

# Welcome to the Webinar: Critical Infrastructure Protection

*Current Cyber Threat Landscape and Japan-Netherlands Collaboration*

# Joris den Bruinen

General Director The Hague  
Security Delta

# Table of contents

- 10:00 - 10:05 Introduction
- 10:05 - 10:15 Welcome by Ambassador
- 10:15 - 10:30 Threat landscape in Japan
- 10:30 - 10:45 Threat landscape in Europe
- 10:45 - 11:00 New technology in the threat landscape
- 11:00 - 11:15 Example of NL-JP collaboration
- 11:15 - 11:20 Q&A and wrap up

# Peter van der Vliet

## Ambassador of The Netherlands in Japan

# Hiroshi Sasaki

Senior Security Advisor  
McAfee

Security Research Expert,  
Cyber Tech. Lab, ICSCoE

# Cyber threat landscape of Critical Infrastructure and Manufacturing sector in Japan

- Cyber strategy initiative office, McAfee Co., Ltd.
- Cyber Tech. Lab, ICSCoE (Industrial Cyber Security Center of Excellence)

**Hiroshi Sasaki, CISSP**



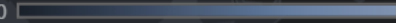
# ICE Break

## COVID-19 related Cyber threat landscape

COVID-19 campaigns typically use pandemic-related subjects including testing, treatments, cures, and remote-work topics to lure targets into clicking on a malicious link, download a file, or view a PDF.

<https://www.mcafee.com/enterprise/en-us/lp/covid-19-dashboard.html>

# COVID-19 Related Malicious File Detections

0  157K

Jan 2 to Jun 16, 2020



Total Malicious Detections

538,083

Total Unique Hashes

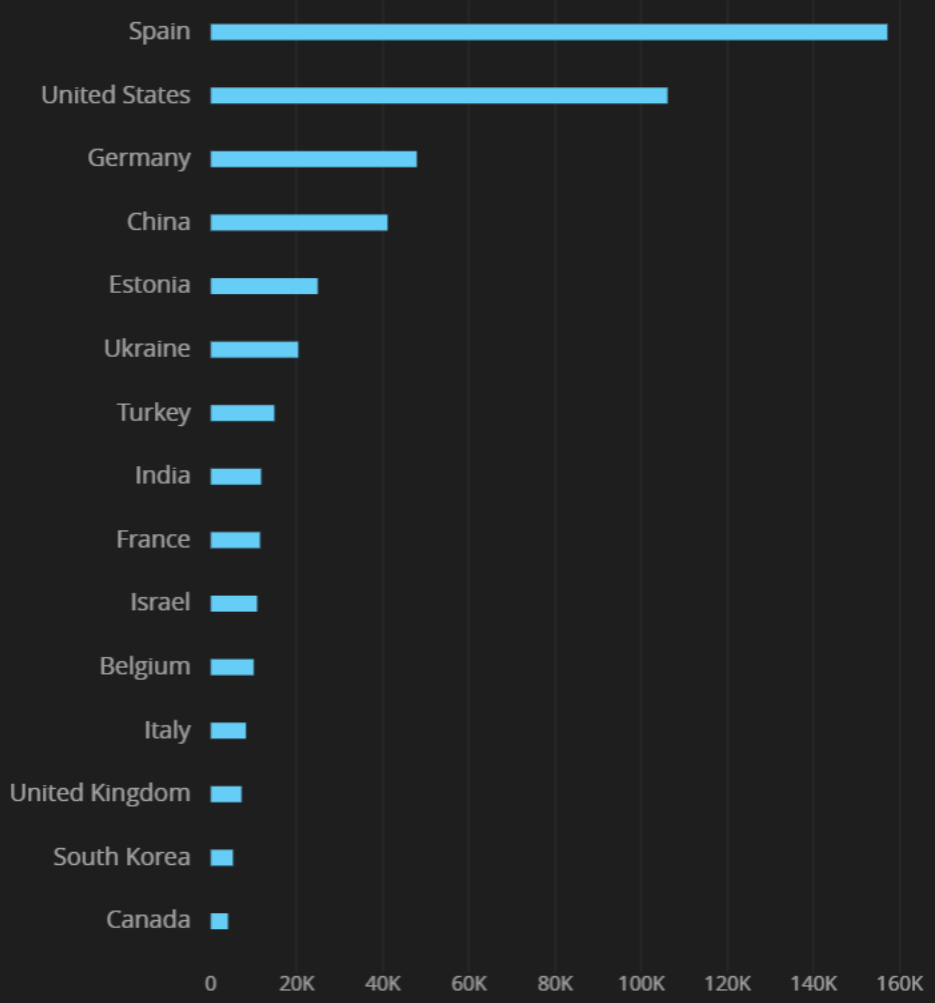
1,687

Total Unique Organizations

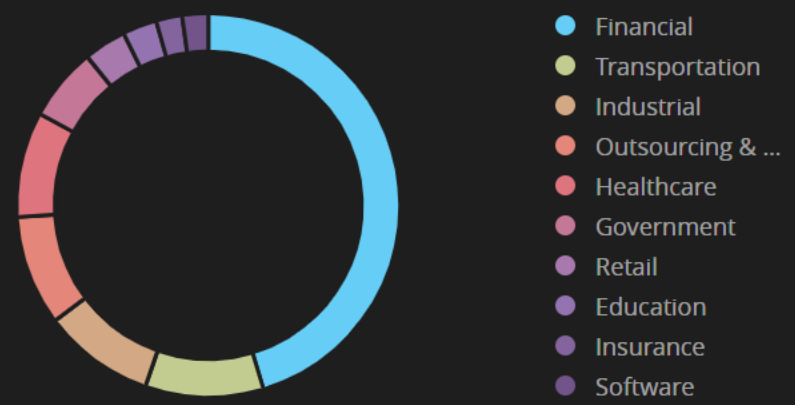
2,859



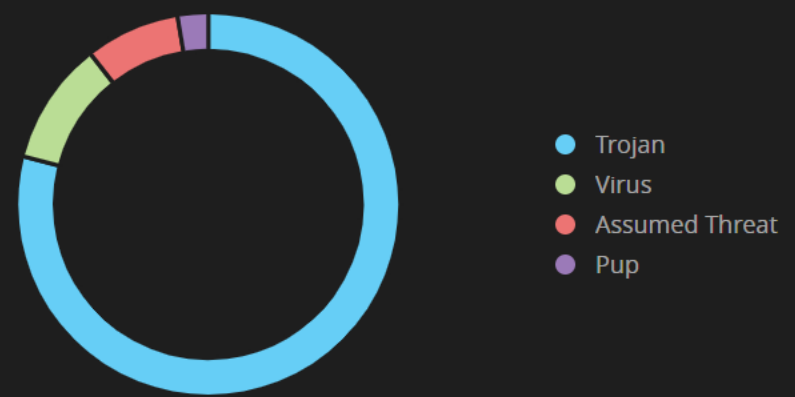
### Top Countries with Malicious Detections



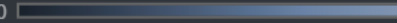
### Top Verticals with Malicious Detections



