

REALISTIC GLOBAL CYBER ENVIRONMENT

RGCE and Solutions

Cyber Range for Improving Resilience

Realistic, advanced and isolated. Designed to meet the needs of organizations for improving competence and capabilities.

JYVSECTEC
by jamk

www.jyvsectec.fi

**RGCE and Solutions - Cyber Range for
Improving Resilience**

Version 2

Marko Vatanen, Jamk University of
Applied Sciences

Graphic design and layout: Heli Sutinen, Jamk

Images: Adobe Stock

© JYVSECTEC – Jyväskylä Security Technology,
2026, www.jyvsectec.fi

Printed by Grano

1

Realistic Global Cyber Environment..... 4

Full-Scale Cyber Security Exercises 5

Applications of RGCE 6

A Fully Functional RGCE Internet 7

Cyber Range Internet.....8

Realistic User Simulation and Network Activity 9

2

Threat-Driven Approach to Cyber Attacks 10

Cyber Exercises with JYVSECTEC 11

Realistic Digital Business Environments 12

Business sectors 15

3

RGCE Summary 20

Contacts.....21

1

Realistic Global Cyber Environment

JYVSECTEC's in-house developed cyber range, RGCE (Realistic Global Cyber Environment), is a live comprehensive digital world in an isolated private cloud. RGCE includes a representation of the global Internet with realistic business sector organization environments and global services.

RGCE has been developed to address the growing complexity of modern digital ecosystems, where organizations operate within interconnected networks and where cyber incidents can rapidly escalate beyond technical boundaries into operational and societal impact.



Full-Scale Cyber Security Exercises

RGCE cyber range enables full-scale cyber security exercises that include technical cyber attacks and process-based business decision-making in realistic scenarios. RGCE is also used in various research and development projects to develop new capabilities on cyber defense and using AI in cyber security. By providing a controlled yet highly realistic environment, the RGCE cyber range allows organizations to train,

test, and develop their capabilities without risk to production systems. It serves as a platform not only for training and exercises but also for research and development, enabling the exploration of new technologies, including the application of artificial intelligence in cyber security.



By leveraging RGCE for training and exercises, organizations are no longer restricted to small labs or red vs. blue exercises, which are not representative of the organization's environment and its typical business services, architectures, and technologies.

Applications of RGCE

The RGCE uses both commercial and open-source technologies to provide state-of-the-art training and exercises that immerse participants in realistic cyberattacks to train them on how to properly prepare for, respond to, and manage a broad variety of threats and incidents.

In addition to the underlying organizational environments and their associated technologies, RGCE provides comprehensive capabilities for **exercise management, control, reporting, and situational awareness.**

The cyber range also includes dedicated tools for incident response, threat intelligence, digital forensics, and communication, enabling participants to address and resolve large-scale cyber incidents in a coordinated manner.

Artificial Intelligence and large language models play a key role within the environment, supported by on-premises high-performance computing resources. These capabilities enhance both the realism of simulations and the development of advanced cyber security practices.



Incident Response



Threat Intelligence



Digital Forensics



Communication



RGCE cyber range includes dedicated tools enabling participants to address and resolve large-scale cyber incidents in a coordinated manner.

Offering of RGCE

- ▶ Realistic ready-made business-sector-specific organizational environments
- ▶ Capability for tailored organization environments
- ▶ Modern technologies, architectures, and tools for exercise and cyber defense
- ▶ Scalable and extensive environment for cyber security research and development
- ▶ Organization-focused training and development on handling cyber incidents
- ▶ Realistic threat actors with real cyber attacks
- ▶ Organizational data structures and content with end-user simulations

A Fully Functional RGCE Internet

One of RGCE's unique features is its global Internet and how it functions in the same manner as the real Internet, but it is fully controlled by JYVSECTEC. This enables usage of real domain names, IP addresses, and various technologies implemented in the real world. The internet core is a set of Autonomous Systems with BGP routed connectivity as in the real world, with real AS numbers, interconnections, and structures. All the functionalities are made as similar as possible to their real-world counterparts.

