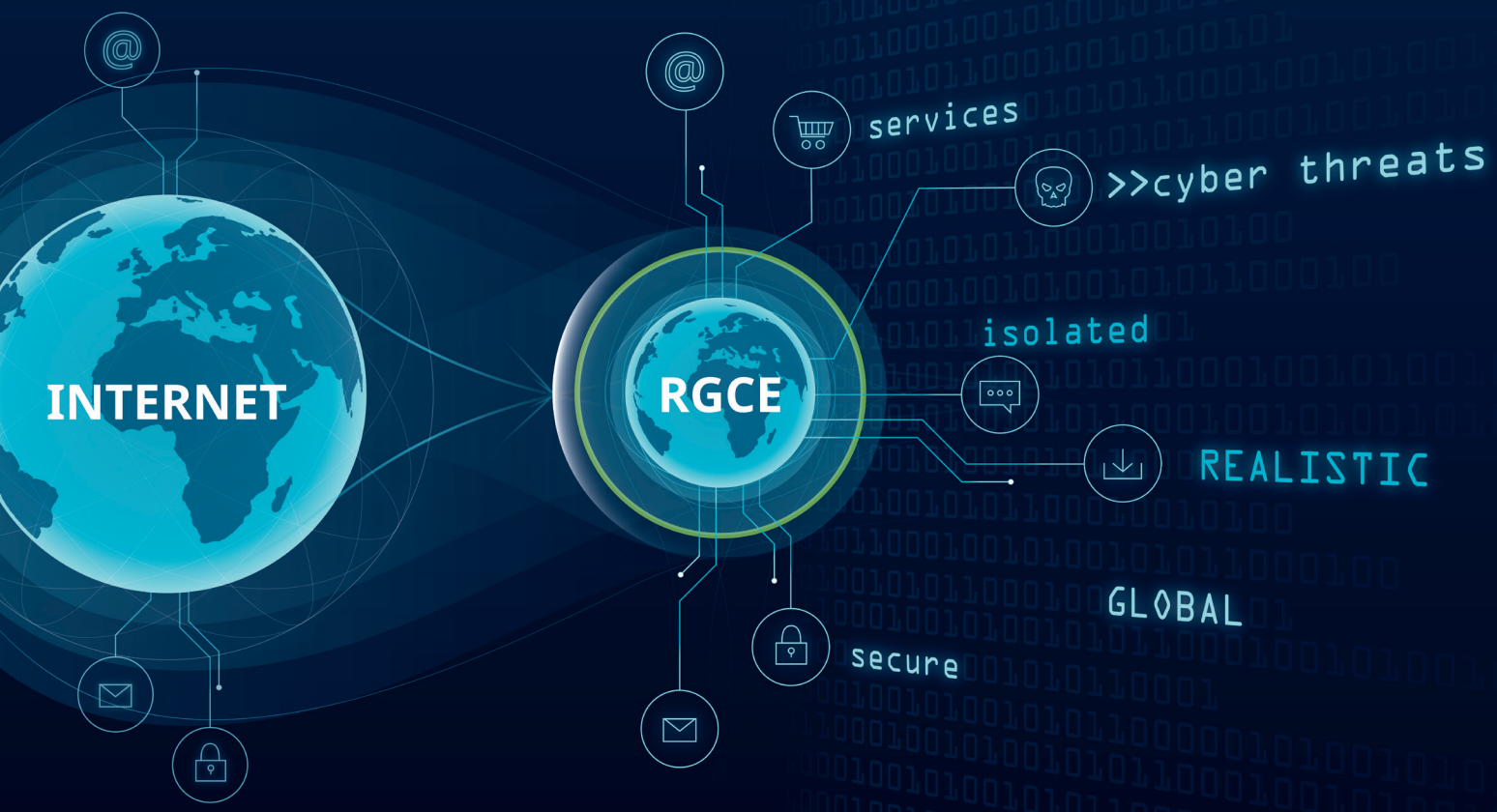



# JYVSECTEC CYBER RANGE

*RGCE and solutions*

# Realistic Global Cyber Environment

Realistic Global Cyber Environment (later RGCE) is a fully functional live cyber range. RGCE brings together a realistic global world and real organization environments in an isolated sandbox which utilizes modern ways to combine virtualization techniques, physical devices, and business specific systems. The cyber range provides realistic Internet, corporate environments, threat actors' attack campaigns, automated user simulation, and tools and technologies for training and exercise purposes as well as research and development. It is also possible to create tailored environments for organization's specific training, exercise, or research and development needs.

