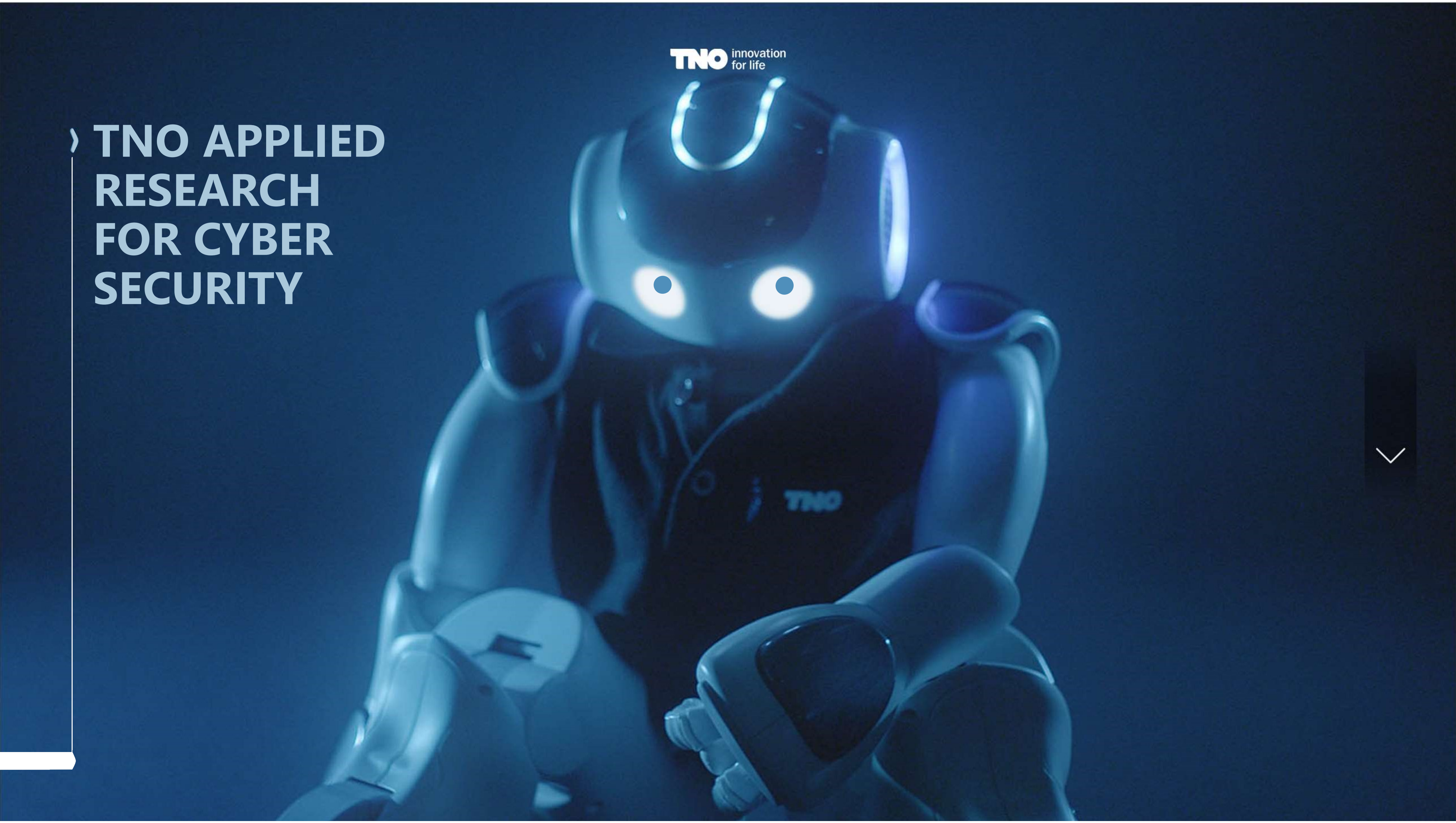


TNO APPLIED RESEARCH FOR CYBER SECURITY

TNO innovation for life

SMART SOLUTIONS FOR CLIENTS & PARTNERS

KNOWLEDGE TRANSFER (10%)

Knowledge exploitation by spin-offs, licences, in partnership with other companies

DEVELOP FUNDAMENTAL KNOWLEDGE (10%)

Together with universities

CLIENTS & PARTNERS

KNOWLEDGE APPLICATION (40%)

Contract research for and with clients

KNOWLEDGE DEVELOPMENT (40%)

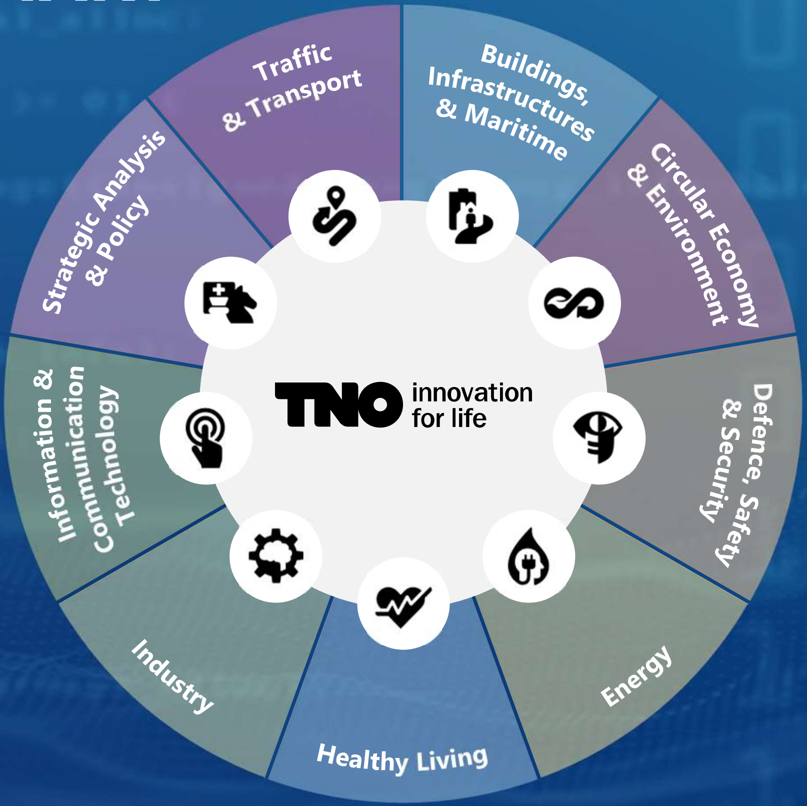
In public-private partnership with partners from the golden triangle