Examples of RGCE Internet Services

- ▶ 3-Tier model of multiple Internet Service Providers with fully functional BGP routing and realistic structure with public IP addresses
- ▶ Realistic Domain Name Service (DNS) architecture with root DNS servers, TLD servers, Authoritative name servers, and resolvers
- ▶ Global PKI Infrastructure and ACME support
- ▶ Global Time services
- ▶ Controlled update and software repositories for various operating systems
- ▶ Dark web TOR Onion network
- ▶ Cryptocurrency
- ▶ Malware analysis sandboxes

Cyber Range Internet

RGCE's Internet also has a wide variety of different public services for example news sites, social media, discussion forums, video and image sharing services, as well as instant messaging services. These services also include search engines, email services, and other cloud-based services which can be used during trainings and exercises.



Misinformation campaigns, hybrid operations, and crisis communications are vital parts of modern cyber exercises.

Realistic User Simulation and Network Activity

Automated user and traffic simulation is a key part of cyber ranges to provide realistic and versatile traffic and usage of services. Network traffic and user automation within RGCE is automatically generated using traffic and user generation software designed, developed, and maintained by JYVSECTEC. With the software it is possible to create large groups of legitimate users within the organization environments or to simulate external and “Internet users” which can be controlled from a centralized system.

The traffic and user generation software also provides capabilities to create botnets for performing network-based attacks (e.g. brute force attacks, flooding, port scanning, vulnerability scans, DDoS attacks) and other low-level attacks.



2

Threat-Driven Approach to Cyber Attacks

JYVSECTEC's mindset and approach to performing cyber-attacks is to simulate attack vectors and threat actors that are Threat-Driven with their Tactics, Techniques and Procedures (TTPs). RGCE supports techniques across the MITRE ATT&CK framework and the cyber kill chain and therefore enables realistic attacks at the technical level. The cyber attacks are not limited to gaining just footholds but can demonstrate the full impact of a threat actor's actions, motivations, and objectives. In RGCE we execute full-scale cyber attacks that replicate realistic threat actors and their methods.

Cyber Exercises with JYVSECTEC

With JYVSECTEC you can train in a variety of different types of cyber security scenarios. We design holistic exercises that start by creating background stories for the training audience. This provides the training audience with a proper understanding of the situation surrounding the exercise and immerses them in the scenario. This is done to ensure that the actual cyber security scenarios will demonstrate threats that line up with the storylines.

The scenario, including its events and injects, is designed with threat actors that pose realistic risks to an organization. The risks are realized by exploiting them with realistic vulnerabilities while

keeping the target audience and training objectives in mind. These activities are achieved by complex and thorough attack simulation by JYVSECTEC Red Team specialists. If the scenario requires it, all aspects of the cyber kill chain are included from the pre-compromise phase through the compromise and post-compromise phases with advanced attacker simulations that utilize complex command and control channels. This means that the attackers are doing all the following steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control and Actions on Objectives.

We simulate a multitude of different actors per scenario:

- ▶ Human errors
- ▶ Configuration errors
- ▶ Script-kiddie
- ▶ Insiders and disgruntled employees
- ▶ Criminals
- ▶ Hacktivists
- ▶ Activists
- ▶ Nation or State sponsored actors

Types of attack vectors and techniques simulated in RGCE:

- ▶ Various types of DDoS attacks
- ▶ Botnets
- ▶ Ransomware
- ▶ Phishing campaigns
- ▶ Watering holes
- ▶ Malware
- ▶ Defacements
- ▶ Steganography
- ▶ APT campaigns
- ▶ Viruses, worms, Trojan horses

Realistic Digital Business Environments

RGCE includes over 70 organizational environments that represent different business sectors and operational models. Each environment contains IT infrastructure, OT/ICS environments (when applicable), Business services, cyber security controls, and realistic architecture reflecting how organizations are structured and operated in practice. These technical environments for each organization contain its own IT infrastructure with Active Directory, DNS,

File sharing, Intranet, NTP, certificates, Windows Admin Center, and other enterprise-level services like Helpdesk, VPN, HR and documentation. Dedicated cyber security controls are also provided for each organization. These include SIEM (with proper logs from devices, workstations, servers, applications), Full-packet capture analysis, Endpoint Detection and Response systems, NGFWs, web proxy, and service monitoring.

