R2D2

Reliability, Resilience and Defense technology for the grid

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Horizon Europe Grant agreement N° 101075714.

etra I+D
S2 GRUPO Anticipating a cyber secure world
elpros
guardtime
SCC
Cyber Noesis
ΕΠΙΣΕΥ ICCS
ems services
HEDNO
Elektro Ljubljana Obnovljivi viri energije
NEW by EDP & CTG
edp
institute MIHAILO PUPIN
University of Cyprus
Imperial College London
Rte international

13th Infocom Security Conference

Athens, 26.04.2023

R2D2

… safeguards the griD

Kostas Papadatos

Founder/Managing Director, Cyber Noesis

Funded by
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. Horizon Europe Grant agreement N° 101075714.

Reliability, Resilience and
Defense technology for the grid

Agenda

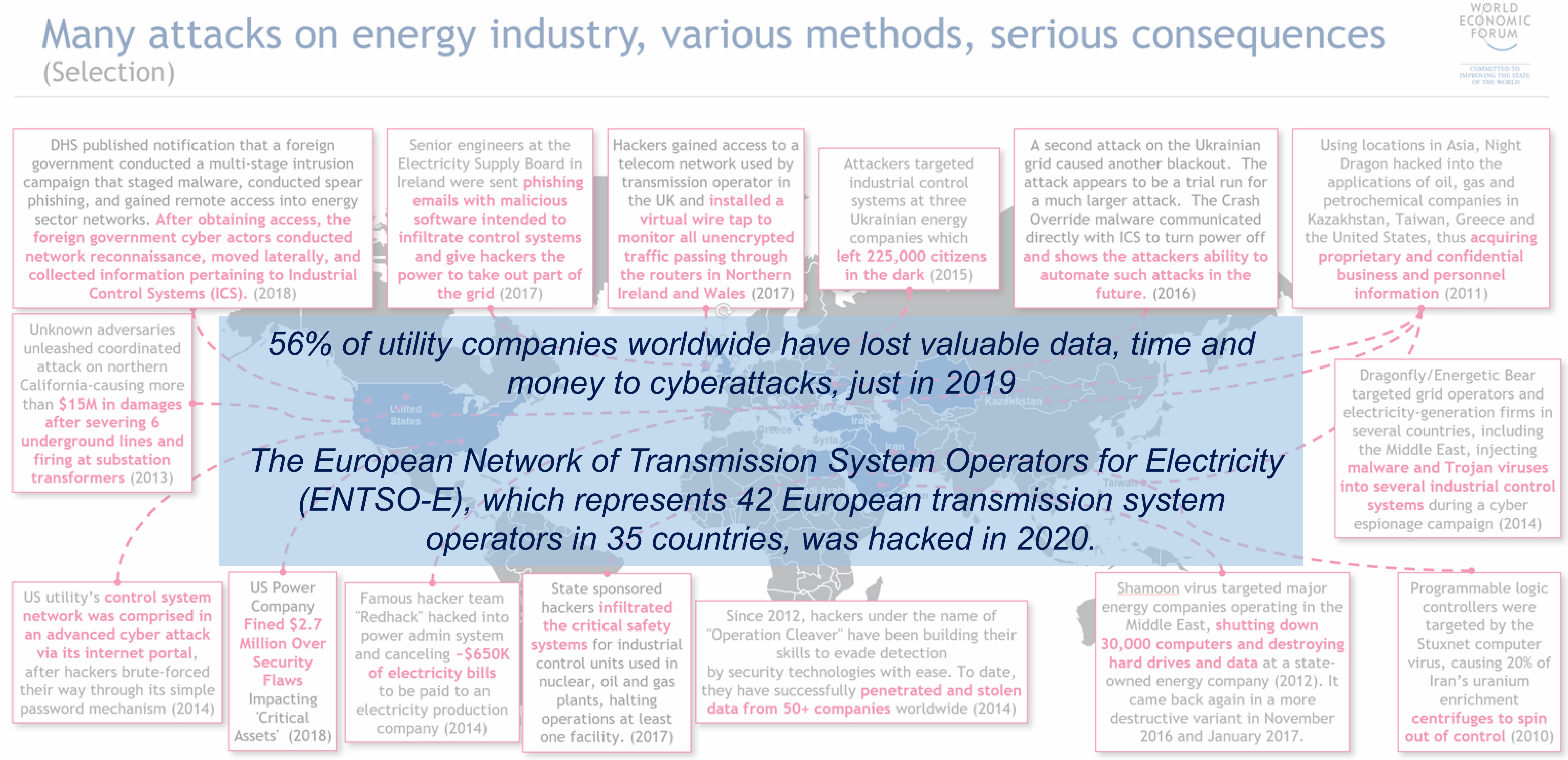
- Power Grids Under Attack!
- The “POWER” game … Cybersecurity meets Resilience
- (re)Introducing a friend: R2D2

A large-scale blackout would have socioeconomic ramifications for households, businesses and vital institutions.

For example, a six-hour winter black-out in mainland France could result in damages totalling over €1.5 billion

Power Grids Under Attack!

Power Grids Under Attack!



