JYVSECTEC

Jyväskylä Security Technology

DEFEND YOUR NETWORKS.

www.jyvsectec.fi/en

JYVSECTEC
Jyväskylä Security Technology

jamk.fi
Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO
Regional Council of Central Finland

Leverage from
the EU
2014–2020

European Union
European Regional
Development Fund

Cyber Security Exercises for Energy Sector

Tero Kokkonen

+35850 438 5317
tero.kokkonen@jamk.fi

www.jyvsectec.fi/en

JYVSECTEC® Jyväskylä Security Technology

jamk.fi Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO Regional Council of Central Finland

Leverage from the EU 2014–2020

European Union European Regional Development Fund

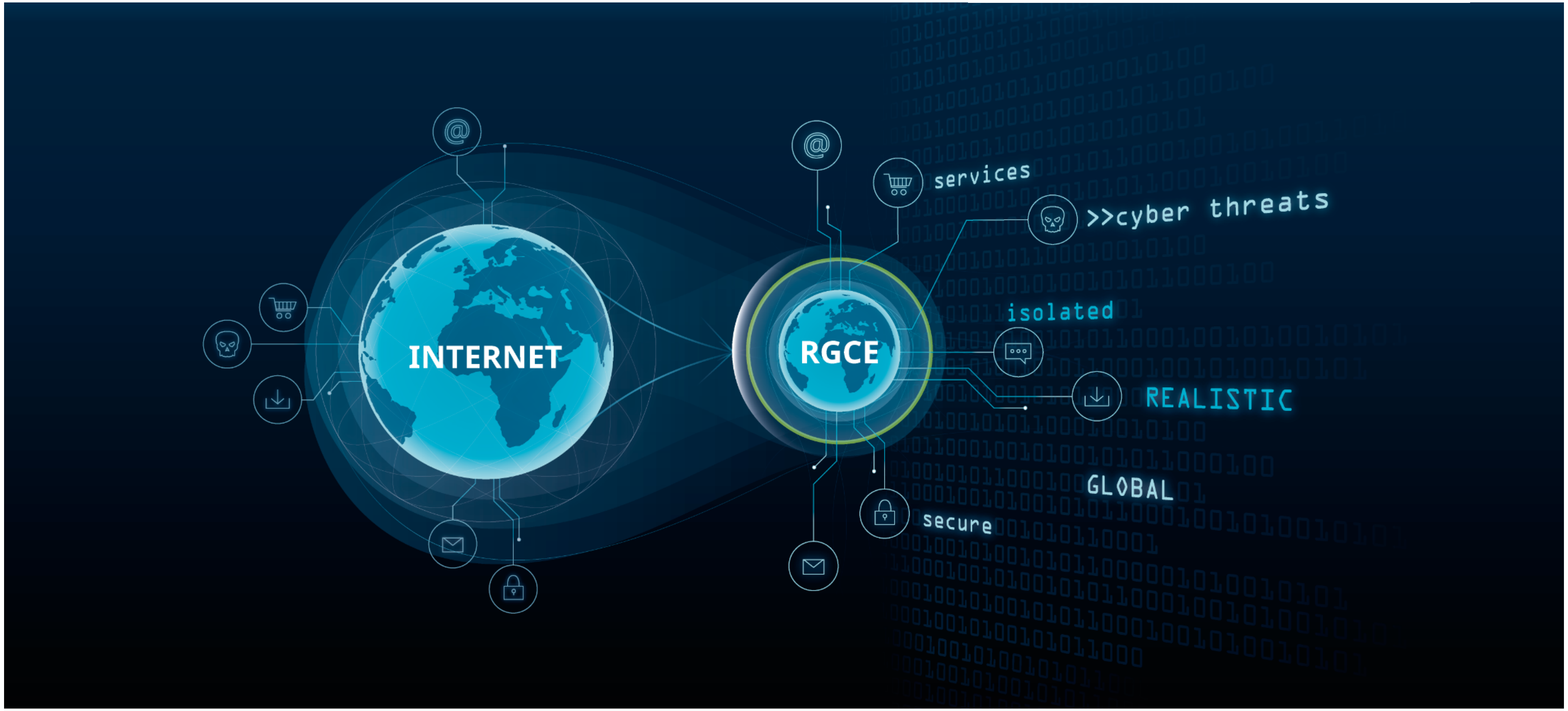
JYVSECTEC – Jyväskylä Security Technology