Business sectors and operational environments include

- ▶ Commerce
- ▶ Critical infrastructure
- ▶ Energy
- ▶ Finance
- ▶ Internet Service Provider (ISP)
- ▶ Cloud Services Provider
- ▶ Logistics
- ▶ Software
- ▶ Healthcare
- ▶ Food Production
- ▶ Governmental and national organizations
- ▶ Security Operations Center (SOC)

Sector-Specific Digital Twins

A distinguishing feature of RGCE is the inclusion of sector-specific implementations that replicate the processes, dependencies, and critical functions unique to different industries. As digital ecosystems continue to grow in complexity and interconnection, achieving true cyber security preparedness requires more than theoretical knowledge. It requires practical experience in environments that reflect real-world conditions and challenges. RGCE has been developed to fully replicate these challenges that the new technologies bring to organizations.



One of the unique features is that we replicate business services precisely with our own developed software solutions. These custom-made systems, or so-called digital twins, and applications contain realistic generated data, transactions, and data flows between different systems. The replication is done as closely as possible to real-life counterparts.

MARKO VATANEN

Chief Technology Officer, JYVSECTEC



Industry Interdependencies & Multi-Sector Domain Approach

The RGCE organization environments have numerous interdependencies within the business sector. For example, the financial sector includes banking transactions, invoicing and SWIFT-connections represented and stock exchange processes with settlement services. There are also interdependencies

between different sectors, e.g. ISPs are providing connectivity services for multiple organizational sites or the financial sector provides payment services to organizations in other sectors. A multi-sector domain approach is an important part of RGCE to represent the real-world counterparts and their role in society.

