



DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT
ECONOMIC AND SCIENTIFIC POLICY **A**



Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

Cyber Security Strategy for the Energy Sector

Study for the ITRE Committee

DIRECTORATE GENERAL FOR INTERNAL POLICIES
POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

Cyber Security Strategy for the Energy Sector

STUDY

Abstract

This study is provided by the Policy Directorate at the request of the ITRE Committee.

The EU energy infrastructure is transitioning into a decentralised, digitalised smart energy system. Already, energy operations are increasingly becoming the target of cyber-attacks with potentially catastrophic consequences. Development of energy specific cyber security solutions and defensive practices are therefore essential. Urgent action is required, including empowering a coordination body, to promote sharing of incident information, development of best practice and relevant standards.

This document was requested by the European Parliament's Committee on Industry, Research and Energy (ITRE).

AUTHOR(S)

Mr David Healey, Analysys Mason Limited
Mr Sacha Meckler, Analysys Mason Ltd
Mr Usen Antia, Analysys Mason Ltd
Mr Edward Cottle, Analysys Mason Ltd

RESPONSIBLE ADMINISTRATOR

Frédéric GOUARDÈRES

EDITORIAL ASSISTANT

Irene VERNACOTOLA

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU internal policies.

To contact Policy Department A or to subscribe to its newsletter please write to:
Policy Department A: Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@ep.europa.eu

Manuscript completed in October 2016.

© European Union, 2016.

This document is available on the Internet at:

<http://www.europarl.europa.eu/studies>

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the publisher is given prior notice and sent a copy.

CONTENTS

LIST OF ABBREVIATIONS	4
LIST OF FIGURES	5
EXECUTIVE SUMMARY	7
1. INTRODUCTION	9
2. CURRENT SITUATION IN THE EU ENERGY SECTOR	10
2.1 Existing environment of the energy sector across the EU	10
2.2 Current performance and reliability of energy systems (EU and national)	10
2.3 Evolution of ICT to control energy infrastructure	11
3. CYBER SECURITY SITUATION	15
3.1 Cyber Security Strategies in the EU and its International Counterparts	15
3.2 Known or Potential Cyber security threats and impacts to utility infrastructures	18
3.3 Summary of Data and Security Breaches	20
3.4 Investment Situation and Requirements	22
3.5 Market innovations addressing Cyber security	22
4. LEGISLATIVE AND POLICY SITUATION	24
4.1 Existing instruments	24
4.2 Challenges and opportunities	27
5. FINDINGS AND RECOMMENDATIONS	30
ANNEX	35
Annex 1	35
Annex 2	35
Annex 3	36
REFERENCES	37

LIST OF ABBREVIATIONS

APT	Advanced persistent threat
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team for EU institutions
CI	Critical infrastructure
CIIP	Critical information infrastructure protection
CSA	Cyber Security Agency
CSIRT	Computer Security Response Team
DoS	Denial of service
DSO	Distribution system operator
EE-ISAC	European Energy Information Sharing and Analysis Centre
ENISA	European Network and Information Security Agency
EPCIP	European Programme for Critical Infrastructure Protection
ERNICIP	European Reference Network for Critical Infrastructure Protection
ES-C2M2	Electricity subsector cyber security capability maturity model
ETSI	European Telecommunications Standards Institute
GCHQ	Government Communications Headquarters (UK)
ICS	Industrial control systems
IR	Interagency report
IT	Information technology
JRC	Joint Research Council
NIS	Network information security
NISP	Network and information security platform
NIST	National Institute of Standards and Technology
OSGP	Open Smart Grid Protocol Alliance
OT	Operational technology
PPPs	Public–private partnerships
SCADA	Supervisory control and data acquisition
SGAM	Smart grid architecture model
SGTF	Smart Grids Task Force
SO	System operation
TNCEIP	Thematic network on critical energy infrastructure protection
TSO	Transmission system operator

LIST OF FIGURES

Figure 1: Smart Grid Architecture Model (SGAM)	12
Figure 2: Heat map of investments in smart grid projects in Europe	13
Figure 3: ICS-CERT logged security incidents by sector	19
Figure 4: Overview of the Cyber Attack on the Ukraine Power Grid	21
Figure 5: Actors responsible for threat assessment	26

EXECUTIVE SUMMARY

This study provides an assessment of existing European policies and legislation to address cyber security in the energy sector and recommends additional policy prescriptions that may be necessary to protect Europe and its citizens. The assessment is based upon a review of the profound changes that the energy system is undergoing. It is against these current and future challenges that existing Cyber security policy and actions must be measured.

Current situation in the EU energy industry

The energy sector in Europe is experiencing changes at a scale and pace that are unprecedented in more than a century. These are driven by the urgency of actions required to mitigate climate change and decarbonise the energy system. New energy technologies such as renewable generation, electricity storage and electric vehicles will have far-reaching social and economic benefits. These transformations, however, depend upon the deployment of 'smart' technology, which underpins other digitalisation strategies to deliver the benefits associated with smart cities, health, transport and logistics. The smart energy system is therefore created through the significantly greater use of ICT in the digitalisation of energy production and distribution. The resulting energy transformation will see increasing decentralisation of the energy system and greater inclusion of the consumer across the energy value chain.

Cyber threats to the energy industry

The expansion of intelligent networked devices throughout the energy distribution system, together with the supporting integrated communications networks, creates an urgent requirement for a co-ordinated energy cyber security strategy. The range of potential attacks (or 'threat vectors') is multiplied, both by the growing sophistication of cyber attackers and by the increasing number of accessible targets within the smart energy ecosystem.

The smart energy transition across the EU incorporates key characteristics which directly impact development of effective cyber security policy. Firstly, a smart and decarbonised EU energy system will likely expand upon the existing interconnection and interdependency of the networks across Member States: as a result, orchestrated cyber-attacks could have a domino effect across multiple Member States. Secondly, the current status of smart energy system development is not at all consistent across the EU and this could pose specific challenges in harmonising an EU cyber security strategy for the energy sector.

