**Critical Infrastructure Protection:** Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

**Project: H2020–CIP-01-2016–740898**

# *Critical Energy Infrastructure Security Stakeholder Group Manifest*

## Defending the European Energy Infrastructures

**November 2017**

European Commission

DEFENDER

# Defending the European Energy Infrastructures

**Project: H2020–CIP-01-2016–740898**

# Critical Energy Infrastructures
# Security Stakeholder Group Manifest

**Abstract:**

The H2020-740898 DEFENDER project is the result of the EC selection towards Securing Critical Energy Infrastructures (CEI). Backed by a consortium of 19 leading European technological and legal companies, utilities, Law Enforcement Agencies and research Institutions, DEFENDER aims to offer technological innovations and advances to safeguard existing and future European CEI operation over cyber-physical-social threats.

Beyond the technological innovations, DEFENDER aims to create a safer and more sustainable European CEI ecosystem based on a “culture of security”, supported by the initiation of a Pan-European Critical Energy Infrastructure Security Stakeholder Group (CEIS-SG), which will guide and integrate the Energy Infrastructure sector’s continuous effort to improve the security and resilience of its critical infrastructure.

This manifest aims to initiate the CEIS Stakeholders Group, as a think tank and information exchange ecosystem targeting safer and more sustainable European Critical Energy Infrastructures.

# Disclaimer

This document may contain material that is copyright of certain DEFENDER beneficiaries, and may not be reproduced or copied without permission. All DEFENDER consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The DEFENDER Consortium is the following:

| Participant number | Participant organisation name | Short name | Country |
|---|---|---|---|
| 01 | Engineering-Ingegneria Informatica SPA | ENG | Italy |
| 02 | THALES Research & Technology | THALES | France |
| 03 | SingularLogic S.A. | SiLO | Greece |
| 04 | SIEMENS SRL | SIEM | Romania |
| 05 | Ineo Energy & Systems (Energy Generation) | ENGIE | France |
| 06 | Studio Tecnico BFP srl (Wind Farms/SME) | BFP | Italy |
| 07 | Electricity Transmission Operator (TSO) | ELES | Slovenia |
| 08 | ASM Terni SpA (DSO) | ASM | Italy |
| 09 | Ministero Dell' Interno | PdS | Italy |
| 10 | Dr. Frucht Systems Ltd | DFSL | Israel |
| 11 | Venaka Media Limited | VML | UK |
| 12 | Power-Ops Limited | POPs | UK |
| 13 | e-Lex | ELEX | Italy |
| 14 | Institute for Corporate Security Studies | ICS | Slovenia |
| 15 | Rheinisch-Westfälische Technische Hochschule Aachen | RWTH | Germany |
| 16 | TEI of Sterea Ellada/Electrical Engineering Dept. | TEISTE | Greece |
| 17 | Uninova | UNI | Portugal |
| 18 | Jožef Stefan Institute | JSI | Slovenia |

The information in this document is provided “as is” and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

# Table of Contents

# Acronyms

| | |
|---|---|
| B2B | Business to Business |
| B2C | Business to Customers |
| CEI | Critical Energy Infrastructures |
| CEIS-SG | Critical Energy Infrastructures Security Stakeholders |
| EC | European Commission |
| EV | Electrical Vehicles |
| H2020 | Horizon 2020 |
| IT | Information Technology |
| LEA | Law Enforcement Agency |
| LPT | Large Power Transformer |
| O&M | Operation and Management |
| PV | Photovoltaic |
| RES | Renewable Energy Sources |
| SCADA | Supervisory Control and Data Acquisition |

# 1 Introduction

In early 2016, the European Commission under the Horizon H2020 (H2020) framework initiated a Call for Proposals (H2020-CIP-01) towards the protection of the following critical infrastructures: Water Systems, Energy Infrastructure, Transport Infrastructure and means of transportation, Communication Infrastructure, Health Services, Financial Services. The objective of the call has been to create Innovation Actions that should cover: prevention, detection, response, and in case of failure, mitigation of consequences over the life span of the infrastructure, with a view to achieve the security and resilience of all functions performed by the installations, and of neighbouring populations and the environment.

The H2020-740898 DEFENDER (Defending the European Energy Infrastructures) project is the selection towards Securing Critical Energy Infrastructures (CEI). Backed by a consortium of 18 leading European technological and legal companies, utilities, LEAsand research Institutions, DEFENDER aims to offer ***technological innovations*** to safeguard existing and future European CEI operation over cyber-physical-social threats. The DEFENDER project will adapt, integrate, upscale, deploy and validate a number of different technologies and operational blueprints with a view to develop a) novel protective concepts for lifecycle assessment, resilience and CEI self-healing systems, offering "security by design" and b) advanced intruder inspection and incident mitigation systems. Beyond the technological innovations, DEFENDER aims to create a safer and more sustainable European CEI ecosystem based on a "***culture of security"***, where trusted information exchange between trained employees, volunteers, CEI operators and LEAs and underlying novel cooperative sharing business models will complement cyber-physical protection, while preserving the privacy of the citizens involved.

The Culture of Security will be further triggered by the set up of a ***Pan-European Critical Energy Infrastructure Security Stakeholder Group (CEIS-SG).*** The purpose of the CEIS-SG is to help, guide and integrate the Energy Critical Infrastructure sector's continuous effort to improve the security and resilience of its critical infrastructure and to describe how the Energy Sector contributes toward the European critical infrastructure security and resilience goals. Specifically, it includes the discussion of the many evolving risks and threats in the Energy Sector, as well as an increased emphasis on the Energy and cross-sector interdependency issues.