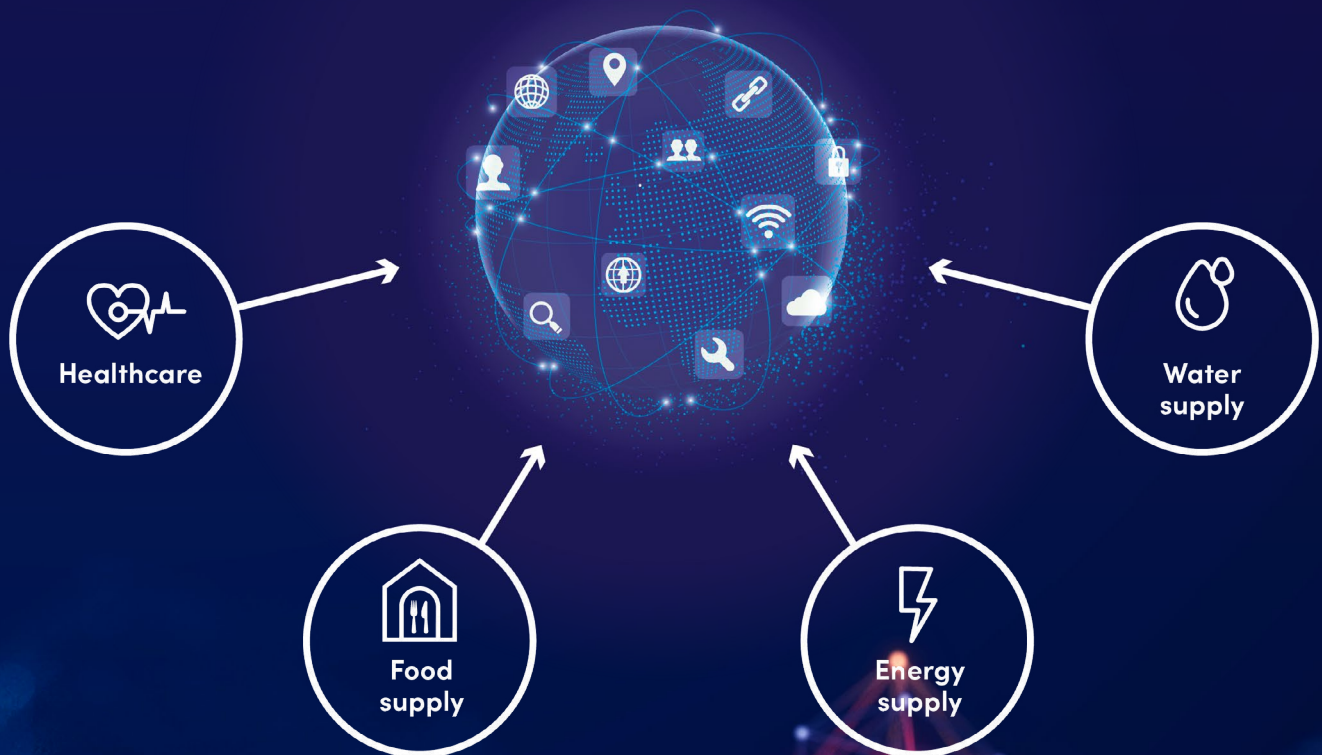


The interconnected nature of the sector environments is a central aspect of the RGCE. Organizations within the environment are not isolated islands but are linked through dependencies and shared services, reflecting real-world relationships between industries. This design allows cyber exercises to reveal how incidents can propagate across sectors, creating cascading effects that extend beyond individual organizations.

Business sectors

Realistic digital world replication requires authentic representations of operational business environments. RGCE organizations model a variety of business sectors through realistic implementations of business services, applications, and data. This high-fidelity approach supports comprehensive full-scale exercises while enabling