There have been recent significant advances relating to general Cyber Security policy in Europe. The European Union Agency for Network and Information Security (ENISA) is playing an effective lead role across multiple sectors, publishing insightful reports and working with the many EU organisations active in the field of cyber security. The publication of the Network Information Security (NIS) Directive incorporates clear intentions relating to cross-sectoral development. Closer ties are also being forged between the EU and NATO on the subject. An analysis of European and international developments in cyber security strategy indicates there is a high degree of commonality in the key strategic themes, though there is variation in how these are applied in different Member States.

The smart energy systems being deployed today are completely dependent upon the convergence of information technology and operational technology systems. Historically, these two domains have been carefully segregated with very different operating paradigms. The development of smart energy has also led to exponential growth of networked intelligence throughout the energy grids and also the consumer premises. The result is that a massively expanding 'attack surface' now forms the operational foundation of the energy ecosystem. As the energy system is also fundamentally interconnected with every other critical infrastructure network, the cyber security threat to the energy sector impacts every aspect of our modern society.

The unsurprising result is that the energy sector is already a clear and increasing target for cyber-attacks. A recent report from the Industrial Control System Cyber Emergency Response Team found that in the USA energy systems have the second highest number of reported cyber security incidents. Furthermore, research indicates that the number of incidents which are reported are only a small proportion of the incidents that actually occur.

Co-ordination of cyber security measures

Critically, there appears to be insufficient information sharing and co-ordination of action in the energy sector. A number of steps are being taken to implement cross-sector strategies and platforms which will address some of these issues. However, these measures are not commensurate with the nature, diversity, scale and direction of recent and future challenges.

Research, development and innovation in cyber security is undoubtedly occurring in the energy sector, however this appears to be mostly ad hoc and not the product of specific coordinated and focussed objectives. Therefore, outcomes are unlikely to be comprehensive, nor will they necessarily address the immediate priorities in the EU energy sector.

This situation is broadly mirrored in terms of relevant policy activity within the EU. Numerous activities are ongoing to address cyber security in general and applying the NIS Directive in particular. This includes three 'pillars' to 1) assess minimum standards, 2) ensure the development of capabilities through audits and sanctions, and 3) encourage cross-border information sharing. Whilst there is diversity and inconsistency at a Member State and sectoral level, good progress is being made regarding ICT cyber security and protection of critical infrastructure and critical information infrastructure. The immediate and potentially catastrophic nature of the cyber threat across the Energy sector, however, demands an urgent and focussed policy response.

Conclusions and recommendations

There are numerous additional activities necessary to realise an effective cyber security strategy to address the specific characteristics of the energy sector in Europe. The majority of these should be implemented in legislation and become EU law. Since it is the execution of the cyber security strategy itself that is most critical to its success, the priority is the introduction of effective direction and focus: to this end, our most important recommendation is to appoint a central authority with the power and capability to implement all the other recommendations effectively.

In addition to actions that would be implemented in legislation, we are also suggesting a number of enabling and supporting actions that we believe may be more effectively achieved through non-legislated means. Our key recommendations, both legislative and non-legislative, are listed below; each is given a score between 1 and 5, with 5 being the highest in terms of importance and impact.

Recommendations for legislated implementation

- Appointment of a central authority for Energy sector cyber security (5)
- Mandatory reporting of security incidents (5)
- Provisions to require relevant information sharing (5)
- Alignment of cyber security activities across all critical infrastructure to include ICS-SCADA solutions and operations (3)
- Development of security standards for energy systems (3)
- Establishment of a certification board (3)

Recommendations for non-legislated implementation – executed through other means

- Harmonisation of security requirements across the EU (3)
- Promotion of consumer awareness and engagement (2)
- Establishment of a stakeholder network for energy security (2)
- Common approaches across Member States concerning communications systems for smart energy (2)

1. INTRODUCTION

The energy industry is essential to the functioning of every country's economy and society and forms an integral part of all critical infrastructure (CI) systems. The digitisation of the energy supply chain is creating networks that are increasingly dependent on sophisticated ICT systems to operate energy infrastructure and services. In this context, it is vital to consider ICT threats to be the dominant concern regarding energy sector security

European governments have worked individually and collectively to establish mechanisms for protecting their energy systems from external threats and as these systems become increasingly interconnected and interdependent, the need for EU-wide co-ordination becomes critical. Threats to energy cyber security in one Member State have the potential to disrupt infrastructure across the EU region, possibly inflicting significant financial and physical damage, including loss of life.

Analysys Mason has been engaged by the Committee on Industry, Research and Energy of the European Parliament to provide an overview of current legislative and non-legislative cyber security practices in the energy sector and to recommend possible directions for future action.

This study therefore aims to outline current and possible future actions to address the above requirements and concerns, by:

- providing an overview of the present transformation across the energy sector;
- identifying key developments in the area of cyber security;
- reviewing the policy and legislation environment; and
- presenting relevant findings and recommendations.

2. CURRENT SITUATION IN THE EU ENERGY SECTOR

2.1. Existing environment of the energy sector across the EU

The energy infrastructure in Europe is still largely shaped by its history: the systems in each Member State tend to have been developed in line with that state's particular historical context. Nevertheless, in almost all cases they are based on a system of centralised generation and control. In this structure, the energy landscape is dominated by the large generating plants and the transmission system operators (TSOs), and the network consists of a relatively simple one-way flow of energy from a few major production centres towards consumers. The TSOs are able to work to a predictable profile of customer demand/loading, and any threats and risks to system stability and security are contained within a relatively small number of operational assets, as the vast majority of the network lacks a smart dimension.

However, these systems are beginning to adjust to a fundamental change in the generation and delivery of energy. The long-term sustainability of energy systems requires decarbonisation, which is dependent on a move from large centralised generating plants to a more distributed system of generation using renewable energy sources. These changes will ripple throughout the energy industry; at present the prime focus is on the electricity sector.