Many attacks on energy industry, various methods, serious consequences (Selection)

WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD

DHS published notification that a foreign government conducted a multi-stage intrusion campaign that staged malware, conducted spear phishing, and gained remote access into energy sector networks. After obtaining access, the foreign government cyber actors conducted network reconnaissance, moved laterally, and collected information pertaining to Industrial Control Systems (ICS). (2018)

Senior engineers at the Electricity Supply Board in Ireland were sent phishing emails with malicious software intended to infiltrate control systems and give hackers the power to take out part of the grid (2017)

Hackers gained access to a telecom network used by transmission operator in the UK and installed a virtual wire tap to monitor all unencrypted traffic passing through the routers in Northern Ireland and Wales (2017)

Attackers targeted industrial control systems at three Ukrainian energy companies which left 225,000 citizens in the dark (2015)

A second attack on the Ukrainian grid caused another blackout. The attack appears to be a trial run for a much larger attack. The Crash Override malware communicated directly with ICS to turn power off and shows the attackers ability to automate such attacks in the future. (2016)

Using locations in Asia, Night Dragon hacked into the applications of oil, gas and petrochemical companies in Kazakhstan, Taiwan, Greece and the United States, thus acquiring proprietary and confidential business and personnel information (2011)

Unknown adversaries unleashed coordinated attack on northern California-causing more than $15M in damages after severing 6 underground lines and firing at substation transformers (2013)

56% of utility companies worldwide have lost valuable data, time and money to cyberattacks, just in 2019

The European Network of Transmission System Operators for Electricity (ENTSO-E), which represents 42 European transmission system operators in 35 countries, was hacked in 2020.

Dragonfly/Energetic Bear targeted grid operators and electricity-generation firms in several countries, including the Middle East, injecting malware and Trojan viruses into several industrial control systems during a cyber espionage campaign (2014)

US utility's control system network was comprised in an advanced cyber attack via its internet portal, after hackers brute-forced their way through its simple password mechanism (2014)

US Power Company Fined $2.7 Million Over Security Flaws Impacting 'Critical Assets' (2018)

Famous hacker team "Redhack" hacked into power admin system and canceling ~$650K of electricity bills to be paid to an electricity production company (2014)

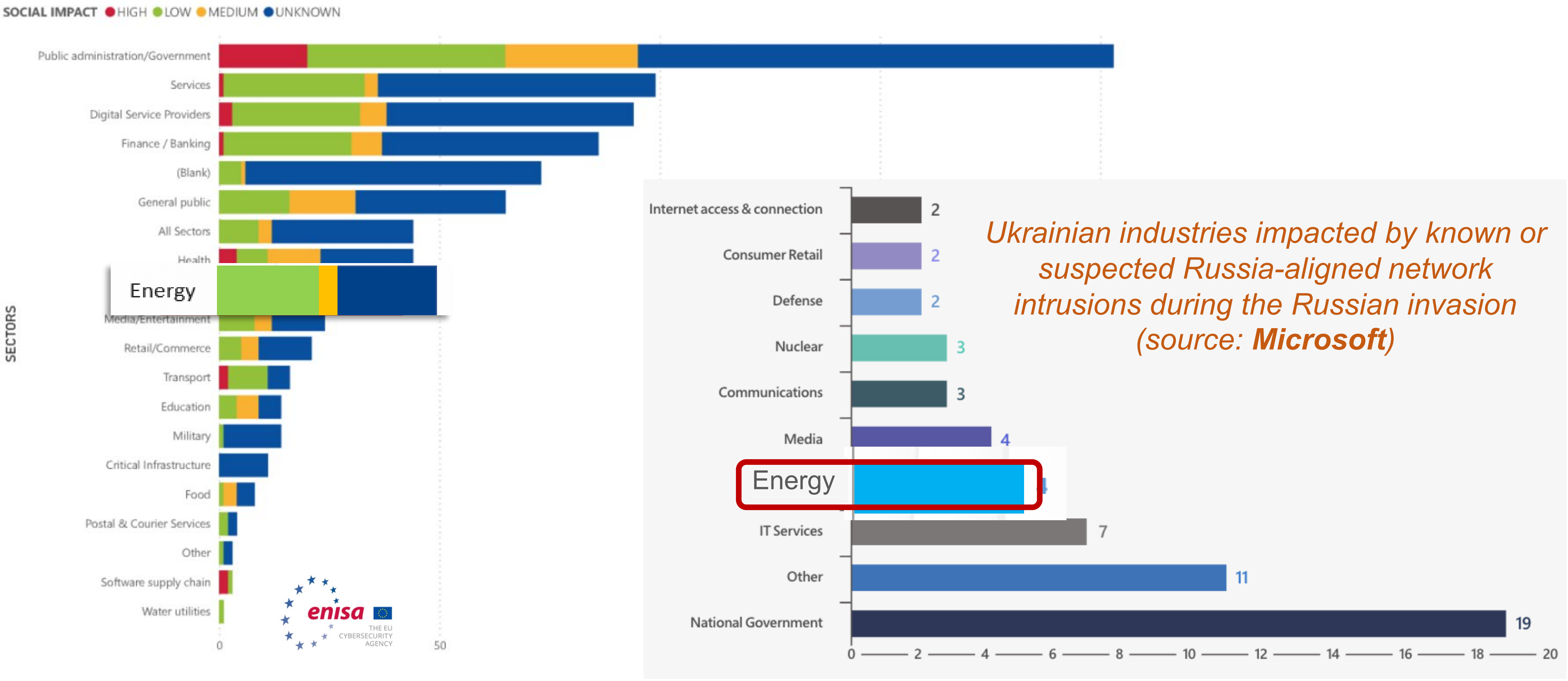
State sponsored hackers infiltrated the critical safety systems for industrial control units used in nuclear, oil and gas plants, halting operations at least one facility. (2017)

Since 2012, hackers under the name of "Operation Cleaver" have been building their skills to evade detection by security technologies with ease. To date, they have successfully penetrated and stolen data from 50+ companies worldwide (2014)

Shamoon virus targeted major energy companies operating in the Middle East, shutting down 30,000 computers and destroying hard drives and data at a state-owned energy company (2012). It came back again in a more destructive variant in November 2016 and January 2017.