### Threat Types



# COVID-19 Related Malicious File Detections

0  157K

Jan 2 to Jun 16, 2020



Japan  
Detections: 1,502

© OpenStreetMap contributors

Total Malicious Detections

538,083

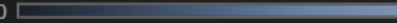
Total Unique Hashes

1,687

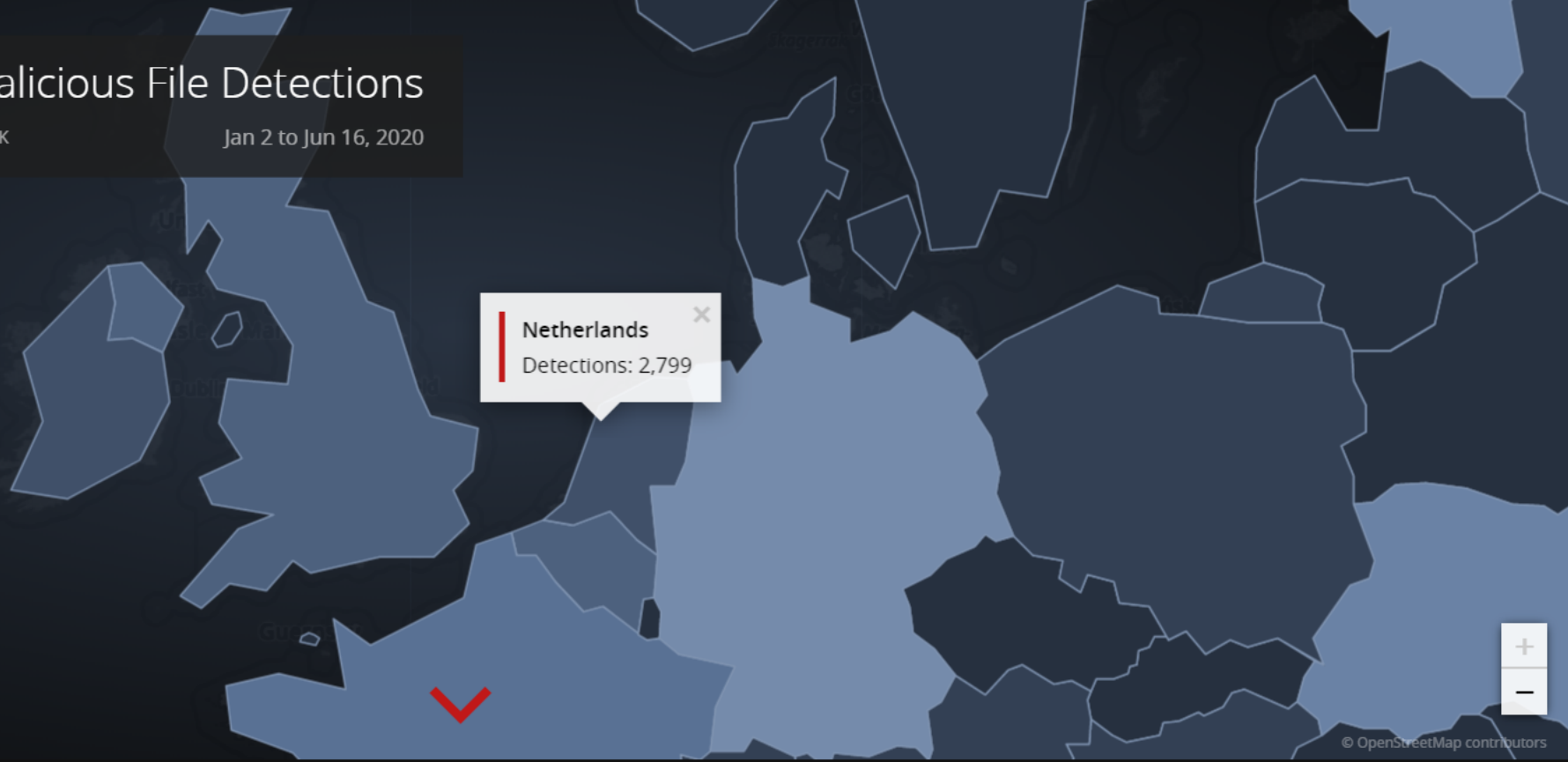
Total Unique Organizations

2,859

# COVID-19 Related Malicious File Detections

0  157K

Jan 2 to Jun 16, 2020



Total Malicious Detections

538,083

Total Unique Hashes

1,687

Total Unique Organizations

2,859

# Self-Introduction

## Hiroshi Sasaki

Senior Security Advisor,  
Cyber Strategic Initiative Office, CISSP  
McAfee Co., Ltd.

### **Mission:**

**To Cultivate CULTURE of Critical Infrastructure (CI) Protection/ IoT Security**

Joined McAfee in December 2012 after working for 14 years as **a developer of industrial control system.**

Aiming to foster culture of industrial cyber security, providing enlightenment such as lectures, writing and consulting services.

### **Part time job:**

- **Sr. Expert, Cyber Tech. Lab, ICSCoE (Industrial Cyber Security Center of Excellence) (July 2017~)**
- **IT security Officer of Ministry of Economy, Trade and Industry (May 2016~)**

# Cyber threat landscape of Critical Infrastructure (using OT system) and Manufacturing sector in Japan

- COVID-19 will **accelerate the cyber security risk** of CI sectors.
  - DX (Digital Transformation) , move to cloud, remote operation etc.
- **CI sectors** are not heavily cyberattacked so far.
- CI sectors heavily rely on **Manufacturing sectors**.
  - Japan equips the wide-range and deep-vertical supply chain for ICS systems
- Manufacturing sector is targeted by **Ransomware** campaign.
- Protecting **company's brand** and **supply chain partners** need the **active disclosure of cyberattack** in **POST-COVID-19** era.

# COVID-19 will accelerate the cyber security risk of CI sectors

COVID-19



- Stay home
- Social distance
- Reduce transportation



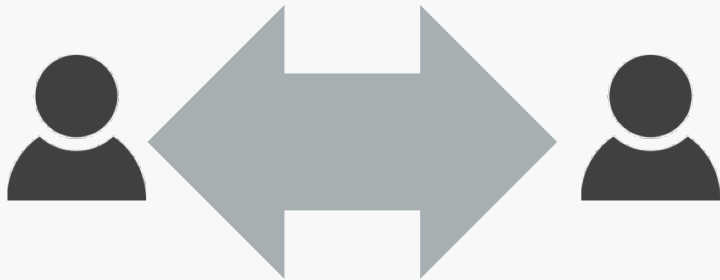
CI sectors



- Remote maintenance
- Move to Cloud
- Digital Transformation



Cyber security risk



# Evolution of Cyber threat vectors : Special to General

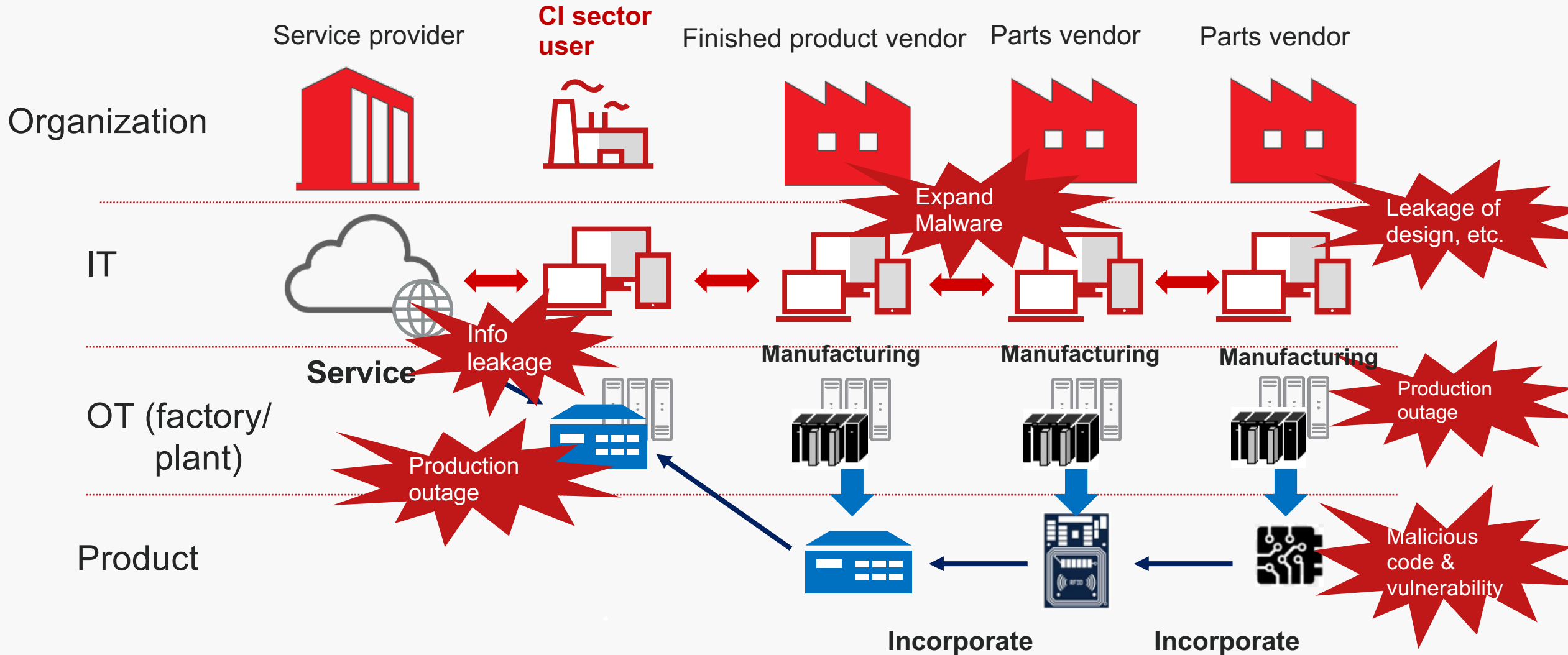
**Economic Purpose's Ransomware targeting ICS related system becomes popular recently.**