The decarbonisation of electricity is largely achieved by the proliferation of renewable and sustainable energy generation assets (e.g. wind, tidal, hydro and solar for electricity, plus biogas for gas). These distributed assets create new challenges in terms of balancing and management functions, which in turn create the need for greater consumer and demand-side participation in the energy system (a challenging aspect of the system change, and also among the most rewarding). Finally, environmental improvement for health and other reasons is also a key factor, driven in part by the smart city agenda and the related wish to decarbonise mobility by increasing the use of electric vehicles.

Despite these trends, however, total carbon emissions from power generation in the EU *increased* by 2% in 2015, which has been attributed to coal generation being selected over gas generation in many cases.¹ Various factors have contributed to this, including the ineffectiveness of the European Emission Trading Scheme, and the effects of misaligned policies. In the UK for example the capacity market supports legacy coal and new-build diesel generator farms, rather than stimulating investment in demand-side response and new gas generation. Nonetheless, at a European level, renewable energy sources together represent the single largest component of the generation mix, making up 29% of European energy production.

2.2 Current performance and reliability of energy systems (EU and national)

The modernisation of electricity grids will build on existing assets and systems, but will also require a fundamental shift from a system dominated by the centralised operations of TSOs to the more decentralised activities of distribution system operators (DSOs). An important implication of this is that system stability will no longer be maintained by disconnection of load at the distribution level as a backstop; this function will primarily be DSO-led, with decentralised operations, and the TSO will act as the backstop to ensure system stability under stress.

In recent years, performance and reliability have been fairly simple to maintain, given the declining demand for electricity in Europe: according to research by Pira Energy,² demand

¹ https://www.agora-energiawende.de/fileadmin/Projekte/2016/EU-Review_2015/Agora_State_of_Affairs_EU_2015_WEB.pdf

² <http://www.wsj.com/articles/then-and-now-how-the-utility-industry-has-changed-1473818402>

fell by almost 6% between 2007 and 2015, despite economic activity rebounding and eventually exceeding the levels seen before the financial crisis.

Although traditional approaches to the provision of capacity have generally been sufficient to ensure continuity and security of supply, the significant shift to renewable energy sources requires modernised approaches that provide the right policy and market stimulus to support the operational and technical changes to the system.³ Significant work is still needed in this area, as has been highlighted by the system-balancing challenges posed by building additional interconnectors between Spain and France, as well as the negative cost of energy on the German wholesale market on a particularly windy and sunny day in 2015. All these indicators point to the need for a far more data-driven and flexible energy system, both on the supply and the demand side.

An additional feature of the development of smarter grids is the increased potential for cross-border interconnection, a facility that is used by all Member States – especially in the electricity network. Interconnection will play a key role in transforming the energy system in the most cost-efficient manner, as has been highlighted by a recent McKinsey report.⁴

2.3. Evolution of ICT to control energy infrastructure

As electricity grids are developed to accommodate these new requirements and capabilities, they move from being a network of simple wires to being a more intelligent system that depends upon communications and software. This significant augmentation in the level of intelligence of the energy grid will affect the operational, market and business models as well as regulatory aspects of the system. This digitalisation of the energy systems within Member States is described in more detail in the *Digital Energy System* report⁵ by the European Technology Platform for Smart Grids, which highlights the key use cases that need to be deployed. The report confirms the inevitability of greater digitalisation, noting however that many players have yet to adapt their strategies.

The report sets out a blueprint for the further digitalisation of the energy system. This will require significant and widespread investment in further ICT infrastructure, most noticeably in the distribution network and in DSOs' operational capability. It will also require investment in the transmission system and a revision of TSOs' operational capabilities and priorities. All these developments will require the redesign of investments in ICT for the market operation and regulatory regimes within and between Member States.

The extent and variety of access points to these more extensive ICT systems mean a significant increase in potential vulnerabilities. These changes will increase the number of potential threat vectors that need to be considered from a security perspective, and in particular from the point of view of cyber security.

It should be noted that a more distributed and decentralised energy system also provides numerous security *benefits*, in that it is easier to isolate the impacts of an attack to a regional part of the system: this is an intrinsic quality of distributed systems that makes them more resilient and stable. Nevertheless, in a Pan-European context digitalisation of the energy systems would also result in greater interdependency of these systems, and hence from a security perspective this interdependency needs to be well understood, and the various permutations of how an attacker may seek to co-ordinate an attack to exploit such interdependency need to be accounted for and actively monitored. Such monitoring and countermeasure control should be handled centrally by the TSOs (or another combined

³ <http://www.raponline.org/wp-content/uploads/2016/05/rap-keybrightcapacitymechanismsforpowersystemreliability-2013-oct-8.pdf>