TNO innovation for life

WE DO THIS BY TAKING A MULTIDISCIPLINARY APPROACH

TNO TURNOVER
(MLN EURO)

483


TNO innovation for life
Traffic & Transport
Buildings, Infrastructures & Maritime
Circular Economy & Environment
Defence, Safety & Security
Energy
Healthy Living
Industry
Information & Communication Technology
Strategic Analysis & Policy

TNO NUMBER OF EMPLOYEES

3265

Source: TNO annual report 2018

TNO UNIT ICT KEY FIGURES

UNIT ICT TURNOVER
(MLN EURO)
40

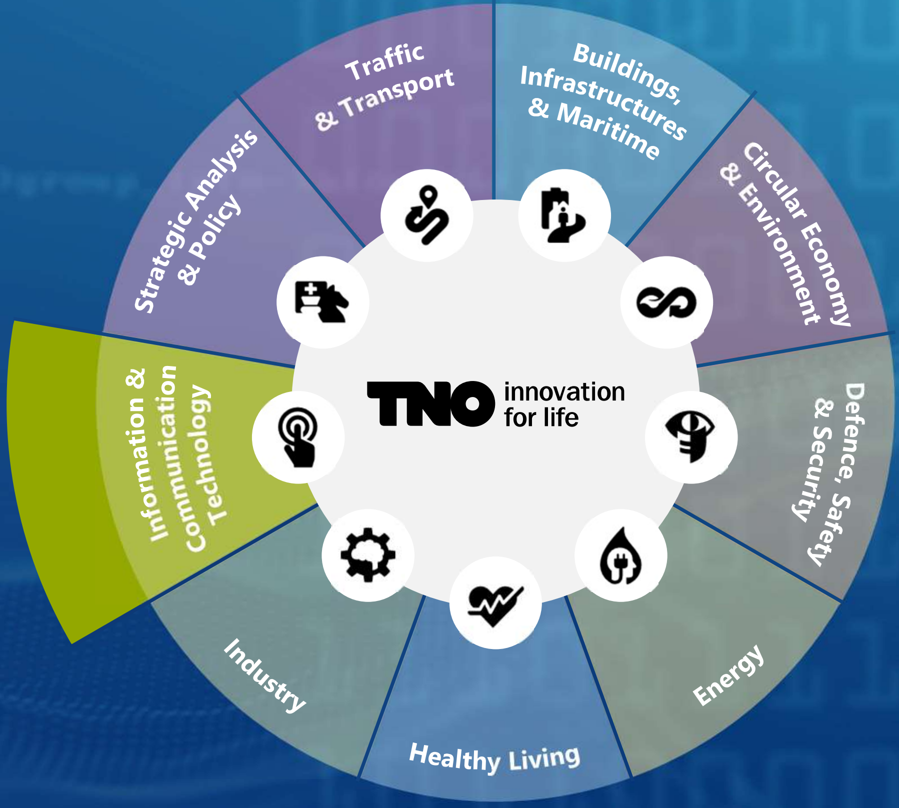
MULTIPLIER
3,5

UNIT ICT NUMBER OF RESEARCHERS
250

UNIT ICT NUMBER OF PROFESSORS/LECTURERS
10

UNIT ICT NUMBER OF CLIENTS PER YEAR
95+

ACTIVE IN
15+
COUNTRIES



TNO innovation for life

Traffic & Transport

Buildings, Infrastructures & Maritime

Circular Economy & Environment

Defence, Safety & Security

Energy

Healthy Living

Industry

Information & Communication Technology

Strategic Analysis & Policy

Source: TNO internal figures 2018

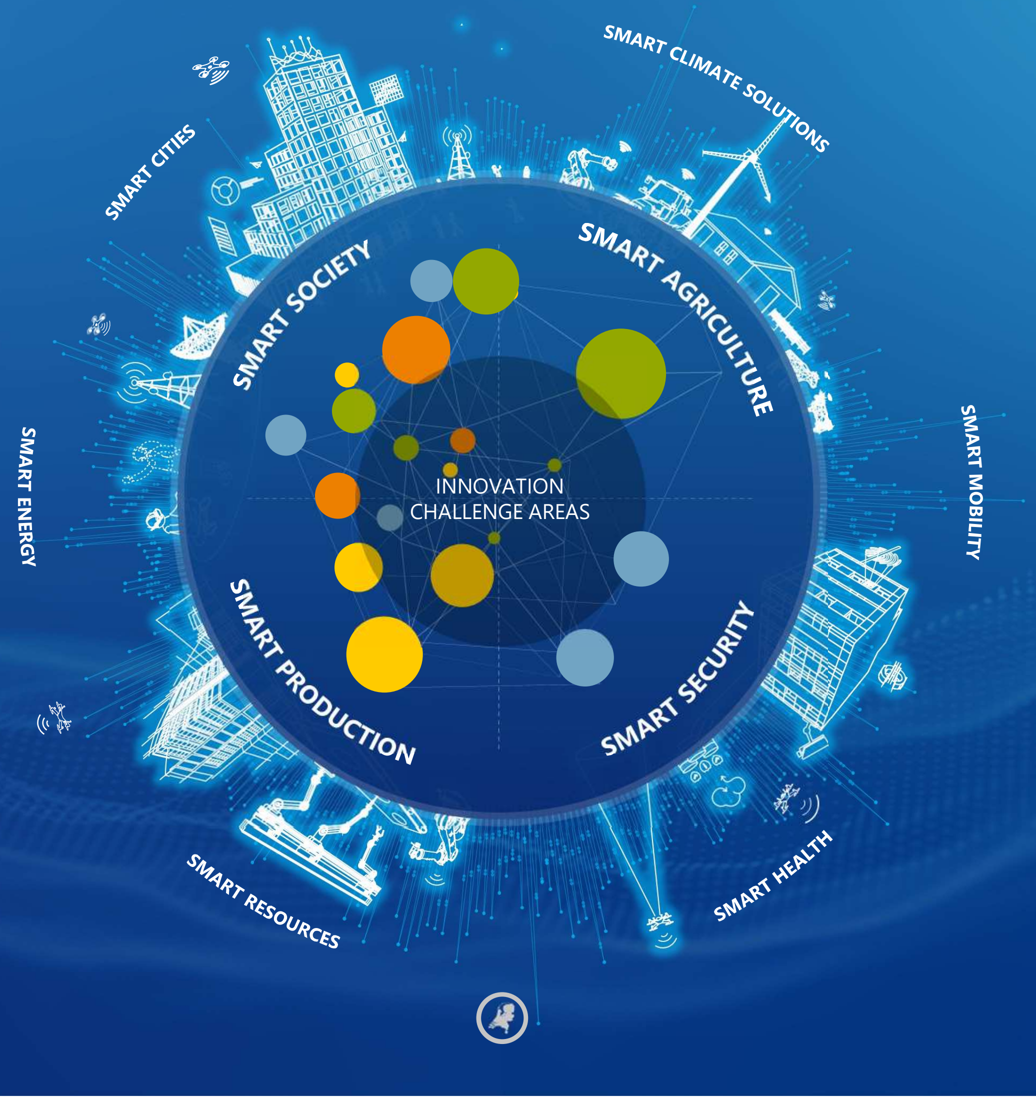
TNO innovation for life

UNIT ICT PMC CLUSTER
FAST OPEN INFRASTRUCTURES

"Making a difference in a generic, highly flexible ICT infrastructure that delivers instantly and ubiquitously accessible ultra-high bandwidth connectivity, massive storage and processing as well as application platforms that adapt to utilize the available resources optimal."