Attack	Feature
Stuxnet	<ul style="list-style-type: none"> <li>- Crash purpose, <b>Political motivation</b></li> <li>- Highly sophisticated &amp; targeted attack</li> <li>- One single target</li> </ul>
Operation Dragonfly	<ul style="list-style-type: none"> <li>- Reconnaissance, Test purpose</li> <li>- General Target</li> <li>- General technology, understanding <b>ICS operation</b></li> </ul>
Ukraine 2015	<ul style="list-style-type: none"> <li>- Crash, Outage purpose</li> <li>- Targeted attack and several targets</li> <li>- <b>Direct Operation</b> via Internet</li> </ul>
Crashoverride/Industroyer 2016	<ul style="list-style-type: none"> <li>- Crash, Outage purpose</li> <li>- Targeted attack and one single target</li> <li>- highly understanding <b>ICS protocol</b></li> <li>- <b>Modularization, Time bomb</b></li> </ul>
TRISIS-TRITON-Hatman 2017	<ul style="list-style-type: none"> <li>- Crash, Outage purpose</li> <li>- Targeted attack and one single target</li> <li>- highly understanding ICS <b>safety</b></li> </ul>
Norsk Hydro 2019	<ul style="list-style-type: none"> <li>- <b>Economical</b> purpose</li> <li>- Ransomware Campaign</li> <li>- <b>IT outage effects OT production</b></li> </ul>

# CI sectors heavily rely on **Manufacturing sectors.**

CI sectors heavily rely on the **vendor reliability** and the **product reliability.**





# Ransomware campaign to Manufacturing sector



RANSOMWARE | THREAT ANALYSIS

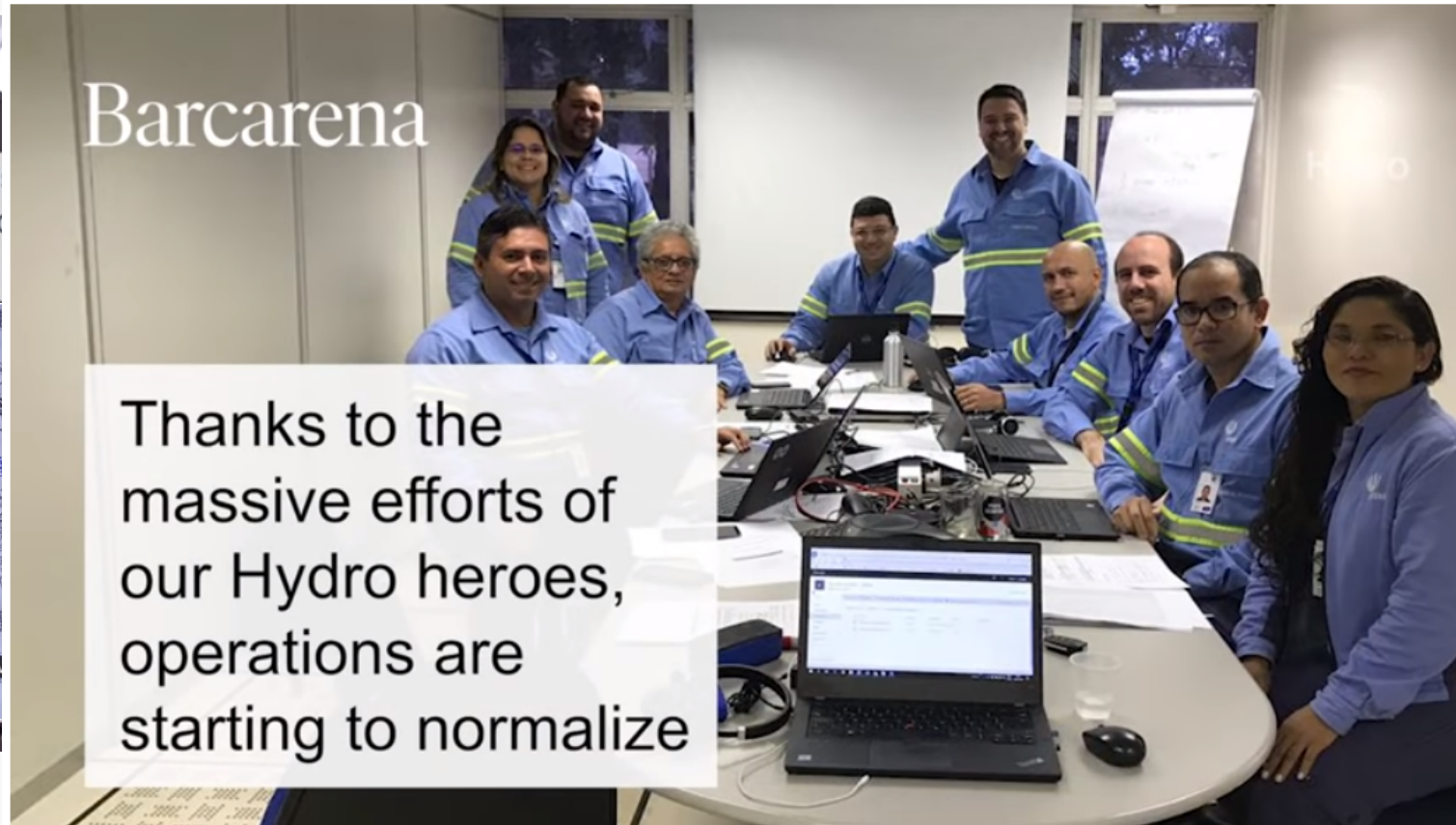
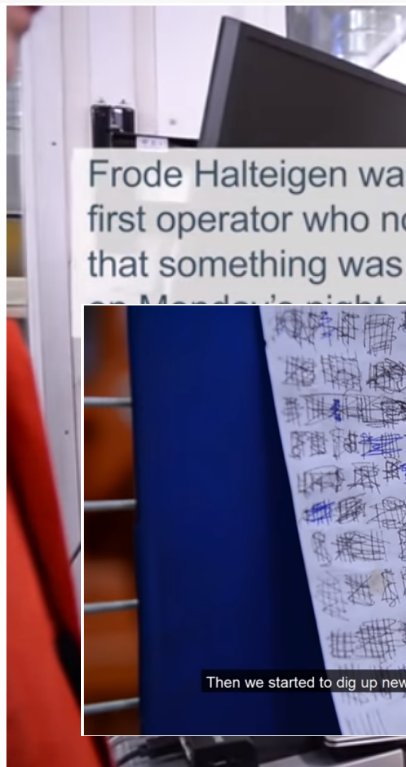
## Honda and Enel impacted by cyber attack suspected to be ransomware

- Several CI and manufacturing companies are hit by ransomware (snake) on June 8 2020.
- Snake/EKANS has the capability to **terminate ICS related process** in the Windows OS terminal.
- **Some media** reported **Honda** might be hit by the ransomware and **stopped the production** of several factories globally. (almost recovered by June 11)
- Honda has had **no announcement** of the cyberattack due to the security reason so far.