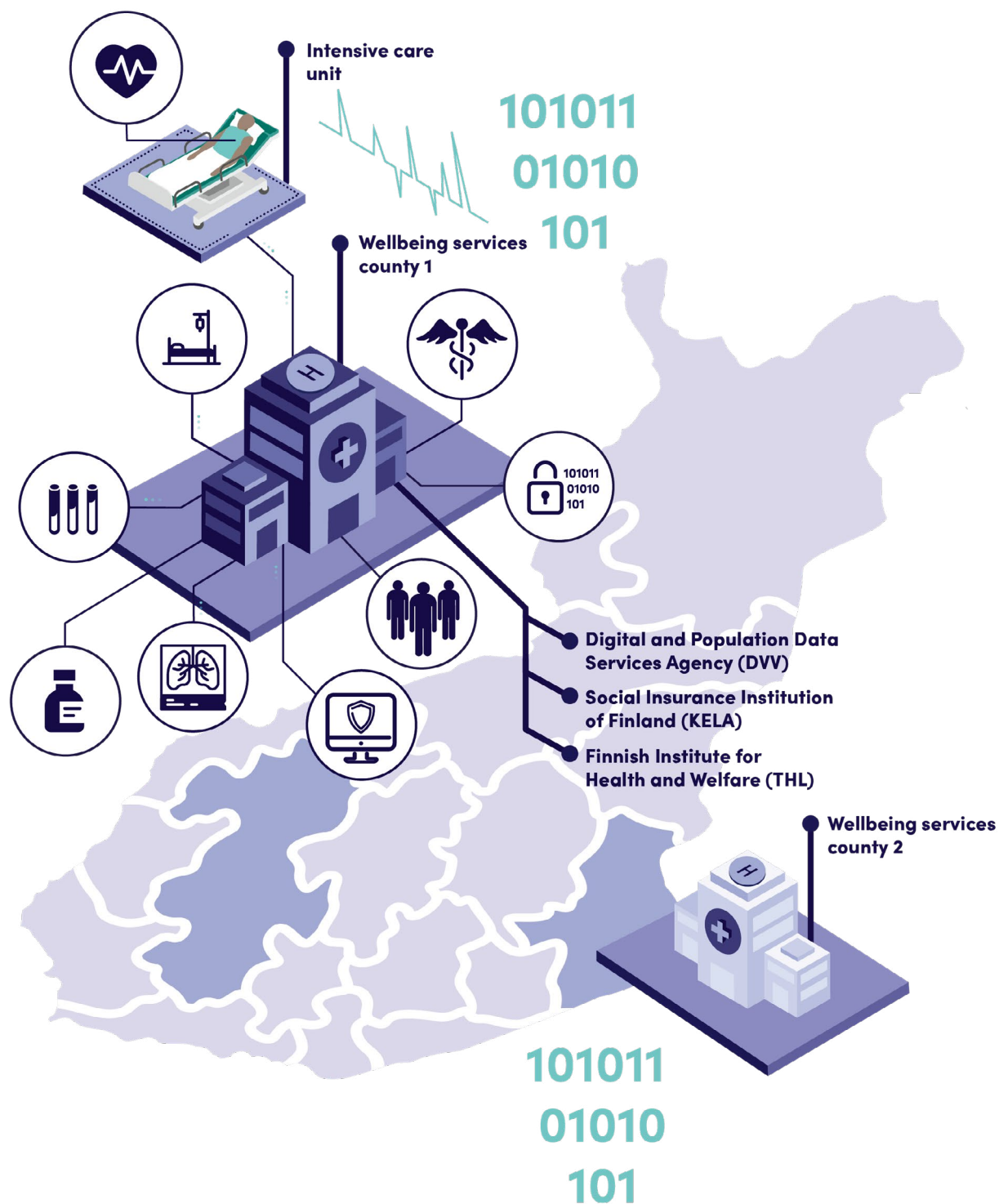
research and development of effective methods for securing and defending diverse organizational environments. The business sector portfolio is continuously expanded and enhanced through ongoing R&D activities and tailored to support evolving exercise, training, and research needs.



Healthcare

RGCE includes multiple hospital and healthcare district organizations with electronic health record systems, imaging systems, laboratory systems, patient monitoring, and intensive-care-unit systems to enable realistic impacts that cyber attacks could have on patient safety. Also, patient care is automated, so patients visit doctors, and they give prescriptions, referrals to tests and labs to generate realistic patient data.

All individuals, from patients to staff members, are generated by our in-house Stork system, which creates realistic background information for them (to RGCE). Major processes in hospitals with realistic data are automated, so patients see doctors, undergo laboratory and imaging tests, receive prescriptions, and obtain patient care.