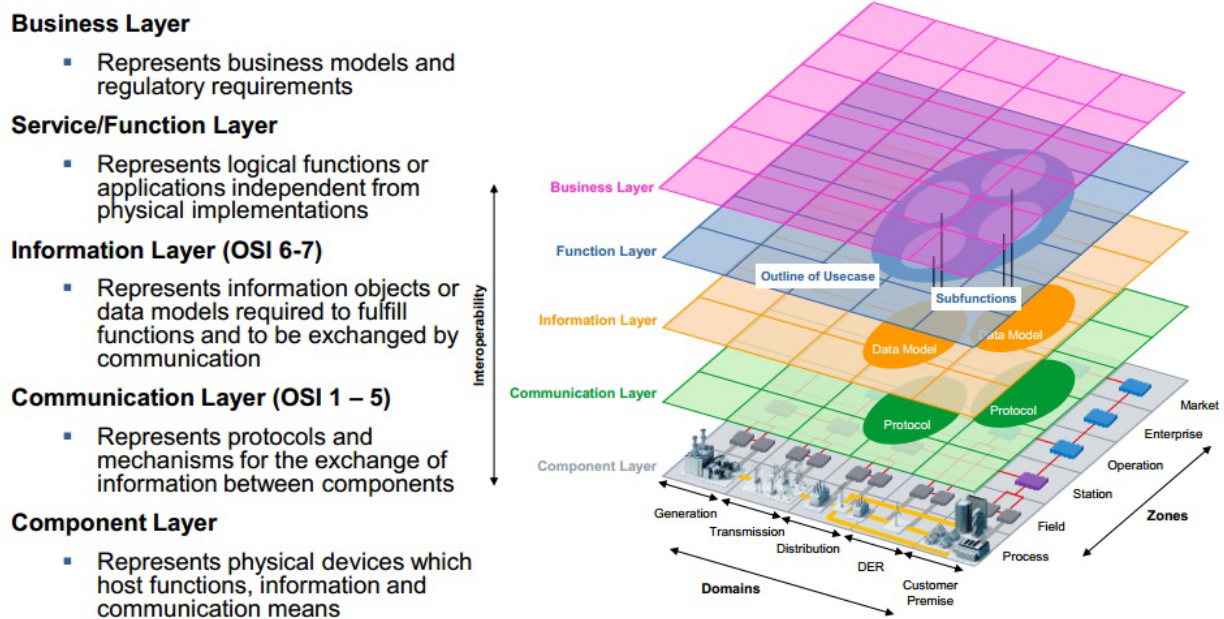
⁴ www.mckinsey.com/~/media/.../transformation_of_europes_power_system.ashx

⁵ <http://www.smartgrids.eu/documents/ETP%20SG%20Digital%20Energy%20System%204.0%202016.pdf>

central authority), in line with their future responsibility as a backstop to maintain system operation. Planning for some elements of this responsibility are already under way, as indicated by work done by the European Network of Transmission System Operators for Electricity in its policy assessment for its ten-year network development plan.

The framework architecture that defines the future state of the system has been described a number of times and continues to evolve, requiring ongoing regulatory action and disruptive research. The CEN-CENELEC-ETSI smart grid co-ordination group has established a significant basis for the transformation of the system with its smart grid reference architecture⁶ and in particular with the establishment of the Smart Grid Architecture Model (SGAM), which is visualised in Figure 1 below.

Figure 1: Smart Grid Architecture Model (SGAM)



Source: [CEN-CENELEC-ETSI Joint Working Group on standards for smart grids, 2014]

In particular, this model highlights the need for greater integration between the *operational technology* (OT) – traditionally the power-related ‘hard’ assets – and *information technology* (IT) – the more business- and function-related enterprise assets. The need for this integration is highlighted in the *Digital Energy System* report referred to earlier. A particular resulting area of contention is the different security profiles and approaches that are used by OT and IT, many of which are based fundamentally on intrinsic technology design.

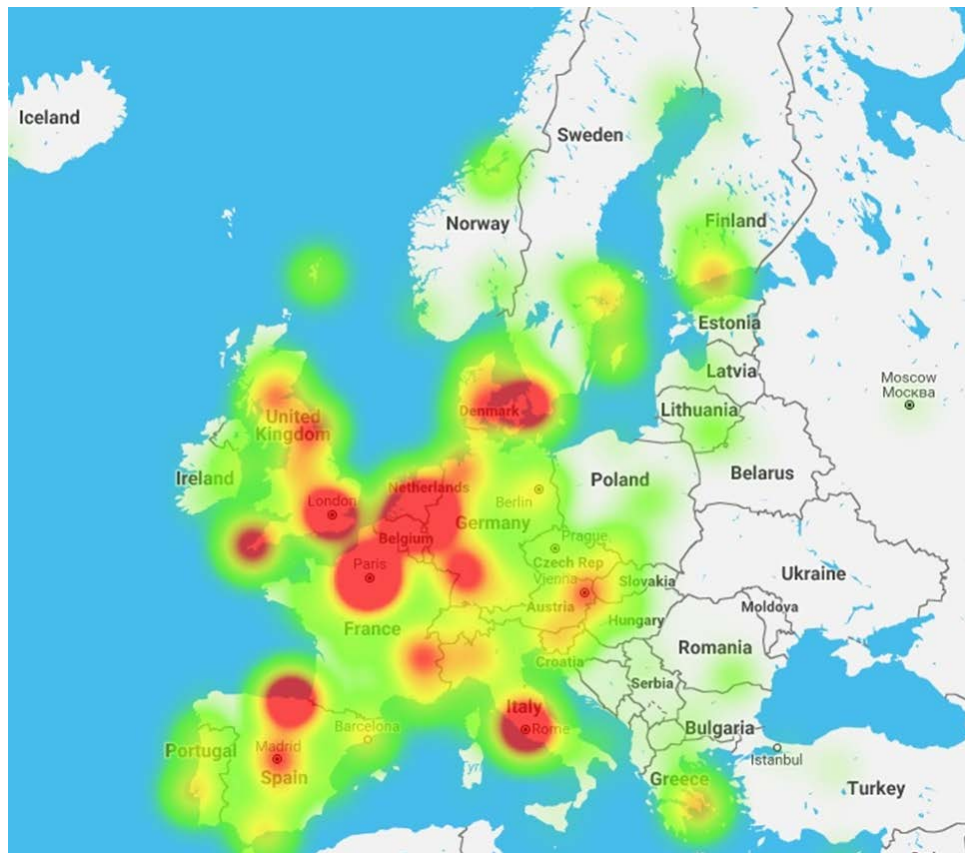
Although a fundamental revision of the structure and organisation of energy grids is inevitable, there are nonetheless stark differences in the readiness and level of interest of different Member States to embark upon significant changes to their energy systems. To some degree this is expected to be influenced by the varying historical capabilities and endowments of different Member States.