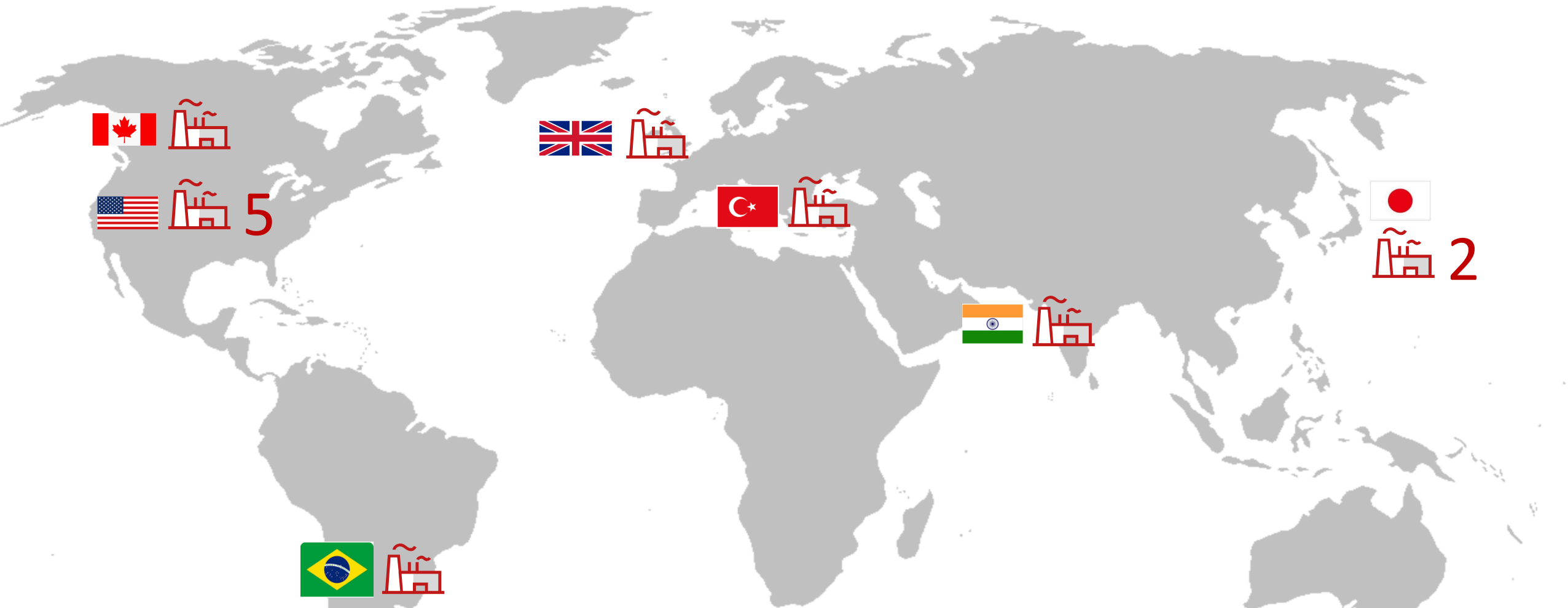
<https://blog.malwarebytes.com/threat-analysis/2020/06/honda-and-enel-impacted-by-cyber-attack-suspected-to-be-ransomware/>

# Active external communication worked well

Norway's aluminum producer Norsk Hydro (more than 35,000 employees in 40 countries worldwide) was hit by Ransomware on March 19, 2019. It is estimated to have reached 300 to 350 million NOK (equivalent to \$ 40 million) in the first week (as of March 25). Their Facebook reports the incident right after it. They also create a public relations video to explain the situation. **The external communication is the good reference for protecting company's brand.**



# Lessons Learned from observation. 2



Expand the bad effect of malware globally.  
It might expand the supply chain partners.

# Cyber threat landscape of Critical Infrastructure (using OT system) and Manufacturing sector in Japan

- COVID-19 will **accelerate the cyber security risk** of CI sectors.
  - DX (Digital Transformation) , move to cloud, remote operation etc.
- **CI sectors** are not heavily cyber-attacked so far.
- CI sectors heavily rely on **Manufacturing sectors**.
  - Japan equips the wide-range and deep-vertical supply chain for CI sectors.
- Manufacturing sector is targeted by **Ransomware** campaign.
- **Protecting company's brand and supply chain partners need the active disclosure of cyberattack in POST-COVID-19 era.**

# Q & A

Thank you.



McAfee, the McAfee logo, and MVISION are trademarks or registered trademarks of McAfee LLC or its subsidiaries in the U.S. and/or other countries. Other names and brands may be claimed as the property of others. McAfee technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. No computer system can be absolutely secure.

Copyright © 2020 McAfee LLC.

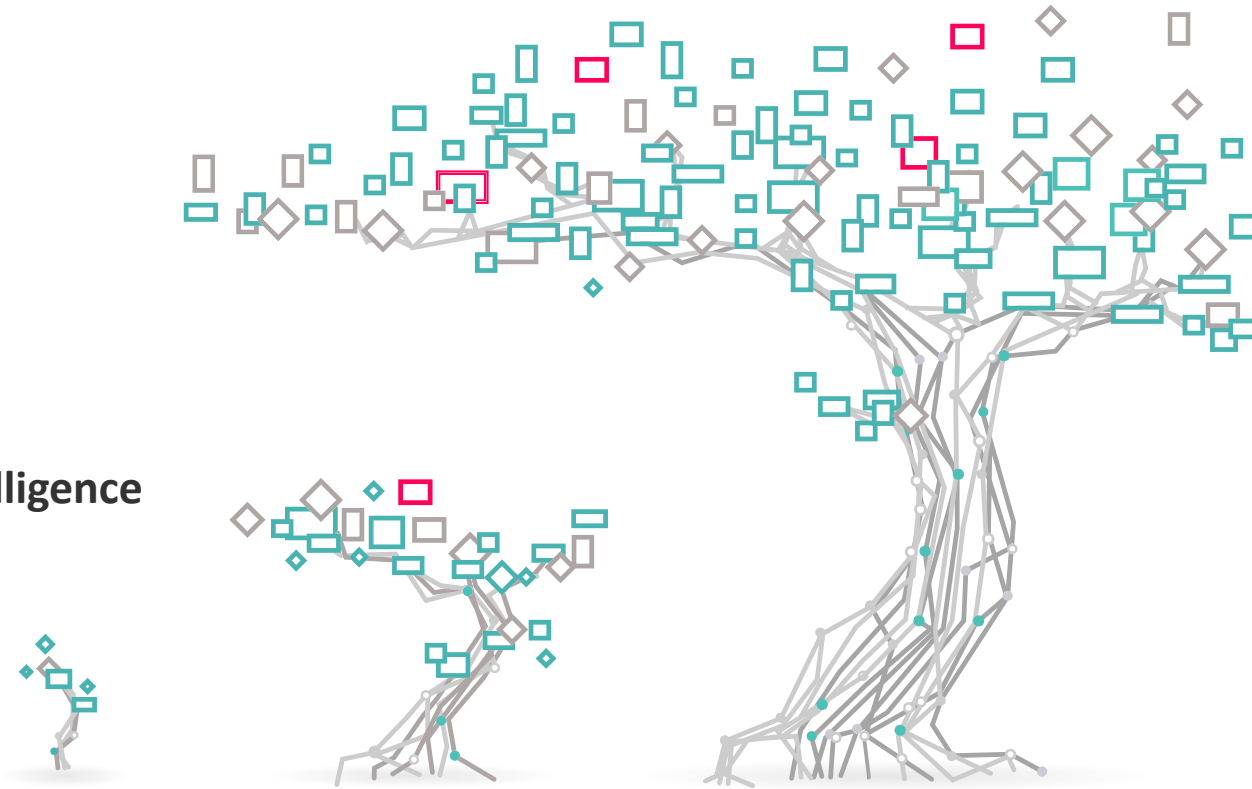
# Ippolito Forni

Senior CTI Analyst at  
EclecticIQ

# Threat Landscape of Critical Infrastructure in the Netherlands and Europe

Ippolito Forni

Threat Intelligence Consultant & Senior Cyber Threat Intelligence Analyst, EclecticIQ





# Critical Infrastructure in the Netherlands

---

## Category A

- National transport and distribution of power
- Gas production
- National transport and distribution of gas
- Oil supply
- Drinking water supply
- Flood defences and water management
- Storage, production and processing of nuclear materials

## Category B

- Regional distribution of electricity
- Regional distribution of gas
- Internet and data services
- Internet access and data traffic
- Voice services and text messaging
- Geolocation and time information by GNSS
- Air Traffic
- Vessel Traffic Service
- And more....