Programmable logic controllers were targeted by the Stuxnet computer virus, causing 20% of Iran's uranium enrichment centrifuges to spin out of control (2010)

REAL INCIDENTS in Energy Sector



*Ukrainian industries impacted by known or suspected Russia-aligned network intrusions during the Russian invasion (source: **Microsoft**)*

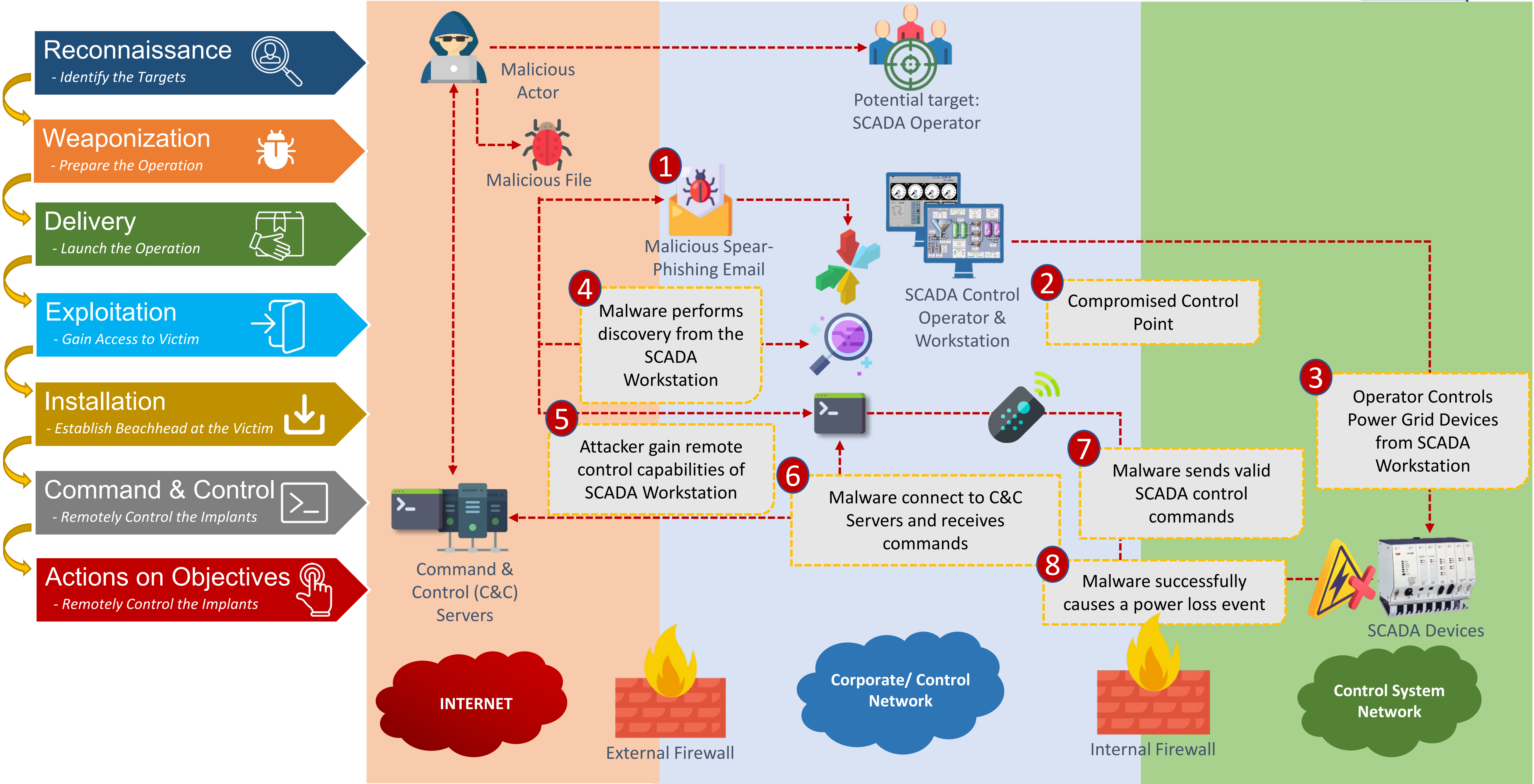
Heightened risk for OT networks

- ICS-capable **malwares** :
  1. Stuxnet
  2. Dragonfly/Havex
  3. BlackEnergy2
  4. CrashOverride or Industroyer
  5. Trisis or Triton
  6. **NEW:** Industroyer2
  7. **NEW**: INCONTROLLER (or PIPEDREAM)

Cyber Attacks on Electric Operations

- Three (3) new activity groups (Kostovite, Petrovite, and Erythrite) with intent or capability to target OT networks have been identified (out of 18 in total)
- **Currently, most adversaries in this space prioritise pre-positioning and information gathering over disruption as strategic objectives**
- State-backed actors targeting OT networks will continue dedicating resources and developing extensible ICS malware