JYVSECTEC's cyber range uses commercial and open source technologies to provide state-of-the-art trainings and exercises that immerse people by realistic cyber attacks to train them on how properly prepare for, respond to, and manage a broad variety of threats. In addition to organization environments' tools and technologies, RGCE provides comprehensive platforms for exercise management, reporting, and situational awareness.

> *Usage of RGCE is made easy, you will access virtual machines in the environment through a web browser. This also makes sure that **your own workstations will not get infected or harmed** during trainings and exercises.*

Organizations can bring personnel from technical specialists to upper management, to train and exercise organization's capabilities on handling cyber incidents. RGCE also provides possibilities for organizations to train co-operation with their service providers and other third party organizations on handling cyber incidents. Using RGCE for training and exercises you are no longer restricted to small lab networks or to virtual environments that are not representative of your organization's environment and its' typical services, traffic, and usage.

## Benefits of using JYVSECTEC's cyber range

- Ready-made industry specific organization environments
- Capability for tailored organization environments
- Assessments of individual and team cyber security performance
- Individual training for cyber security and pen-testing operators
- Cyber security training for teams and organizations
- Digital Forensics and Incident Response trainings and exercises
- Process and procedures testing for real-time responses to cyber incidents
- Risk reduction for the introduction of new cyber security solutions into production environments

# RGCE's Internet

RGCE's global world functions the same way as the real Internet, but it is fully controlled by JYVSECTEC. This enables use of global threats e.g. BGP route hijacking and Distributed Denial of Service (DDoS) attacks. The Internet of RGCE has similar counterparts as the real Internet has and the structures, services, and functionalities are made as similar as it is possible.

### Examples of the services and features:

- **Tier I, II and III Internet Service providers with fully functional BGP routing and realistic structure with public IP addresses**
- **Realistic name service architecture including root DNS servers**
- **Global PKI Infrastructure for certificates**
- **Global Time services**
- **Controlled update and software repositories for various operating systems**
- **TOR Onion network**

*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.*

## User and traffic simulation

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

RGCE also uses commercial solution to provide certain applications and test patterns with Ixia's Breakingpoint solution.

# Threat-Driven approach to cyber attacks

With JYVSECTEC you can train in a variety of different types of cyber security scenarios. JYVSECTEC 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). JYVSECTEC designs 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 immerse them in the scenario. This is done in order to ensure that the actual cyber security scenarios will demonstrate threats that line up with the storylines.

Scenario with the events and injects are designed with threat actors that pose a 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.

If the scenario needs, it all aspects of cyber security kill chain are present from pre-compromise to compromise and post compromise phases with advanced APT 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 Objective.

## We simulate a multitude of different actors per the scenario and here are few examples:

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

## Examples of some of the different 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**

# Physical facilities

RGCE is connected to JYVSECTEC situation room with various display technologies, e.g. multi-touch displays, projectors, and televisions to control various image sources centrally using a control panel. The situation room is suitable for e.g. going through various technologies in the training, as a situation center in a cyber security exercise for the leaders or for studying and comparing various technologies.

> *The largest exercises have had more than 150 participants but also smaller (5-15 participants) exercises are held regularly.*

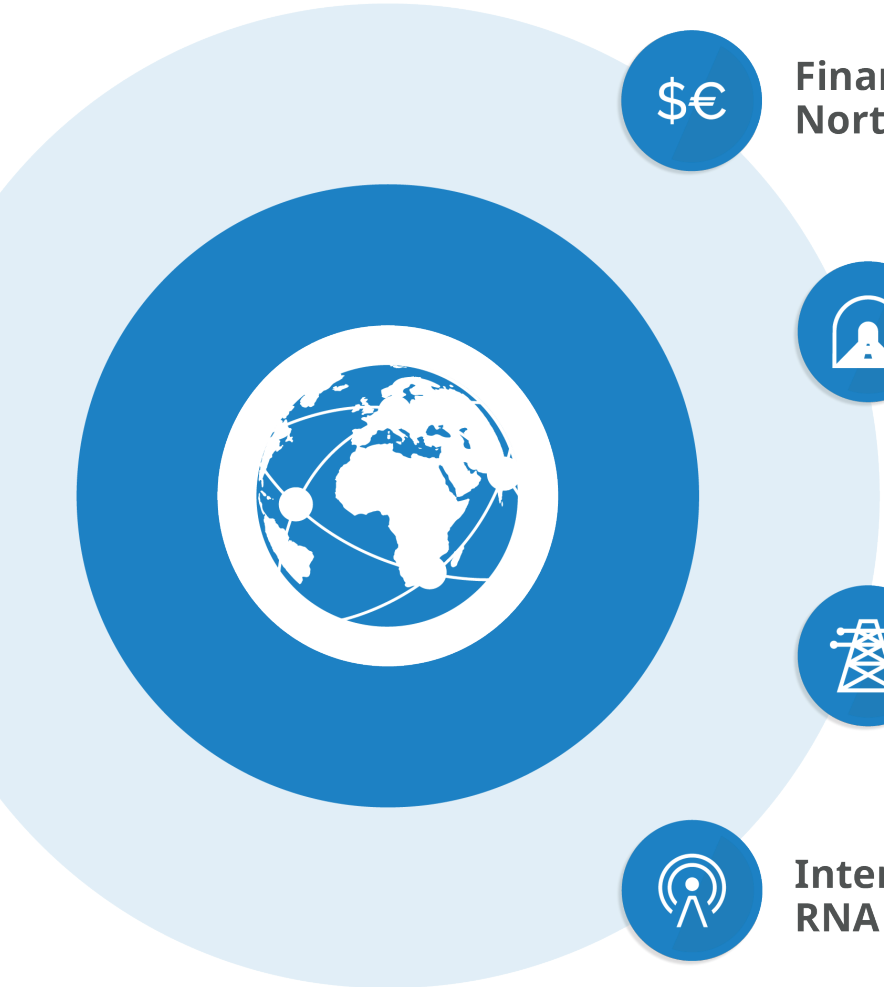
In addition to situation room, JYVSECTEC has multiple facilities for different organizations/teams usage in exercises. JYVSECTEC has capabilities to host large amount of participants in cyber exercises.