- JYVSECTEC - Jyväskylä Security Technology
  - Cyber security focused research, development and training center located in JAMK University of applied sciences, Institute of Information Technology
- Cyber Range: RGCE - Realistic Global Cyber Environment

www.jyvsectec.fi/en

RGCE

Realistic Global Cyber Environment



www.jyvsectec.fi/en

JYVSECTEC Jyväskylä Security Technology

jamk.fi Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO Regional Council of Central Finland

Leverage from the EU 2014–2020

European Union European Regional Development Fund

RGCE

Realistic Global Cyber Environment

Functions like the Internet

The environment has been modeled after the real structures and functionalities of the Internet starting from public IP addresses and geographical locations to the core services of the Internet (e.g. name services, update repositories, certificate infrastructure). Routing between Internet operators models operators functioning on various levels both globally, regionally and locally.

Isolated and controlled environment

RGCE offers a risk-free environment for use of attacks, known vulnerabilities and real malware. Considering that RGCE is isolated network environment it can be used without jeopardizing, compromising or contaminating real production environments, production networks or systems in production use.

Simulates real network traffic

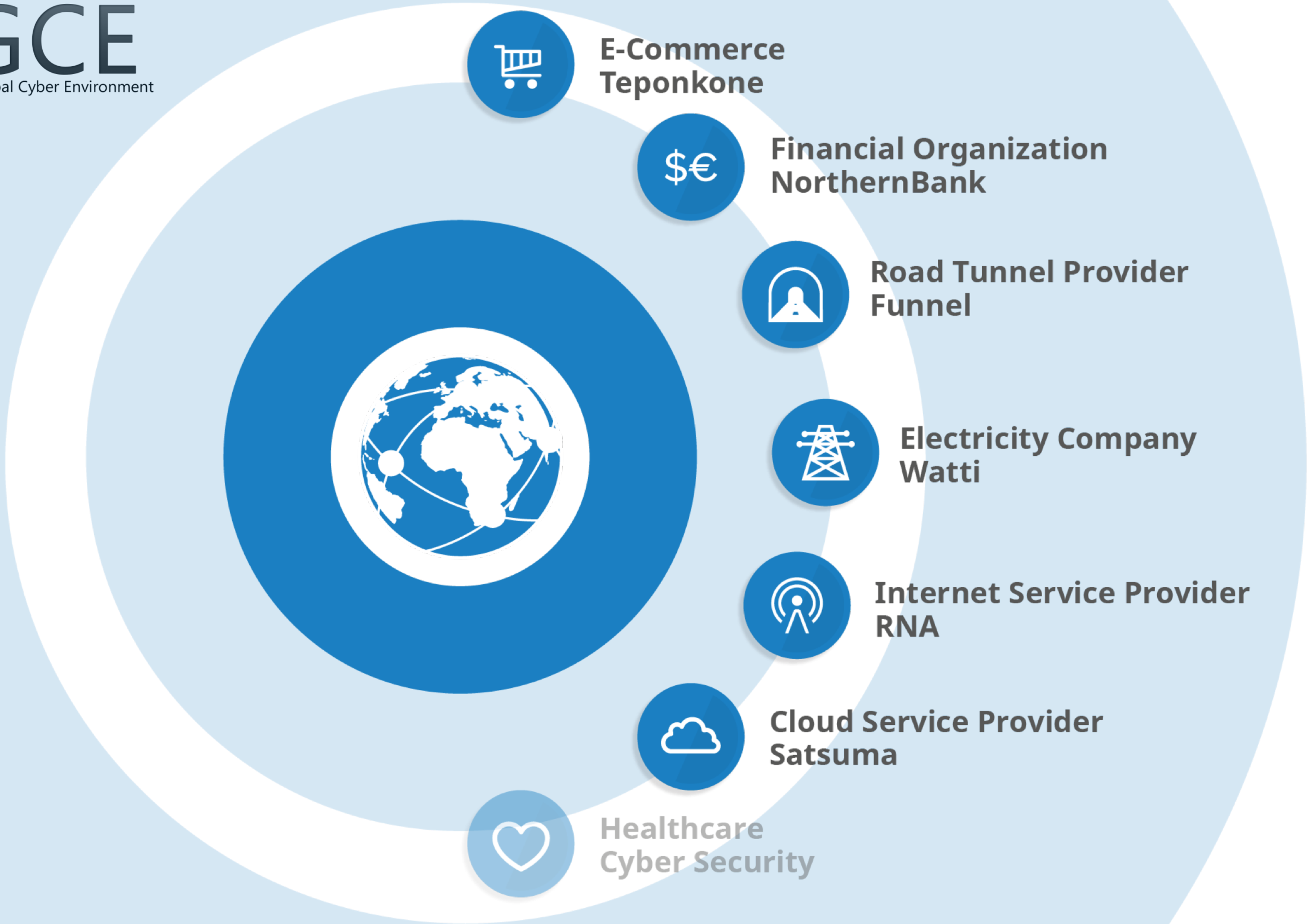
Network traffic within RGCE has been automatically generated using traffic generation software designed, developed and maintained by JYVSECTEC. Traffic generation software utilizes same functional principles as botnets. Bots are controlled by Web based User Interfaces and command servers for modeling realistic user behavior and end user traffic on the Internet. In addition, we also use commercial solutions to produce automated user and attack traffic in the environment.