Industroyer Malware Attack



Reconnaissance
- Identify the Targets

Weaponization
- Prepare the Operation

Delivery
- Launch the Operation

Exploitation
- Gain Access to Victim

Installation
- Establish Beachhead at the Victim

Command & Control
- Remotely Control the Implants

Actions on Objectives
- Remotely Control the Implants

Malicious Actor

Potential target: SCADA Operator

Malicious File

1 Malicious Spear-Phishing Email

SCADA Control Operator & Workstation

2 Compromised Control Point

3 Operator Controls Power Grid Devices from SCADA Workstation

4 Malware performs discovery from the SCADA Workstation

5 Attacker gain remote control capabilities of SCADA Workstation

6 Malware connect to C&C Servers and receives commands

7 Malware sends valid SCADA control commands

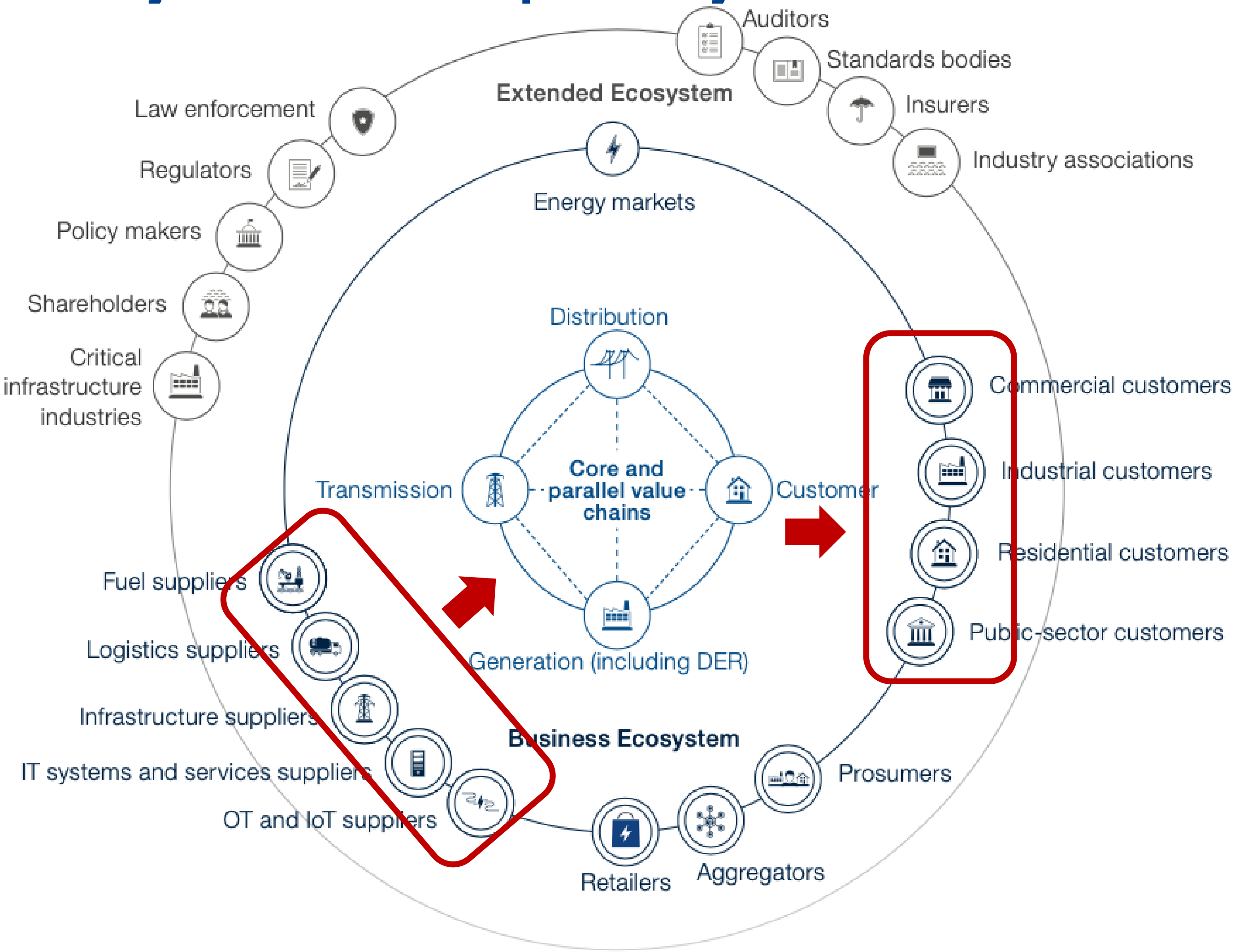
8 Malware successfully causes a power loss event

Command & Control (C&C) Servers

SCADA Devices

The “POWER” game … Cybersecurity meets Resilience

Electricity ecosystem complexity



WEF: Cyber Resilience in the Electricity Ecosystem: Principles and Guidance for Boards

Cyber Security Prime threats

Zero-day exploits are the new resource used by cunning threat actors.

A new **wave of hacktivism** has been observed since the Russia-Ukraine war.

DDoS attacks are getting larger and more complex and used in cyberwarfare (moving towards mobile networks and IoT).

Are we missing one perspective?

Ransomware: 60% of affected organisations may have paid ransom demands

AI-enabled disinformation and deepfakes flooding government agencies with fake contents, can easily disrupt the rulemaking process and the community interaction.

Threat groups **have increased interest and capability in supply chain attacks** and attacks against MSPs (Managed Services Providers).