*JYVSECTEC's situation room*

# Industry specific organization environments

JYVSECTEC's cyber range also has many different industry specific organization environments. These currently include financial organization (NorthernBank), Internet Service Providers, Road tunnel provider (Funnel), and Electricity Company (Watti).

Industry specific organizations are comprehensive environments that represents certain field of business, their services, and technical environments (including also business specific systems not just IT devices/services).



**Financial organization NorthernBank**

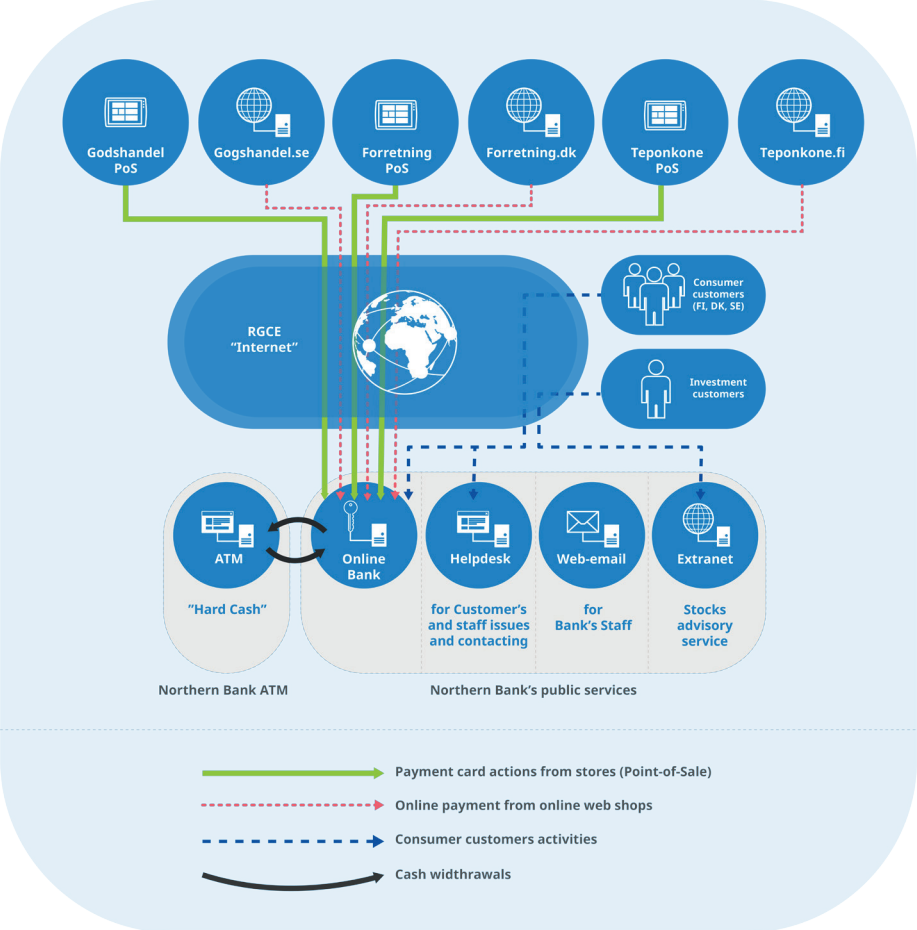
**Road tunnel provider Funnel**

**Electricity company Watti**

**Internet service provider RNA**

# Financial organization NorthernBank

NorthernBank is an independent nordic based banking company which provides online banking, loans, invoices, e-payments, point-of-sale systems, and cash services for corporations and private customers. NorthernBank's business services are illustrated in the following figure.