The CEIS-SG will be a group of executive volunteers and decision makers to share information on CEI risks, incidents, threats and countermeasures, exchange best practices, periodically review and challenge risk management practices to confirm that established security controls remain in place and changes in the energy delivery system or emerging threats do not diminish their effectiveness.

The CEIS-SG ecosystem will promote:

1) Information sharing at pan-European level on CEI threats and best security practices;
2) Risk-informed decision-making and the tools and mechanisms to facilitate it;
3) Adaptive learning, where experiences serve as opportunity to inform and adjust future actions;
4) CEI security preparedness planning and roadmap towards securing Critical Energy Infrastructures.

This document is the manifest towards the initiation of the CEIS Stakeholders Group and a safer and more sustainable European CEI.

# 2 Energy Sector Overview

Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks, and most importantly ***combined cyber-physical attacks***, which are much more challenging and it is expected to become the most intrusive attack**.**

This is particularly true for the **Critical Energy Infrastructures (CEI)**. As reported by the US Department for Homeland Security, during 2015, the Industrial Control Systems Cyber Emergency Response Team responded to 245 incidents; the Energy sector tops the list with 79 incidents (32%)[1]. Taking into account the importance of energy in our life and its influence to other critical infrastructures, CEI requests significant attention.

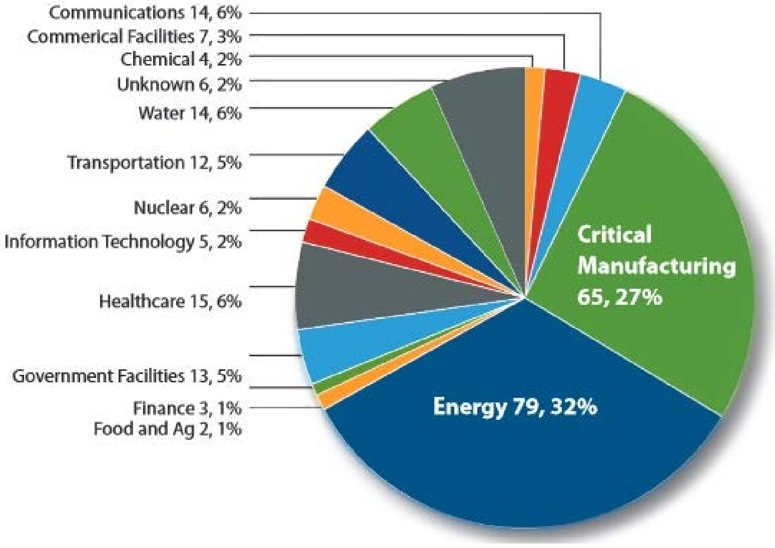

**Figure 1: Incidents of Cyber Attacks in US in 2015**

Today, CEI are characterized by vast, geographically-dispersed, widely-diverse infrastructure of assets forming a multifaceted operational environment with complex ownership and regulatory structures, accompanied by ubiquitous human involvement at different levels (CEI O&M, monitoring & control). Indeed as shown in Figure 2, Critical Energy Infrastructure is composed of power generation plants, either traditional (e.g. fossil fuelled, hydro-electric plants or nuclear plants) or distributed Renewable Energy Sources (RES) generation plants (either photovoltaic PV Parks or Wind Farms), which all together fulfil the electrical energy demands as requested by energy consumers, transmission and distribution networks and energy producers/Consumers (prosumers) end-users and Electrical Vehicles (EVs).

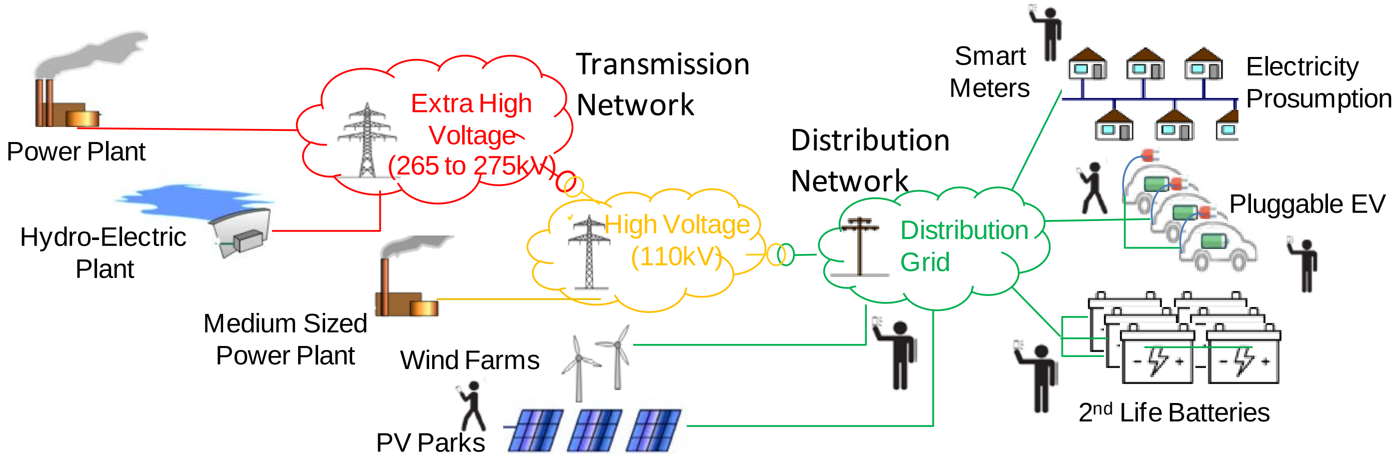

**Figure 2: Critical Energy Infrastructure**

**The power Transmission System and the power Distribution Grid Network Infrastructure** lie at the very heart of any CEI system. A lot of existing advanced monitoring and control technologies are able to effectively deal with either physical (due to natural hazards or malicious attacks, including terrorism actions) either technical (e.g. due to abnormal operating conditions as a result of accidental faults caused by infrastructure aging or by instability created by intermittent decentralized RES power generation), or cyber-security threats at individual level. However, the reciprocal interaction and related impacts of threat types is not adequately captured and accordingly managed.