Energy Systems Resilience Threats

Cascading failure effects in power grids when **one of the elements fails.**

Terrorism

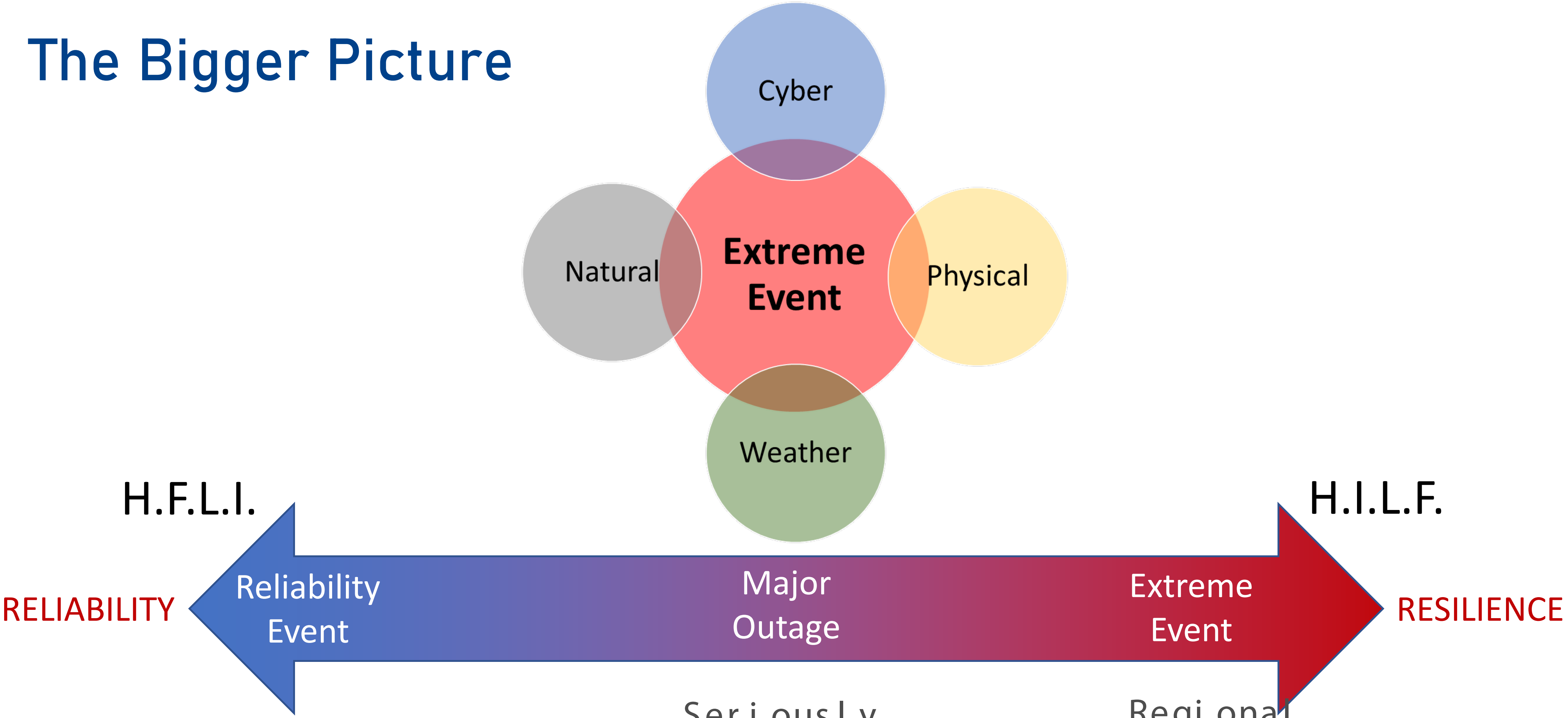
EPES **vulnerabilities** due to **human factors** (operational errors, accidental events, or malicious behaviours)

EPES **vulnerabilities** due to **technical factors** (faults, voltage and frequency fluctuations, intermittent generation, etc.)

Extreme weather events are becoming progressively more frequent, even in areas where in the past they used to occur very rarely.

Climate emergency is stressing power grids

The Bigger Picture



Cyber

Natural

Extreme Event

Physical

Weather

H.F.L.I.

H.I.L.F.

RELIABILITY

Reliability Event

Major Outage

Extreme Event

RESILIENCE

Common Outages

(up to few hours)

Seriously disrupt power supply

Regional Outages for long period

(re)Introducing a friend: R2D2

(re)Introducing a friend: R2D2

R2D2 ID card

R2D2: Reliability, Resilience and Defence technologies for the grid

Call: HORIZON-CL5-2021-D3-02-07 - Reliability and resilience of the grid: Measures for vulnerabilities, failures, risks and privacy – (IA)