*NorthernBank overview*


*Online Bank*

Users of online web shops can pay their purchases via e-payment solution provided by NorthernBank for E-Commerce web shops.

NorthernBank maintains and operates its own IT infrastructure to provide the business services for customers including supporting services for IT management. NorthernBank has public and internal services, IT administration systems and tools, internal operational services, and backend banking services.

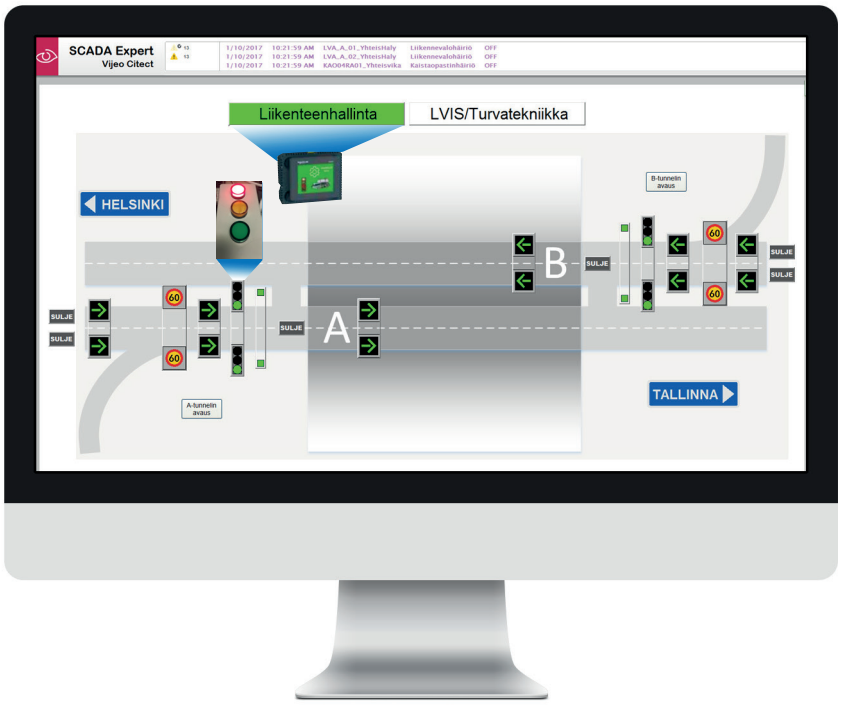
# Road tunnel provider Funnel

Funnel is a provider for Helsinki-Tallinn road tunnel which goes in the bottom of the Baltic Sea. Funnel maintains and operates the automation process for tunnel's traffic control systems and provides 24/7 monitoring for tunnel's systems. Funnel's main business is to provide SCADA-automation service, monitoring, and operation for field devices located in the tunnel.

Funnel's environment is divided to two different segments; office and other services, and automation services. The automation environment consists monitoring and engineering facilities, data center for Industrial Control Systems (ICS), ISP's connectivity (MPLS-VPN) to logic controllers (PLCs) which controls the field devices located in the tunnel, and CCTV monitoring system for traffic and field device monitoring.

Automation process is made with Schneider Electric's Vijeo Citect SCADA system, SCADA Client Server (for Human-machine-interface, HMI), SCADA Coms Server (for communication to PLC), and Schneider Electric's Programmable logic controllers (PLC). Protocols used in the automation are OPC, Schneider's proprietary protocols, and Modbus TCP.

Funnel's office environment includes corporate's workstations, internal and external services, and IT management systems and tools for office and automation environments.