# Recent Critical Infrastructure Attacks in Europe

In mid April



Energy giant **Energias de Portugal (EDP)**

A major player in the energy industry arena, operating in 19 countries across 4 continents.



- Encrypted data
- Exfiltrated 10 TB of data
- Threatened to publish it



Ragnar Locker  
ransomware family

The ransom demand in this attack was 1580 Bitcoins which, at the time of writing, converts to approximately US\$15 million.

# Recent Critical Infrastructure Attacks in Europe

In mid May



British power grid company **Exelon**

Exelon is responsible for UK's balancing and settlement code (BSC). "We also compare how much electricity generators and suppliers say they will produce or consume with actual volumes. We then work out a price for the difference and transfer funds. This involves taking 1.25 million meter readings every day."



- Encrypted data
- Exfiltrated an undisclosed amount of data
- Threatened to publish it



the Sodinokibi (a.k.a. Revil) ransomware family

# Recent Critical Infrastructure Attacks in Europe

In early June



the Italian energy company  
giant **Enel**



The investigation is still ongoing so very little details are available.

It appears the same Snake ransomware family might have also targeted a Japanese automotive giant.



Snake ransomware family  
(a.k.a. Ekans) , designed  
to target Industrial  
Control Systems

# Cyber Criminals and Nation States 4-Stages Cyber Attacks

Results from Cybereason ICS honeypots

## Stage 1

Brute-force passwords on publicly accessible remote interfaces.



## Stage 2

Upload of malicious utilities and payloads to gain domain administrator privileges.



## Stage 3

Scan of the internal network for lateral movement.



## Stage 4

Ransomware deployment and encryption.

# What Mitigation Measures Are Countries Taking?

---

Critical Infrastructure Partnerships:

## **“The European Network for Cyber Security (ENCS)**

is a non-profit member organization that brings together critical infrastructure stake owners and security experts to deploy secure European critical energy grids and infrastructure. Founded in 2012, ENCS has dedicated researchers and test specialists who work with members and partners on applied research, defining technical security requirements, component and end-to-end testing, as well as education & training.”

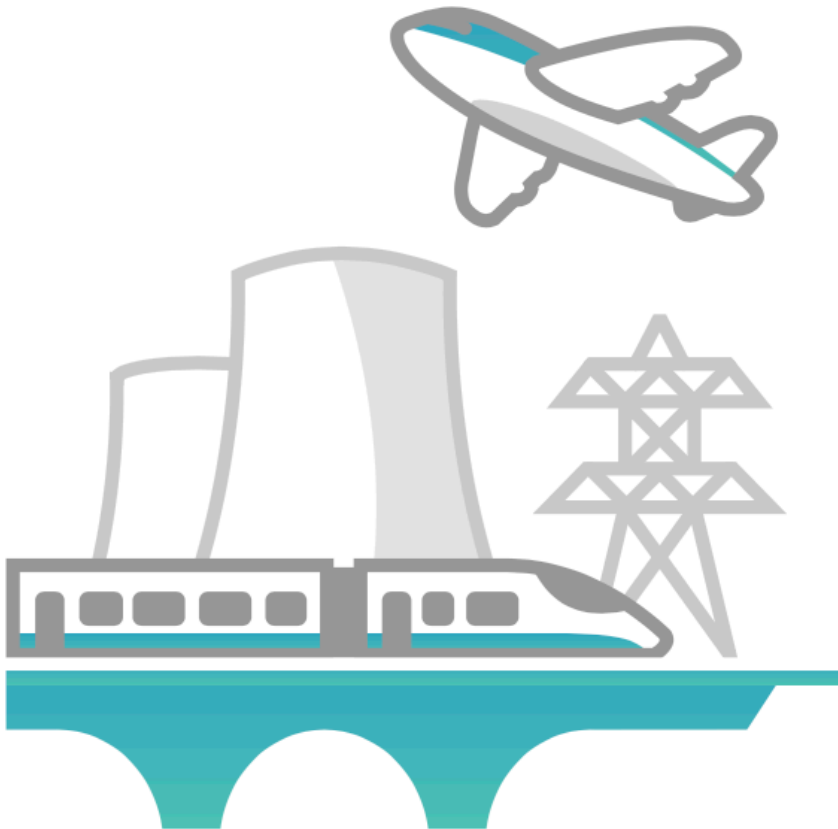
- *Intelligence, information and knowledge sharing between members.*
- *Workshops and Events.*
- *Collaboration in sharing the latest theoretical advances into real world environments.*

## New Critical Infrastructure Categories?

---

With COVID19, new realities came to light:

- Conferencing tools like Zoom have been paramount to the business continuity of many organizations, including government ones.
- German Task Force for COVID-19 medical equipment was targeted in an ongoing phishing campaign. In the current pandemic, should PPE and medical equipment procurement processes be considered Critical Infrastructure?



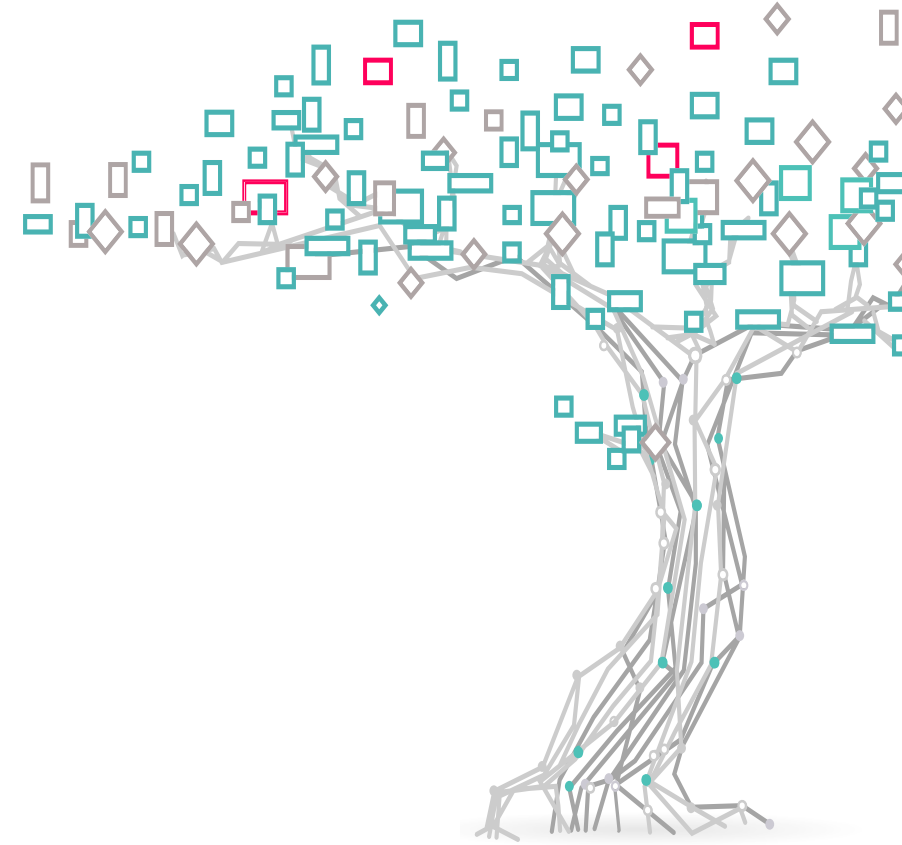
## About Eclectiq

Eclectiq enables intelligence-powered cybersecurity for government organizations and commercial enterprises. We develop analyst-centric products and services that align our clients' cybersecurity focus with their threat reality. The result is intelligence-led security, improved detection and prevention, and cost-efficient security investments.