Total Budget: € 9.747.375,00

Total EU Grant: € 7.335.337,50

18 Partners – 4 Demos

Start date: 01/10/2022

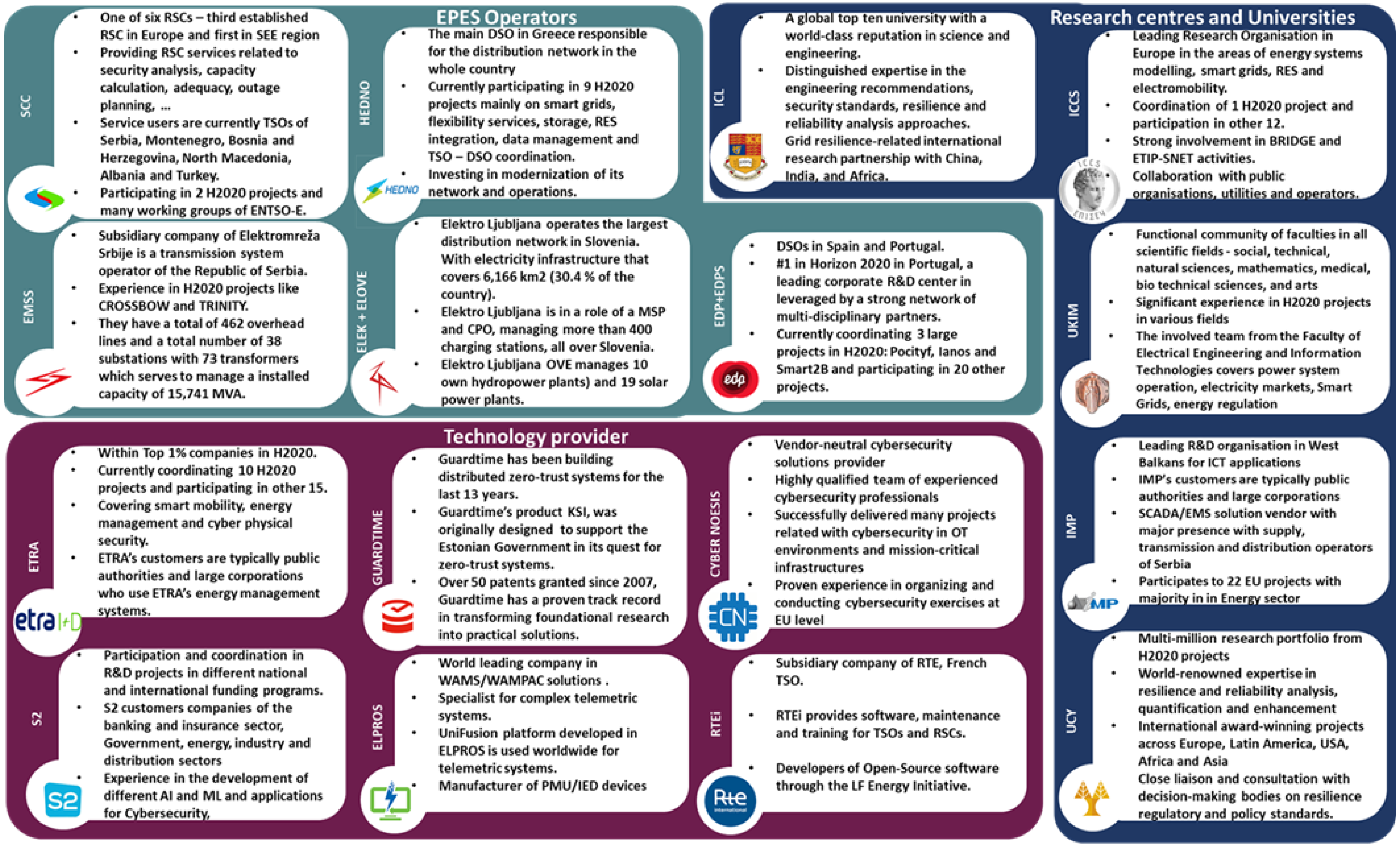
End date: 30/09/2025

Duration: 36 months

2 reporting periods

(re)Introducing a friend: R2D2

R2D2 Consortium



EPES Operators

SCC
- One of six RSCs – third established RSC in Europe and first in SEE region
- Providing RSC services related to security analysis, capacity calculation, adequacy, outage planning, …
- Service users are currently TSOs of Serbia, Montenegro, Bosnia and Herzegovina, North Macedonia, Albania and Turkey.
- Participating in 2 H2020 projects and many working groups of ENTSO-E.

HEDNO
- The main DSO in Greece responsible for the distribution network in the whole country
- Currently participating in 9 H2020 projects mainly on smart grids, flexibility services, storage, RES integration, data management and TSO – DSO coordination.
- Investing in modernization of its network and operations.

EMSS
- Subsidiary company of Elektromreža Srbije is a transmission system operator of the Republic of Serbia.
- Experience in H2020 projects like CROSSBOW and TRINITY.
- They have a total of 462 overhead lines and a total number of 38 substations with 73 transformers which serves to manage a installed capacity of 15,741 MVA.

ELEK + ELOVE
- Elektro Ljubljana operates the largest distribution network in Slovenia. With electricity infrastructure that covers 6,166 km2 (30.4 % of the country).
- Elektro Ljubljana is in a role of a MSP and CPO, managing more than 400 charging stations, all over Slovenia.
- Elektro Ljubljana OVE manages 10 own hydropower plants) and 19 solar power plants.

EDP+EDPS
- DSOs in Spain and Portugal.
- #1 in Horizon 2020 in Portugal, a leading corporate R&D center in leveraged by a strong network of multi-disciplinary partners.
- Currently coordinating 3 large projects in H2020: Pocityf, Ianos and Smart2B and participating in 20 other projects.

Research centres and Universities

ICL
- A global top ten university with a world-class reputation in science and engineering.
- Distinguished expertise in the engineering recommendations, security standards, resilience and reliability analysis approaches.
- Grid resilience-related international research partnership with China, India, and Africa.

ICCS
- Leading Research Organisation in Europe in the areas of energy systems modelling, smart grids, RES and electromobility.
- Coordination of 1 H2020 project and participation in other 12.
- Strong involvement in BRIDGE and ETIP-SNET activities.
- Collaboration with public organisations, utilities and operators.

UKIM
- Functional community of faculties in all scientific fields - social, technical, natural sciences, mathematics, medical, bio technical sciences, and arts
- Significant experience in H2020 projects in various fields
- The involved team from the Faculty of Electrical Engineering and Information Technologies covers power system operation, electricity markets, Smart Grids, energy regulation

IMP
- Leading R&D organisation in West Balkans for ICT applications
- IMP's customers are typically public authorities and large corporations
- SCADA/EMS solution vendor with major presence with supply, transmission and distribution operators of Serbia
- Participates to 22 EU projects with majority in in Energy sector

UCY
- Multi-million research portfolio from H2020 projects
- World-renowned expertise in resilience and reliability analysis, quantification and enhancement
- International award-winning projects across Europe, Latin America, USA, Africa and Asia
- Close liaison and consultation with decision-making bodies on resilience regulatory and policy standards.

Technology provider

ETRA
- Within Top 1% companies in H2020.
- Currently coordinating 10 H2020 projects and participating in other 15.
- Covering smart mobility, energy management and cyber physical security.
- ETRA's customers are typically public authorities and large corporations who use ETRA's energy management systems.

GUARDTIME
- Guardtime has been building distributed zero-trust systems for the last 13 years.
- Guardtime's product KSI, was originally designed to support the Estonian Government in its quest for zero-trust systems.
- Over 50 patents granted since 2007, Guardtime has a proven track record in transforming foundational research into practical solutions.

CYBER NOESIS
- Vendor-neutral cybersecurity solutions provider
- Highly qualified team of experienced cybersecurity professionals
- Successfully delivered many projects related with cybersecurity in OT environments and mission-critical infrastructures
- Proven experience in organizing and conducting cybersecurity exercises at EU level

S2
- Participation and coordination in R&D projects in different national and international funding programs.
- S2 customers companies of the banking and insurance sector, Government, energy, industry and distribution sectors
- Experience in the development of different AI and ML and applications for Cybersecurity.

ELPROS
- World leading company in WAMS/WAMPAC solutions .
- Specialist for complex telemetric systems.
- UniFusion platform developed in ELPROS is used worldwide for telemetric systems.
- Manufacturer of PMU/IED devices

RTEi
- Subsidiary company of RTE, French TSO.
- RTEi provides software, maintenance and training for TSOs and RSCs.
- Developers of Open-Source software through the LF Energy Initiative.