As for the CEI generation side, the traditional **Power Generation Plants** (i.e. fossil fuelled, hydro-electric plants and nuclear plants) are now more and more complemented by **renewable energy sources (RES)**, such as wind farms and photovoltaic (PV) parks. As a matter of fact, on Sunday 15 May 2016, RES supplied nearly all of German domestic electricity demand [2], while on 6 June 2016, North Sea region countries (Belgium, Denmark, France, Germany, Ireland, Luxembourg, the Netherlands, Norway and Sweden) agreed to create good conditions for the development of offshore wind energy hinting that RES sites proliferation is a manner of time [3]. Like network assets, generation plants represent key CEI's facilities, exposed at both cyber and physical attacks. Such attacks may result in insufficient generation capability and power supply interruption at the end-users' side, which may, in turn, negatively affect business activities for a variety of (mainly business-oriented) end-users. Although bulk generation plants are usually more susceptible to physical threats, smaller scale intermittent RES generation plants may be widely exposed to both physical and cyber threats; the lower security requirements derived from the growing usage of interoperable IT management platforms and communication protocols are introducing new security gaps in the dispersed generation networks, making CEI security overarching difficult to manage, hence more susceptible to attacks that could wreck enormous damage on the entirety of a CEI. As such, ***Cyber-Physical protection* of CEI generation sites is of paramount importance**.

In parallel, the energy customers become ***energy prosumers*** in a new, decentralized open electrical energy production framework, allowing everyone to actively interact with the energy system. Smart devices and the related IT management platforms deployed at the level of decentralized energy resources (i.e. prosumers) such as *Smart Meters* and *Smart Inverters*, offer many advantages to B2B (and B2C via aggregators) consumers and the utilities as they can cooperate directly in a variety of collaborative value added flexibility provisioning services. The existence of energy prosumers incur additional cyber risks, stemming from the lack of definite data protection and privacy management tools, potentially allowing for the disclosure of confidential information on electricity consumption and load shapes hence negatively affecting the prosumer entrepreneurial activity. As such ***Cyber protection of CEI* last-mile is also mandatory**.

Last but not least, **humans** should be brought in the front of the effective CEI security management lifecycle, by considering different perspectives. People may be effectively used as virtual sensors to contribute to threat detection and can be eventually leveraged as **first order responders** to accidents, disasters or attacks, given that data privacy requirements are met. Interestingly, they should be simultaneously considered as potential threats subject to detection and mitigation, when potential non malicious workforce activities are considered e.g. due to lack of experience, insufficient training or lack of motivation, or attention, etc.

**CEIS-SG Vision:** The European Union should protect legacy CEI and design a new generation of more resilient and self-healing European Critical Energy Infrastructure able to survive large scale, combined, cyber-physical-social incidents and accidents, and guarantee the continuity of operations, while minimizing their cascading effects in the infrastructure.

# 3 Critical Energy Infrastructures' threat categories

The risk environment of the Energy Sector continues to evolve over time as technology advances, market patterns shift, and environmental factors. Risk is defined as a function of consequences: human and economic, vulnerabilities and threats.

Various organizations, from government(es. LEAs) and research institutions, conduct a wide variety of risk and threats assessments of the Critical Energy Infrastructure. Considerable media attention has also been devoted to threats towards energy infrastructure, including physical and cyber security threats, natural disasters, space weather events, and possible terrorist attacks. Once threats have been identified, consequences and vulnerabilities can be quantified to determine the cost benefits of risk mitigation measures. In many cases the consequences may be even cascading towards other critical infrastructures. However, the types of threats faced by the electricity infrastructure vary widely, as well as the meaning of "risk" as perceived by each organization. This section provides a high-level overview of the various types of risks and threats in the Energy Sector.

## 3.1 Energy Infrastructure main risk categories

Based on literature studies [1][4][5][6][8] and on the CEIS-SG and the DEFENDER consortium (i.e. Energy Utilities, IT companies, law companies, research institutions) extensive expertise in securing critical infrastructures and cyber security, a wide variety of issues were considered CEI Security threats. Despite the differences in what constitutes risk, several issues as the key risks and threats are identified:

- Physical Security and Resilience
- Natural Disasters and Climate Resilience
- Aging Infrastructure and the risk of low Infrastructure investment
- Cyber security threats;
- Growing gap in workforce development
- New unknown risks emerging from the combination of cyber and physical attacks and risk assessment

The CEIS-SG will collaborate with many initiatives to address the following evolving risks & threats in CEI, also providing feedback to other critical infrastructure authorities.

**CEIS-SG Goals:** Assess and analyze physical, human and cyber threats and vulnerabilities of Critical Energy Infrastructures and their cascading consequences to interrelated Critical Infrastructures and secure the existing and new CEI at pan-European level through informed risk management, risk mitigation activities and countermeasures deployment, while accounting for the costs and benefits of security investments.

### 3.1.1 Risk 1: Physical Attacks

Electric power generation, transmission and distribution systems are susceptible to physical attacks, with generally little risk to the attacker. Specific points of vulnerability and physical terrorist attacks can be better understood by considering each major element of power systems: generators, substations, transmission towers, natural gas pipes, distribution components, system control centres.