Offers facilities of a normal organization environment

The structure of the RGCE environment enables the implementation of operator, data center, company and organization environments for training or exercise use. In realistic environments it is possible to model and test as well as evaluate the real threats, vulnerabilities and attack vectors they are faced.

www.jyvsectec.fi/en

RGCE
Realistic Global Cyber Environment



E-Commerce
Teponkone

Financial Organization
NorthernBank

Road Tunnel Provider
Funnel

Electricity Company
Watti

Internet Service Provider
RNA

Cloud Service Provider
Satsuma

Healthcare
Cyber Security

www.jyvsectec.fi/en

JYVSECTEC
Jyväskylä Security Technology

jamk.fi
Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO
Regional Council of Central Finland

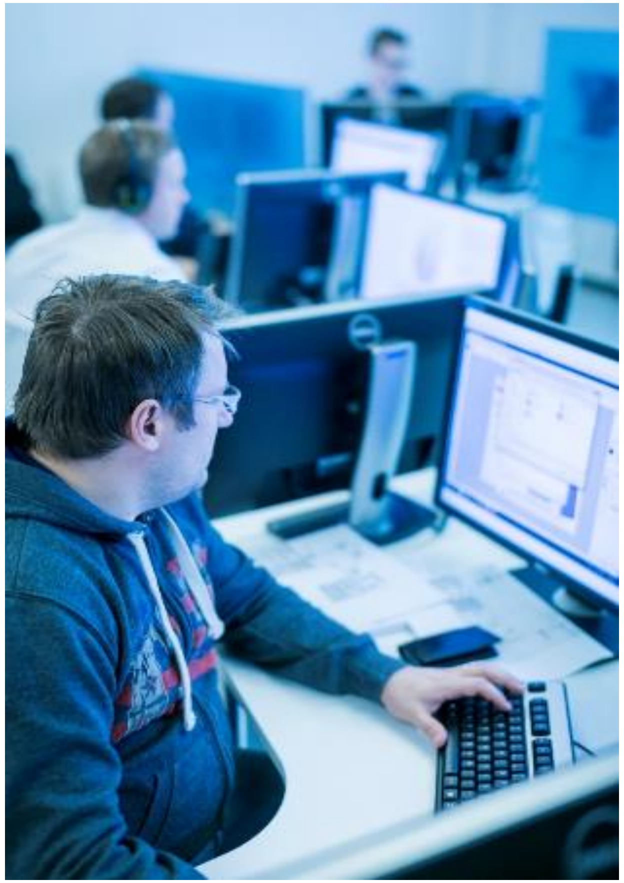
Leverage from
the EU
2014–2020

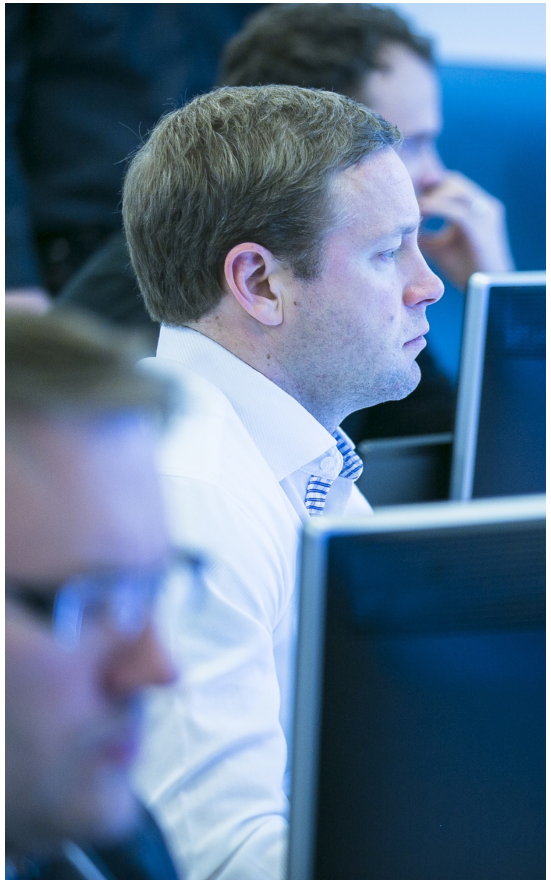
European Union
European Regional
Development Fund

Cyber Security Operation Room

www.jyvsectec.fi/en

Cyber Security Operation Room





www.jyvsectec.fi/en

JYVSECTEC®
Jyväskylä Security Technology

jamk.fi
Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO
Regional Council of Central Finland

Leverage from
the EU
2014–2020

European Union
European Regional
Development Fund

Implemented by two programs

- JYVSECTEC program 9/2011 – 01/2015 (2,9 M€)

Vipuvoimaa EU:lta 2007–2013 Euroopan unioni Euroopan aluekehitysrahasto AIRBUS DEFENCE & SPACE AJECO descom JYKES Relator

- JYVSECTEC Center and JYVSECTEC Center RGCE programs, 03/2015 - 04/2018 (2,1 M€)

Vipuvoimaa EU:lta 2014–2020 Euroopan unioni Euroopan aluekehitysrahasto AIRBUS elisa FINGRID Telia

www.jyvsectec.fi/en

Cyber Security Exercises

- Finland´s Cyber Security Strategy
  - ”The goal of exercises is to enhance the participants’ chances of exposing the vulnerabilities of their own actions and systems, in developing their capabilities and training their personnel.”
  - ”The key actors will improve their tolerance, including contingency planning and exercises, so as to be able to operate under cyber attacks.”