Our solutions are built specifically for analysts across all intelligence-led security practices such as threat investigation, threat hunting, and incident response, and are tightly integrated with their IT security controls and systems.

Eclectiq operates globally with offices in Europe, United Kingdom, and North- America, and via certified value-add partners.

Learn more at [www.eclectiq.com](http://www.eclectiq.com)





# Thank You

Questions - [iforni@eclecticiq.com](mailto:iforni@eclecticiq.com)

## **Further reading:**

- *Webcast - How to Leverage CTI to Defend From Ransomware: <https://go.eclecticiq.com/resources/how-to-leverage-cti-to-defend-from-ransomware1>*
- *Covid-19 Threat Intelligence Weekly Report: <https://blog.eclecticiq.com/covid-19>*
- *Evolving Ransomware Threat in the Energy Sector: <https://blog.eclecticiq.com/evolving-ransomware-threat-in-the-energy-sector>*
- *2020 Tokyo Summer Olympics From a CTI Perspective: <https://blog.eclecticiq.com/2020-tokyo-summer-olympics-from-cti-perspective>*



INTELLIGENCE POWERED DEFENSE

# Alberto Pelliccione

CEO at ReaQta



Securing Critical Infrastructures

Europe's Leading A.I. Endpoint Defense Platform



**Alberto Pelliccione - CEO**

<https://www.linkedin.com/in/albertopelliccione>

URGENT PROBLEM

## Critical Operations Drive Value Up for Attackers

Rise in cyber-attacks is showing a profitable niche for criminals

### TRAVELEX

PAID \$3.2M  
Sodinokibi Ransomware

- Several GB of Sensitive Data Encrypted & network outage across its endpoints
- Estimate loss without paying the ransom: \$30M to \$95M
- Reuters reported that Travelex employees were serving thousands of customers using pen and paper

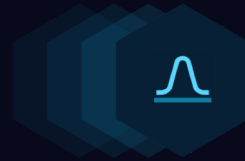


There is a strong incentive to attack increasingly more sensitive infrastructures

CASE STUDY

# Energy Distribution

Tracing the steps of a sophisticated attack against a large power distribution company.



## INITIAL BREACH

Identifying the anomaly on the supply-chain and how the attacker leveraged a trusted channel to gain a foothold into the infrastructure.



## LATERAL MOVEMENT

Attackers working to discover the network topology and moving laterally to gain access to high-privilege computers.



## RANSOMWARE RELEASE

Weapon releasing to cause widespread damage and extort money from the company.



## PROTECTING THE INFRASTRUCTURE

Initiating full response to rapidly clean up the infrastructure and remove the attacker.

ATTACK STAGES

Learn • Detect • Track • Respond • Protect

### Supplier Breach

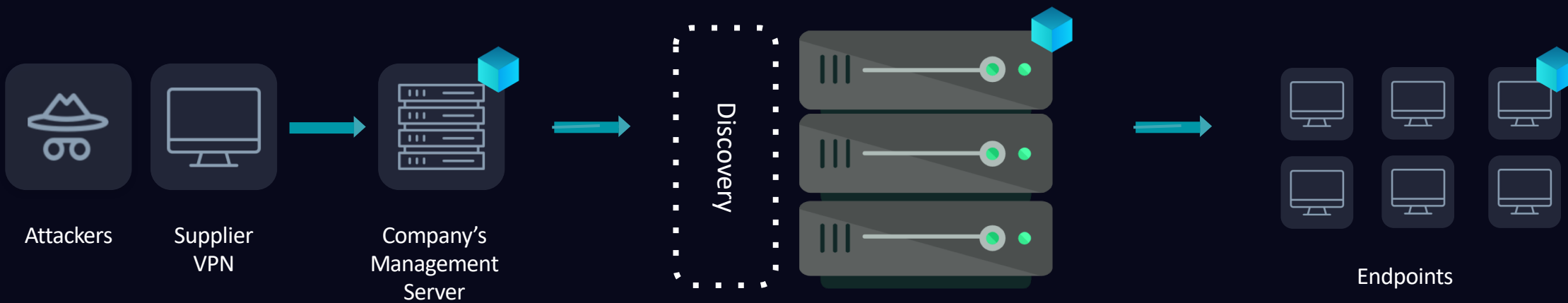
Real-Time Detection

### Lateral Movement

Data Collection & Behavioral Analysis

### Ransomware Release

Response & Remediation



INITIAL BREACH

DOMAIN CONTROLLER

RANSOMWARE

CASE STUDY

# Attack Timeline

Tracking progress, step-by-step

## 02/March - 13:35 - Supplier

Supplier is compromised. The attacker starts to move into their network, they obtain access to a VPN concentrator used to access 5 different Critical Infrastructures.

## 06/March - 02:29 - Power company network is accessed

Attackers step into the network via highly trusted channel. They immediately begin to map the network to identify the Domain Controllers. They install several keyloggers.

## 08/March - 03:55 - Ransomware Release

Attackers deploy Ryuk ransomware using centralized deployment to ensure that the ransomware reaches every device.

## 08/March - 09:50 - Remediation

Response plan is activated, attackers are removed by the security team. There was no downtime for the entire infrastructure, no data was compromised.

DISCOVERY

# A.I. + Automation

Automating detection and tracking allowed for a timely and effective response, without side-effects.



## Initial Breach

Supply-chain attack models flagged the creation of a new user on a management endpoint.



## Discovery + Lateral Movement

Anomaly detection flagged a new and highly unusual lateral movement. MITRE ATT&CK automated hunting flagged all the discovery activities.



## Malicious Payload Delivery

Artifacts analysis flags the distribution of an untrusted binary coming from the Domain Controller. The binary is also identified as unique, starting the tracking process on the endpoints.



## Ransomware Activation

Behavioral analysis immediately shows signs of ransomware activity. The ransomware is automatically blocked with no loss of data.



# Key Takeaways

## **DO NOT TRUST THE WEAK LINKS**

Attackers will find the path of least resistance, which is often a supplier or a MSP (Managed Service Provider). Gaining access to a supplier or MSP grants the attackers access to multiple targets at once.

## **LEARNING TO AUTOMATE IS KEY**

In absence of prior knowledge about an attacker (no intelligence, lack of indicators) detections must be automated to speed-up the discovery and initiate granular tracking on all the affected devices. Make use of MITRE ATT&CK as much as possible.

## **A.I. EMPOWERS SECURITY TEAMS**

A.I. is becoming more and more a necessary ally. Security teams won't be alert 24/7 and a few seconds can make a huge difference. A.I. automates repetitive tasks and is incredibly good at spotting anomalies, often better than human analysts (and always much faster!)

## **ATTACKERS ARE SPECIALIZING**

New attack tools (EKANS ransomware for instance) are specializing to target ICS networks. Embracing new paradigms, automated threat hunting and full monitoring is today a requirement to secure Critical Infrastructures.



Securing Critical Infrastructures

Europe's Leading A.I. Endpoint Defense Platform

Thank you!