*Funnel automation HMI*

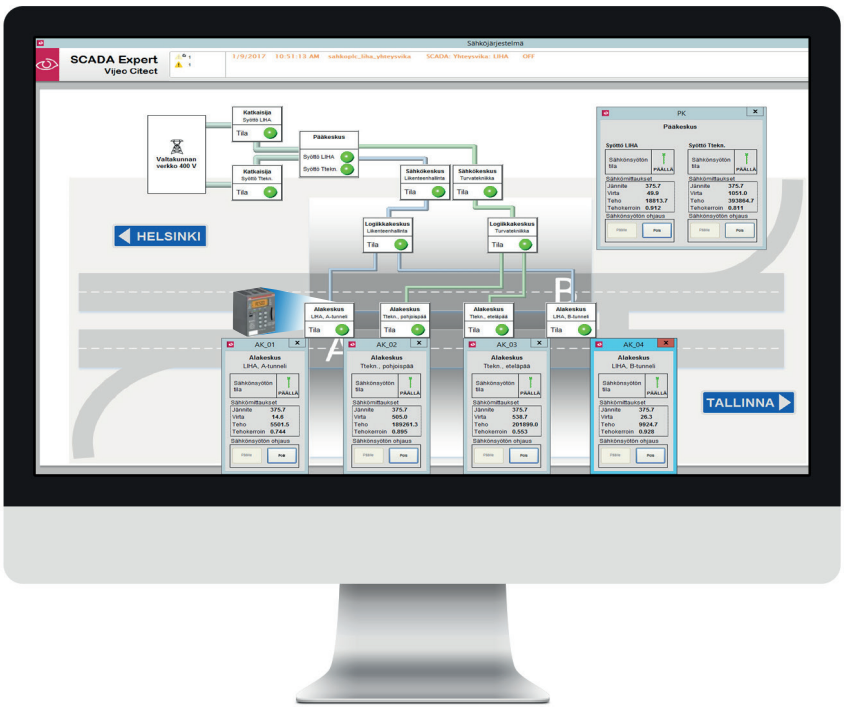
# Electricity Company Watti

Watti is an electricity provider for Funnel's road tunnel. Watti maintains and operates the automation process for tunnel's electricity systems and provides 24/7 monitoring for tunnel's electricity. Watti's main business is to provide SCADA-automation service, monitoring, and operation for electricity to PLCs and field devices located in the tunnel.

Watti's environment is divided to two different segments; office and other services, and automation services. The automation environment consists monitoring and engineering facilities, data center for Industrial Control Systems (ICS), ISP's connectivity (MPLS-VPN) to logic controllers (PLCs) which controls the field devices located in the tunnel, and CCTV monitoring system PLC device monitoring.

Automation process is made with Schneider Electric's Vijeo Citect SCADA system, SCADA Client Server (for Human-machine-interface, HMI), and ABB's Programmable logic controllers (PLC). Protocols used in the automation are OPC, Schneider's proprietary protocols, and IEC 60870-5-104.

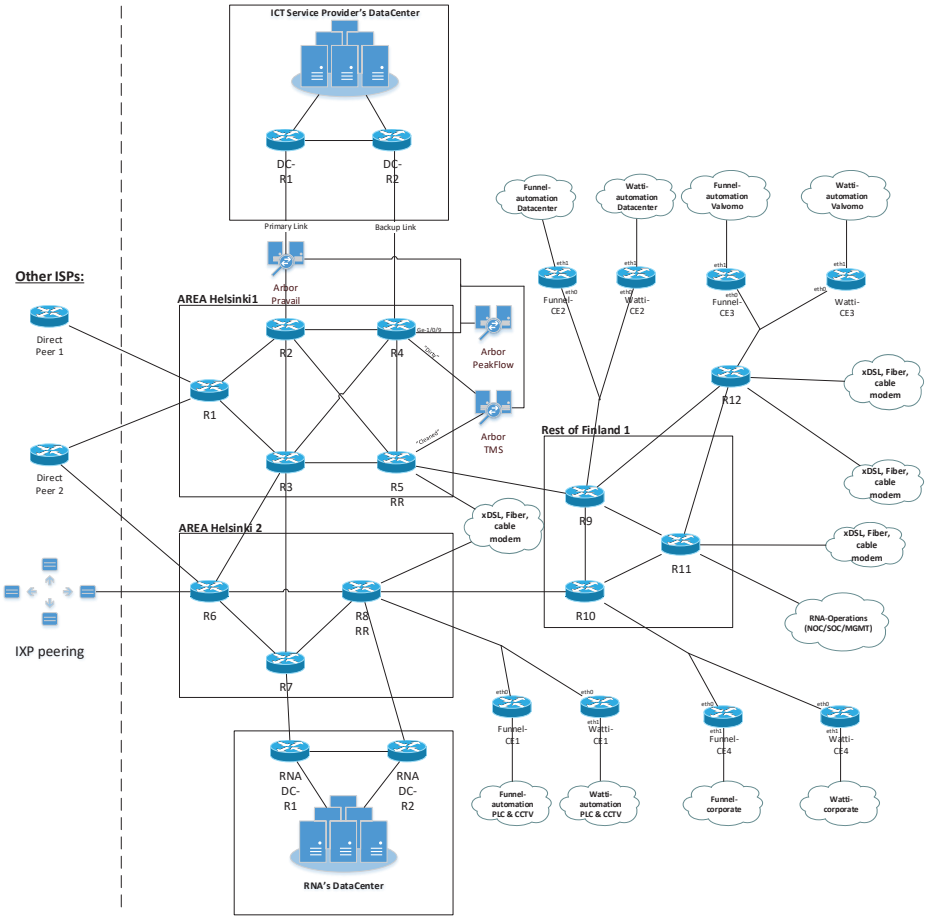
Watti's office environment includes corporate's workstations, internal and external services, and IT management for corporate and automation environments.