Indicatively, in April 2013, attackers used high-powered rifles to destroy several transformers at a transmission substation in USA (California). Although the targeted utility avoided a blackout, the incident incurred more than $15 million in damages that required nearly a month to repair [7].

The Critical Energy Infrastructure also faces significant physical security risks, ranging from stealing the copper from the Energy Infrastructure network components, in many cases cutting off links and loops even under significant voltage, to attacks to the physical electric infrastructure such as Large Power Transformers (LPTs) and the infrastructure that control cyber components. Physical attacks to the grid can "*adversely impact the reliable operation of the Bulk-Power System, resulting in instability, uncontrolled separation, or cascading failures*." [8]  Though there are LPT manufacturers (e.g. ABB, Siemens) and one of the most important LPT testers (DNV-GL) within the European Union supply and procurement of LPTs can be challenging, as it can take more than 12 months to replace an LPT due to its long and complex procurement process. Recent terrorist attacks in Belgium, France and Germany have shown that terrorists are closer than we think.

The overwhelming majority of attacks (74%) on energy targets during 2010-2014 were bombings. Even though bombings were also the most common attack type for terrorist incidents in general during this time period, they accounted for a lower percentage (54%) as compared with attacks on energy targets. Facility and infrastructure attacks, which include arson and sabotage tactics, are the second most common type of attack against energy targets. They are also more than twice as prevalent, accounting for 11% of attacks, as compared with terrorist incidents in general (4.5%)[9].

### 3.1.2 Risk 2: Natural Disasters

Extreme weather-related events, including lightning and storms, have historically been the biggest threat to CEI. Natural disasters, such as floods, earthquakes, forest-fire and others, may significantly impact the transmission and distribution network, and the reliability of electricity grids.

Though early energy production and distribution systems are designed to respond to weather variability such as daily changes in temperature, CEI is vulnerable to direct impacts from severe weather events and extreme weather disasters. Specifically, in US, hurricane Sandy in October 2012 cut power to more than 10 million homes and businesses in 17 states along the East Coast, in some cases for weeks [11].

Europe is also vulnerable to extreme weather-related events and natural disasters. In 2014, storm Darwin left about 280,000 electricity citizens in Ireland without supply, while in October 2017, due to storm Ophelia, approximately 360,000 electricity customers were left without power as a result of over 3,200 individual faults on the network across the Ireland. ESB announced that “Fallen trees on overhead lines are responsible for most of the damage to the network,… five to ten per cent of those who’ve lost supply may not see their electricity back for more than 10 days”[12].

### 3.1.3 Risk 3: Aging Energy Infrastructure and Assets

Significant numbers of critical infrastructure assets (such as poles, electrical equipments, substations), in the US have reached or are approaching the end of their designed life span [13]. The situation is similar or even worse in many EU critical energy infrastructure components. Although an infrastructure does not fail because of advanced age alone, aging assets may have degraded performance or functional obsolescence that increases the risk of failure.

Especially in case of CEI transmission and distribution network, installation/ renovation is very costly, and typically requires long lead times for planning and involves stakeholder processes, public policy, and construction challenges. For example, in US, in 2015, investor-owned electric utilities and stand-alone transmission companies invested $35 billion in transmission and distribution infrastructure (5% increase in distribution and 24% increase in transmission investment over 2014) [14]. In conducting a comprehensive long-term assessment of the assets and systems as well as for future investments, Energy Utility owners and operators are increasingly considering building resilience into new infrastructure through a variety of approaches, including energy infrastructure security “by design”. Moreover, the energy utilities in collaboration with governmental policy makers and regulators are working towards the challenges of raising the needed capital to fund transmission and distribution networks development, along with cross boarder links and cross-connects.

Here is should be noted that aging infrastructure risks affecting structural parts of the assets are out of scope, such as dams and/or casing aging risk assessment in hydropower plants, or bulk generation fossil-fuelled plants.

### 3.1.4 Risk 4: Cyber security

Critical infrastructure is vulnerable to all type of attacks and increasingly to attacks committed through the Internet [15].

Cyber threats to CEI are an evolving security challenge that can impact European security, public safety, and the economy in general. As the private sector owns and operates most of the CEI assets and networks, and governments are responsible for national security, securing CEI against cyber threats is a shared responsibility of both the public and private sectors. An example of direct attack is ISIS’ attempt to hack US electrical power companies in October 2015.

In Europe, till recently the most well known event, was the Ukrainian power grid cyber attack in December 2015, where cyber attackers hacked the Ukrainian utilities’ networks, gained access and manually switching off 43 power to electrical substations [16]. In December 2016, Ukraine suffered another cyber attack. This time it was fully automated, as hackers struck an electric transmission station north of the city of Kiev, blacking out a portion of the Ukrainian capital equivalent to a fifth of its total power capacity. The outage lasted about an hour, so it can hardly be characterized as a catastrophe; still it shows that electricity network remains venerable to cyber attacks [17].

It is generally recognized that smart devices and SCADA will be an entry to CEI, allowing practically anyone to gain access and interact with the infrastructure. However, EU community, via a number of research projects (e.g. H2020 SUCCESS project[18]) and own resources works with industry to develop new cybersecurity solutions for energy delivery systems through an integrated planning and research and development effort. The aim of the SUCCESS project is to reduce the risk of energy disruptions due to cyber incidents as well as survive an intentional cyber attack with no loss of critical function. A comprehensive risk management approach may provide a means to develop a cybersecurity strategy tailored to the unique requirements of each Energy Utility or Energy asset owner.

### 3.1.5 Risk 5: Aging workforce

Human Factor is always a risk. However, the growing potential gap in available skilled personnel to replace the retiring workforce has been a real concern in the Energy Sector for some time. More than half of utility workers will be eligible to retire in the next few years, taking years of experience with them, yet attracting a new generation of skilled workers is challenging.