UNIT ICT PMC CLUSTER
EMBEDDING SYSTEMS INNOVATION

"Making a difference in the High Tech industry by addressing the challenge of mastering architecting and design of ever increasing complex systems through new and radically improved systems/software design and engineering methods."



UNIT ICT PMC CLUSTER
DATA SHARING

"Making a difference in data sharing provides enormous opportunities for companies. Data is the new fuel."

UNIT ICT PMC CLUSTER
TRUSTED ICT

"Making a difference in preventing risk of financial loss, disruption or damage to the assets and reputation of an organization from some sort of failure of its information technology systems."

TNO innovation for life

REGIONAL INNOVATION ECOSYSTEMS

UNIT ICT PMC CLUSTER
FAST OPEN INFRASTRUCTURES

kpn · vodafone · ERICSSON · TNO innovation for life · HUAWEI · SURF

Telco/ICT

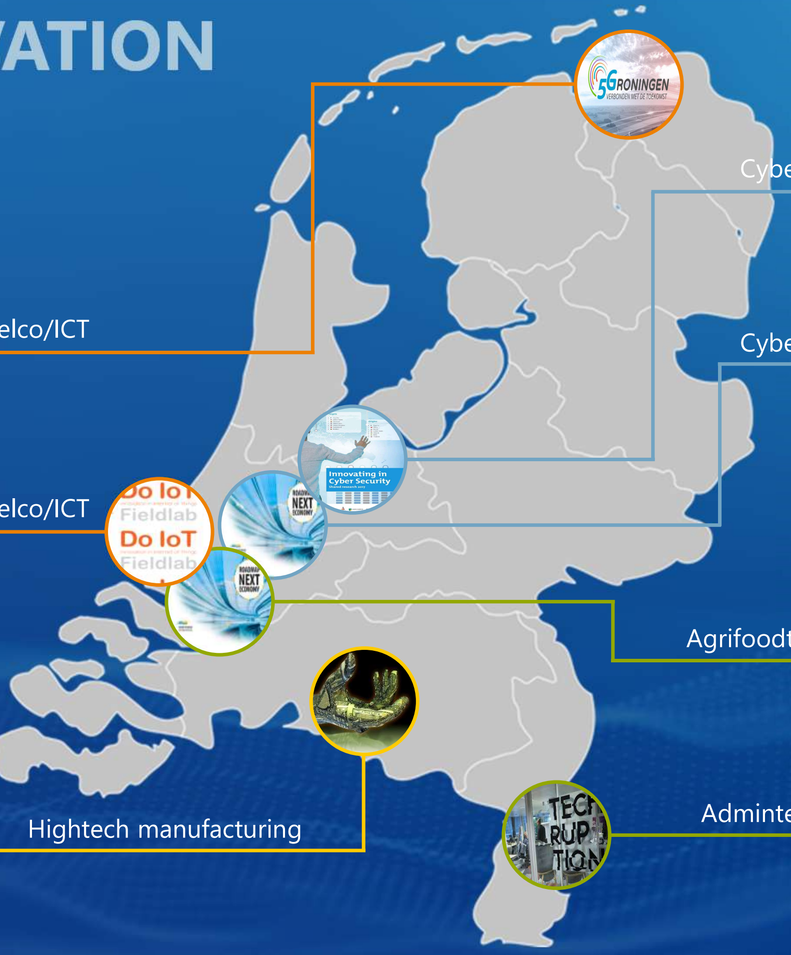
TU Delft · MRDH METROPOOLREGIO ROTTERDAM DEN HAAG · BTG · provincie ZUID HOLLAND · esa

Telco/ICT

UNIT ICT PMC CLUSTER
EMBEDDING SYSTEMS INNOVATION

PHILIPS · Radboud Universiteit · NXP · océ A CANON COMPANY · TU Delft · THALES · ASML · TU/e Technische Universiteit Eindhoven University of Technology