Alberto Pelliccione - CEO

<https://www.linkedin.com/in/albertopelliccione>

# Petra van Schayik

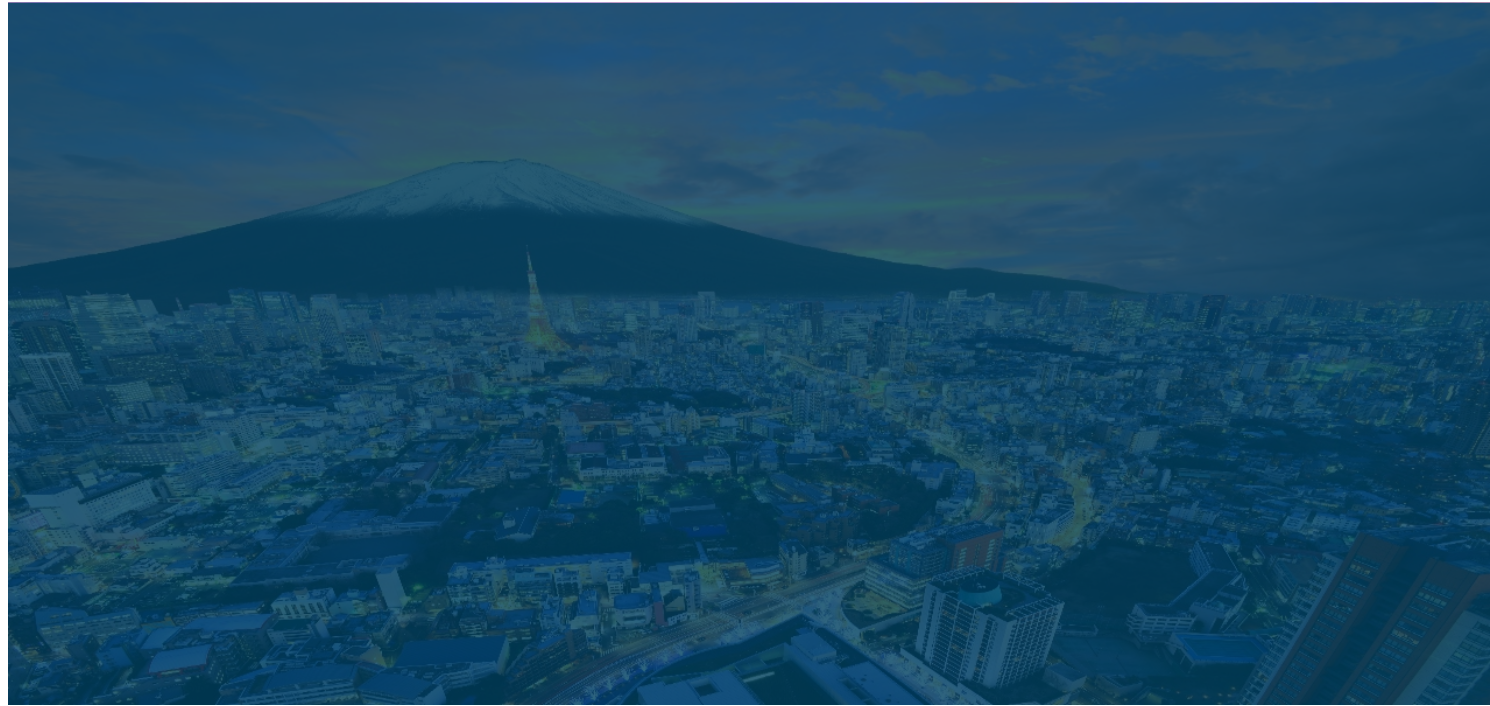
CEO at Compumatica  
secure networks

# Takashi Oishi

Director International  
Business Development  
Office TEPCO

Japan – The Netherlands  
collaboration

TEPCO - Compumatica



**Webinar 17-06-2020**



*Cybersecurity with a personal touch*

# Compumatica

Company profile



**EUROPEAN VENDOR**

---



**NO BACKDOORS**

---



**PRIVATE  
COMPANY**

---



**CUSTOMER  
DEVELOPMENT**

---



# Certifications

Certified solutions by



**EUROPEAN UNION**

---



**NATO**

---



Rijksoverheid

**THE NETHERLANDS**

---



# CYBER ATTACKS INCREASINGLY TARGET CRITICAL INFRASTRUCTURE



I-Ieitec • RCX @heitec · 18 u

Ransomware: Hackers took just three days to find this fake industrial network and fill it with malware |

[zdnet.com/article/ransom...](https://zdnet.com/article/ransom...)

The risk is real, 3 days to get industrial networks being fully infected.

#cybersecurity #ics #ot



Ransomware: Hackers took just three days to find this fake industrial ne...  
Researchers set up a tempting honeypot to monitor how cyber criminals would exploit it. Then it came under attack.

[zdnet.com](https://zdnet.com)



# Law and the effect on utilities in Europe

## Regulations

- Personal data needs to be secured
- Data in transport needs to be protected

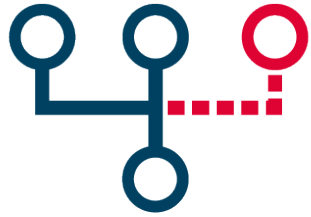
## Measures

- ✓ Extra security layers to prevent data leakages and malware breaches
- ✓ Encryption data communications between all offices, including plants, etc.



# MagiCtwin

How Dutch technology helps utilities to protect their network.



**SECURE SEPERATION  
OF NETWORKS**

---



**UNIDIRECTIONAL  
TRAFFIC**

---



**STRICT TWO-WAY  
TRAFFIC**

---



**INDUSTRIAL  
PROTOCOLS**

---





# MagiCtwin

How Dutch technology helps utilities to protect their network.



**PROTECTING THE  
CRITICAL ASSETS**

---



**ORGANISATION IN  
CONTROL OF DATA**

---



**SECURE CONNECTION  
TO CLOUD**

---



**CERTIFIED  
TECHNOLOGY**

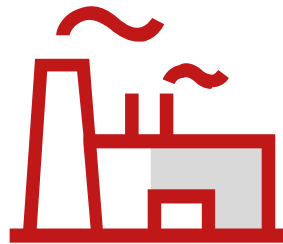
---



# TEPCO & Compumatica

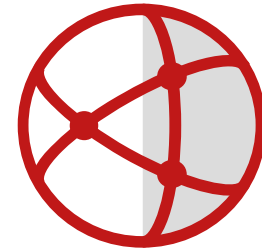
MOU to develop a Japanese – Dutch secure solution

- **PMCN protocol**
- **Testing specific protocols like PMCN in a test environment with MagiCtwin software**
- **Compatibility testing with ForeScout Silent Defense solution in TEPCO Power Grid Network**
- **Joint-opportunities in Japan and beyond (South east Asia)**



**NEXT GENERATION  
SCADA**

---



**AVAILABILITY ATTACKS**

---



# Compumatica

SECURE NETWORKS

*Cybersecurity with a personal touch*

Petra van Schayik  
[petra.vanschayik@compumatica.com](mailto:petra.vanschayik@compumatica.com)

Takashi Oishi  
[oishi.takashi@tepco.co.jp](mailto:oishi.takashi@tepco.co.jp)

# Japan-Netherlands Collaboration

Knowledge summit at Tokyo Olympics

We welcome new ideas for collaboration

*NL Embassy, Eric van Kooij: [eric@hollandinnovation.jp](mailto:eric@hollandinnovation.jp)*

*Kikuo Hayakawa: [hayakawa@hollandinnovation.jp](mailto:hayakawa@hollandinnovation.jp)*

*Hague Security Delta, Bert Feskens: [bert.feskens@thehaguesecuritydelta.com](mailto:bert.feskens@thehaguesecuritydelta.com)*

	<b>Speaker</b>	<b>Email</b>
Compumatica	<b>Petra van Schayik</b>	petra.vanschayik@compumatica.com
EclecticiQ	<b>Ippolito Forni</b>	iforni@eclecticiq.com
McAfee	<b>Hiroshi Sasaki</b>	Hiroshi_Sasaki@McAfee.com
ReaQta	<b>Alberto Pelliccione</b>	a.pelliccione@reaqta.com
TEPCO	<b>Takashi Oishi</b>	oishi.takashi@tepcoco.jp

## Security at First Sight™

Forescout Technologies is the leader in device visibility and control. Our unified security platform enables enterprises and government agencies to gain complete situational awareness of their extended enterprise environments and orchestrate actions to reduce cyber and operational risk. Forescout products deploy quickly with agentless, real-time discovery and classification of every IP-connected device, as well as continuous posture assessment.

### Why Forescout

#### Reduce the Risk of Business

##### Disruption from Security Incidents or Breaches

Continuously monitor your extended enterprise to prevent, detect and remediate noncompliant devices that threaten security and increase costs.

#### Ensure and Demonstrate Security

##### Compliance

Continuously assess your security environment to ensure tools meet your organization's compliance objectives.