To gain some idea of the level of interest and readiness, one can look at the expenditure in each Member State on smart grid innovation and demonstration projects. In 2014, the EC’s

⁶ http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

Joint Research Centre (JRC) published the report *Smart Grids Outlook 2014*,⁷ which provides comparative data on smart grid investment as a proxy for interest and readiness; the results are illustrated by the heat map below (Figure 2).

Figure 2: Heat map of investments in smart grid projects in Europe



Source: [JRC online heat map tool, available at <http://ses.jrc.ec.europa.eu/>]

This data visualisation provides a clear indication of the asymmetrical nature of the interest and readiness for transformation in the energy sector: Eastern Europe is in stark contrast to Western Europe in terms of recent investments in trialling smart grid technology. Specific policies are likely required in Eastern Europe to ensure technology transfer and greater investment in preparation for a changing energy system. We note that the relatively low investment in Nordic countries does not accurately indicate their readiness for more advanced energy systems, as in general terms the systems in these nations started from a different position than Western Europe.

In so far as security is concerned, Eastern and Western Europe may not be implementing the same systems and therefore the same security policies, and will likely require a specific process and period for harmonisation across these regions. This will require specific attention in terms of EU and Member State cyber security policy.

This highlights another important attribute of security policy in general: it is often during the transition from one set of policies or paradigm to another that systems are at their most vulnerable. This is due to the fact that operational practices and procedures are new and not yet validated. Unpractised operators and integration of the new solution with other systems may open security flaws. This uncertainty during any such change process is one of the

⁷ http://ses.jrc.ec.europa.eu/sites/ses.jrc.ec.europa.eu/files/u24/2014/report/Id-na-26609-en-n_smart_grid_projects_outlook_2014_-_online.pdf

reasons that may ICT departments often include a dedicated Change Control function. It is therefore important that best efforts should be made to minimise the time that systems and security policies are in transition. In the best case, transition will result in higher costs due to maintaining multiple policies and applying additional security measures during transition; in the worst case, it will expose the system to numerous additional threat vectors.

In addition to the core concerns about technical security, which have received much attention, it is important to highlight the increased social and market cyber security threats within the energy sector. These threats present parallels to concerns related to fraudulent activities such as phishing scams, identity theft and social engineering, which are commonplace around financial products and services. In the energy market, these threat vectors would probably manifest in a layer above the Business Layer that exists in the SGAM. Although they are likely to be commercially orientated attacks, they could also be designed to create harm if they are done at a significant scale or when combined with other attacks.

Furthermore, consideration needs to be given to the greater number of *combinational* attacks that could be launched within and across Member States. For example, although exploitation of certain discrete assets by malicious agents may not in itself pose a threat, an attack on numerous assets (by a single agent or by numerous agents acting in concert) could pose a significant threat. The same also holds true for co-ordinated attacks across multiple Member States. All of these combinational threat vectors will require a significant overhaul of security capabilities and in particular cyber security. Such combinational attacks are an increased threat not because it necessarily means there will be more actual attacks (although figures in section 3 clearly indicate that this is also the case). The main threat is in the number of different types and directions of attack that could ensue, some of which may not even be identified as attack components until later, such as social engineering to modify consumer's behaviour and thereby increase the vulnerability of the system at a specific point in the network.

3. CYBER SECURITY SITUATION

The world of cyber security is developing at an ever increasing pace. Those on the side of developing solutions and strategies for defence have begun to realise the importance of cooperation and information sharing in effectively addressing potential cyber-threats. Malicious and hostile sources have however continued to develop tools and applications in what is often termed the Cyber arms race.

The accelerating ICT capabilities and continuing reductions in related capital and operational costs is accelerating penetration of intelligent devices throughout the Energy and other CI systems. A report by Motorola Solutions suggests wherever a digital technology or an intelligent device has been implemented, even something as simple as control of a valve on a pipeline, there is a risk of it being used as an unauthorised entry point and taken over for malicious intent⁸.

The development of smart energy networks is driving the proliferation of pervasive networked intelligence. Symantec highlights that the growth in the number of connected systems, including Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) networks and similar distributed management technologies; means that the risks of cyber-attacks can only increase⁹.

Energy utilities are therefore becoming ever more reliant upon the flexibility and responsiveness that smart energy systems provide and therefore face mounting increases in the scale and range of threats. The major energy infrastructures elements facing cyber threats are as follows:

- IT systems which support “back office” business and administrative functions.
- OT systems that monitor and manage energy networks, including generation sources, transmission and distribution grids and also consumer based energy assets including smart meters.
- The communications systems that provide networked intelligence across OT, IT and emergent and smart energy domains which are also often interconnected with other public and private communications networks

3.1 Cyber Security Strategies in the EU and its International Counterparts

3.1.1 EU Cyber Security Strategies and initiatives

The electricity systems in the EU and in each Member State are fundamental to the operational stability of all other Critical Infrastructures. A major objective of the EU cyber security strategy is to reduce the vulnerabilities of CI and increase their resilience¹⁰. Cyber resilience refers to the ability to prepare for, respond to and recover from a cyber-attack, in order that an organisation or infrastructure under a cyber-attack can continue to operate during such an attack¹¹.

The EU's first comprehensive policy document on cyber security, the *Cyber Security Strategy of the European Union*, was adopted in February 2013.¹² The strategy outlined in that document provides the overall framework for EU initiatives on cyber security and cyber-crime.

⁸ Cyber security: A growing threat to the energy sector – An Australian perspective March 2016

⁹ Targeted Attacks Against the Energy Sector (2014) Symantec Security response, Version 1.0

¹⁰ http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

¹¹ Cyber security: A growing threat to the energy sector – An Australian perspective March 2016

¹² *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013

It is supported and developed by the NIS Directive¹³ adopted by the EU Parliament in July 2016. This Directive provides a set of unified network and information security rules that demand regulatory obligations in the co-ordination of national cyber security policies. It provides legal measures to boost the overall level of cyber security, and aims to identify good practices that organisations across the entire value chain can follow in order to tackle cyber security risks.