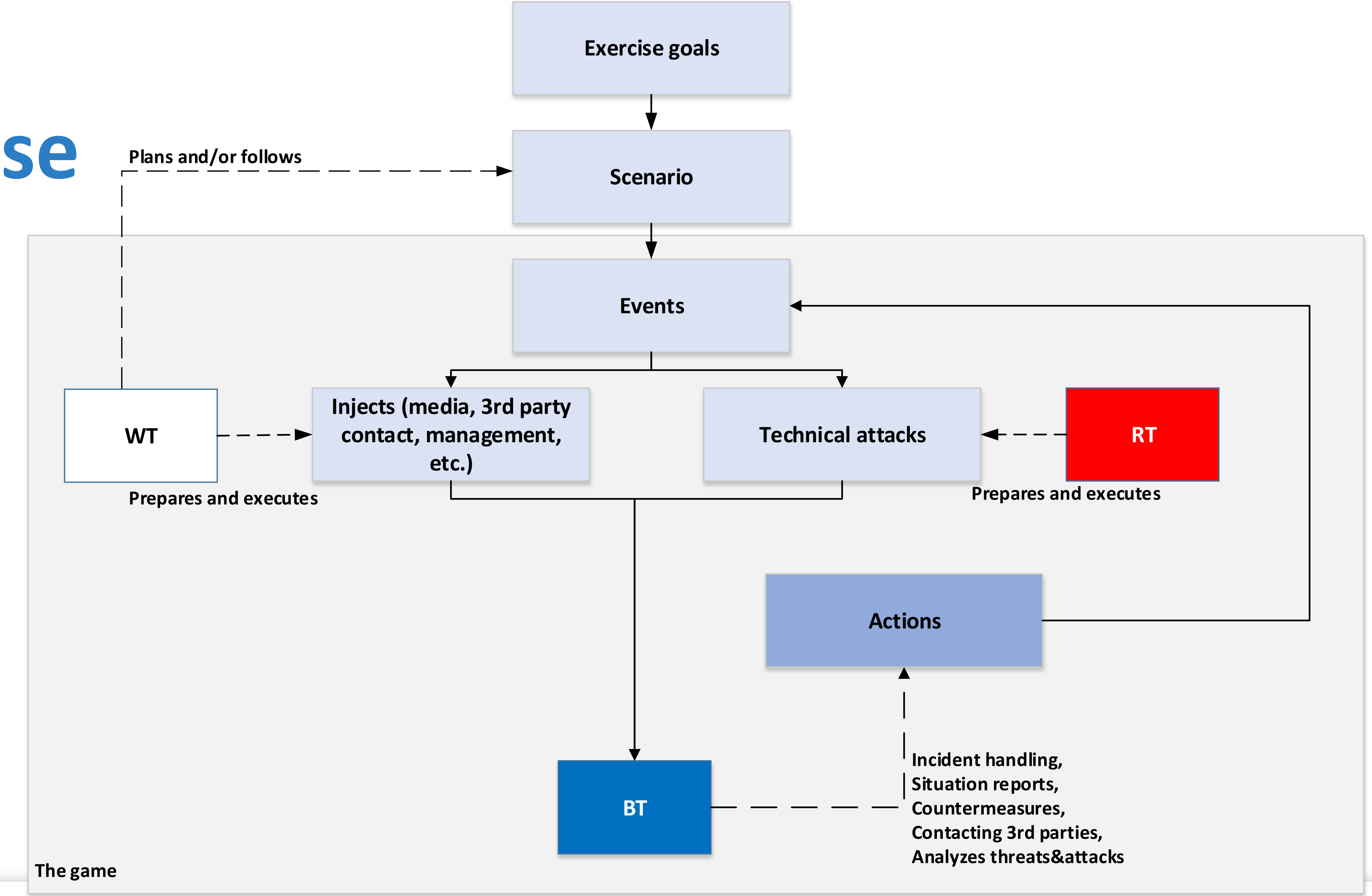
Exercises in RGCE Cyber Range

- Capabilities for tailored organization environments
- Ready-made industry specific organization environments
- Personnel from technical specialists to management and decision makers
- Co-operation with service providers and other third party organizations on handling cyber incidents
- Assessments of cyber security performance for individual and teams

Exercise Teams

- Blue Team is the group of people who are defending their information technology assets against cyber threat
  - Reporting the observations, creating their own situational awareness and maintaining own security posture under cyber-attack
  - Simulates the real organization and there can be one or many Blue Teams in the exercise
- Red Team is the group of people who are simulating the threat actors in the exercise
  - Executes the cyber-attacks against Blue Teams
- White Team is leading and controlling the exercise
- Green Team is maintaining the Cyber Range

Exercise



JYVSECTEC Jyväskylä Security Technology

jamk.fi Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO Regional Council of Central Finland

Leverage from the EU 2014–2020

European Union European Regional Development Fund

Industry Sector Cyber Security Exercise

- Participants are casted to either road tunnel provider (Funnel) or electricity company (Watti). They are controlling and defending industrial control systems (ICS) and office environments from various threats and risks.
- Example Scenario:
  - The road tunnel between Helsinki and Tallinn is about to open.
  - The security situation Baltic Sea area has changed quite drastically and environmental organizations are protesting the tunnel project. Particularly Fresh Baltic Sea (FBS) organization have had strong campaigns against the tunnel.
  - The exercise starts just a day before the grand opening.

DFIR, Digital Forensics and Incident Response exercise

- DFIR is an exercise for IT managers, Security managers, and technical specialists to train themselves on handling already happened cyber-attack.
- Scenario involves a financial company NorthernBank. In the scenario this bank has a suspicion of a potential breach occurred which needs to investigated by the trainees.
- Participants will operate as members of Incident response Team created by Bank and have access to the Bank IT infrastructure and services.
- Potential attacks: Social Engineering, Malware, Network based attacks, Man-in-the-Middle attacks (MitM), Remote access Trojans (RAT), Antivirus bypassing, Defacements, Ransomware, Covert command and control channels, Distributed Denial of Service (DDoS), APT campaigns…