*Watti automation HMI*

# Internet Service Provider RNA

RNA is Finnish located Internet Service Provider which operates nationwide providing services for corporations and consumer customers. RNA's core network coverage is focused on larger cities but it has also loops to smaller regions in Finland. Core network provides connectivity services for corporations and consumer customer networks (xDSL, fiber, etc.). Traffic engineering and MPLS-VPN services are the basis for the corporate customers. Other services are offered case-by-case. Distributed Denial of service (DDoS) services are also offered to the largest customers with Arbor Networks Peakflow, TMS, and Pravail technologies.




*RNA's network*

RNA maintains and operates its own data center to provide infrastructure services, customer services, external services, and hosted services for customers. RNA control peerings to other upstream ISP providers and provides transit services for other Service Provider. RNA's own data center hosts infrastructure services, customer services, and hosting service.

Network and Security operations centers (NOC&SOC) are a vital solution that RNA has to maintain reliable and secure ISP services for customers. NOC&SOC utilizes modern technologies and processes to monitor and maintenance RNA's core and access networks, and Data Center services.

# Other environments

In addition to financial, ICS, and ISP environments, RGCE contains smaller environments like Software Defined Networking capable Internet Service Provider, retail&commerce environments, and ICT service and cloud providers.


*E-Commerce Teponkone.fi*

# Trainings and exercises

## Digital Forensics and Incident Response exercise

Digital Forensics and Incident Response exercise (DFIR) is an exercise for IT managers, Security manager, and technical specialist to train themselves on handling already happened cyber-attack.

### The scenario

The scenario used in the exercise involves a financial company NorthernBank, which provides banking services for Retail&Commerce Companies and consumer customers. NorthernBank's environment consists online banking services, E-payment service, ATM and credit card payment services, internal & external services, and IT management tools and services. In the scenario this bank has a suspicion of a potential breach occurred which needs to investigated by the trainees.

**Potential attacks may include the following (depends on the threat actor used for the exercise):**

- **Social Engineering**
- **Malware**
- **Ransomware**
- **Defacement**
- **Network based attacks**
- **Man-in-the-Middle attacks (MitM)**
- **Remote access Trojans (RAT)**
- **Antivirus bypassing**
- **Covert command and control channels**
- **APT campaigns**

**Participants will be casted on certain roles (total of 10 persons):**


Participants have wide variety of tools in use and they will operate as members of Incident response Team created by Bank. Members have access to the Bank IT infrastructure and services. These services include both commercial and open source solutions (e.g. Next-Generation Firewall (Paloalto Networks), Web application firewall (F5), log analysis tools, workstations maintenance and analysis, Centralized endpoint protection (F-Secure)). There are also many RGCE's globally available services to be used; malware analysis, multiple AV-scanners for detecting potentially harmful software etc.

***Duration: 2 days***
***Group size: 10 participants maximum***

# Industry sector exercise

Industry sector exercise is an exercise where participants are casted to either Funnel or Watti organization to control and defend industrial control systems (ICS) and office environments from various threats and risks.

Industry sector cyber security exercises allow organizations to demonstrate critical capabilities, thus exposing how efficiently they integrate their staff, processes, and technology to defend their information assets and cyber-reliant services. Cyber security exercises also enable organizations to experiment with new ideas and proposed capabilities.

> *Exercises can help educate organizations to strengthen their ability to mitigate impacts to business and national security objectives resulting from targeted cyber attacks. They can enhance existing efforts within an organization to protect their critical assets.*

When exercises include a hands-on component, they can take an organization into demonstrating their ability to protect, detect, and respond to various threats.

Conducting cyber security exercises can improve information and cyber security when combined with the skills to communicate problems and solutions in collaboration with others. The improvements can help an organization to improve normal operating processes and skills as well as train an organization to handle difficult circumstances that require decision-making under time pressure when significant values are at stake (such as material wealth and human life). Information and cyber security exercises complement regular preparedness and crisis management exercises and therefore are of great importance for organizations.