The EU General Data Protection Regulation (GDPR)¹⁴ was adopted in April 2016 and is due to be formally adopted in 2018. The GDPR is intended to strengthen data protection rights of individuals and provide businesses with clear, modern and applicable rules of operation.

These policy instruments are supported by international agreements. For example, in February 2016, the EU and NATO increased their cyber defence co-operation and signed a technical arrangement between the NATO Computer Incident Response Capability and CERT-EU. The agreement enables sharing of technical information as well as best practices in the prevention, detection and response to cyber incidents.

In addition, a number of organisations and groups have been established. For example, activities on network and information security are supported by the European Network and Information Security Agency (ENISA), as well as by the Computer Emergency Response Team for the EU institutions (CERT-EU).

In September 2015, DG Energy implemented the Energy Expert Cyber Security Platform (EECSP) with a mandate to provide guidance to the Commission on policy and regulatory directions at the European level, in particular addressing the energy sector. The EECSP appointed an Expert Group as “an informal and temporary Commission expert group” to advise the Commission on policy and regulatory strategies related to energy-specific cyber security issues. It is due to report to DG Energy on its findings and recommendations at the end of 2016.

Also launched in 2015, the European Energy Information Sharing and Analysis Centre (EE-ISAC) is a private-public partnership between four EU energy utilities and other sector stakeholders. EE-ISAC was the result of the European research project DENSEK, which was realized with the financial support of DG Home Affairs.

3.1.2. International Cyber Security Strategies

Similar cyber security initiatives are being undertaken outside the EU, notably in the USA. In February 2013, President Obama issued an Executive Order entitled *Improving Critical Infrastructure Cyber Security*¹⁵ which led to the creation of the *Framework for Improving Critical Infrastructure Cybersecurity*, developed by the US National Institute of Standards and Technology (NIST) and issued in February 2014.¹⁶ This provides a common platform which organisations can use to assess and manage cyber security risks. It aims to enable organisations, regardless of sector, size, degree of cyber risk or sophistication, to apply the principles and effective practices of risk management to improve the security and resilience of CI.

¹³ EU Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union, 6 July 2016.

¹⁴ EU Regulation 2016/679 On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, available from <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

¹⁵ <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>

¹⁶ <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

In January 2015, a collaboration between the US Department of Energy and the electricity, oil and gas industries produced the *Energy Sector Cybersecurity Framework Implementation Guidance*, which defines cyber security tools and processes specifically for use in the energy sector.¹⁷ An important risk management tool advocated in the guide is the Electricity Subsector Cyber Security Capability Maturity Model (ES-C2M2). Developed to address the unique characteristics of the electricity sector, it helps electricity organisations of all types evaluate and make improvements to their cyber security programmes. For example, the model can be used to:

- identify areas where cyber security capabilities can be strengthened;
- effectively and consistently evaluate and benchmark cyber security capabilities;
- assist in the implementation of best practice in knowledge sharing, down to a sub-sector level, as a means to improve cyber security capabilities; and
- assist in the prioritisation of actions and investments to improve cyber security.

Other tools that are worth mentioning include:

- the CIP Standards, which provide regulatory cyber security requirements which aim to assist in securing the energy system assets; and
- *Guidelines for Smart Grid Cyber Security*¹⁸ developed by a Working Group of the National Institute of Standards and Technology (NIST), which provides an analytical framework to develop tailored cyber security strategies to specific smart grid-related characteristics, risks, and vulnerabilities.

Two other pieces of legislation were passed in the USA in 2015; the Protecting Cyber Networks Act and the National Cyber Security Protection Advancement Act. These pieces of legislation are aimed at improving the sharing of information between the private sector and government agencies. The second piece of legislation offers some liability protection for private entities that do so.

In 2009, Australia released its Cyber Security Strategy, that seeks to improve the detection analysis, mitigation and response to sophisticated cyber threats covering systems of national interest including energy. Two agencies have been established to monitor and respond to cyber-crime; The Australian Cybercrime Online Reporting Network was developed for small and medium-sized businesses and the Australian Securities and Investments Commission, Australia's corporate and financial services regulatory body, encourages businesses to use the NIST Cyber Security Framework.

Singapore established the dedicated Cyber Security Agency (CSA) in April 2015, which oversees national cyber security functions. So far, the establishment of the CSA has led to Singapore signing memorandums of understanding with the UK, France and India, in each case committing to collaborate on cyber security. The CSA has delivered a five-year National Cyber Security Masterplan (2018) which strives to make Singapore a 'secure and trusted hub' with special attention paid on the nation's critical infocomm infrastructure¹⁹.

In July 2015, the Chinese government released for public comment a consultation draft of a new Cyber Security Law. This law increased obligations on network operators, which are required to have cyber security protocols in place and to take steps to protect against cyber-attacks. The Cyber Security Law also imposes obligations on providers of information network

¹⁷ http://energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf

¹⁸ https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

¹⁹ <https://www.csa.gov.sg/news/publications/national-cyber-security-masterplan-2018>

products and services. Key IT hardware and equipment must meet mandatory security qualifications and acquire government certification before being sold.

The examples above highlight two key characteristics of developing national cyber strategies:

1. In particular, that there are a number of common and recurrent themes with varying degrees of transparency in terms of their application
2. There is a diversity of approaches adopted by various nations in how they apply these themes, which it can be assumed relate to the particular contextual and structural attributes of the nation in question.

Importantly it is both the approach and the manner of its execution that is likely to greatest bearing on the effectiveness of any cyber security strategy.

3.2 Known or Potential Cyber security threats and impacts to utility infrastructures

3.2.1. Known or Potential Cyber security threats to utility infrastructures

In the progression to smart energy networks the IT and OT environments within energy utilities have become more interconnected and reliant upon one another. In addition, communication technologies and system heterogeneity are increasing the technological complexity of the energy networks. The security challenges of sub-systems, combined with an increasingly distributed and multi-functional environment, therefore only increases the energy system vulnerability and potential level of cyber threats.