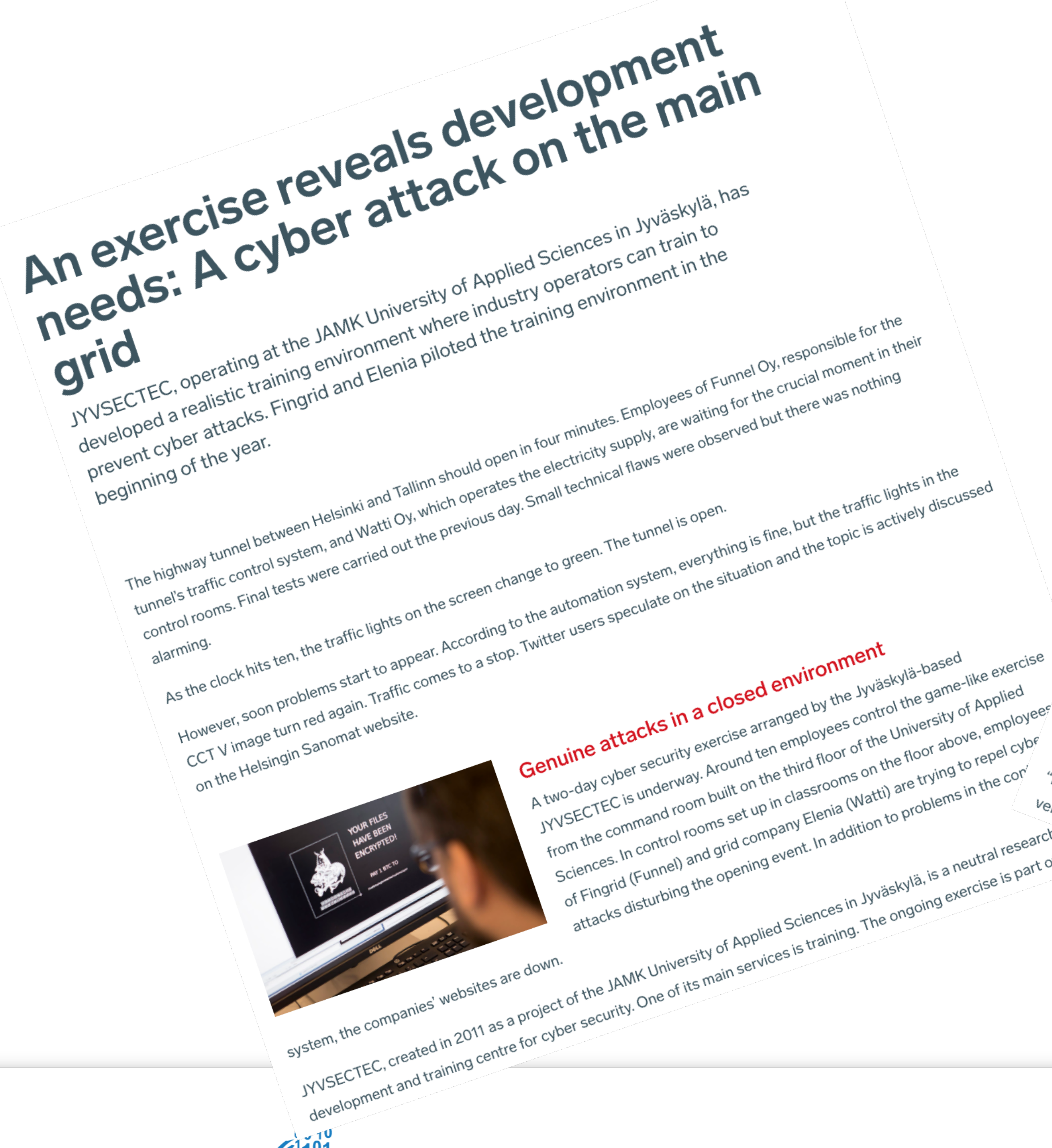
JYVSECTEC® Jyväskylä Security Technology
jamk.fi Institute of Information Technology
PIRKANMAA
KESKI-SUOMEN LIITTO Regional Council of Central Finland
Leverage from the EU 2014–2020
European Union European Regional Development Fund

Cyber Security Exercises, references

- National Cyber Security Exercises with Finnish Defence Forces and other national security authorities yearly since 2013
  - https://www.defmin.fi/ajankohtaista/tiedotteet/valtionhallinnon_viranomaiset_harjoittelevat_kyberosaamista_jyvaskylassa_8.-11.5.2017.8418.news
- Several Cyber Security Exercises with private companies
- Participating international Cyber Security Exercises (Locked Shields, Cyber Coalition)

