Accelerating the Energy Transition: **Cybersecurity, Digitalisation and the Electricity Grid in Europe**

26th February 2021

CURRENT
Enabling Network Technology throughout Europe

AGENDA

Welcome & Introduction by Robert Mork Vice President International Regulatory Affairs, Heimdall Power

- **Bas Kruimer,** Business Director Intelligent Networks & Communication, DNV-GL Netherlands Energy Advisory
- **Konstantinos Moulinos,** Energy Cybersecurity Expert, European Union Agency for Cybersecurity (ENISA)
- **Anjos Nijk,** Managing Director, European Network for Cybersecurity (ENCS)
- **Andrea Foschini,** Convenor Cybersecurity Network Code, ENTSO-E
- **Mario Jardim,** chair of T&D Europe Cybersecurity Task Force and Power Systems Cybersecurity Leader, Schneider Electric
- **John Cullinane**, formerly Chief Information Officer and Board Member, WGL Holdings
- **Rick Cutter,** Co-founder And Managing Director, Cloud for Utilities

Questions from Audience

Previous WEBINARS

1. Accelerating the Energy Transition:
   Optimized Power Grids for a Clean and Green Future (October)

2. Accelerating the Energy Transition:
   The Role that Direct Current (DC) Grids can Play (December)

3. Accelerating the Energy Transition:
   Dynamic Line Ratings for Optimised Grids (January)

All available on YouTube

CURRENT
Enabling Network Technology throughout Europe

Introduction to currENT

Our vision is a European power network that is the recognised world leader in enabling decarbonisation through the efficient use of modern grid technology.

CURRENT
Enabling Network Technology throughout Europe

Our Members

Our members develop and supply innovative technologies that optimise and maximise the use of the existing power network, to:

- Enable the integration of an increasing share of renewables
- Enhance the mitigation of climate change in line with COP 21 and the European Green Deal
- Help TSOs, DSOs and governments meet their European and national energy and climate objectives, without compromising on security of supply or affordable customer bills
- Help TSOs and governments provide fast-to-deploy solutions when the detailed needs of the medium term future are difficult to anticipate. In doing so they avoid stranded investments that customers ultimately shoulder through their bills.

SUPERNODE™

Ampacimon
Smart solutions for a dynamic grid

SMART WIRES

CURRENT
Enabling Network Technology throughout Europe

OTLM
KNILL GRUPPE

amsc

HEIMDALL POWER

LINEVISION

Bas Kruimer

Business Director Intelligent Networks & Communication, DNV-GL Netherlands Energy Advisory

CURRENT
Enabling Network Technology throughout Europe

Cybersecurity, Digitalisation and the Electricity Grid in Europe

Webinar, February 26, 2021, 11.00-12.30 CET

Bas Kruimer, business director intelligent networks & communication
DNV-GL Netherlands Energy Advisory

- will discuss the **grid of the future**, and how digitalisation will be central to managing its benefits and challenges.

CYBERSECURITY in UTILITY GRID OPERATIONS

(E+G+W)

Business Challenges

1. Reduce overall operational cost
2. Improve performance
   - *Services + capacity*
   - *Increase grid availability + safety*
   - *Security of supply + Cybersecurity*
3. Dealing with **RENEWABLE RESOURCES**
4. Adapt business model → new services

Digital Transformation

1. Data Driven Systems + Processes
2. IT-OT Integration + Data Conversion
3. Introducing IoT – Internet of Things

1. Manage the risks involved
2. Manage impact on all actors involved
3. What are the security implications

Protect **CROWN JEWELS**

Secure **BUSINESS CONTINUITY**

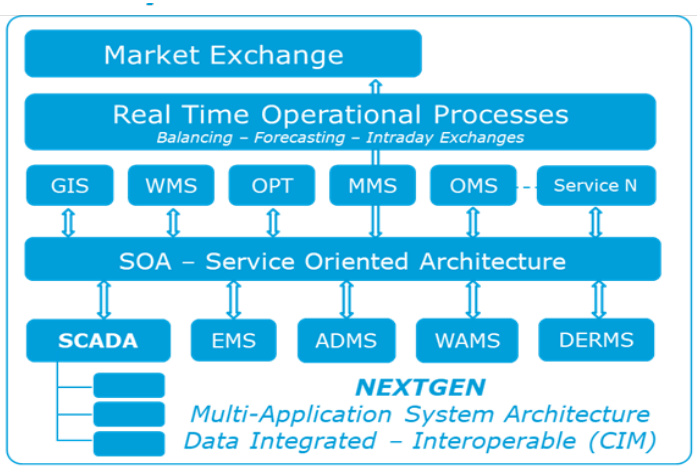
EU + Country Regulation

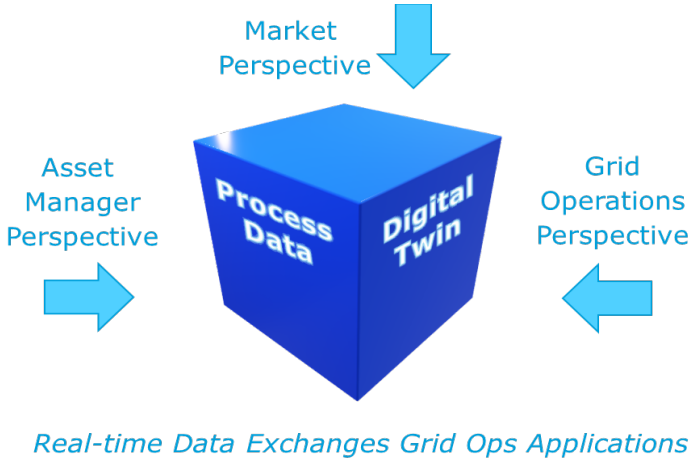
1. GDPR General Data Protection
2. **NIS** Network Information Security

ISO 27001
IEC 62351
IEC 62443

Digitalisation – Digital Transformation – Building the new Grid Ops MACHINE

Applications





Real-time Exchanges

Automation

Communication

SA RTU	Distribution Automation	Smart Meters
Transformer Sensors	Smart Cable Guard	DERMS Aggre-gators
DLR	IoT Sensors	Home Energy Mgt System