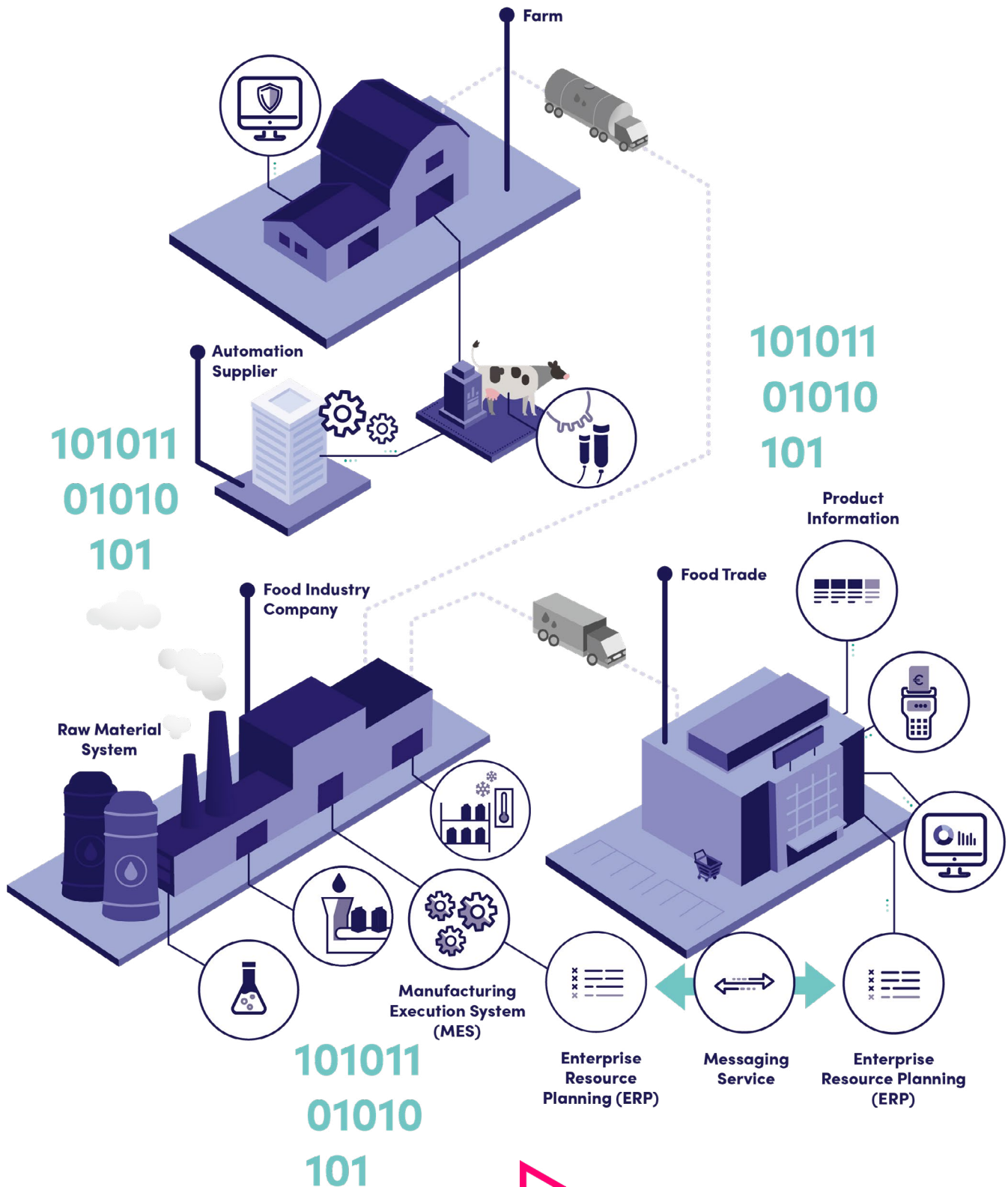


Healthcare replication with hospitals, national authorities and wellbeing services counties.

Food Supply

The RGCE environment includes a comprehensive replication of the entire food production value chain: smart farms and primary production, food processing and production facilities, logistics and distribution networks transporting goods to retailers, retail and sales channels delivering products to consumers.

The implementation is designed to reflect real-world complexity by incorporating: multiple types of resources and goods, realistic production processes and interdependencies between different actors and systems across the supply chain.



Food production value chain implementation including farms, production facilities, and commerce.

Logistics



The RGCE includes many different cargo transport organizations with enterprise resource planning systems, extranet ordering systems, electronic data interchange (EDI) systems and messages, warehouse management systems, traffic management systems, and other business-critical systems for truck transportation, harbours, airports, carriers, and shipping companies.

The logistics environment also includes a traffic simulator for managing transport routes and transport vehicles (trucks, airplanes, and ships) for logistics companies, so cargo is transported between locations from an import and export perspective. Each step of the logistics chain has been implemented in RGCE with realistic cargo containers, data, and tracking.