Hightech manufacturing



UNIT ICT PMC CLUSTER
TRUSTED ICT

Cybersecurity

Rabobank · achmea · de volksbank · ABN·AMRO · ING

Cybersecurity

kpn · HSD The Hague Security Delta · Secura · provincie ZUID HOLLAND · Compumatica SECURE NETWORKS · HUDSON CYBERTEC · Den Haag · elastic

UNIT ICT PMC CLUSTER
DATA SHARING

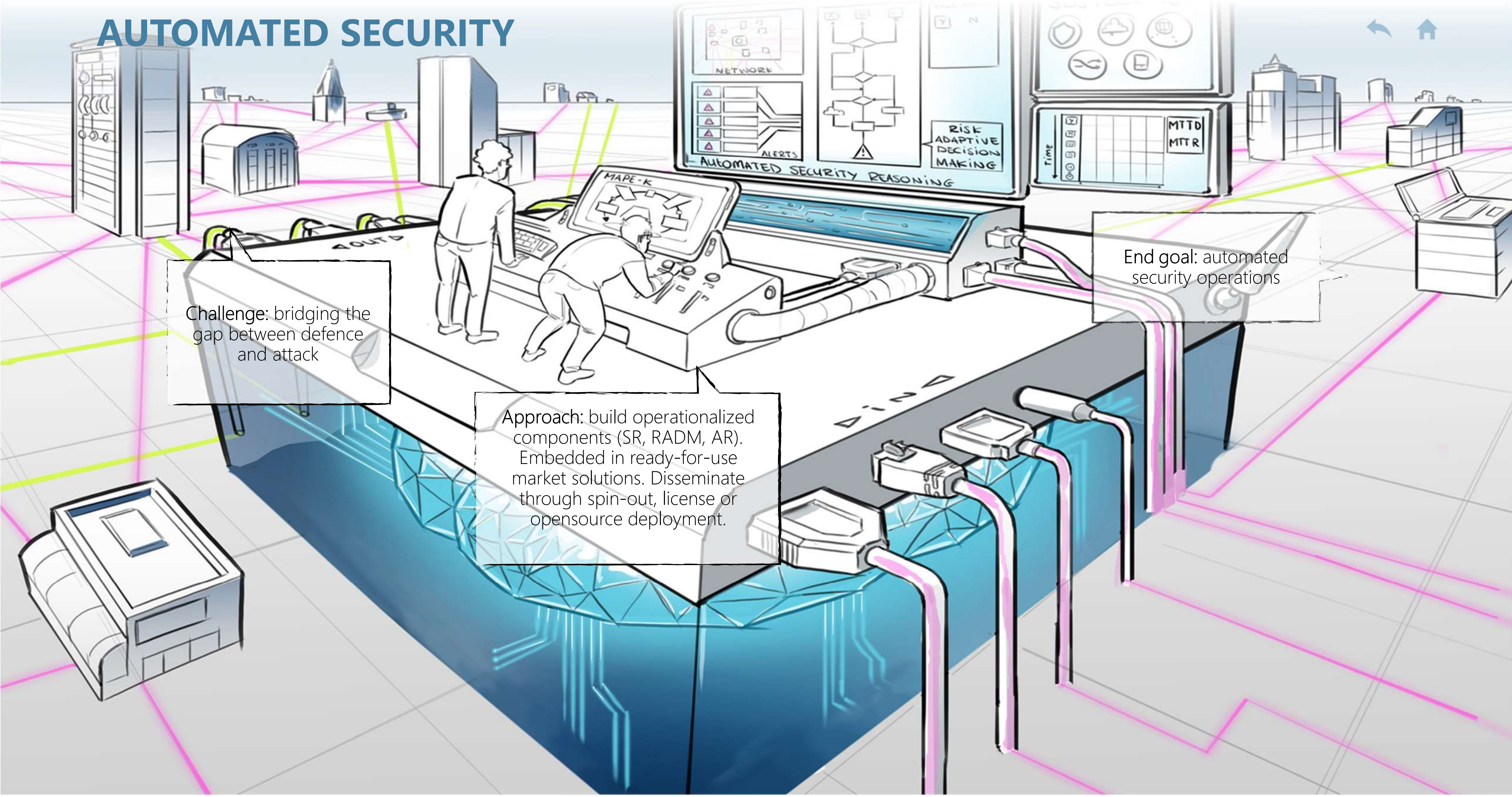
Agrifoodtech

WORK IN PROGRESS · GREENPORT West-Holland

Admintech

Centraal Bureau voor de Statistiek · apg · CZ · kamer van koophandel · Rabobank · Brightlands Knowledge crossing borders · provincie limburg · accenture High performance. Delivered. · Maastricht University · Eneco

AUTOMATED SECURITY



Challenge: bridging the gap between defence and attack

Approach: build operationalized components (SR, RADM, AR). Embedded in ready-for-use market solutions. Disseminate through spin-out, license or opensource deployment.

End goal: automated security operations

AUTOMATED SECURITY

CHALLENGE

Challenges for our clients typically include:

- *How can I effectively manage the increasing amount of security alerts by automation of security operations?"*
- *"Is security automation a viable approach for my SOC or CSIRT – considering global competition for skilled security analysts and a general lack of knowledge sharing and transfer?"*
- *"How do I manage – and optimize – a multitude of security tools?"*
- *"Would security automation allow me to reduce the Mean Time To Detection (MTTD) and Mean Time To Response (MTTR)? And if so, how can I achieve these results?"*

