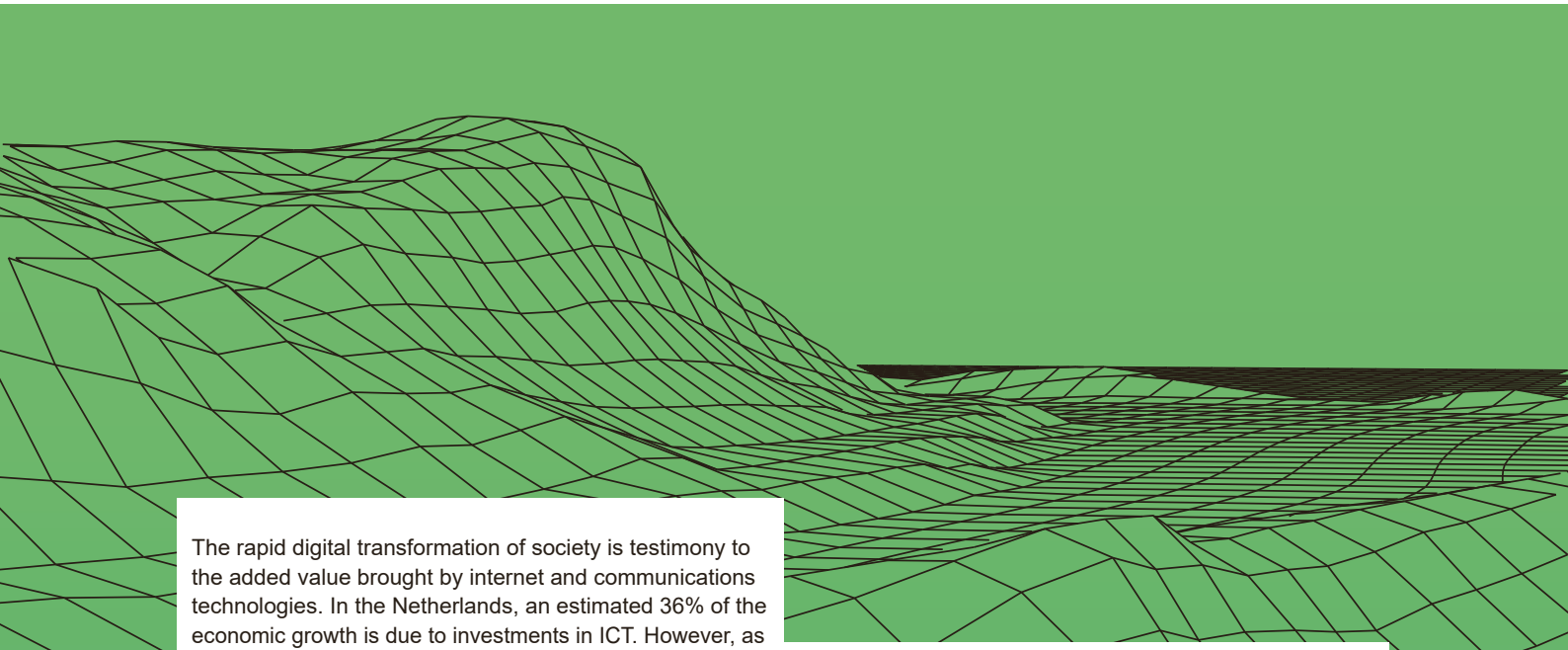
Towards system resilience in an interconnected world



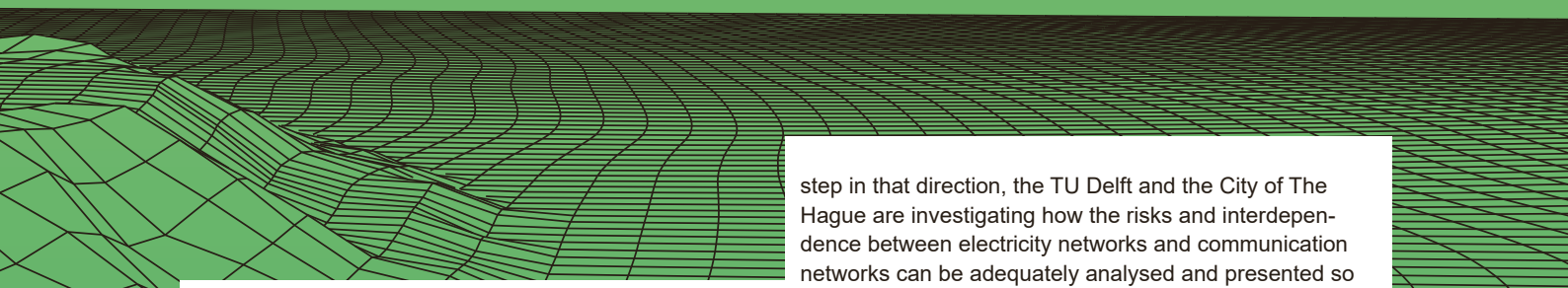
The rapid digital transformation of society is testimony to the added value brought by internet and communications technologies. In the Netherlands, an estimated 36% of the economic growth is due to investments in ICT. However, as people and ICT systems increasingly interconnect, dependencies are also introduced, posing risks to the security and availability of those systems. We have seen a multitude of cybersecurity incidents with significant societal impact already hit the news, ranging from ransomware to denial-of-service attacks inflicted by malicious entities. Digital infrastructures can also be affected by outages through other factors, such as human error due to increased complexity in operating networks, natural disasters, ageing of hardware, excessive traffic workloads, power disruptions, and so on. Moreover, many actors are typically involved in using or managing digital infrastructure, ranging from service providers to customer groups, multinationals, government agencies, NGOs, and critical infrastructure providers. The challenge is operating such complex multi-stakeholder systems and making them resilient. Systems thinking is required: the science, design, and engineering of complex systems. Such systems thinking should focus on functional properties, such as what the system should do, and non-functional properties that relate to how we would like those systems to work, in line with our norms and values: the human dimension!