Cyber Security Exercises for electricity companies

- Industry sector exercise, piloted with Fingrid and Elenia
  - https://www.fingridlehti.fi/en/exercise-reveals-development-needs-cyber-attack-main-grid/
- Continuation for pilot exercise with Fingrid and Helen
  - https://www.fingridlehti.fi/en/cyber-security-ensured-genuine-exercises/
- Electricity companies has tradition for training and exercises, but the exercises in realistic technical RGCE Cyber Range enables new and necessary features



An exercise reveals development needs: A cyber attack on the main grid

JYVSECTEC, operating at the JAMK University of Applied Sciences in Jyväskylä, has developed a realistic training environment where industry operators can train to prevent cyber attacks. Fingrid and Elenia piloted the training environment in the beginning of the year.

The highway tunnel between Helsinki and Tallinn should open in four minutes. Employees of Funnel Oy, responsible for the tunnel's traffic control system, and Watti Oy, which operates the electricity supply, are waiting for the crucial moment in their control rooms. Final tests were carried out the previous day. Small technical flaws were observed but there was nothing alarming.

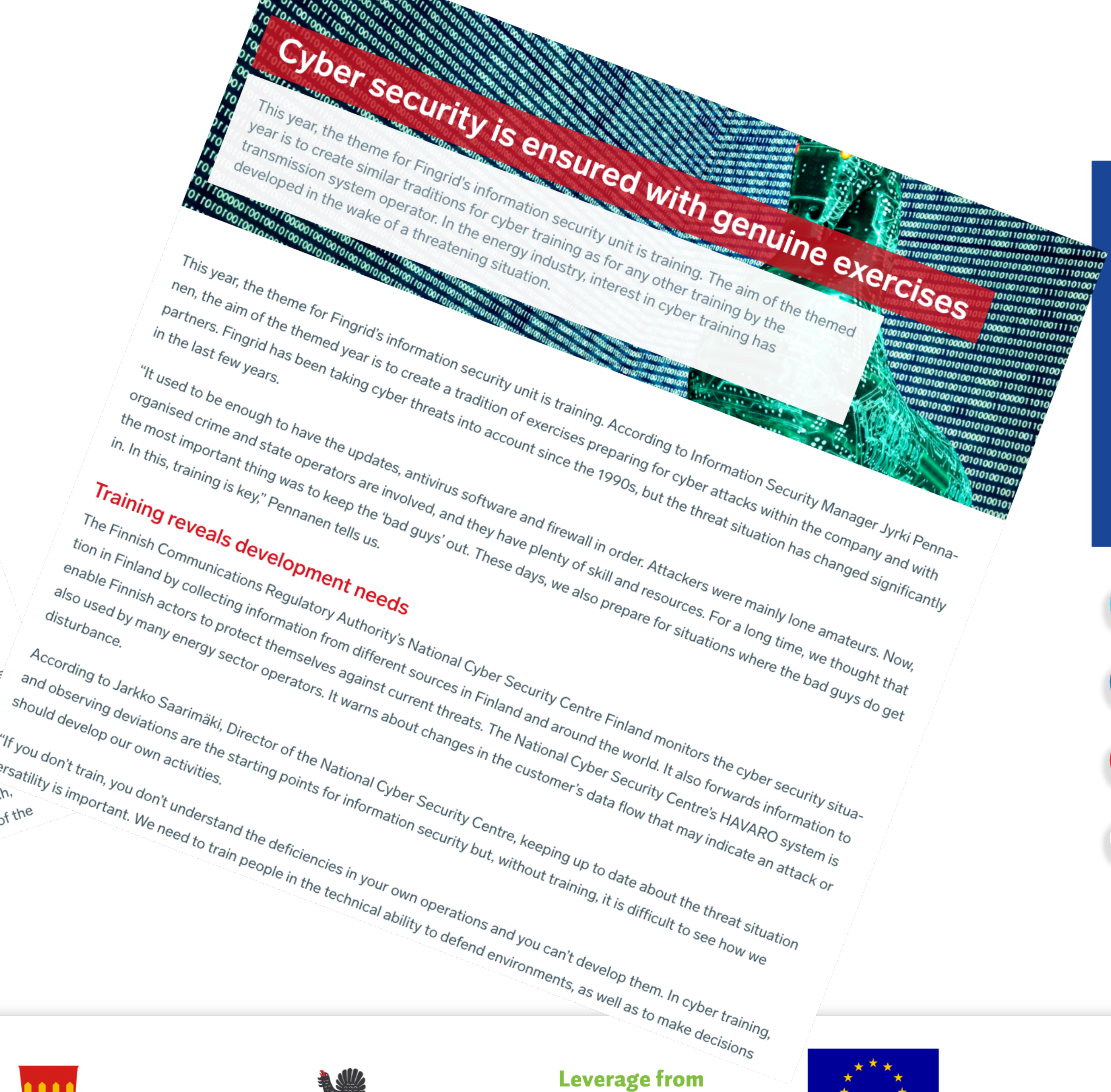
As the clock hits ten, the traffic lights on the screen change to green. The tunnel is open.