Structured DATA of Assets

Single version of the **TRUTH**
Quality Data:
- Value
- Time
- Timely

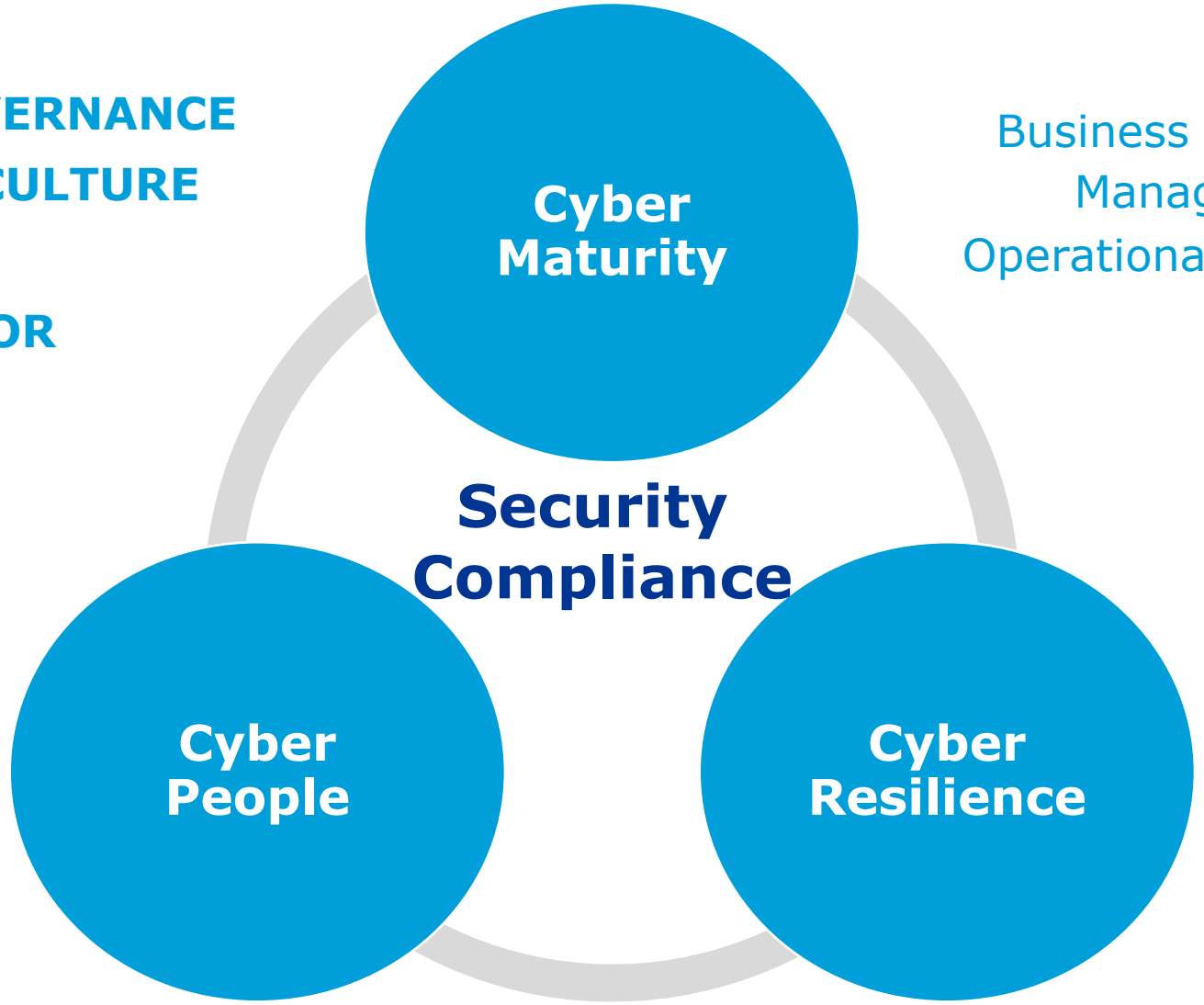
Data Exchange via **Common Data Model** many different user groups / use cases:
- internal
- external

Structured Data

Secure Architectures – Security by Design – Security Standard

The Pillars of Utility CYBERSECURITY

LEADERSHIP + GOVERNANCE
ORGANIZATION + CULTURE
Allocate FUNDING
MEASURE + MONITOR



Business Continuity
Manage Risk
Operational Excellence

Awareness
Behavior Change
Sustainable
Security
Organisation

Prepare
Protect
Detect
Respond
RECOVER
REPORT

YOU WILL BE CYBER ATTACKED…….

WHEN WILL YOU BE HACKED

HOW ARE YOU PREPARED

HOW WILL YOU DEFEND

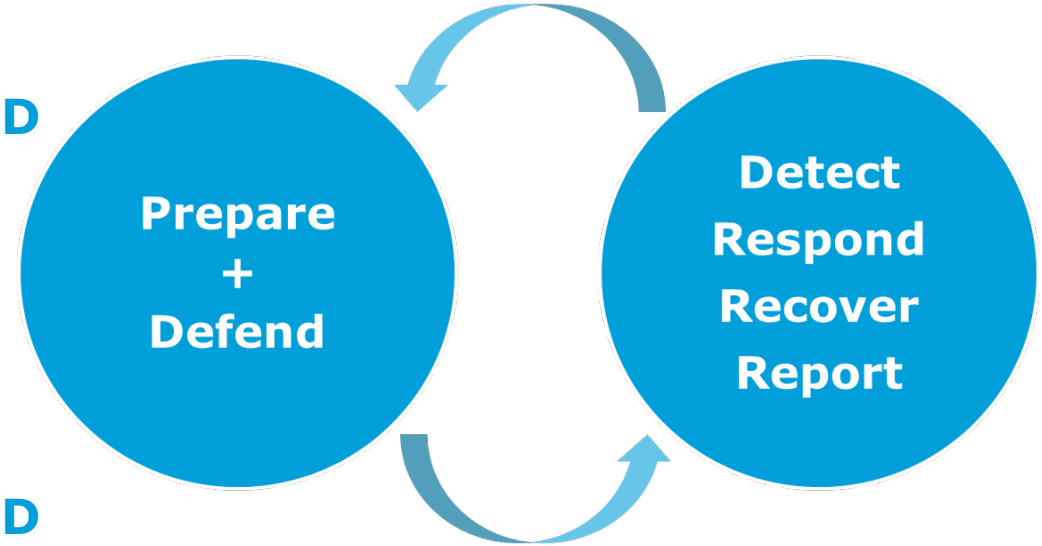
WHEN YOU WILL BE HACKED

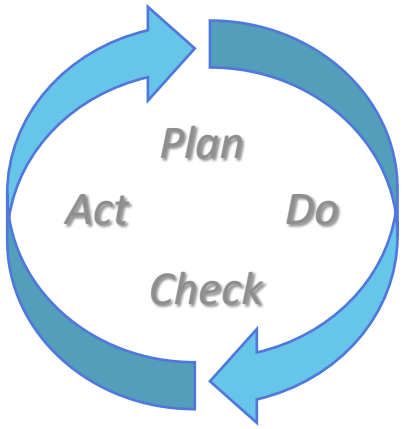
HOW WILL YOU DETECT

HOW WILL YOU RESPOND

HOW WILL YOU RECOVER

HOW WILL YOU REPORT





CYBERSECURITY

in **IT** and in **OT**

will help drive the

DSO-TSO

DIGITAL

TRANSFORMATION

Next Gen Grid Operations
Building the MACHINE

Bas Kruimer
Bas.Kruimer@dnv.com
+31 6 1506 3602

www.dnvgl.com

SAFER, SMARTER, GREENER

Konstantinos Moulinos

Energy Cybersecurity Expert,
European Union Agency for
Cybersecurity (ENISA)

CURRENT
Enabling Network Technology
throughout Europe

EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENERGY SECTOR CYBERSECURITY – ENISA ACTIVITIES

Accelerating the Energy Transition: Cybersecurity, Digitalization and the Electricity Grid in Europe