From a cybersecurity perspective, system resilience is a critical concept. One could argue that the terms ‘cybersecurity’ and ‘system resilience’ are fundamentally linked: the level at which a system, an infrastructure or an organisation is ‘cybersecure’ is defined by its resilience: the degree to which it can withstand attacks, the time it takes to recover main functions, and the aptitude to learn and adapt to new circumstances. These abilities stem from an intricate interplay of technological, organisational, human, and infrastructural elements and typically cannot be acquired through simple product purchases or the adoption of universal standards. Cybersecurity emerges from a wide range of instruments and processes, such as vulnerability assessment, secure product design, cyber-skill development, monitoring and reaction facilities, robust recovery strategies, and failure forensics: aspects that nicely align with the current research themes of the TU Delft Safety & Security institute. Such instruments and processes are relevant for the resilience of any system, whether we are looking at a singular digital system, a specific infrastructure, or an entire business sector.

To safeguard current systems and futureproof the systems of tomorrow, we need to take significant steps forward in our understanding of ‘cyber system resilience.’ New European regulations, such as the Critical Entities Resilience (CER) Act and the Network & Information Security (NIS) 2 Directive, also call for cyber resilience and prescribe all kinds of related measures, but more is needed to establish system resilience. What makes a system more or less cybersecure, and what must we change to create a more resilient system? While these questions may seem abstract, they are more relevant now than ever. The rapid development of AI technologies, new digital infrastructures such as 6G, and the inevitable arrival of quantum computers will fundamentally change the threat landscape over the next decade. Our digital landscape will morph into a ‘digital continuum’ of (largely

When it comes to social security, there is broad consensus in the Netherlands that policy and implementation should focus more on the human dimension instead of the 'system's realit'. And for good reasons. Yet, Fernando Kuipers, Martijn Neef, and Daan Rijnders argue that cybersecurity requires more systems thinking to achieve resilience and respect the human dimension.

text Fernando Kuipers, Martijn Neef and Daan Rijnders



decentralised) compute, storage, and communications resources, with new capabilities and opportunities and potentially new vulnerabilities. Malicious actors will also use these new technologies to craft new lines of attack and test our system resilience to extremes.

Cyber resilience is about safeguarding digital systems against threats known and unknown, and in the understanding that current cybersecurity technologies and approaches (a) will not be enough to withstand the attacks of the future and (b) have to be made more cost-effective from a long-term perspective. Therefore, Cyber system resilience deserves the attention of research and innovation parties with the ambition to jointly create the groundwork for future digital infrastructures. Within that ambition, there are many outstanding challenges to be solved. For example, we need techniques to measure cyber resilience, new design paradigms that put cybersecurity at the heart of systems, new monitoring, recovery and mitigation strategies that can cope with unknown threats, etc. Every sector will benefit from such system-centered approaches; everywhere with IT/OT-based infrastructures and a complex interplay between humans and systems. In logistics, at sea, healthcare, energy, and any other domain where deep transitions occur.

Realising system resilience is clearly complex and, hence, best tackled jointly and interdisciplinary. As stipulated in the Dutch Cybersecurity Strategy, innovation policy already paves the way forward: we need to invest in cybersecurity technology, skills and processes to ensure the autonomy, resilience and robustness of our vital systems. As a first step in that direction, the TU Delft and the City of The Hague are investigating how the risks and interdependence between electricity networks and communication networks can be adequately analysed and presented so that practitioners can better assess and manage risk. This will help to develop better crisis response strategies and take more effective preventive measures.

Joining forces nationally to take a (global) leadership role in the shaping of cyber-secure and resilient systems will not only dwindle the costs associated with the current omnipresent cyber security attacks, but it will also position the Netherlands as a secure, resilient, and hence trusted location for data and communications services.

Fernando Kuipers established and leads the Networked Systems group at TU Delft, where he works on Internet and communications technologies. He co-founded the PowerWeb Institute, is a member of the Board of the TU Delft Safety & Security Institute, and is the founding scientific director of the Do IoT fieldlab.

Martijn Neef is the Knowledge and Innovation Cybersecurity Coordinator at the Directorate of Digital Economy of the Dutch Ministry of Economic Affairs and Climate Policy.

Daan Rijnders leads the Cyber Secure The Hague program for the City of The Hague, which focuses on The Hague's unique risk profile as an International City of Peace & Justice and the cyber resilience of the local critical infrastructure & processes.

Scan the QR code for the complete digital version of this magazine

Today's grand challenges can no longer be solved with a single perspective or approach

Aukje Hassoldt
Dean TU Delft Faculty of Technology, Policy and Management

progreSSIon

On the occasion of 10 years TU Delft Safety & Security Institute

SAFETY & SECURITY IN A CHANGING WORLD

Safe by Design

"Engineers must learn to talk about ethics"

Field perspective

All in for safety & security

Opinion

We need an inclusive approach to flood risks

Road, air, rail

Safety & security in a transport sector on the move

Discussion

Are sustainability and safety incompatible?

TU Delft Safety & Security Institute

An institute building bridges

TU Delft