Cyber Security

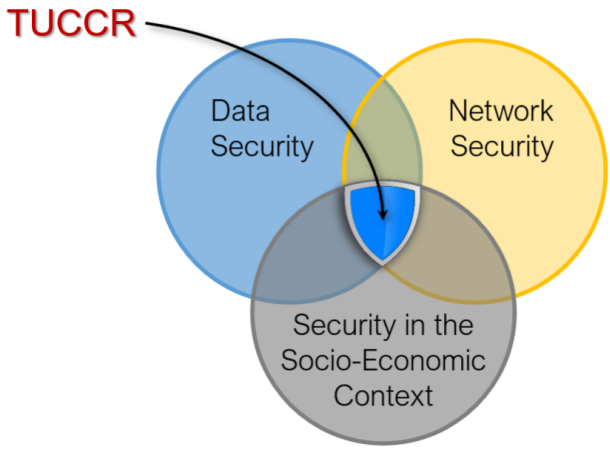
The world is quickly changing into a digital society. All people are being connected through the Internet (Internet of People), all devices are being connected (Internet of Things), all companies are being connected as well as all services that we rely upon. For our digital society the ubiquitous availability of data has become crucial.

However, now that our society has changed into a digital society, we should understand that we completely depend on the correctness of our data as well as the proper operation of the underlying ICT infrastructure. We should trust our data under all circumstances, which requires it to be not only stored and exchanged in a secure and privacy preserving way, but also that we understand where the data comes from and how it will be used. Since our society cannot sustain without the Internet, we must certify that we understand its operation and keep control over it, under all circumstances. Whereas that was easy just one or two decades ago, nowadays it is a real challenge, especially since a small number of big players and nation states gained control over major parts of our ICT infrastructure and services, and thus our society. As a consequence, our digital sovereignty is at stake, and Europe runs the risk of being digitally colonialised by others.

But as well as nation states that use the Internet to gain more influence, traditional criminals have also discovered the Internet to make money by performing large scale attacks on users and systems connected to the Internet. Examples include data exfiltration attacks that frequently lead to mega breaches exposing sensitive data from millions of innocent people to criminals, as well as Ransomware and Distributed Denial-of-Service attacks that bring down the complete service of an organisation. On an almost daily basis, newspapers world wide report about such cyber-attacks and the impact that they have on our digital society.

To address these challenges, the UT established the Twente University Centre for Cybersecurity Research (*TUCCR*) [59]), with the goal to create a long-lasting Public-Private Partnership around cybersecurity at the regional and national level. TUCCR was officially opened on March 5. 2021, and its partners include Betaalvereniging Nederland, BetterBe, Cisco, NCSC, NDIX, Northwave, SIDN, SURF, Thales and TNO. TUCCR has strong connections with national cybersecurity agenda setting organisations, such as dcypher, ACCSS, NCSC, the Dutch Digital Delta and TNO, but also with international projects and organisations, such as CONCORDIA [70] and the CODE cybersecurity center [71] in Munich.

The mission of TUCCR is to make our society resilient against cyber-harm by researching digital technologies in the societal and economic context for their robustness against cyber-harm and by developing solutions that provide the necessary level of resilience and security. To this end, we investigate associated cyber-security challenges with a specialised focus on real-world data and network security in the socio-economic context (see Figure 1). We cover the complete range of steps necessary to develop secure solutions for the real world, starting from the analysis of known cyber-harm, - attacks and -vulnerabilities and their proper modelling, to the engineering of targeted protection, mitigation, detection, and response solutions, all the way to their implementation and extensive testing. In each of these steps, we are paying explicit attention to the demands imposed by the socio-economic context and the involved human factor, which can be part of the problem and part of the solution at the same time.



We target societal and economic impact by driving innovation. To ensure this, our research is highly use-inspired and largely driven by real-world challenges found at the TUCCR partners, but also elsewhere. We perform open and well-documented research to ease reproducibility and collaboration and to allow for effective knowledge transfer. Key components in this are, besides publishing our research at the top security conferences and in journals, the release of open-source tools and datasets as well as the creation of minimum viable products and businesses.

To deliver the next generation of cybersecurity experts that meet the demands in industry, government, and academia, our research and entrepreneurial ambitions are tightly coupled with our educational programmes. Our cybersecurity graduates have a T-shaped profile with 2/3 of deep technical knowledge and 1/3 of socio-economic knowledge in cybersecurity. See our cybersecurity master programmes for more details: 4TU Cybersecurity Master Specialisation [72] and EIT Digital Master in Cybersecurity [73].