Konstantinos Moulinos, ICT cybersecurity expert, ENISA

26 | 2 | 2021

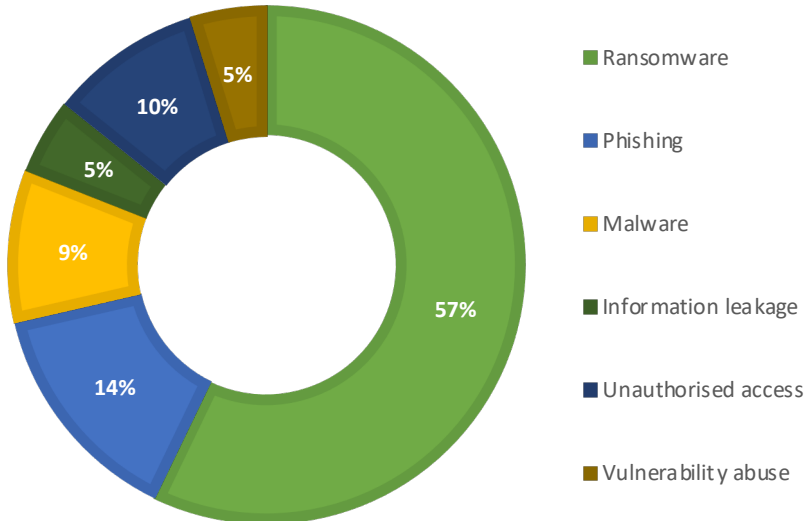
ROLE OF ENISA IN THE ENERGY SECTOR

- Build the strategic relationship with DG ENER, ACER, ENTSO-E, E.DSO
- Follow up and influence the policy making

STATE OF PLAY - ENERGY

- **Attacks against power girds are increasing**
- **NISD review**
  - New areas: power generation, electricity market operators, hydrogen etc
  - Size threshold instead of identification
  - More harmonized security requirements and incident reporting
- **ECI Directive review (CER Directive)**
- **Network code cyber security for the electricity (end 2021)**
  - Smart Grid Task Force report with recommendations to EU COM (2019)
  - ENISA has provided input to the consultation (May 2020)
  - Consultation is on going (currently informally)

ENERGY SECTORS ATTACKS 2020*



*Based on the analysis of 100 attacks in the context of EE-ISAC

ENERGY SPECIFICITIES

- **Real-time requirements**
- **Cascading effects**
- **Mixture of legacy and stet-of-the-art technology**

Commission Recommendation of 3.4.2019, on cybersecurity in the energy sector, C(2019) 2400 final

CHALLENGES

- **Collaboration with the private sector is missing from the NISD**
- **Gaps in the governance (national and EU level)**
- **Small and medium (majority of DSOs) operators are not in scope of the NISD**
- **Responsible disclosure of vulnerabilities**
- **Gaps in coordination during crisis**
- **Insufficient overview of the big picture as per the threat landscape and early warning capability**
- **Dependencies on other sectors are not taken into account**

THANK YOU FOR YOUR ATTENTION

Vasilissis Sofias Str 1, Maroussi 151 24
Attiki, Greece

+30 28 14 40 9711

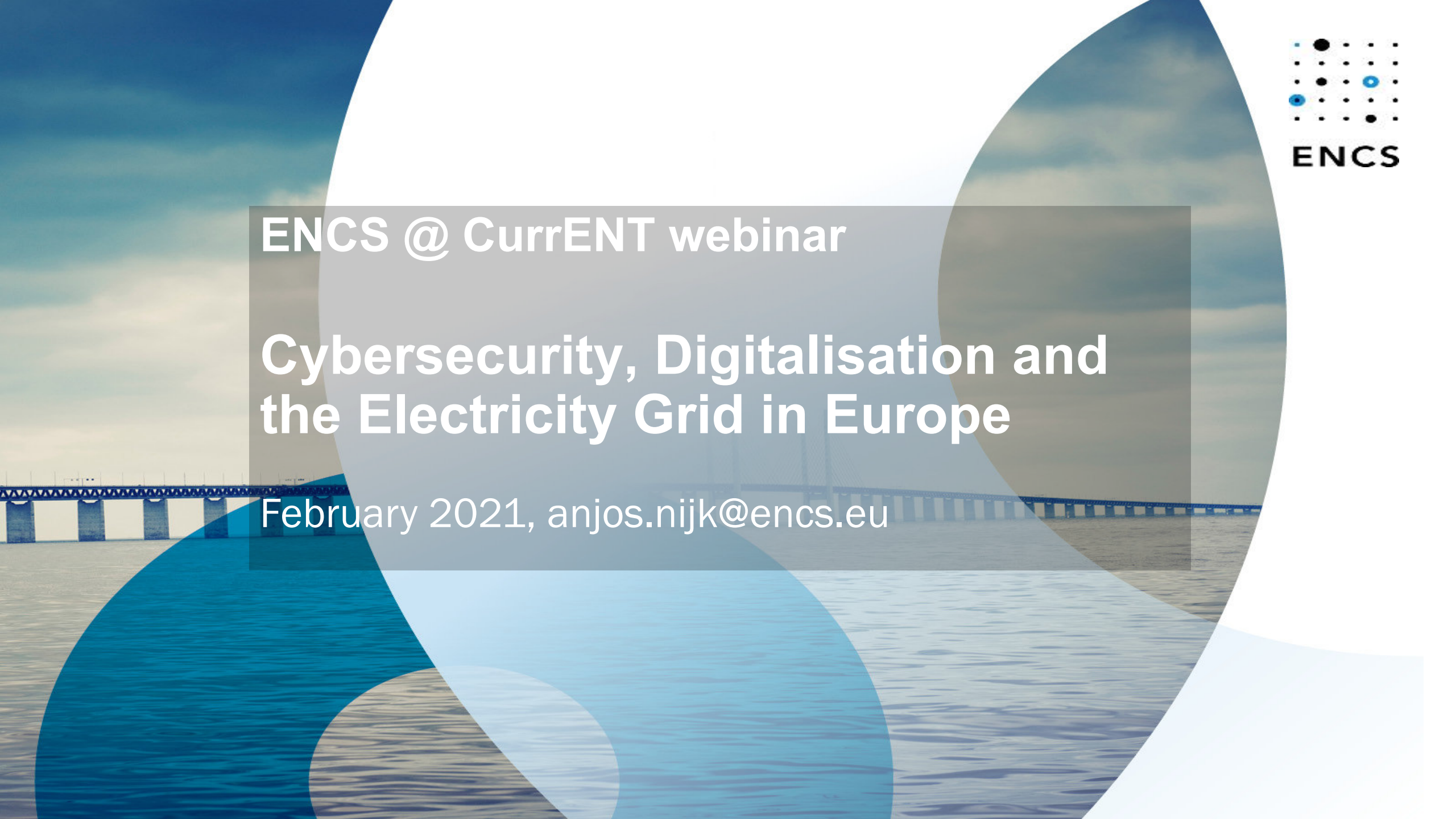
info@enisa.europa.eu

www.enisa.europe.eu

Anjos Nijk

Managing Director, European Network for Cybersecurity (ENCS)

CURRENT
Enabling Network Technology throughout Europe



ENCS

ENCS @ CurrENT webinar

Cybersecurity, Digitalisation and the Electricity Grid in Europe

February 2021, anjos.nijk@encs.eu

European Network for Cyber Security

ENCS is an independent, non-profit organization owned by grid operators that helps its members cost-effectively reduce cyber-security risks