Especially the percentage of the lineworker workforce expected to retire within the next five to ten years could approach 40-50% in some organizations.  The loss of institutional knowledge is a critical concern, especially for a profession heavily dependent on mentoring and on the job training. Although the number of lineworker training institutions has grown considerably, analysis indicates a significant forecasted shortage in the availability of qualified candidates. In US it is estimated that the shortage in the availability of qualified lineworker may be as high as 20% of the current workforce [19]. In 2010, as a reaction to the aging workforce in the electricity sector, the US Department of Energy awarded nearly $100 million of funding to support 54 workforce training programs in the utility and electrical manufacturing industries to train approximately 30,000 people [20].

Similar problems (in many cases even more pressing ones) are also visible in Europe and the European energy sector stakeholders have been undertaking proactive measures to address the prospective shortage of trained personnel via industry-wide workshops and conferences. The ***CEIS-SG*** is another effort to promote a Culture of CEI Security along with best practices at pan-European level, contributing towards the creation of experienced workforce.

## 3.2 Critical Infrastructures' Interdependencies

The last couple of years, technical innovations and developments in digital information and telecommunications dramatically increased interdependencies among the critical infrastructures. The energy infrastructure provides essential fuel to all other critical infrastructure sectors, as without energy, none of them can operate properly [18]. In turn, it depends on other critical infrastructure sectors, such as communications and information technology.

Figure 3 provides a simplified illustration of interdependencies among 16 critical infrastructure sectors, including the 4 critical sectors (i.e. Energy, Water, Communications, and Transportation) that provide lifeline functions to all critical infrastructure sectors.

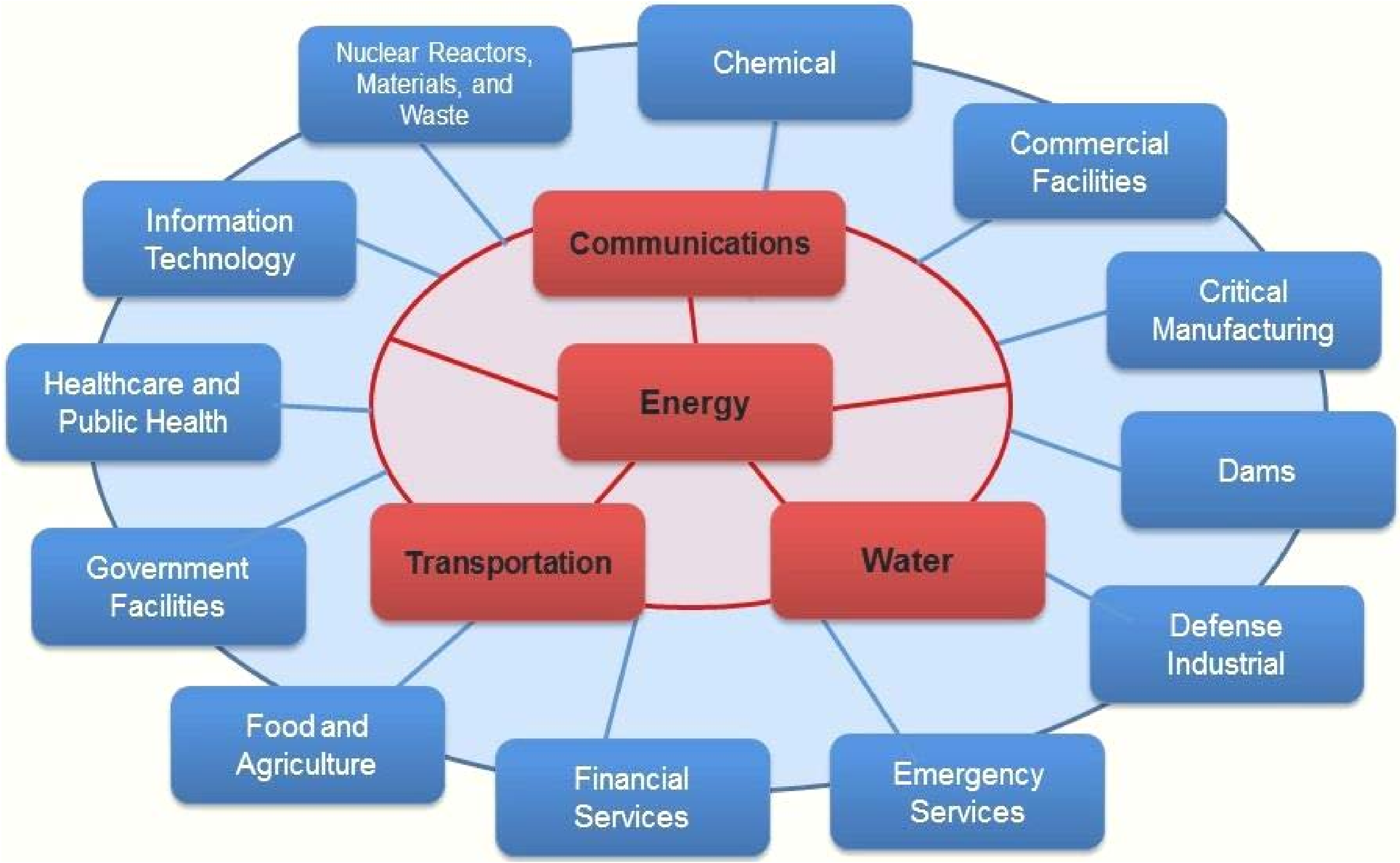

**Figure 3: Critical Infrastructure Interdependencies [18]**

Table 1 (based on [22]) provides a high level overview of the interdependency among the critical infrastructures and the services that they offer and consume. As shown in Table 1, the Electricity Critical Infrastructure provide essential power to Communication, Transportation, and Water Sectors, and in return both subsectors rely on them for fuel delivery (transportation), electricity generation (water for production and cooling), as well as control and operation of infrastructure (communication).