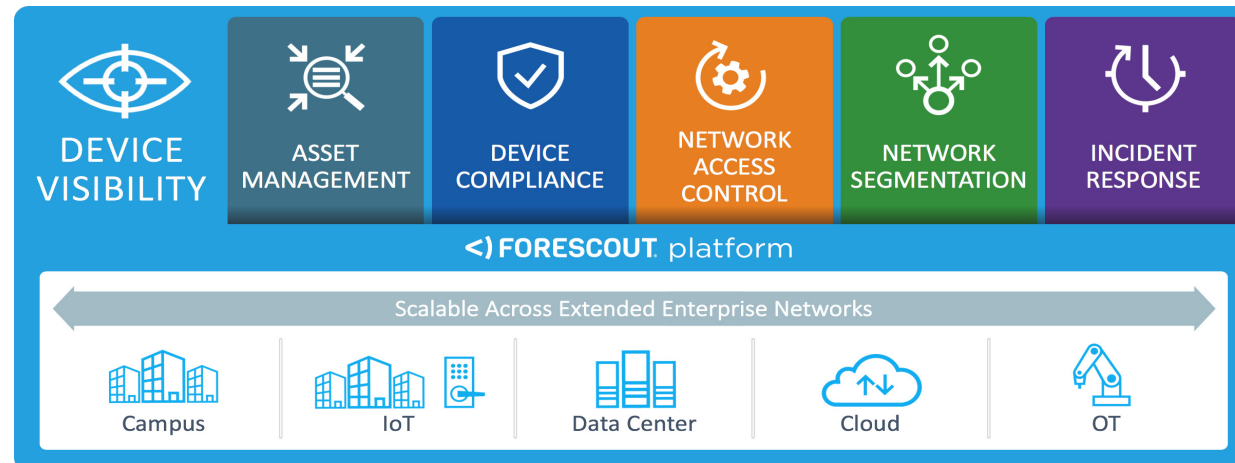
#### Increase Security Operations

##### Productivity

Integrate existing security and IT management tools and automate processes to drive security operations efficiencies.

### What we Solve

Yesterday's security approaches required software agents, which are of little use if devices don't have them or they become disabled. The Forescout platform deploys quickly and safely across heterogeneous campus, data center, cloud and OT networks to address the following uses cases—without requiring software agents:



### Forescout Stats

#### Industry

Enterprise security

#### Customers

More than 3,700 enterprises and government agencies in over 90 countries\*

25% of the Global 2000

#### Employees

1,200+ worldwide\*

#### CEO

Michael DeCesare

#### Headquarters

San Jose, California

#### Publicly traded

FSCT

### What is Device Visibility and Control?

The ability to see 100% of devices connected to the campus (including IoT), data center, cloud and OT environments coupled with the capability to secure those devices with the appropriate level of controls.

\*As of December 31, 2019

# Interested in establishing your business in Europe?



**Innovation  
Quarter**

invest &  
innovate in  
West Holland

Contact

**Martijn van Hoogenhuijze**

Senior Account Manager Cybersecurity

+31 6 533 04 281

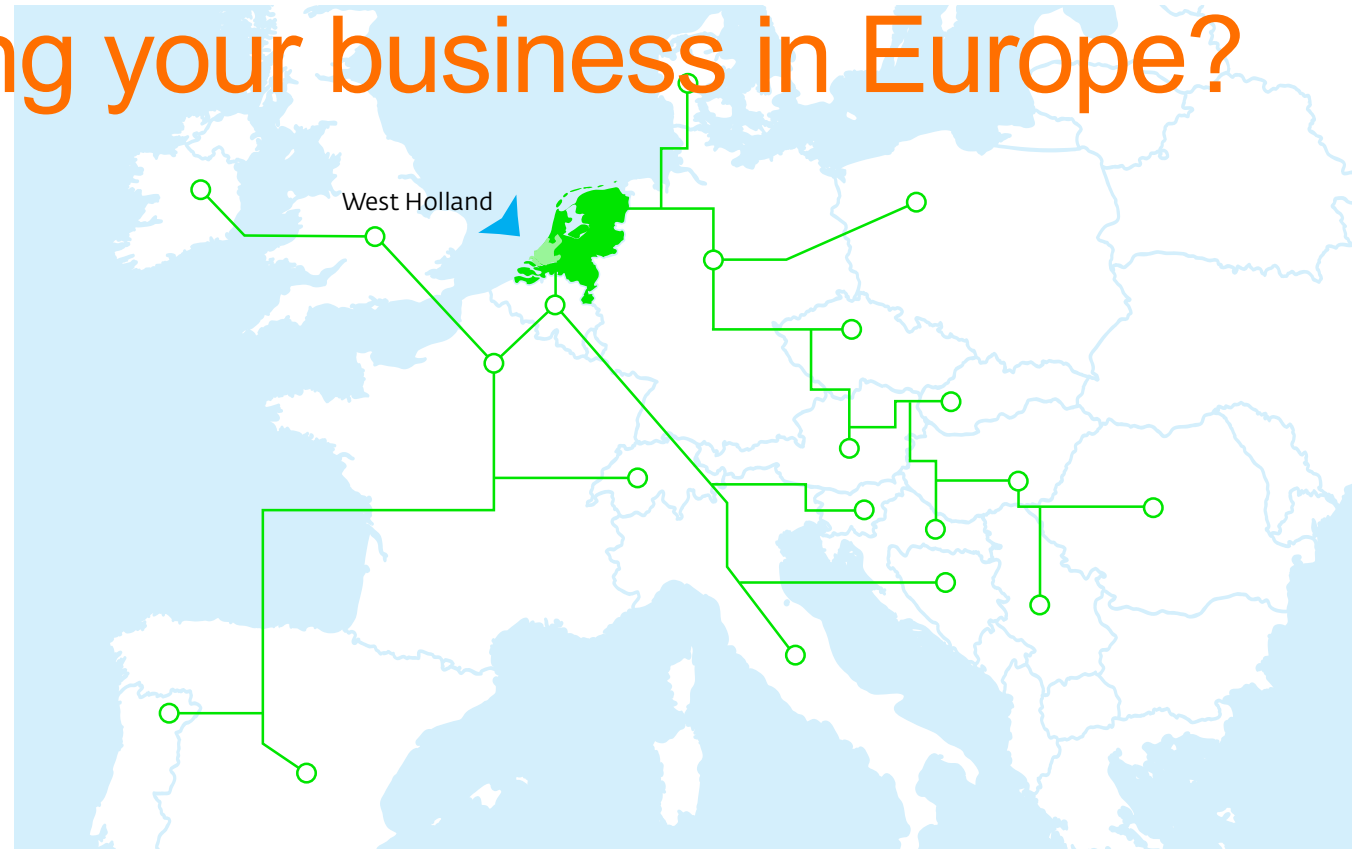
[martijn.vanhoogenhuijze@innovationquarter.nl](mailto:martijn.vanhoogenhuijze@innovationquarter.nl)

Contact IQ

+31(0)88-4747255

[info@innovationquarter.eu](mailto:info@innovationquarter.eu)

[www.innovationquarter.eu](http://www.innovationquarter.eu)



*InnovationQuarter is the Economic Development Agency for the West Holland region in the Netherlands. We provide free assistance and advice to international companies looking to locate in West Holland. In addition, we facilitate co-operation between companies, academic institutions and government. Moreover, InnovationQuarter funds innovative and fast-growing businesses in the region.*

#### **WEST HOLLAND OFFERS YOU**

- A strategic location in the heart of Europe
- Highly educated and multilingual workforce
- Excellent quality of life
- A competitive tax climate
- A dedicated foreign investment team, offering confidential, free of charge services to international companies.



*Safety and security science is about the scientific analysis of undesired events, disasters and accidents (both intentional and unintentional).*

DSyS brings together scientists from more than thirty different Delft University of Technology chairs. This enables DSyS to provide high-quality research capacity to national and international consortia and networks on a wide range of topics, such as safe transport, robots, remote sensing, drones and aerial surveillance, shipping and aviation safety, storage and logistics, forensics, terrorist threat to critical infrastructures and the design of safe cities.

# Thank you