Smart grids are a relatively new concept and therefore experience or relevant information regarding security threats or incidents is minimal. As a result, many application-level protocols have been designed without adequate levels of intrinsic security mechanisms which fully address the impacts of a fully integrated smart energy network. A few examples of resulting issues that have been identified include:

1. In 2014, a team of university researchers from Portugal, found a flaw in an encryption standard developed by the Open Smart Grid Protocol (OSGP) Alliance, intended to secure smart grid networks in the EU and adopted by the European Telecommunications Standards Institute (ETSI)²⁰.
2. The UK's Government Communications Headquarters (GCHQ) in 2014, intervened in the UK's smart meter roll-out plans due to the proposed use of a single decryption key for all communications between smart meters and energy service providers. This approach created the potential for chaos across the network, as a single hacker could conceivably disable the entire population's electricity meters²¹.
3. Similar concerns were raised from a study conducted by security researchers in Spain in 2014, where millions of network-connected electricity smart meters were deemed susceptible to cyber-attack due to lack of proper security controls²².

It is important to note that many of the threats that have resulted in breaches are likely to have been managed confidentially and have not been shared industry-wide. This is tantamount to the loss of critical knowledge, and undermines the ability for the industry as a whole to effectively manage risk from cyber threats Coordinated efficient exchange of

²⁰ <http://www.computing.co.uk/ctg/news/2407891/dumb-crypto-in-smart-grids-smart-meter-encryption-standard-fundamentally-flawed-claim-researchers>

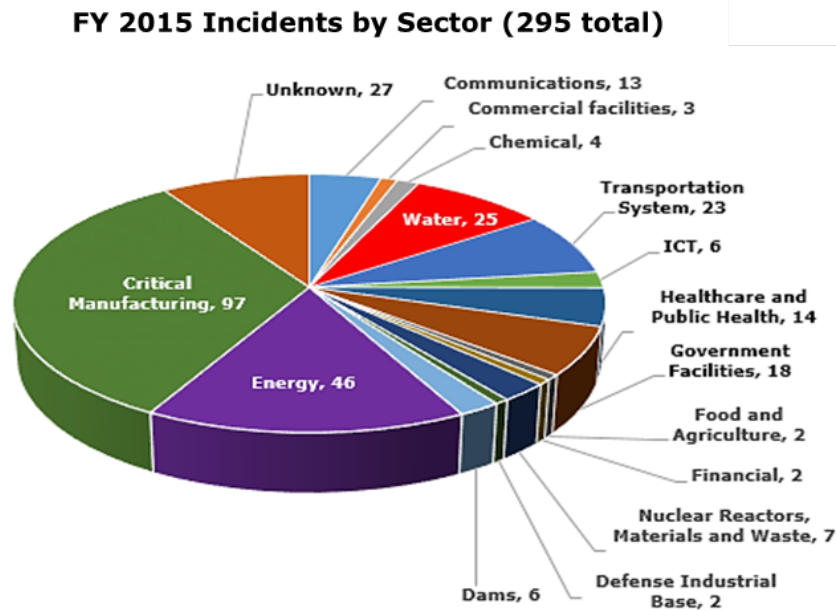
²¹ <http://www.computing.co.uk/ctg/news/2451772/gchq-forced-to-intervene-to-prevent-catastrophically-insecure-smart-metering-plan>

²² <http://securityaffairs.co/wordpress/29353/security/smart-meters-hacking.html>

incident related information between key EU stakeholders represents a serious barrier to ensuring adequate cyber security solutions are implemented across the EU energy sector.

In 2015, ICS-CERT in the USA received and responded to 295 incidents. The critical manufacturing sector accounted for 97 of these incidents, with the energy sector reporting 46 cyber security incidents. 37% of these incidents were examples of 'spear-phishing', making it the leading access vector for incidents in 2015 and reported to ICS-CERT²³.

Figure 3: ICS-CERT logged security incidents by sector



Source: [https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf]

Details on the nature and range of known and perceived threats to smart grid are listed and discussed in Annex 1.

3.2.2. Cyber Security Impacts to Utility Infrastructure

Among the most challenging aspects for policy makers in the field of cyber security (particularly CI), is the lack of information on the scale of potential threats and specific information on incident impact. It should also be noted that national and regional data across the EU on this issue is particularly scant. This makes it difficult to accurately assess the socio-economic impact of an incident (nationally and EU-wide) and the resulting recovery cost.

In a 2016 report produced by ENISA²⁴ on the cost of cyber incidents affecting CII within specific EU states, key findings include:

- Finance, ICT and energy sectors appear to have the highest incident costs
- Countries often tolerate malicious activity as long as it stays at 'acceptable' levels (around 2% of national income); measuring the exact impact is difficult
- Often actions are only taken to prepare for and invest in incident response after an event of significant impact has occurred
- A large majority of organisations still have not implemented basic security controls
- Attackers are streamlining and upgrading their techniques, while companies struggle to fight old tactics

²³ https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

²⁴ The cost of incidents affecting CIIs, August 2016 ENISA

- In most cases, attackers are able to compromise an organisation within minutes, while time to recover takes considerably longer
- The large majority of vulnerabilities were exploited one year or more after the vulnerability was revealed; vulnerability remediation such 'patch management' is therefore still a weak link or low priority
- The report recommends that Governments need to collect and publish data on cybercrime, and help countries and companies to make better choices about risk and policy.

In a global study on the cost of cybercrime produced by the Ponemon Institute in 2015, companies within the utility sector experienced the second highest annualised cost in losses from cyber-attacks in contrast to other sectors studied (healthcare, automotive and agriculture)²⁵.