ENCS

The emerging smart grid

more than 50 different actors

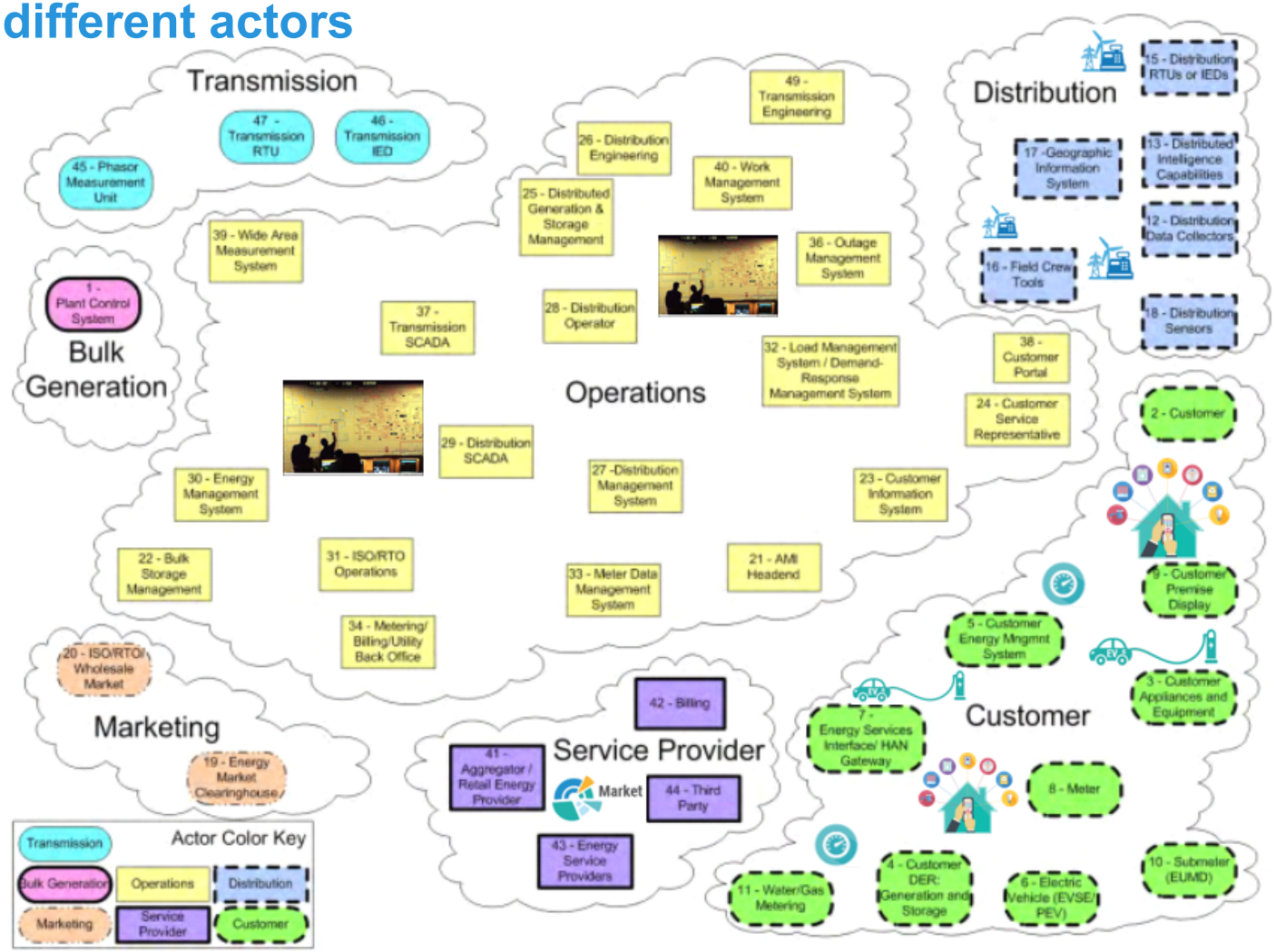


Figure 2-2 Composite High-level View of the Actors within Each of the Smart Grid Domains

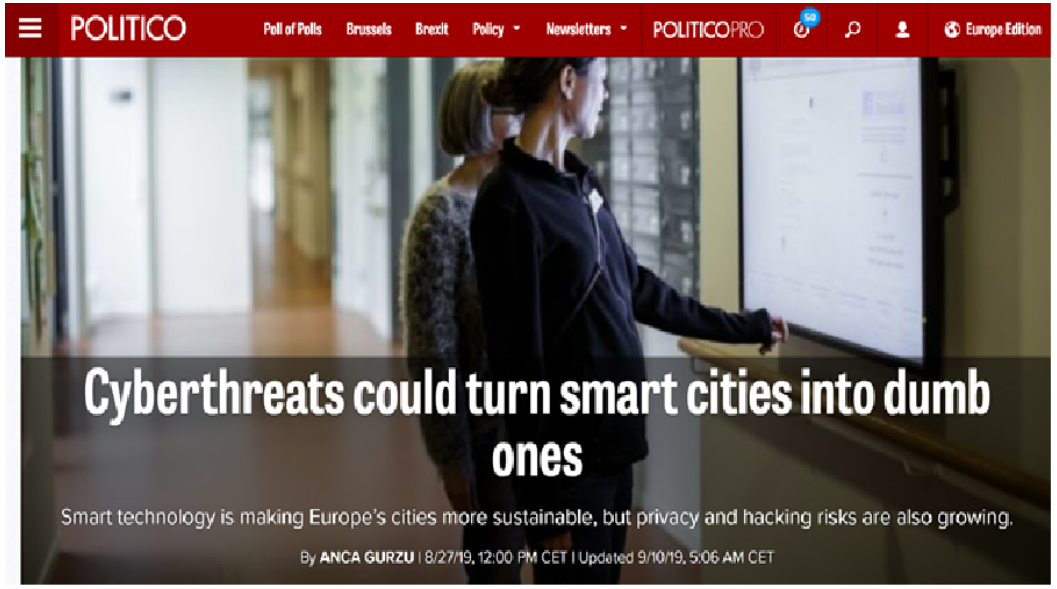
Can you hack 150,000 EV chargers?

ENCS

- Home fridge/freezer: 0.2 kW
- Hot water immersion heater: 4 kW
- Electric vehicle charging (public – Mode 3): 22 kW

Device Power Production or Consumption	Number of Same Devices Causing 3 GW Load
1 kW	3.000.000
10 kW	300.000
20 kW	150.000

Number of Devices that can cause an 3 GW Load



Are we keeping up?