Finance and Insurance

Finance and insurance sector includes banks with core banking systems, web services for companies' invoice and payment data transfers and for receiving reconciliation data on incoming payments, as well as bank statements, SWIFT-network connectivity replication for SEPA transactions between banks, stock exchange connections and services, online banking services for customers. Finance sector includes also insurance companies for personal and corporate insurance, and pensions.

These organizations have core systems, customer handling systems, payment systems, and investment systems. Customer handling includes healthcare records and information that insurance company's staff handle. The Finance, payroll and HR services and accounting service providers are part of the implementation as they generate a large quantity of payment data between corporations.



Water Supply



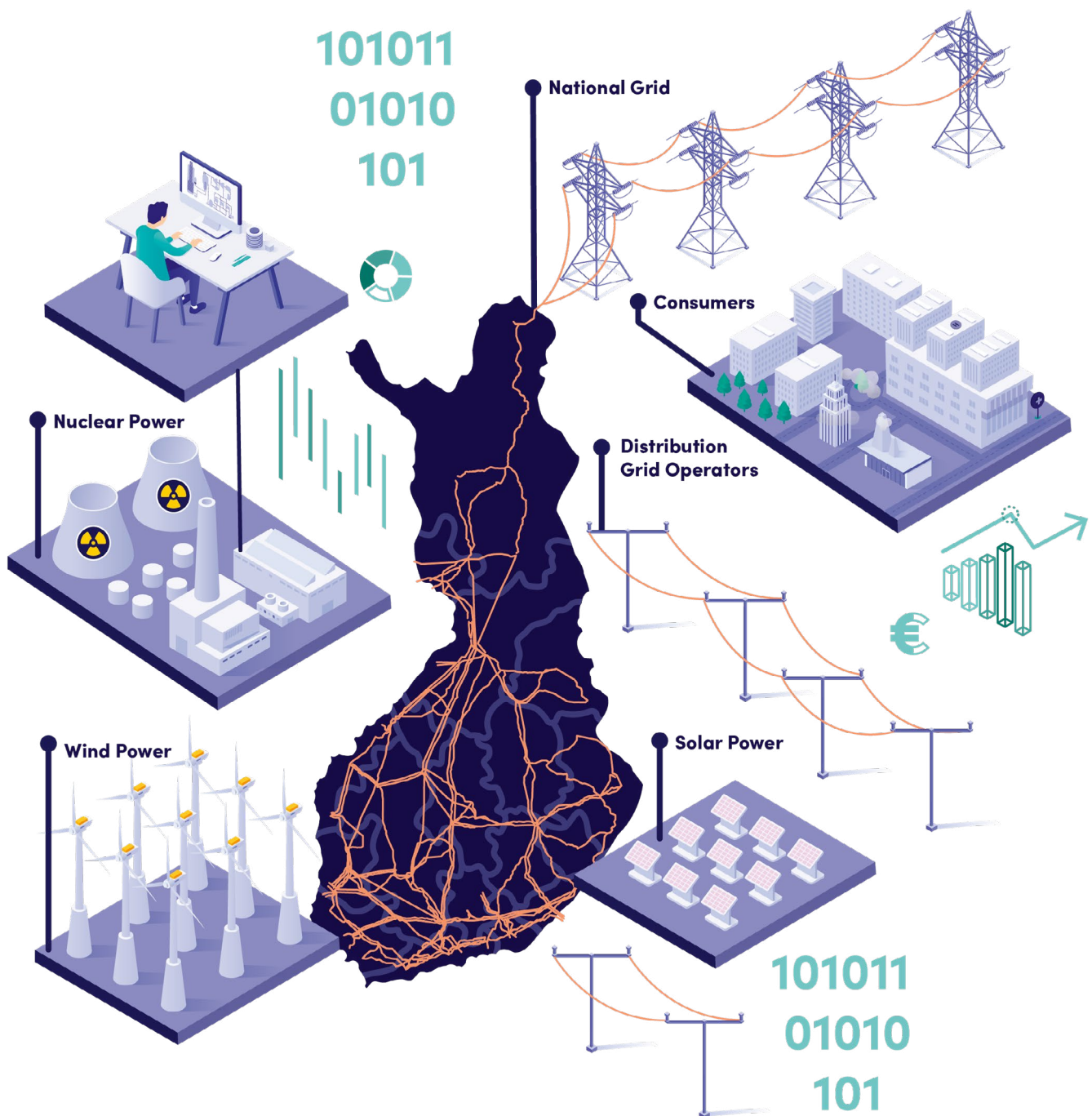
Clean water production, water distribution network, and wastewater treatment facilities are part of the RGCE critical infrastructure organization setup. Water organizations encompass OT environments and ICS systems replicating all water processes from clean water production to consumed water (i.e. wastewater) treatment. The implementation includes supporting systems and a comprehensive set of PLCs and SCADA systems.