## The scenario

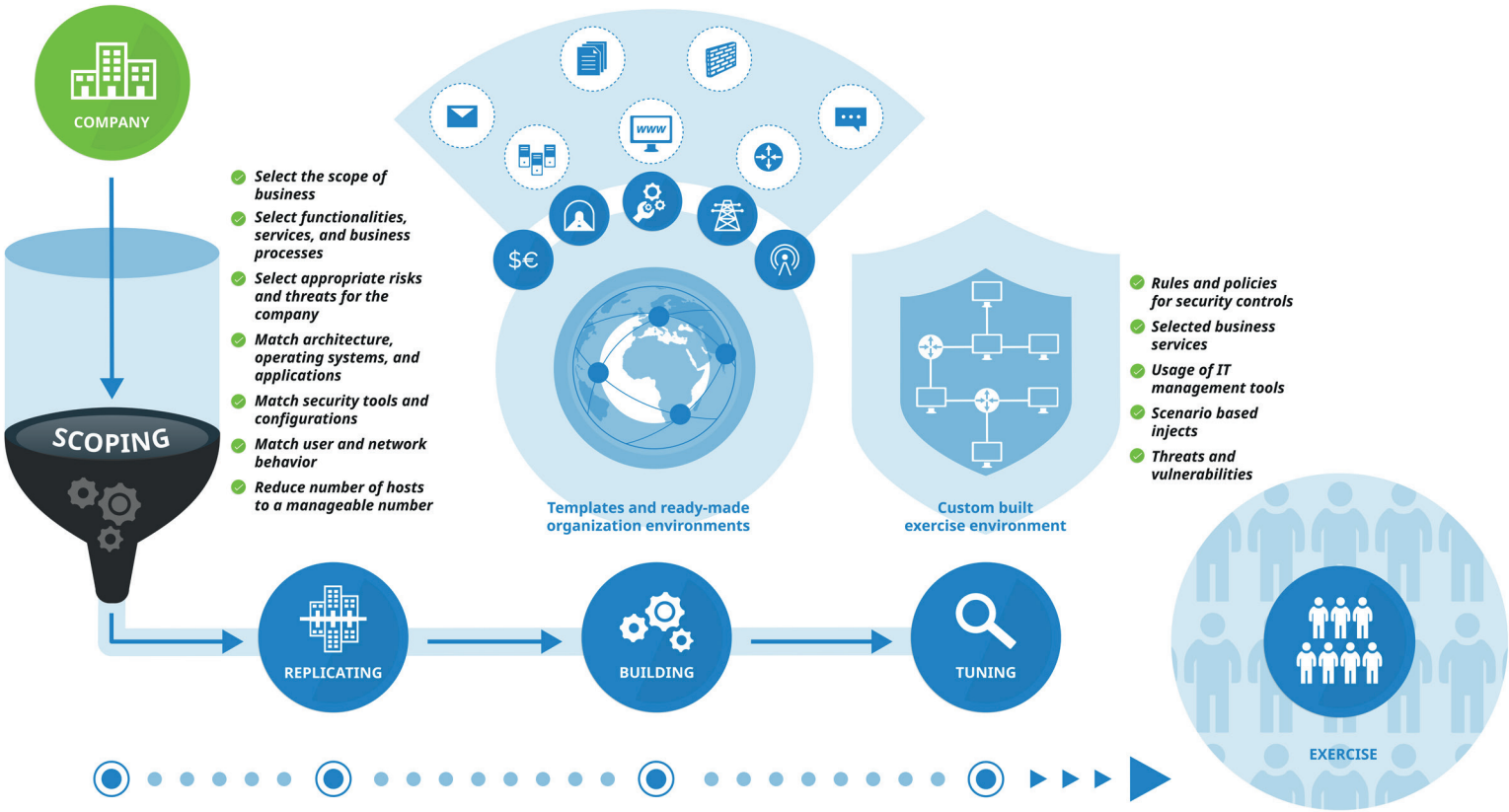
The brand new road tunnel between Helsinki (Finland) and Tallinn (Estonia) is about to open. The planning and preparations for tunnel started in early 2000s and it was reported to improve competitiveness of Finland and Estonia. The tunnel would bring the two metropolitan areas closer together which would open new possibilities for the countries and companies. Tunnel's construction started in 2011 and would be the longest tunnel in the world when it will be opened. The security situation in the area of the Baltic Sea has changed quite drastically from the beginning of the project. Environmental organizations have been always in opposition to the tunnel project and their actions have grown the closer the opening has come. Particularly Fresh Baltic Sea (FBS) organization have had strong campaigns against the tunnel. The exercise starts just a day before the grand opening.