ENCS

- Increasing nation state actor activity
- Increasing criminal activities - Criminals get business models working
- Fast development and distribution of malware

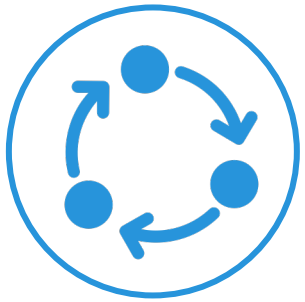
Changing the paradigm

- Attack side:
  - Thinking and acting opportunity based
  - Focus on maximum result
  - Willing to invest (skills, resources)
- Defense side:
  - Thinking and acting risk based
  - Focus on minimum level of security to protect weakest link
  - Security is considered as a cost, not a benefit

Knowledge development in three security programs

ENCS

Policy



- Security officers
- ISMS implementation (ISO 27000)
- New legislation and regulation

Architecture

- Security architects
- Secure system design (zoning)
- Procurement of secure equipment

Operations

- Security operations analysts (SOC)
- Security monitoring and incident response
- Vulnerability management

https://encs.eu/documents/

Andrea Foschini

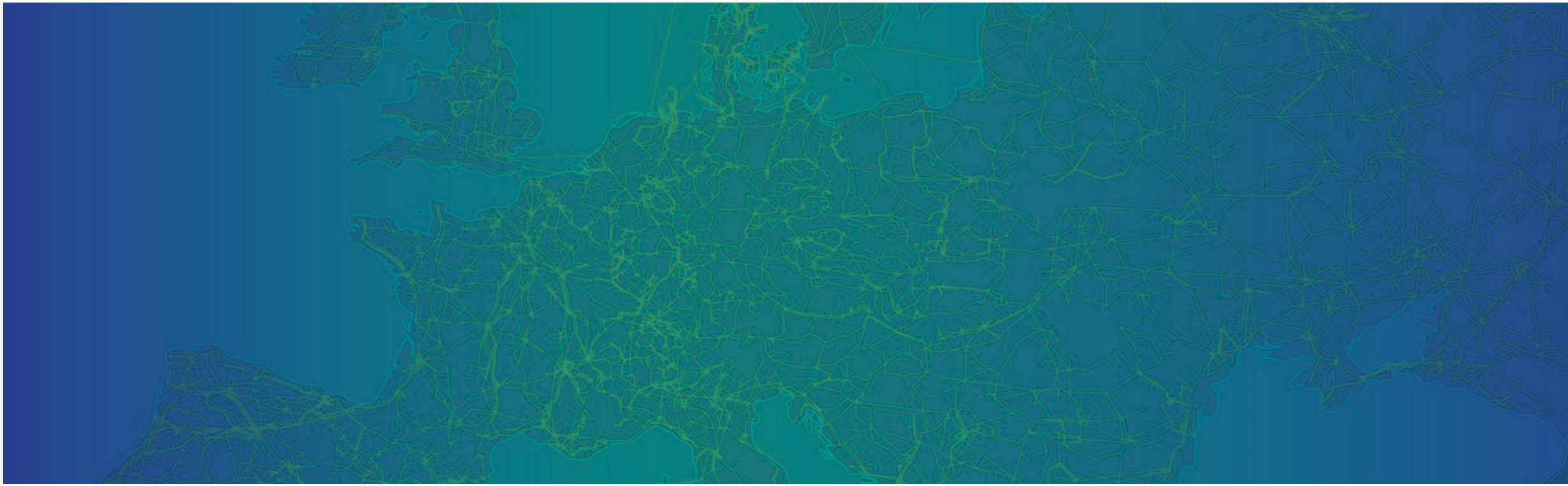
Convener Cybersecurity Network Code, ENTSO-E

CurrENT
Enabling Network Technology throughout Europe

Network Code on Cybersecurity

Energy Community Meeting, 26 February 2021

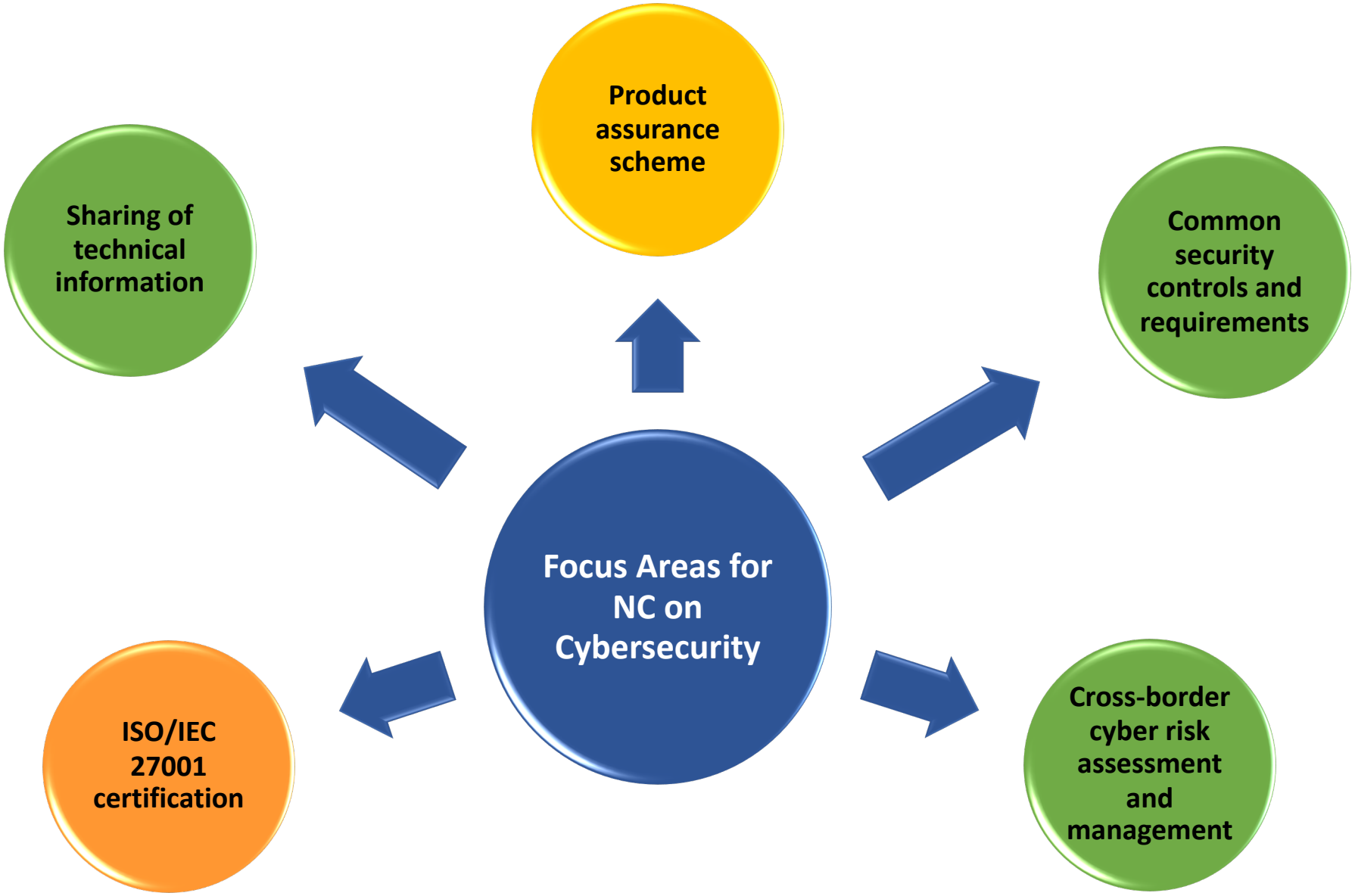
Accelerating the Energy Transition: Cybersecurity, Digitalization and the Electricity Grid in Europe