APPROACH

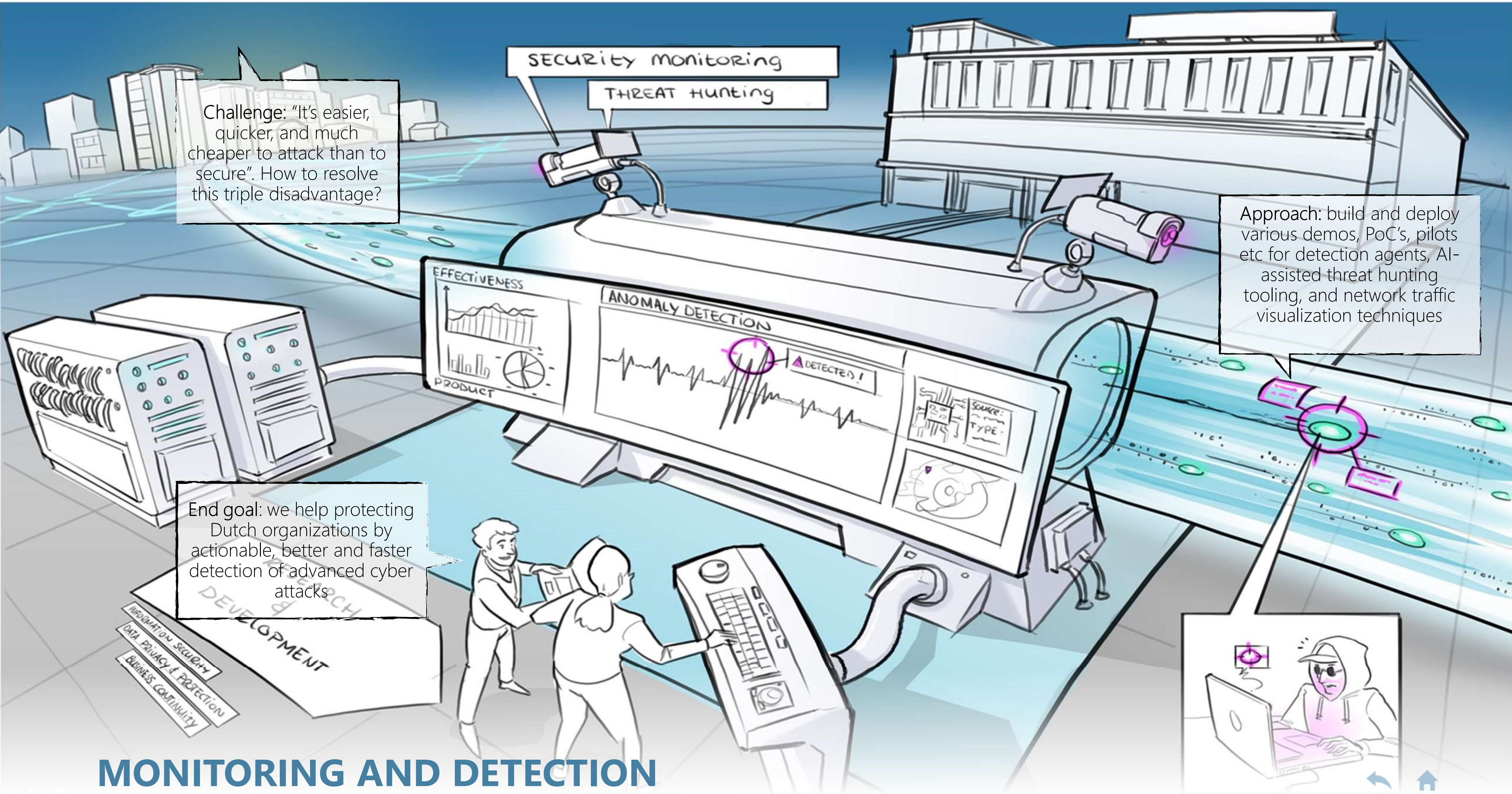
To allow our customers and partners to automate security operations (within a SOC, CERT, or CSIRT) we combine concepts and techniques for security reasoning, risk adaptive decision making (and other concepts from Advanced Security Architecture), and on-demand reconfiguration of ICT infrastructures & security controls (*Automated Response*).

END GOAL

Our end goal is to bridge the gap between attack and defence.

So that our clients and partners can safely and securely transform their organizations in complex, digital transformations and system transitions.

To this end we drive and develop (technical) solutions and concepts for automating cybersecurity operations, that will reduce the Mean Time To Detection (MTTD) and Mean Time To Response (MTTR), drastically reduce the amount of repetitive tasks of SOC analysts, and thereby create a more resilient enterprise ICT infrastructure.



Challenge: "It's easier, quicker, and much cheaper to attack than to secure". How to resolve this triple disadvantage?

Approach: build and deploy various demos, PoC's, pilots etc for detection agents, AI-assisted threat hunting tooling, and network traffic visualization techniques

End goal: we help protecting Dutch organizations by actionable, better and faster detection of advanced cyber attacks

MONITORING AND DETECTION

MONITORING AND DETECTION

CHALLENGE

Challenge:

SM&D focuses on development of innovative technology for finding new cyber threats in company networks and OT for which no signatures exist (yet).

Detection capabilities are based on network (traffic) and other centrally collected data sources.

SM&D supports anomaly-based network monitoring and detection as well as threat hunting against cyber-attacks in tomorrow's highly dynamic ICT environments.