***Duration: 2 to 3 days depending on the selected scale***

# Tailored cyber exercises for different organizations

It is also possible to create a tailored cyber exercise environment and exercise scenario for multiple organizations. This sort of activity demands thorough planning, preparation, and evaluation for creating custom environments and exercises. However, the scale and scoping of the tailored environment is done case-by-case and objective is to represent organization's most important networks, systems, business logic, and services for conducting live exercise.

This kind of tailoring is done as a part of the exercise planning and preparation phase. During the planning the scoping and selection of certain aspects of company is evaluated with the customer.



# Cyber security implementation in practice Training

Technical cyber security implementation in practice training contains a wide variety of commonly used technologies and methods to defend and protect ICT environments.

### Contents of the training include:

- **Threat actors' techniques, tactics, and procedures (TTPs)**
- **Technical attacking vectors**
- **Defending against malware**
- **Distributed Denial of Service attacks and defend methods**
- **User identification**
- **Network and server hardening**
- **Log and event management**
- **Intrusion Detection and Prevention systems**
- **Next Generation Firewalls**
- **Cryptography, encryption, and PKI**
- **Indicators of Compromise (IOC) and intelligence sharing**
- **Red Teaming and the role of the cyber exercises**

Participants will have lectures, live attack demonstrations, and practical examples followed by individual hands-on training scenarios.

***Duration: 3+3 days***
***Group size: 12 participants maximum***

# Essential Penetration testing tools

Participants will have lectures, live attack demonstrations, and practical examples followed by individual hands-on training scenarios. The idea of the training is to give attacker's point of view and deliver hands-on experience of running attacks.

### Contents of the training include:

- **Kali Linux**
- **Network scanning and enumeration (Nmap, etc.)**
- **Web application scanning and penetration (BurpSuite, OWASP_ZAP, Nikto, SQLMap, etc.)**
- **Vulnerability Scanners**
- **WLAN penetration testing**
- **Metasploit framework**
- **Cobalt Strike**
- **Other custom tools often used by attackers**

***Duration: 3 days***
***Group size: 15 participants maximum***

# Operative and Business management trainings

Cyber security management for business management course content includes cyber security terminology and perspective for need of the cyber strategy from the point of view of the business management. Participants will gain an understanding of cyber security entity frame and the tools to manage it. Participants will also be demonstrated the cyber domain and the threat actors, motives and possible threat vectors from the point of business continuity and disaster recovery. Tools of security management, risk management and continuity management will also be presented. Also the task of "How to build the organization´s security culture?" will be handled.

The operative management course includes also the introduction of overall frame of cyber security, but will also focus to the processes of the cyber security management as well as the aspects of the tools that company will have available. Processes will introduce the security incident handling process and the structure of security incident and the available standards of sharing the security information. There is also a possibility to tailor content such as Security Operations Center (SOC) and it´s working principles to the course.

Management training is also possible to combine with the Digital Forensics and Incident Response exercise.

***Duration: 1-2 days***
***Group size: 15 participants maximum***

# Tailored trainings for different organization needs

It is also possible to create a tailored trainings for organization needs to enhance organization resilience to modern threats and to understand the benefits of the new technologies.

# JYVSECTEC – Specializing in cyber security solutions

JYVSECTEC - Jyväskylä Security Technology is the leading independent cyber security research, development and training center in Finland. We operate under JAMK University of Applied Science's Institute of Information Technology which guarantees us a multidisciplinary network of experts at our disposal. Our areas of expertise include Cyber and Information security, Information Technology, Digital Business, and Industrial Internet.

We produce information and cyber security services for the private and public sector, as well as run R&D work in close co-operation with our partners. We specialize in organizing both small and large-scale cyber security exercises in our Cyber Range. In addition, we produce comprehensive training, consulting, accreditation, and certification services that advance our customers' information security level and support the professional development of their employees.

In R&D -activities we have strong expertise and practical experience on national and international. Our project portfolio includes multiple information and cyber security projects.

We have been working towards our mission since 2011. The starting point of our operations is inextricably linked to our first project. JYVSECTEC project was the factor that started a long-lasting development which is now known as an own brand.

## More information about us and our services

**Jarno Lötjönen**
*Business Manager*
+358 40 656 5240
firstname.lastname@jamk.fi

**Marko Vatanen**
*Chief Technology Officer*
+358 40 545 8630
firstname.lastname@jamk.fi

**Location**
JAMK University of Applied Sciences
Institute of Information Technology,
Piippukatu 2,
40100 Jyväskylä, Finland

**jyvsectec@jamk.fi**

www.jyvsectec.fi/en

PIRKANMAA

KESKI-SUOMEN LIITTO
Regional Council of Central Finland

Leverage from the EU 2014–2020

European Union
European Regional Development Fund