entsoe

Reliable Sustainable Connected

Network Code on Cybersecurity – Five Pillars

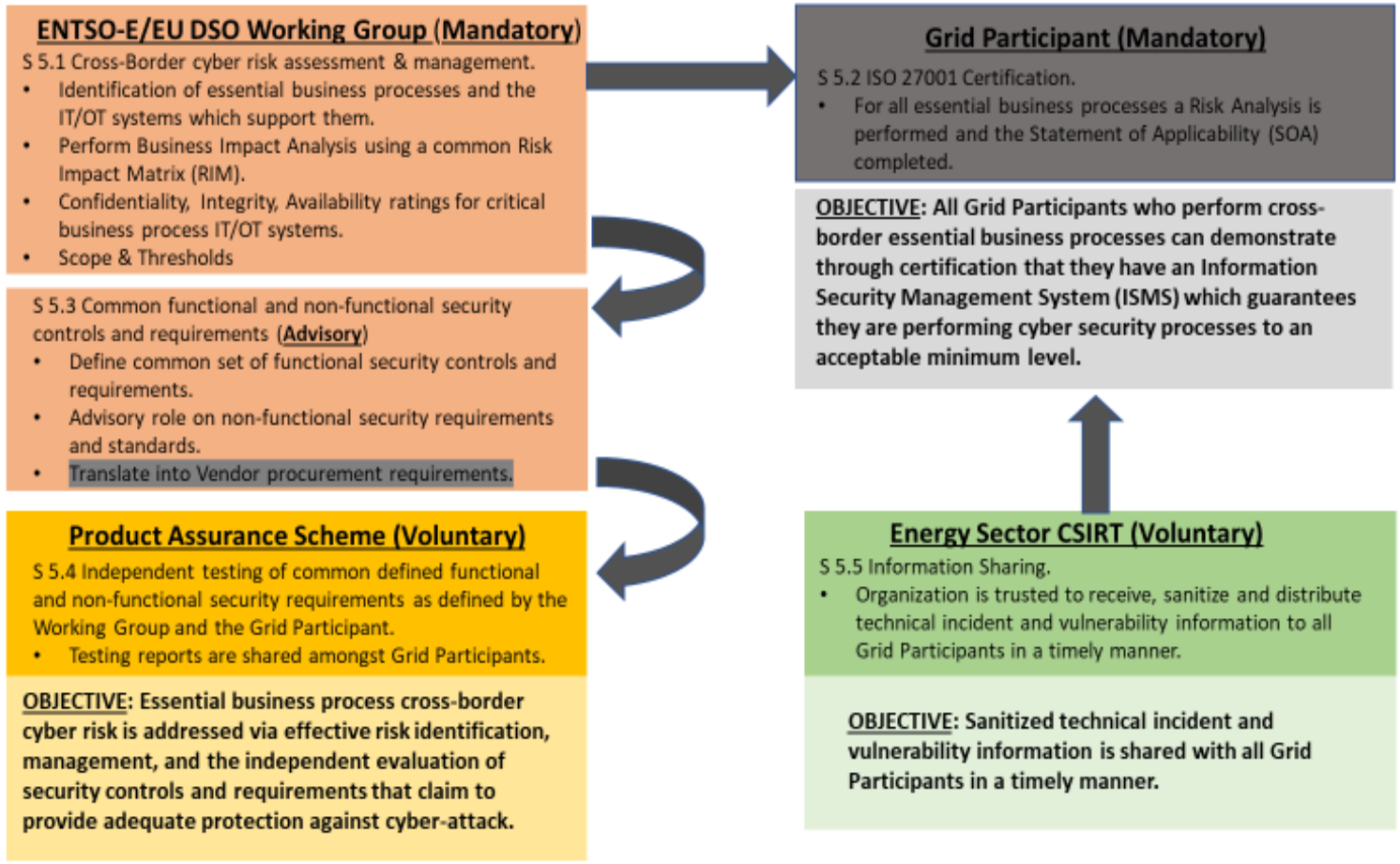


Network Code on Cybersecurity – High-level objectives

Main Actors involved:

- **European Commission.**
- **Regulators.**
- **National Autorities.**

- **Grid participant:** TSOs, DSOs, producers, energy market operators (as per *Directive (EU) 2019/944).*
- **ENTSO-E/EU DSO working group** should be formed with a mandate to perform cross-border cybersecurity risk assessments focused on operational security and safety risk.
- **European trusted Energy CSIRT** is implemented for gathering, evaluation and distributing the energy-sector specific information.



Thank you for your attention!

Backup / Details

Key points

- **Cross border cyber risk assessment -** ENTSO-E/EU-DSO working group with a mandate to perform cyber risk assessments impacting cross border transmission and/or distribution, specifically tasked with the identification of “critical business processes and events” which if successfully cyber-attacked could cause serious cross border transmission and/or distribution issues.

- **ISO/IEC 27001 certification** - Any organization (grid participant) which performs one or more of these identified cross border “critical business processes” and who meets the thresholds set will come into scope for ISO/IEC 27001 certification (mandatory), thus ensuring a common minimum-security level of Cybersecurity for all grid participants performing “critical business processes”.

Key points

- **Functional and non-functional security requirements** - ENTSO-E/EU-DSO working group with mandate to define appropriate functional and non-functional security requirements to adequately protect “critical business processes” from cyber-attack and the IT/OT systems which support them. Security controls based upon ISO/IEC 27002 and 27019, forming a common basis for the procurement of systems, components and services by all grid participants.

- **Product assurance scheme** – energy sector specific scheme, created and used to test/measure the effectiveness of systems, components and services whose security controls claim to conform to the defined set of functional and non-functional security requirements.

Key points

- **European Energy sector CSIRT (Cybersecurity Incident Response Team)** – with a mandate and trusted to receive technical incident and vulnerability information from all grid participants and disseminate this information in a sanitized form so that all grid participants can protect themselves against the same types of cyber-attack.

Mario Jardim

Chair of T&D Europe Cybersecurity Task Force, and Power Systems Cybersecurity Leader, Schneider Electric

CURRENT
Enabling Network Technology throughout Europe

T&D europe

The European Association of the Electricity Transmission and Distribution Equipment and Services Industry

CurrENT Webinar

Cybersecurity-related opportunities and challenges of digitalization in electricity networks

Mario Jardim
Cybersecurity Task Force - chair

Introducing T&D Europe

INTRODUCING T&D EUROPE

Europe's Grid Technology Providers

T&D Europe's members enable the **energy transition** to a **climate-neutral Europe** by 2050.

Over 200,000 people in our industry manufacture, innovate and supply smart systems for the efficient **transmission and distribution of electricity**.

Our technologies and services **future-proof** the grid and make **clean electricity** accessible to all Europeans.

We put our collective expertise to work to craft **a brighter, electric future**.