| **(Sub)sector Generating the Service** | **(Sub)sector Receiving the Service** | | | | |
|---|---|---|---|---|---|
| | Electricity | Oil & Natural Gas (ONG) | Transportation | Communications | Water |
| Electricity | | Electricity for extraction and transport (pumps, generators) | Power for overhead transit lines and Electrical Vehicles | Energy to run cell towers and other transmission equipment | Fuel to operate pumps, water management and treatment |
| Oil & Natural Gas (ONG) | Fuel to operate power plant motors and generators | | Fuel to operate transport vehicles | Fuel for backup power | |
| Transportation | Delivery of supplies, fuel and employees | | | Delivery of supplies, fuel and employees | |
| Communications | Detection and maintenance of operations and electric transmission | Breakage and leak detection and remote control of operations | Identification and location of disabled vehicles, rails and roads | | Detection and control of water supply and quality |
| Water | Cooling and production water | Production water | Water for vehicular operation; cleaning | Water for equipment and cleaning | |

**Table 1: Critical Infrastructures Interdependencies**

# 4 CEI Protection draft roadmap

The CEI threats and needs have already been analysed by the DEFENDER consortium and an initial (draft) roadmap of near-, mid- and long-term milestones on CEI protection is provided in Table 2. The roadmap will be further discussed and analysed during CEIS-SG activities.

| **Strategies** | | | |
|---|---|---|---|
| **1 Risk Assessment** | **2. Protective Measures** | **3. Manage Incidents** | **4. Culture of Security** |
| **Near-term Milestones (Project Duration)** | | | |
| 1.1 Common terms and measures specific to each CEI segment.<br>1.2 CEI segments categorization in Security Tiers | 2.1 Evaluate the robustness and self-healing of new platforms, systems, networks, architectures, and policies | 3.1 Tools to identify incidents across all levels of CEI<br>3.2 Tools to support and implement incidents management commercially available | 4.1 Public awareness of CEI resilience efforts<br>4.2 Pan-European Stakeholders group to share mitigation strategies and define a security roadmap |
| **Mid-term Milestones (4–7 years) By 2024** | | | |
| 1.3 Majority of infrastructure and asset owners baseline their security posture via energy subsector specific metrics | 2.2 Scalable access control for all energy delivery system devices available<br>2.3 Next-generation, interoperable solutions for secure communications | 3.3 Incident reporting guidelines accepted and implemented by each energy subsector<br>3.4 Real-time forensics capabilities and cyber event detection tools commercially available | 4.3 Active Involvement of Humans in the Loop for CEI protection using trusted blockchains' based bidirectional information flows<br>4.4 Compelling business case developed for investment in CEI security |
| **Long-term Milestones (8–10 years) By 2028** | | | |
| 1.4 Cyber-physical risk assessment tools commercially available | 2.4 Self-configuring infrastructure enables operations' continuation during incidents | 3.5 Lessons learned and best practices from cyber/physical incidents shared and implemented | 4.5 Significant increase in the skilled employees and volunteers in CEI security |
| **Goals** | | | |
| **Security monitoring of all CEI levels and across cyber-physical domains** | **CEI architectures able to continue operating during cyber/physical incidents** | **Fast self-mitigation of cyber/ physical incidents, quickly return to normal operations** | **CEI security practices shared among stakeholders, academia, and government** |

**Table 2: DEFENDER Energy Infrastructure protection strategies, roadmap and goals**

# 5 Pan-European CEI Security Stakeholders Group

Protection of the Critical Energy Infrastructures and defending against extremists and organized (physical and cyber) attacks is of highest importance for the European Citizens Life, Well being and Economy. However, the nature of CEI characterized by vast, geographically-dispersed, widely-diverse infrastructure of assets and networks forming a multifaceted operational environment with complex ownership and regulatory structures requires the development of a coordinated, public-private collaboration and protected information exchange among the Energy Infrastructure Stakeholders and policy makers.

By this manifest, the H2020-740898 DEFENDER project, dominated by the European Commission to innovate towards CEI protection initiates the ***Pan-European Critical Energy Infrastructure Security Stakeholder Group (CEIS-SG)*** as a think tank and information exchange ecosystem targeting safer and more sustainable European Critical Energy Infrastructures.

## 5.1 Scope

The CEIS-SG will be an informal instrument among CEI Stake holders and its scope will be to:

(1) Share information at pan-European level on threats, incidents, countermeasures and best practices

(2) Support of risk-informed decision-making and the tools and mechanisms to facilitate it

(3) Facilitate adaptive learning, in which experiences serve as opportunities to inform and adjust future actions;

(4) Coordinate CEI security preparedness planning and roadmap towards securing Critical Energy Infrastructures.

(5) Establish the basis for a minimum set of auditable controls for CEI Tiers across Europe

The CEIS-SG will periodically review CEI threats and countermeasures and challenge risk management practices to confirm that established security controls remain in place and changes in the energy delivery system or emerging threats do not diminish their effectiveness.

Beyond informed consensus and based on CEIS-SG feedback, CEIS-SG may define **certification procedures and methodologies** towards estimation of the CEI risk. Based on CEI specific criteria, such as policies, veto or “preferences”, with different weights, CEIS-SG may define different CEI Secure Tiers (equivalent to Data Centres Tiers), taking into account *availability, redundancy, resilience, survivability*, *incident probability* and *cascading effects*, along with the *time requirements for fast restore/self-heal to normal operation* with the overall *security cost*. This may eventually lead to a CEI certification procedure, paving the path towards new CEI protection products and solutions.