APPROACH

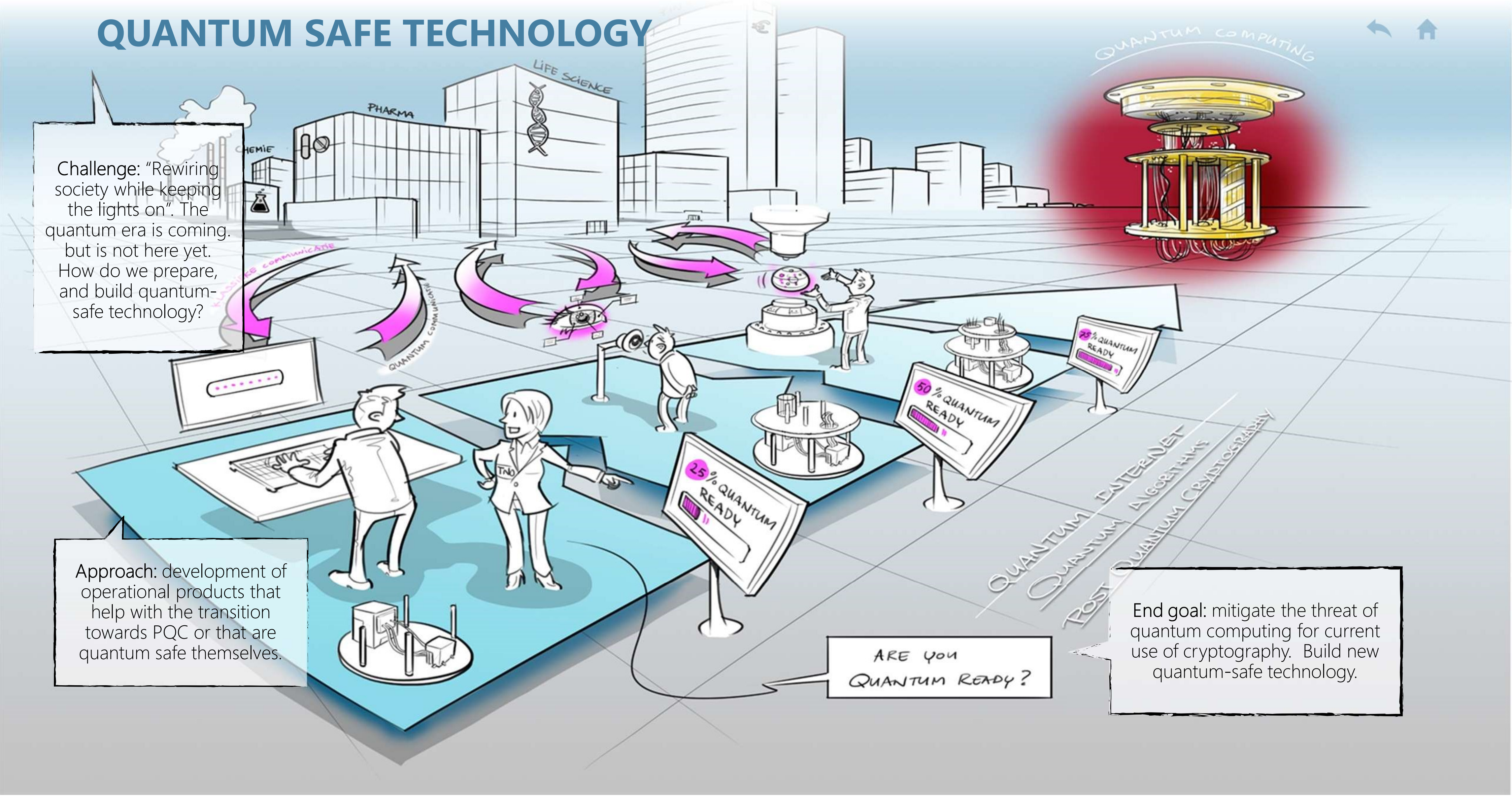
Security Monitoring & Detection (SM&D) is an essential part of – and precondition to – Trusted ICT. It's for good reasons SM&D is part of globally accepted principles for IT security and best practice guidance. Our approach consists of the following supporting activities:

- Technology development, scientific research, and consultancy services for M&D of cyber attacks
- R&D of detection algorithms based on network traffic and other data sources which can be collected centrally.
- Development of innovative technology for anomaly detection (AD) and threat hunting to combat attacks in ICT and IT / OT infrastructures.
- Structured methods to evaluate commercial products and their effectiveness

END GOAL

- Innovative detection agents deployed in various operational environments. TNO agents are based on anomaly detection, combinations of different network traffic data sources (including external sources), Artificial Intelligence (AI) & visualization techniques.
- TNO AI-assisted Threat Hunting tooling operational with support for analysis of internal network traffic (lateral movement) and outgoing network traffic (CnC channels, data exfiltration).
- SM&D implemented in (near) real-time Automated Security control loops.
- New strategic R&D collaborations with SOCs (e.g. of Government Parties) as well as vendors and MSSPs.

QUANTUM SAFE TECHNOLOGY



Challenge: “Rewiring society while keeping the lights on”. The quantum era is coming. but is not here yet. How do we prepare, and build quantum-safe technology?

Approach: development of operational products that help with the transition towards PQC or that are quantum safe themselves.

End goal: mitigate the threat of quantum computing for current use of cryptography. Build new quantum-safe technology.

QUANTUM SAFE TECHNOLOGY

CHALLENGE

Challenge:

Quantum computers will break the encryption that protects the internet as we know it.

Starting with telecom and financials, and a selection of industries such as pharmaceuticals, chemicals ands energy quantum technology is expected to have impact on modelling physical systems. Algorithms using quantum math can unlock customer value by vastly speeding up data-intensive applications in such fields as search, cryptography, and machine learning.

For public sector, policy makers, and governments as well as Defense the challenge mainly lies in keeping classical computing safe as well as deploying quantum-safe technology.

APPROACH

Reinforce our knowledge position and research agenda, to develop and apply quantum technologies in the private and public sector, and to execute on TNO's scientific, societal, and economic goals while strengthening our brand value.

Our approach will focus on:

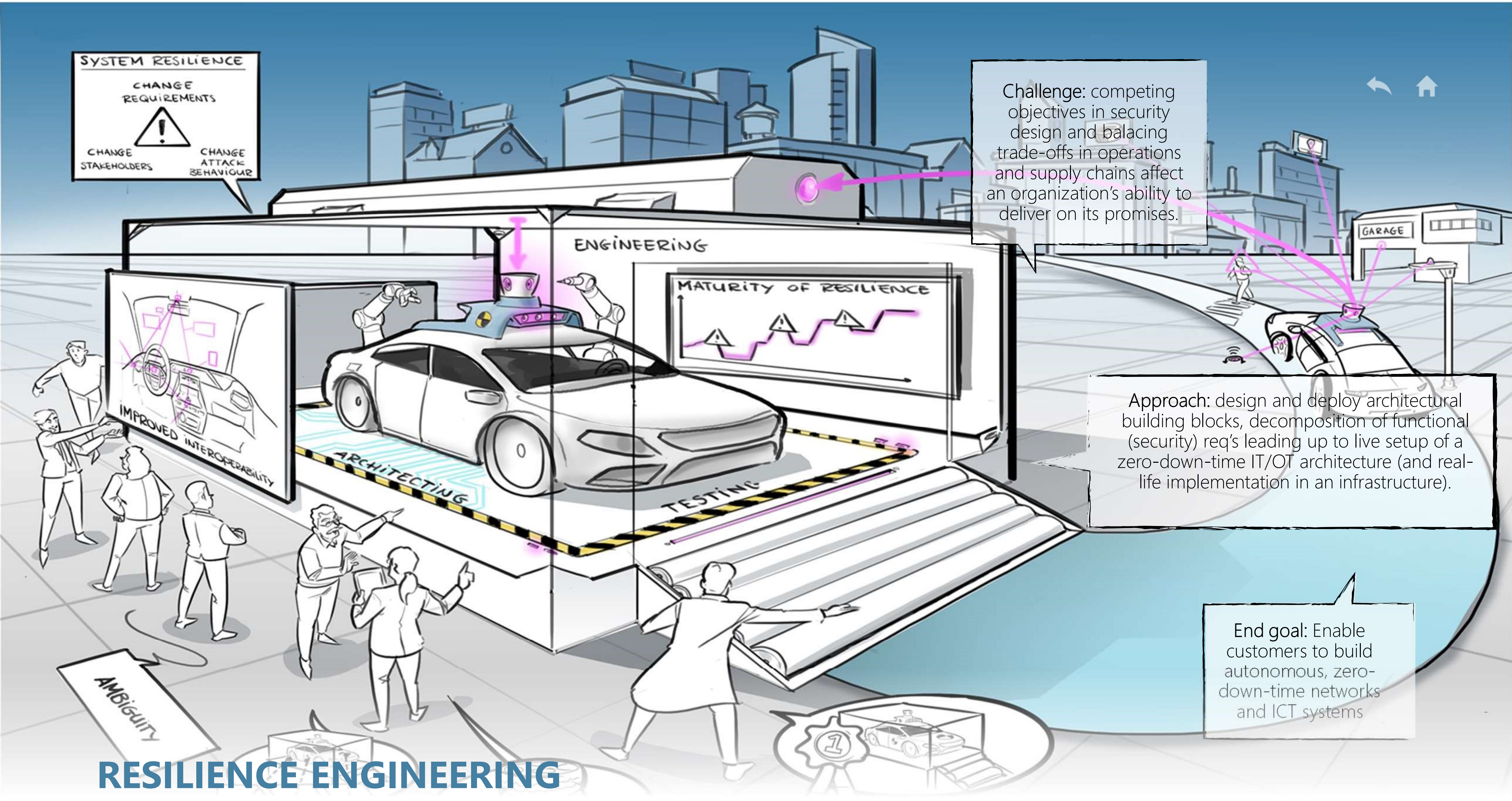
- Secure quantum communication networks, quantum key distribution, and quantum crypto.
- Post-quantum cryptography with both fundamental research and applied research.
- Quantum Computing and quantum algorithms and applications.

END GOAL

End goal: build quantum-safe technology - incl:

- 2020: Hybrid fiber & free-space QKD set-up with commercial partner, focus on business cases, various QS PoC's (PKI, DNSSEC, Proxy), system design quantum end nodes, improved photon rates for NV centers
- 2025: (in collaboration with QuTech) 4-node quantum internet, commercial MDI-QKD product, TNO QKD ground station finalized, TNO recognized as a leader in quantum security for industry, follow-up on QIA, business case for distributed quantum computing, and first (world-wide) experiment.
- 2030: QKD and entanglement distribution using TNO ground and space segment as part of world-wide quantum network, TNO key-player in quantum-safe digital communication, commercial quantum repeater.

RESILIENCE ENGINEERING



Challenge: competing objectives in security design and balacing trade-offs in operations and supply chains affect an organization's ability to deliver on its promises.

Approach: design and deploy architectural building blocks, decomposition of functional (security) req's leading up to live setup of a zero-down-time IT/OT architecture (and real-life implementation in an infrastructure).

End goal: Enable customers to build autonomous, zero-down-time networks and ICT systems

RESILIENCE ENGINEERING

CHALLENGE

Challenge:

- Increasing complexity in supply chains
- Digital transformations: Increasing use of digital assets, data etc
- Ongoing outsourcing of IT: from storage and hosting, to open-source, cloud, virtualization etc.
- Constant state of flux: technological progress, agile development and CI/CD (continuous integration / deployment)
- Remote access, and 'always on' concepts in IoT and IIoT

APPROACH

Approach:

Development line 1: Architecture & Design methods, and supporting tooling, that can deal with the high degree of complexity and dynamics of modern organizations and their IT infrastructures. This leads to, amongst others, complexity reduction and a traceable and explicit relationship between business objectives, stakeholders and their responsibilities.

Development line 2: Translating architecture concepts - which has previously been primarily a human process - into technology. The aim is to limit human effort and where possible to automate it.

