also enables us to validate the effectiveness of solutions from other (commercial) parties.

Automated security: Cyber incidents need a quick response, whereas qualified security analysts are scarce. We believe that automation can be applied to security decision support and response to address these issues. In this focus area we develop solutions for the (semi-) automation of security processes, e.g. through research on the use of advanced machine learning technology to modelling the potential impact of cyber attacks, determining and executing the optimal response to detected cyber attacks and cyber threat intelligence.

Performance of Networks and Systems: This focus area deals with the design of reliable and robust ICT networks and systems as well as other (cyber-physical) systems and how to control the performance of these networks and systems. In the context of performance of networks and systems a similar shift towards automation is foreseen as with automated security. Here the incorporation of self-organisation plays a role in the design and performance control of ICT and other networked systems.

Examples of our projects:

- Development of technology for detection of advanced cyber attacks together with various national and international partners;
- Research on the applicability of advanced cryptographic technology (secure multi party computation) in the medical domain together with partners from Philips, CWI and the UvA;
- Research for our strategic customer defence targeted at extending their cyber security capability;
- Research and advice on the stability of the DNS root in the context of the delegation of substantial numbers of new generic Top Level Domains (such as .google) for ICAN;
- Advice on optimal access network planning for telecom operators;
- Analysis and benchmarking of the security level of the European telecom providers on assignment from the international branch organisation (ETIS);
- H2020 project on post-quantum cryptography in a consortium with European partners.