## 5.2 Membership

The CEI Security Stakeholders group will consist of mass energy producers, asset owners, Energy Utilities and operators, Law Enforcement Agencies representatives, industrial and research partners, as well as European Commission and Governmental officials and policy makers, who already place significant effort into fostering and maintaining trusted CEI. Voluntary participation and partnerships at local and European level will help facilitate the useful exchange of security-related information and maximize the effectiveness of infrastructure protection and resilience efforts. They will also promote the cooperation necessary to speed restoration and recovery with activities such as equipment and personnel sharing.

Membership in the pan-European Critical Energy Infrastructure Security Stakeholder Group will be granted under permission of the European Commission and the CEIS-SG founding members. Each member may have a veto in the inclusion of an additional member under a justified reasoning.

## 5.3 Membership Benefits

The membership benefits for each category of stakeholders are summarized in Table 3.

| Stakeholder Category | Membership benefits |
|---|---|
| CEI Owners/ Utilities | • Achieve a consensus on security issues, functionalities, operations and tools that need to be addressed to protect current and future CEI.<br>• Share information at pan-European level on threats, incidents, countermeasures and best practices<br>• Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe<br>• Stay up to date on new developments, tools and commercial offerings along with funding opportunities in CEI protection |
| TSOs, DSOs, Energy companies | • Increase awareness of lurking CEI threats of assets and infrastructure<br>• Share information at pan-European level on threats, incidents, countermeasures and best practices<br>• Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe<br>• Discuss emerging opportunities and shape new business models<br>• Stay up to date on new developments, tools and commercial offerings along with funding opportunities in CEI protection |
| ICT & Security technology providers | • Increase awareness and feedback on opportunities regarding the joint configuration of ICT, Energy and Smart Grid technologies for critical infrastructures.<br>• Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe<br>• Share information at pan-European level on CEI investment roadmap and stay up to date on new funding opportunities in CEI protection |
| Governmental, European Officials and Policy makers | • Increase awareness on CEI owners, TSOs, DSOs and Energy companies concerns, threats and standardization efforts<br>• Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe<br>• Stay up to date on new developments, tools, research effort and commercial offerings. |
| Law Enforcement Agencies (LEAs) | • Create awareness on potential innovative technologies able to support the territory control<br>• Prepare the ground for shared think-tanks and/or operational units which include both CEI and LEA stakeholders |

| | |
|---|---|
| | • Design novel "business" or service delivery models in which LEA and CEI operators may cooperate at different levels to provide protection and mitigation of risk to energy critical infrastructures (for example LEAs may operate physical and/or cyber threats mitigation services on behalf of CEI operators or CEI operators and LEAs may cooperate for achieving the overarching objective of CEI protection |
| Scientific community and industrial research in the Energy sector. | • Create awareness of the CEI current and future cyber/physical threats, research concepts and the vision for the future secure by design CEI.<br>• Stay up to date on new research and developments along with funding opportunities in CEI protection |

**Table 3: CEIS-SG Membership Benefits per stakeholder category**

## 5.4 CEIS-SG Governance/Structure

The CEIS-SG governance is in draft form and it is subject to be discussed and agreed during the CEIS-SG initial meeting. The proposed governance model is based on the following structure:

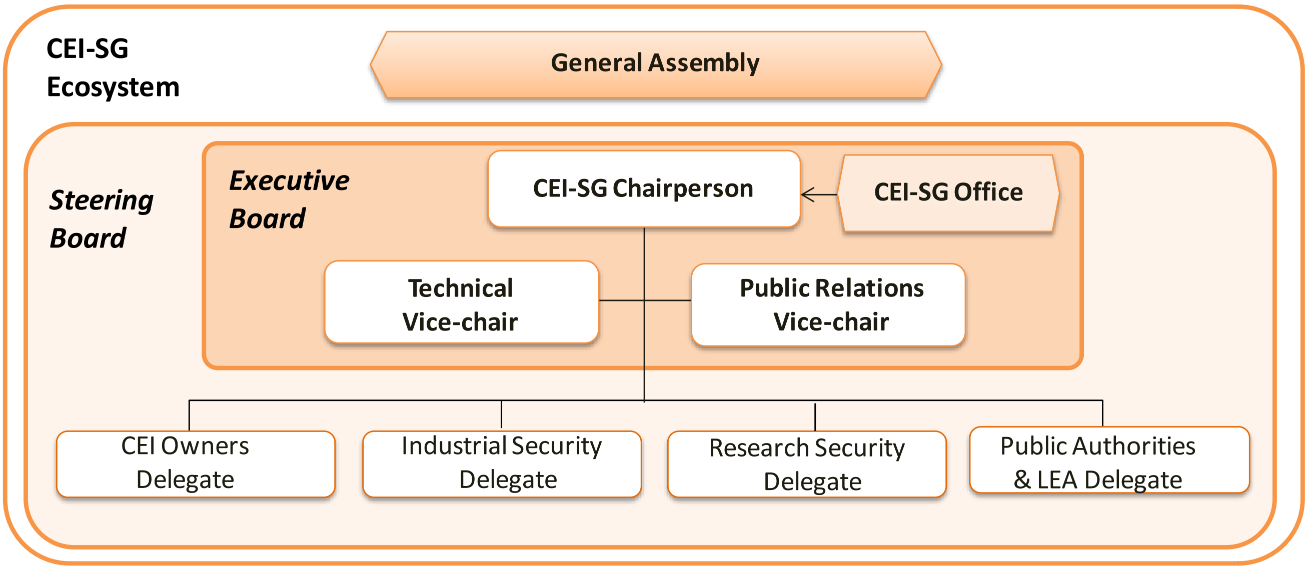

**Figure 4: CEIS-SG Governance**

- ***CEIS-SG General Assembly*** consisting of all stakeholders (i.e. CEIS-SG members).
- ***CEIS-SG Steering Board***: involving a representative set of stakeholders of all domains of the CEI, defining the strategic vision and the key orientations of the group, aiming at converting the CEIS-SG vision into a strategic agenda, and setting the operational goals for achieving this agenda
- ***CEIS-SG Executive Group***: a subset of the Steering Board who, together with CEIS-SG Office, take the responsibility for the day-to-day management of the group activities and the handling of all working relationships
- ***CEIS-SG Chairperson*** is appointed by the General Assembly a representative role and interacts at senior level with other industry players and key representatives from the European and national Public Authorities.

- Two ***CEIS-SG Vice-chairs*** are appointed by General Assembly. One Vice Chairs is appointed to organise in the most efficient way the technical work performed by the CEIS-SG group and the other is the Vice Chair responsible for public relations.

Meeting frequency of the CEIS-SG General Assembly and Steering Board remains to be agreed. The CEIS-SG Executive Board will physically meet at least twice per year, and have phone calls at least once every three months

## 5.5 Membership Fees

During the DEFENDER lifetime there will be no membership fees. All meetings and events costs will be covered by the DEFENDER project and selected sponsorships.

# 6 Referencee

[1] Energy sector tops list of US industries under cyber attack, March 12, 2015 http://www.iot-now.com/2015/03/12/30962-energy-sector-stays-top-of-the-list-of-us-industries-under-cyber-attack-says-homeland-security-report/

[2] http://www.renewableenergyworld.com/articles/2016/05/germany-achieves-milestone-renewables-supply-nearly-100-percent-energy-for-a-day.html

[3] European Commission, "North Seas Countries agree on closer energy cooperation," Press release, Luxembourg, 6 June 2016, http://europa.eu/rapid/press-release_IP-16-2029_en.htm

[4] "EEI Survey Shows Electric Power Industry Made Record Levels of Investment in Transmission and Distribution," Edison Electric Institute, December 18, 2015

[5] Center for Energy Workforce Development (CEWD), http://www.cewd.org/ (accessed September 11, 2014).

[6] DEFENDER Consortium, "D1.1 : Identification of existing threats," DEFENDER Consortium September 2017

[7] Wasington Examiner, "New wave of terror attacks shows energy infrastructure at risk," June 2015, http://www.washingtonexaminer.com/new-wave-of-terror-attacks-shows-energy-infrastructure-at-risk/article/2567159

[8] Order RD14-6-000, Reliability Standards for Physical Security Measures, 146 FERC 61,166, March 7, 2014, http://www.ferc.gov/CalendarFiles/20140307185442-RD14-6-000.pdf (accessed October 10, 2016).

[9] United Nations Security Council, "Physical protection of critical infrastructure against terrorist attacks," Counter Terrorism Committee Executive Directorate, United Nations Security Council TRENDS REPORT, 8 March 2017 https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

[10] Binz, R. et. al., "Practicing Risk-Aware Electricity Regulation: 2014 Update," Ceres, November 2014, http://www.ceres.org/resources/reports/practicing-risk-aware-electricity-regulation-2014-update

[11] http://money.cnn.com/2015/10/15/technology/isis-energy-grid/

[12] Claire Healy, "Lights Out: Storm Ophelia electricity loss could take TEN days to restore across Ireland as 360,000 without power as emergency crews set to work around the clock," The Irish SUN, 16 Oct. 2017, https://www.thesun.ie/news/1676411/storm-ophelia-electricity-loss-could-take-ten-days-to-restore-across-ireland-as-360000-without-power-as-emergency-crews-set-to-work-around-the-clock/

[13] "National Risk Estimate: Risks to Physical Infrastructure from Aging and Failing (NRE)," DHS Office of Cyber and Infrastructure Analysis, December 2014.

[14] Utility Aging Workforce Conference, April 2014, http://www.euci.com/pdf/0414-aging.pdf

[15] World Economic Forum. White Paper. "Global Agenda Council on Cybersecurity" April 2016. http://www3.weforum.org/docs/GAC16_Cybersecurity_WhitePaper_.pdf

[16] Ukrainian Ministry of Energy and Coal, "The Work Group to Study the Causes of the Temporary Malfunction of Power Supply Companies, which took place on December 23, 2015," January 2016. Available: http://mpe.kmu.gov.ua/minugol/control/publish/article?art_id=245082298

[17] BBC news, "Ukraine power cut 'was cyber-attack'", January 2017, http://www.bbc.com/news/technology-38573074

[18] H2020 700416, SUCCESS project, “Securing Critical Energy Infrastructures,” http://www.success-energy.eu/

[19] US Department of Energy, “Workforce trends in the Electric Utility Industry,” August 2006

[20] Department of Energy, “Obama Administration Announces Nearly $100 Million for Smart Grid Workforce Training and Development,” April 8, 2010, accessed December 13, 2016, http://energy.gov/articles/obama-administration-announces-nearly-100-million-smart-grid-workforce-training-and.

[21] US Homeland Security, “Energy Sector-Specific Plan 2015,” (accessed July 11, 2016)

[22] R. Zimmerman, and C. Restrepo, “Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction,” 2009 IEEE International Conference on Technologies for Homeland Security, http://research.create.usc.edu/cgi/viewcontent.cgi?article=1146&context=nonpublished_reports (accessed September 17, 2014).