Ready for the Green Deal

www.tdeurope.eu

National trade association members

Corporate members

Associate members

A decade of improving cybersecurity in the energy industry

T&D europe

A long-term commitment

- Adoption of international cybersecurity frameworks - **ISO/IEC27000** and **IEC62443**
  - Information Security Management System (ISMS) implementation in production sites
  - Supply chain best practices
  - Secure design, integration & commissioning of deliverables
- Implementation of dedicated cybersecurity organizations and CERT teams
- Adoption and enforcement of **secure development** processes lifecycle (IEC62443-4-1)
- Internalization of security by design principles in **product and system** development

Active involvement in energy policies & standardization

- Active contributors to DG-ENER Smart Grid taskforces expert groups
  - Member of **EG2 editorial team** for the recommendations of CS grid codes
- EU Commission / DG-ENER consultations
- Participation in EU and international **cybersecurity standardization** activities :
  - Frameworks
  - Systems
  - Products security
  - Process security
  - Communications security
- Cybersecurity and system interoperability testing activities

The way forward

Open points & concerns

- Focus on **holistic system view** – mission, risk assessment, resilience objectives, system design, defense in depths strategy, deployment and operation
  - Special attention to very **long product lifespan** (20 years) opposed to consumer goods
    - Long term cybersecurity support vs. a one-time product certification
    - Patch management, vulnerability management
  - Cybersecurity **interoperability** of solutions from different suppliers, integrators and service providers
- Security for decentralized energy systems down to low voltage distribution
  - DER system interfaces including electro mobility
- System & products baseline minimum security requirement based on **international standards**
- International cybersecurity **certificates recognition** by EU authorities
- Sufficient industry participation in the **cybersecurity grid code** writing process

Mario Jardim

Schneider Electric

Power Systems - Cybersecurity leader

mario.jardim@se.com

www.tdeurope.eu

@BetterGrids

Rick Cutter

Co-Founder and Managing Director, Cloud for Utilities

John Cullinane

Formerly Chief Information Officer and Board Member, WGL Holdings

CURRENT
Enabling Network Technology throughout Europe

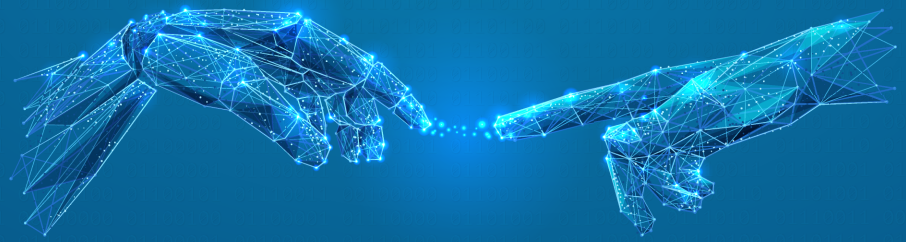
CLOUD FOR UTILITIES

currENT: Accelerating the Energy Transition: Cybersecurity, Digitalization and the Electricity Grid in Europe

Friday, February 26, 2021

Cybersecurity from a US Utility Perspective

CLOUD FOR UTILITIES



THE WALL STREET JOURNAL.
MEDIA PARTNER

2021 Digital + Cloud Summit — July 26-30

- It is well understood that cybersecurity has become as important a concern for utilities as the kinetic infrastructure it serves

- For many utilities, IT teams continue to design and manage traditional closed system architectures due to security concerns *but* this is changing

- Digitalisation is driving new approaches to hybrid designs for control environments

- Our direct experience includes adoption of cloud services for peripheral control environment use cases
  - Secondary recovery services
  - AAA services (automation, analytics and AI)
  - Cyber monitoring & testing

- Adoption of a formal scorecard/dashboard of cyber indicators bridges the gap between tactical IT Team(s) and executive leadership (speaking the same language)
  - Ask the question, how do you know what you don't know?

2021 Digital + Cloud Summit — July 26-30

- Public/private partnerships have been successful in reducing risk
  - EEI/AGA
  - United States Department of Homeland Security
    - INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM (ICS-CERT)
- Policies, guidelines and cyber framework aren't enough to fully safeguard the control environments
- Best design practices coupled with continual monitoring, multi-variable threat and vulnerability analysis and a *great team is* needed to manage high-integrity environments
- Operating a highly effective cyber environment allows for easier adoption of new capabilities
  - Establish and implement security requirements prior to adopting the new capability