- 16 Beneficiaries
- 1 Affiliated Entity
- 1 Associated Partner

(re)Introducing a friend: R2D2

R2D2 OBJECTIVES

1. Contribute to improvement of the overall security and resiliency in power system

2. Deliver a toolkit to model the impact of HILF events, assess PES resilience and determine operational planning measures and investments

3. Increase the cybersecurity and cyber-resilience in OT and IT of the EPES

4. Enhance coordination, interaction, and information exchange between TSO-TSO and TSO-DSO in critical/emergency conditions

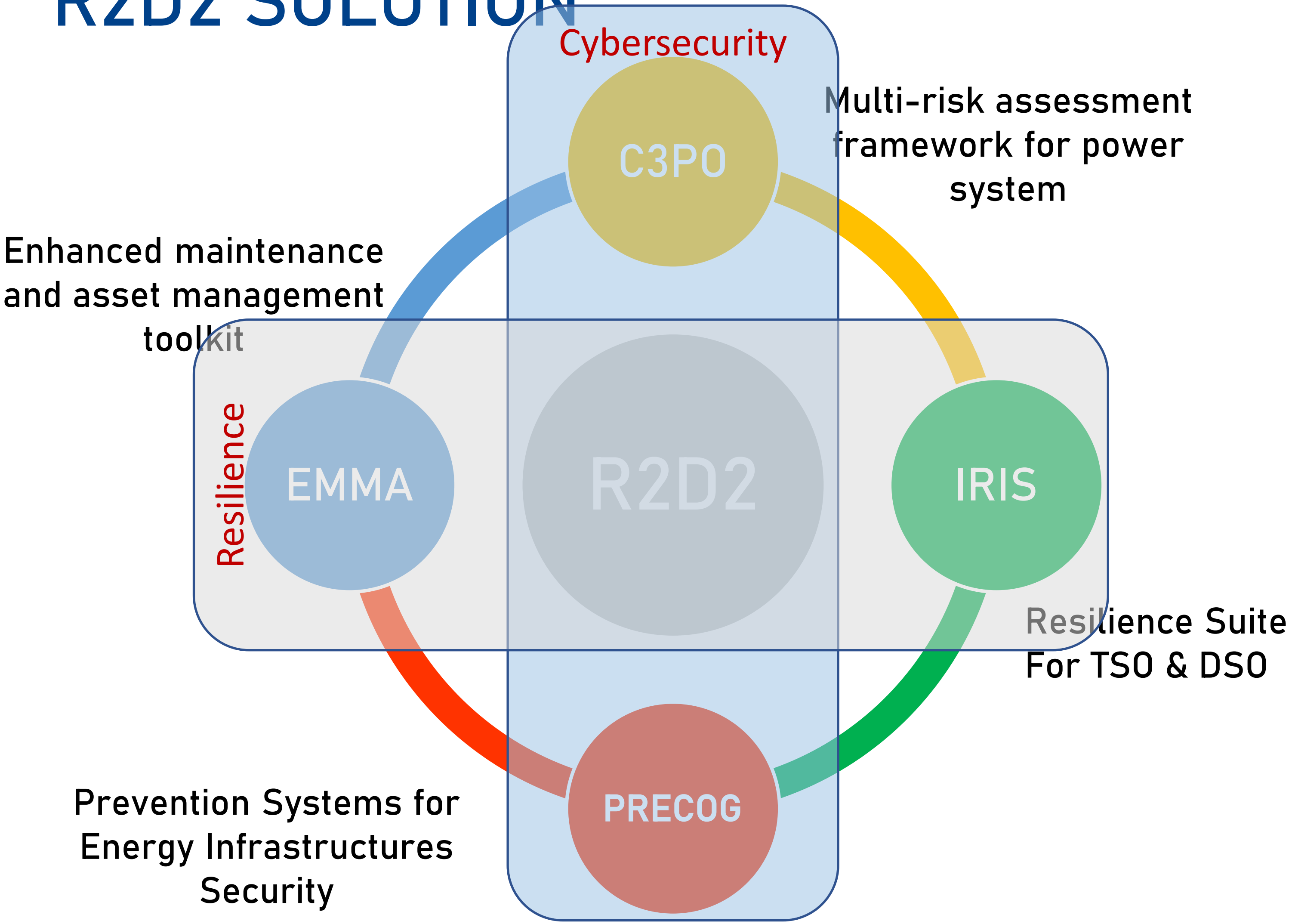
5. Improve reliability of assets through advanced data-driven solution and automated & robotic technologies

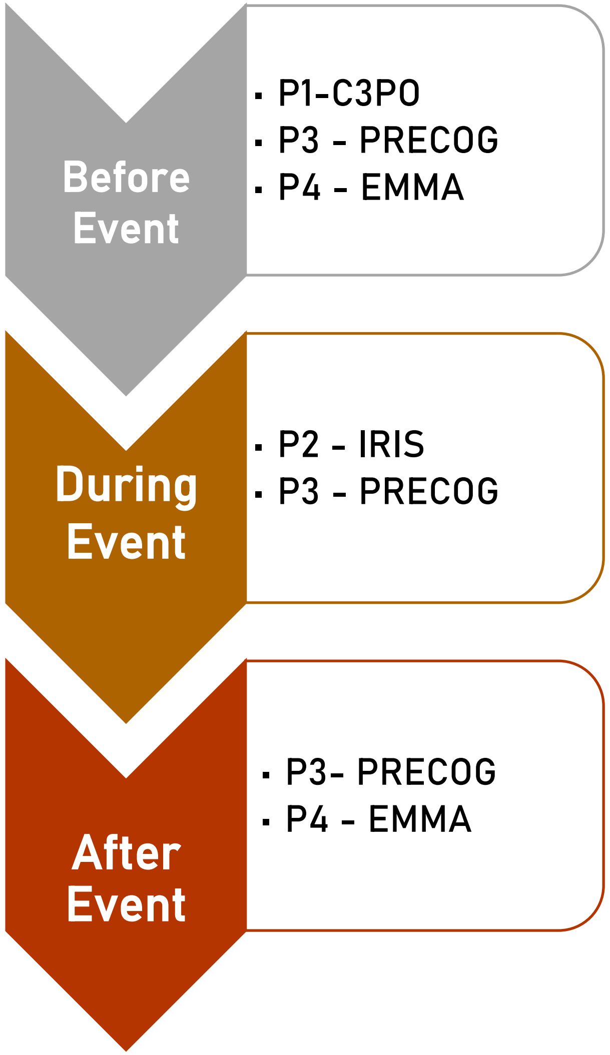
6. Demonstrate project impact and replicability potential during and beyond the project activities