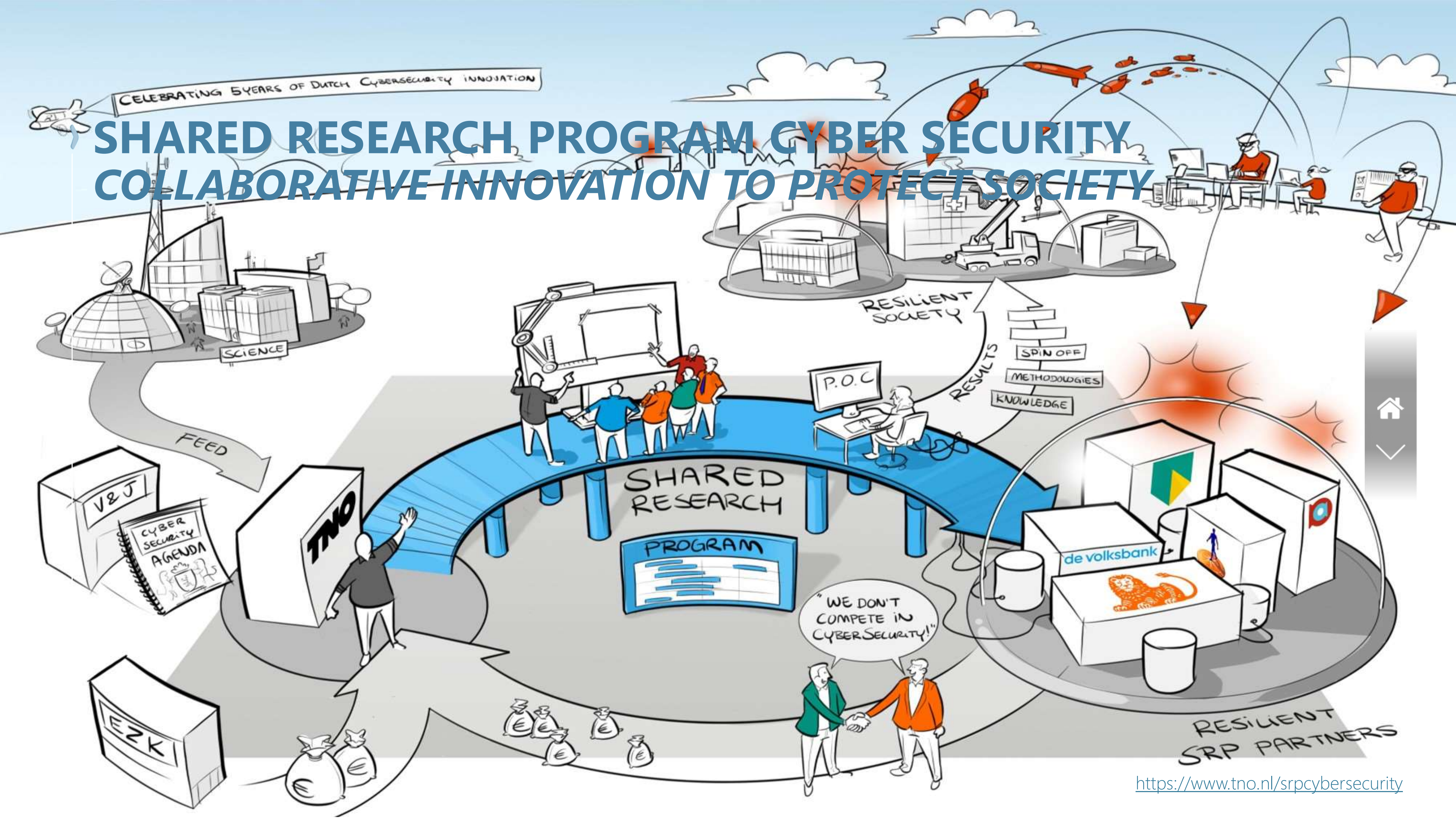
END GOAL

End goal: enable our clients and partners to build autonomous, zero-down-time networks and ICT systems.

To reach this goal we support our clients with:

- a clear and traceable design on decision making processes – manageable by a human being
- capability building to respond quickly to changes in business operations, IT infrastructures or attack vectors ('risk spectrum')
- Assignment of responsibilities (obligations) where each responsible entity is able to meet its obligations (eg complexity reduction, audit trail)
- Establishing a direct link between org. goals and its actual infrastructure and architecture (business-security alignment)

SHARED RESEARCH PROGRAM CYBER SECURITY
COLLABORATIVE INNOVATION TO PROTECT SOCIETY



https://www.tno.nl/srpcybersecurity

SRP CYBERSECURITY

CHALLENGE

- Increasing complexity and number of cyber attacks
- High dependency of financial services on ICT and communication
- Shortage of security skills
- Fast developing security landscape

APPROACH

- Cooperate between financial institutions and TNO to innovative on security solutions
- Share knowledge & resources between partners
- Feed back results to society
- Joint funding
  - Financial institutions
  - Government
- Successful since 2014

RESULTS

- New methods to improve detection of attacks based on anomaly detection, AI and machine learning
- Improved security architecture, utilizing a.o. full stack integrity and risk adaptive decision making
- CTI capability framework and Threat Landscaping model
- Method to measure cyber secure behaviour of employees

Innovating in Cyber Security
Shared research 2019
CELEBRATING 5 YEARS OF DUTCH CYBER SECURITY INNOVATION

PPS AUTOMATED SECURITY OPERATIONS

BRIDGING THE GAP BETWEEN DEFENDERS AND ATTACKERS

YouTube https://www.youtube.com/watch?v=oPYCODpaUb4

PPS AUTOMATED SECURITY OPERATIONS

CHALLENGE

- Advanced attacks are automated
  - Time to compromise a system is short (sec/min)
  - Time to discover a breach (weeks/months)
  - Actual containment breach (weeks)
- Complex & continuously evolving threat landscape (ICT infra)
  - IT, OT
  - blurring of boundaries of IT infrastructures
- Shortage of security personnel

APPROACH

- Reducing Mean Time to Detect and Mean Time to Respond in SOC and CSIRT operations by *automating* Security Operations.
- Combining strenghts and in depth views of each domain's need an an ecosystem consisting of :
  - R&D Institutes
  - Cyber Security Companies
  - IT/OT network appliers
  - Network partners
  - Educational institutes
- Creating a test environment for cybersecurtiy companies and students

RESULT

- Innovative prototypes in the field of monitoring, detection, analysis and response to (imminent) cyber attacks
  - Monitoring and detection techniques
  - Assessing the effective impact of upcoming incidents
  - Automated response, mitigating attacks through recommended Course of Actions
- Availability of market-ready innovations of automated security aiding the defenders developments
- Improving in getting the ICT specialists on the right jobs

TNO innovation for life

THANK YOU FOR YOUR ATTENTION

ANY QUESTIONS?