However, soon problems start to appear. According to the automation system, everything is fine, but the traffic lights in the CCT V image turn red again. Traffic comes to a stop. Twitter users speculate on the situation and the topic is actively discussed on the Helsingin Sanomat website.

Genuine attacks in a closed environment

A two-day cyber security exercise arranged by the Jyväskylä-based JYVSECTEC is underway. Around ten employees control the game-like exercise from the command room built on the third floor of the University of Applied Sciences. In control rooms set up in classrooms on the floor above, employees of Fingrid (Funnel) and grid company Elenia (Watti) are trying to repel cybe attacks disturbing the opening event. In addition to problems in the con system, the companies' websites are down.

JYVSECTEC, created in 2011 as a project of the JAMK University of Applied Sciences in Jyväskylä, is a neutral research, development and training centre for cyber security. One of its main services is training. The ongoing exercise is part of the



Cyber security is ensured with genuine exercises

This year, the theme for Fingrid's information security unit is training. The aim of the themed year is to create similar traditions for cyber training as for any other training by the transmission system operator. In the energy industry, interest in cyber training has developed in the wake of a threatening situation.

This year, the theme for Fingrid's information security unit is training. According to Information Security Manager Jyrki Pennanen, the aim of the themed year is to create a tradition of exercises preparing for cyber attacks within the company and with partners. Fingrid has been taking cyber threats into account since the 1990s, but the threat situation has changed significantly in the last few years.

"It used to be enough to have the updates, antivirus software and firewall in order. Attackers were mainly lone amateurs. Now, organised crime and state operators are involved, and they have plenty of skill and resources. For a long time, we thought that the most important thing was to keep the 'bad guys' out. These days, we also prepare for situations where the bad guys do get in. In this, training is key," Pennanen tells us.

Training reveals development needs

The Finnish Communications Regulatory Authority's National Cyber Security Centre Finland monitors the cyber security situation in Finland by collecting information from different sources in Finland and around the world. It also forwards information to enable Finnish actors to protect themselves against current threats. The National Cyber Security Centre's HAVARO system is also used by many energy sector operators. It warns about changes in the customer's data flow that may indicate an attack or disturbance.

According to Jarkko Saarimäki, Director of the National Cyber Security Centre, keeping up to date about the threat situation and observing deviations are the starting points for information security but, without training, it is difficult to see how we should develop our own activities.

"If you don't train, you don't understand the deficiencies in your own operations and you can't develop them. In cyber training, versatility is important. We need to train people in the technical ability to defend environments, as well as to make decisions

www.jyvsectec.fi/en

Ministry of Defence

- JAMK University Of Applied Science and Ministry of Defence have signed co-operation agreement about development of national Cyber Security

Puolustusministeriö
Försvarsministeriet
Ministry of Defence

ECSO

- ECSO – European Cyber Security Organisation
- JAMK University of Applied Sciences is one of the charter members of the ECSO
- https://www.ecs-org.eu/press-releases/ecso-ec-contract-signature

www.jyvsectec.fi/en

How to reach us

tero.kokkonen@jamk.fi

www.jamk.fi/en

www.jyvsectec.fi/en

Follow us on
Twitter @JYVSECTEC,
LinkedIn and YouTube

www.jyvsectec.fi/en

JYVSECTEC
Jyväskylä Security Technology

jamk.fi
Institute of Information Technology

PIRKANMAA

KESKI-SUOMEN LIITTO
Regional Council of Central Finland

Leverage from
the EU
2014–2020

European Union
European Regional
Development Fund