7. Contribute to the development of a shared knowledge

(re)Introducing a friend: R2D2

R2D2 SOLUTION


Cybersecurity
C3PO
Multi-risk assessment framework for power system
Enhanced maintenance and asset management toolkit
Resilience
EMMA
R2D2
IRIS
Resilience Suite For TSO & DSO
PRECOG
Prevention Systems for Energy Infrastructures Security

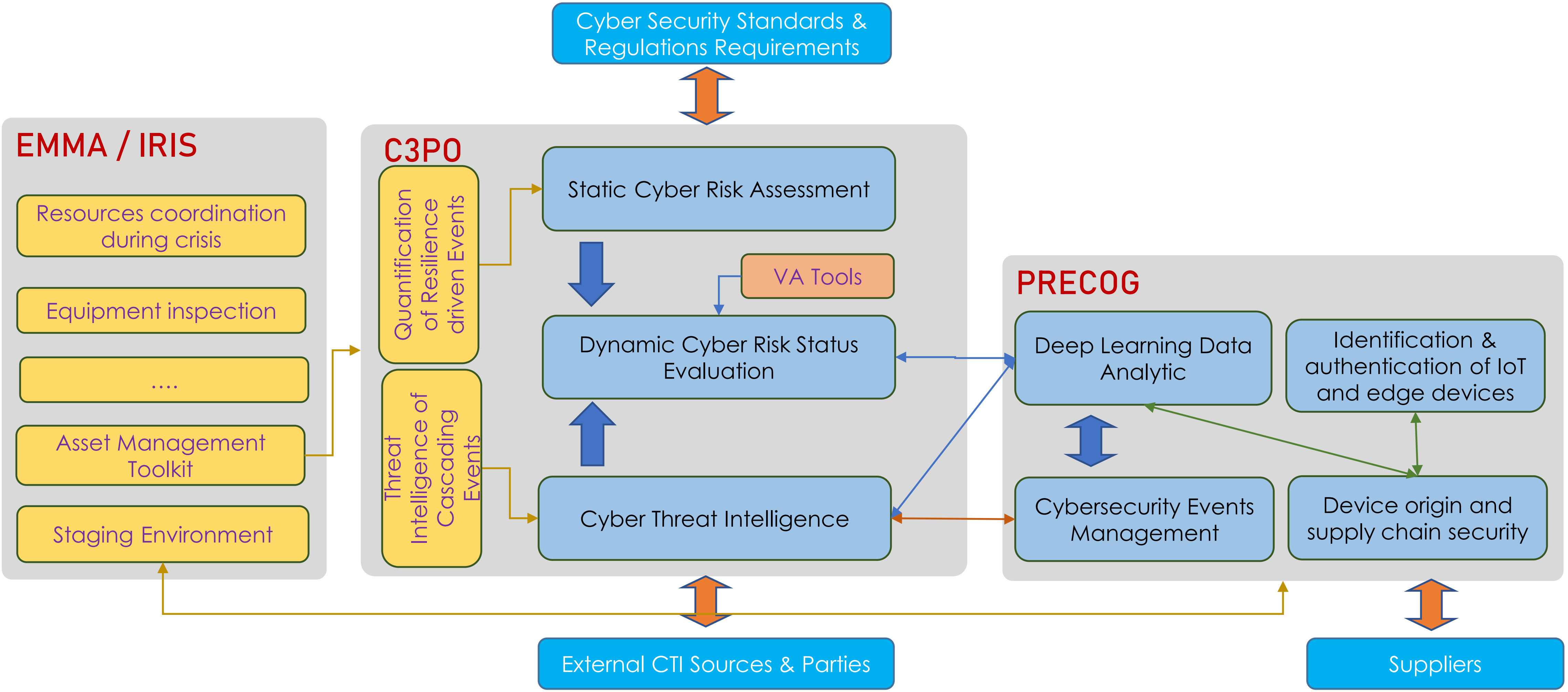


Before Event
- P1-C3PO
- P3 - PRECOG
- P4 - EMMA

During Event
- P2 - IRIS
- P3 - PRECOG

After Event
- P3- PRECOG
- P4 - EMMA

Cyber Security Conceptual Solution Diagram



Cyber Security Standards & Regulations Requirements

EMMA / IRIS

Resources coordination during crisis

Equipment inspection

....

Asset Management Toolkit

Staging Environment

C3PO

Quantification of Resilience driven Events

Threat Intelligence of Cascading Events

Static Cyber Risk Assessment

VA Tools

Dynamic Cyber Risk Status Evaluation

Cyber Threat Intelligence

PRECOG

Deep Learning Data Analytic

Identification & authentication of IoT and edge devices

Cybersecurity Events Management

Device origin and supply chain security

External CTI Sources & Parties

Suppliers

Cyber Noesis contibution

- Static Cyber Risk Assessment
- Dynamic Cyber Risk Status Evaluation
- Cyber Threat Intelligence
- Device origin and supply chain security
- …

Cyber Noesis

Securing Critical Infrastructures And Key Assets

R2D2

THANK YOU!

/ Connect with us:

www.r2d2project.eu

@R2D2EU   in @R2D2project   @R2D2EU