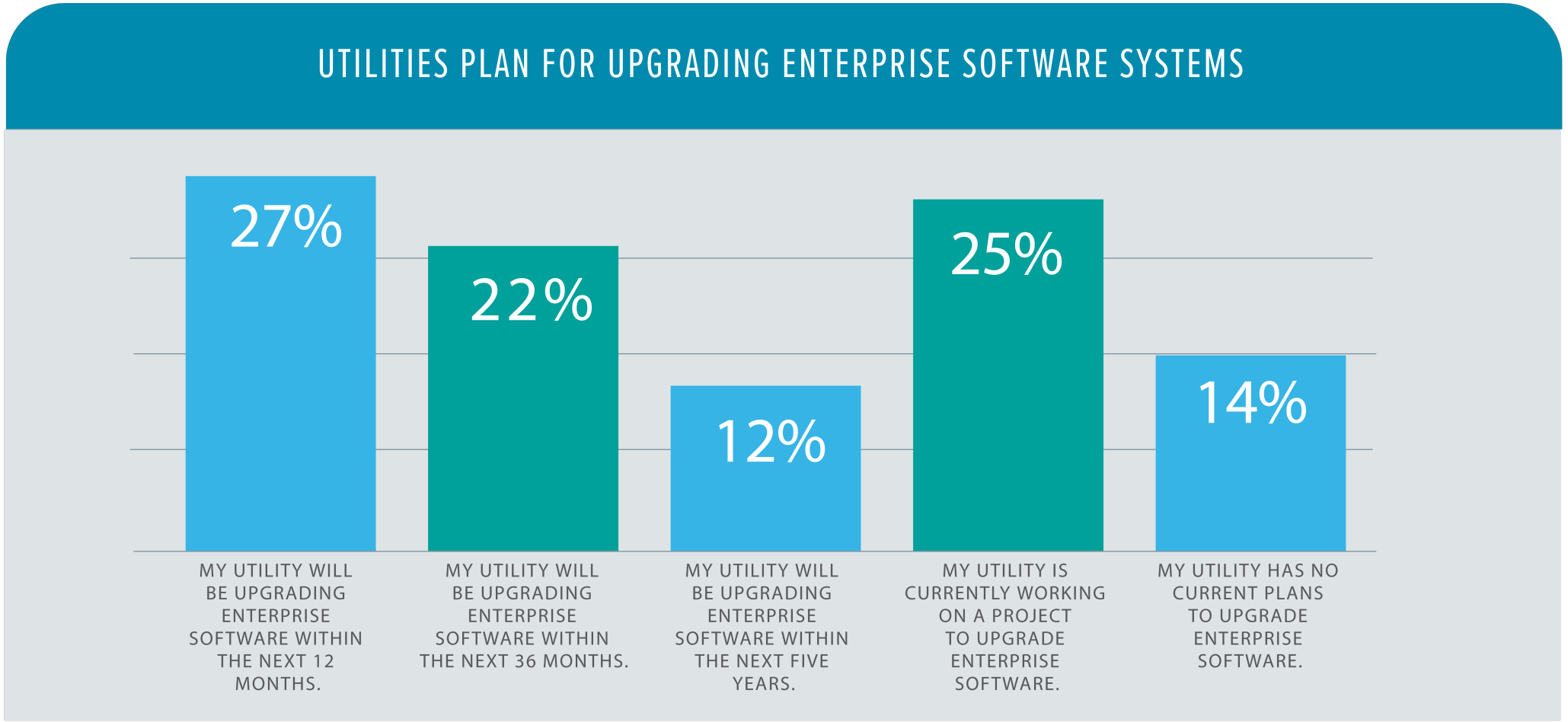
Cloud as a Digitalization Enabler

CLOUD FOR UTILITIES

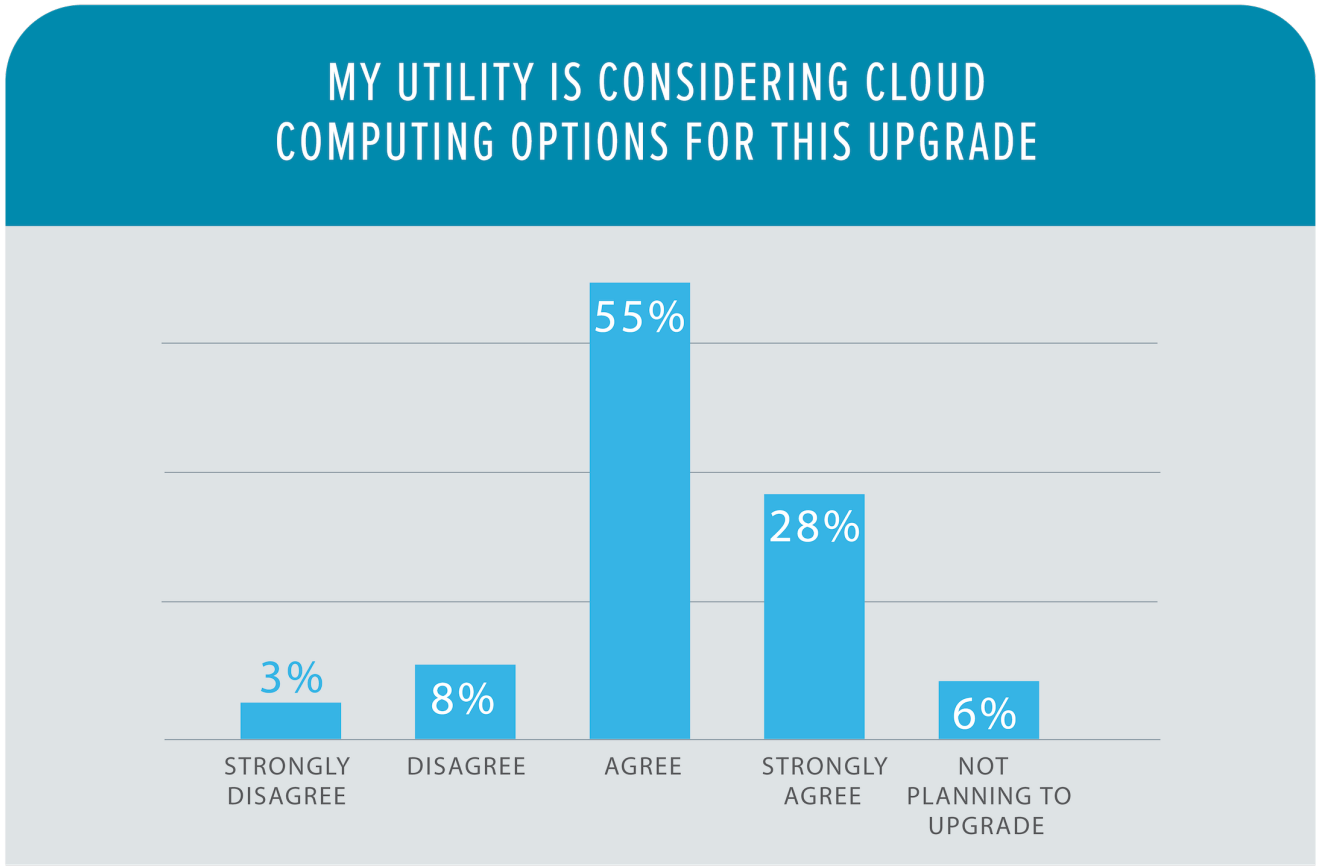
THE WALL STREET JOURNAL.
MEDIA PARTNER

2021 Digital + Cloud Summit — July 26-30

- Pre-Covid Survey published February 2020
- 152 US Utilities were surveyed



2021 Digital + Cloud Summit — July 26-30



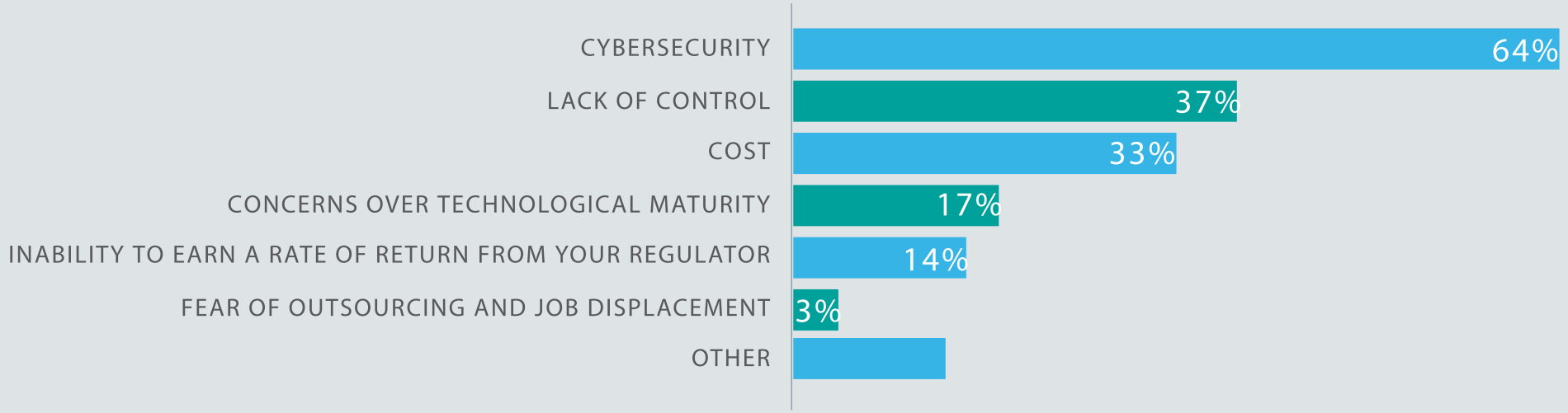
The affirmative responses (83%) have increased by 28.5% from 2017

CLOUD FOR UTILITIES

THE WALL STREET JOURNAL.
MEDIA PARTNER

2021 Digital + Cloud Summit — July 26-30

THE IMPEDIMENTS TO CHOOSING CLOUD OPTIONS (SAAS, IAAS, PAAS)



For the past five years cybersecurity has been among the top 5 enterprise risks for utilities in the United States. We expect this to continue for the foreseeable future

CLOUD FOR UTILITIES

Thank you!

Cloudforutilities.org

Thank you for your attendance

To keep up to date with our activities:

info@currenteurope.eu

https://www.linkedin.com/company/current-europe/

@CurrentEurope

currENT Europe

www.currenteurope.eu

CURRENT
Enabling Network Technology throughout Europe