Maintenance and telemetry services are a vital part of water treatment facilities to provide necessary information on the water processes.

Energy Supply

Energy sector contains various forms of electricity generation (i.e. nuclear, wind, solar, hydropower) operators, distribution network operators, national grid operator, and energy market including reserve markets. District heating solutions are also done as part of the energy sector implementation. District heating operators have power/heat plants, heating network, and customers replicated for city-

wide operations. Operational Technology (OT) environments and Industrial Control Systems (ICS) are critical elements in energy sector; therefore, we have replicated the OT processes for each actor in the sector with realistic systems and services. The OT implementation covers PLCs/RTUs, SCADA systems, process automation, and safety controls.



National level implementation of energy sector with National grid, Distribution System Operators, and various production environments.

3

RGCE Summary

Through a combination of realistic infrastructure, user behavior, threat simulation, and sector interdependencies, RGCE enables organizations to experience cyber security in its full operational context. Rather than focusing solely on technical response, participants gain insight into how cyber incidents influence business processes, decision-making, and organizational resilience. This holistic approach supports the development of capabilities that extend beyond technical defenses to include coordination, communication, and strategic response.

By providing a controlled yet highly realistic environment, the RGCE cyber range allows organizations to train, test, and develop their capabilities without risk to production systems. It serves as a platform not only for training and exercises but also for research and development, enabling the exploration of new technologies, including the application of artificial intelligence in cyber security.

In an increasingly complex and interconnected digital world, preparedness cannot be achieved through theory alone. RGCE offers a practical and immersive approach, allowing organizations to build the expertise and confidence required to operate effectively in challenging cyber scenarios and to strengthen their overall resilience against evolving threats.



Contacts



Marko Vatanen
Chief Technology Officer

+358405458630
firstname.lastname@jamk.fi



Jarno Lötjönen
Business Manager

+358406565240
firstname.lastname@jamk.fi

JYVSECTEC CYBER RANGE

Readiness Through Realism

Cyber resilience is built through experience, not theory. JYVSECTEC Cyber Range provides a realistic environment where organizations can train, test, and exercise their ability to respond to modern cyber threats. By replicating real-world Internet, organizations and their operational dependencies, and attack scenarios, the cyber range enables participants to strengthen both technical expertise and organizational resilience in a safe and controlled private cloud.

Developed through years of national-scale cyber security training and exercises, JYVSECTEC Cyber Range helps organizations improve incident response capabilities, enhance leadership decision-making, validate operational processes, and strengthen collaboration across teams, partners, and critical infrastructure sectors.

Whether preparing for emerging threats, validating cyber security investments, or building long-term resilience, JYVSECTEC Cyber Range transforms cyber security from a technical focus into an organizational capability.

Prepare for modern threats. Build Resilience.



About JYVSECTEC and solutions
www.jyvsectec.fi



Adding **resilience** to digital business

www.jyvsectec.fi

JYVSECTEC
by jamk



Contact:
jyvsectec@jamk.fi



Piippukatu 2,
40100 Jyväskylä



Follow us on
LinkedIn