To demonstrate the potential impact and scale of a catastrophic malicious cyber-attack event within the energy sector, a Lloyds report explores a hypothetical scenario in which a cyber-attack creates an electricity blackout that plunges 15 US states (including New York and Washington DC) into darkness and leaves 93 million people without power²⁶. The scenario, while improbable, is clearly technologically possible. In the scenario, a piece of malware infects electricity generation control rooms in parts of the North-Eastern USA. The malware is triggered and takes control of 50 power generators forcing them to overload and burn out. This temporarily destabilises the entire North-Eastern UAS regional grid. Power is restored to some areas within 24 hours, but others remain without electricity for a number of weeks. The total impact on the US economy is estimated at between \$243 billion, rising to more than \$1 trillion in the most extreme version of the scenario. The total of claims paid by the insurance industry is estimated at between \$21 billion to \$71 billion.

3.3 Summary of Data and Security Breaches

Although information on breaches is understandably confidential and therefore difficult to obtain, the industry consensus is that the threat landscape in energy is increasing and cyber-attacks are becoming much more prevalent. The need for collaboration and information sharing on energy-related cyber security is therefore urgent and vital.

In 2015, ICS-Computer Emergency Response Team (CERT) in the USA reported a total of 295 incidents involving CI, compared to 245 in the previous year. 12% of incidents had evidence of intrusion into the control system environment²⁷. Between 2009 and 2014 the number of reported cyber security incidents in the ICS-SCADA area increased by a factor of 27. More than half of the incidents (59% in 2013) were aimed at the energy and critical manufacturing sectors and around 55% involved advanced persistent threats (APT)²⁸ ²⁹. Further afield the Australian CERT has indicated that it believes around 29% of reported cybercrime incidents occur in the energy sector³⁰.

One of the most recent publicised cyber security breaches within the electricity sector was the Ukraine power grid cyber-attack on 23 December 2015. In this attack, three of the

²⁵ http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf

²⁶ Emerging Risk Report – 2015 Innovation Series, <https://www.lloyds.com/~media/files/news%20and%20insight/risk%20insight/2015/business%20blackout/business%20blackout20150708.pdf>

²⁷ <https://securityintelligence.com/news/ics-cert-reports-increase-in-fy2015-infrastructure-attacks/>

²⁸ APT is a cyber-attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time. The intention of an APT attack is to steal data rather than to cause damage to the network or organisation.

²⁹ Analysis of ICA-SCADA Cyber Security Maturity Levels in Critical Sectors, (2015) ENISA

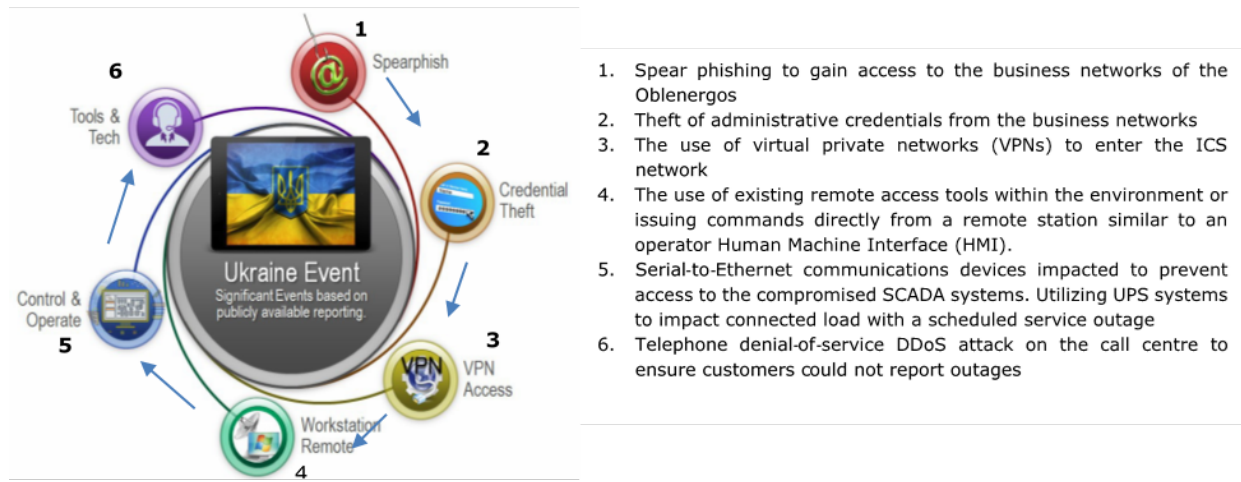
³⁰ Cyber security: A growing threat to the energy sector – An Australian perspective March 2016

regional electricity distribution companies (known locally as 'Oblenergos') in Ukraine were the subject of a co-ordinated series of cyber-attacks implemented over a 30-minute period. The attackers gained unlawful access to and control of the distribution companies' computer and SCADA systems affecting 110kV and 35kV substations. This resulted in outages which lasted several hours, and affected approximately 225 000 people in these regions.

Once they were able to restore electrical service, the Oblenergos continued to operate their distribution systems in an operationally constrained mode. The cyber-attacks in Ukraine are very significant because these are the first publicly acknowledged incidents of an attack against OT systems in a nation's CI resulting in a power outage. The below

Figure 4 outlines the attack process and consequences.

Figure 4: Overview of the Cyber Attack on the Ukraine Power Grid



Source : [https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf]

Other publicly reported cases of cyber-attacks to energy space include;

- On 27 April 2016, a German nuclear power plant (*Gundremmingen*) was discovered to have been infected with computer viruses. Upon further investigation, the viruses appeared to pose no threat to the operations of the facility because they were isolated from the Internet. The viruses were discovered on a computer system retrofitted in 2008 with data visualisation software associated with equipment for moving nuclear fuel rods. One of viruses "W32.Ramnit" was designed to steal files from infected computers, whilst the other "Conficker" was designed to spread through the networks by copying itself onto removable data drives.³¹
- In December 2014, South Korea reported a cyber-attack against the operator of its nuclear power plants. The attackers released sensitive and confidential information online, including the designs and manuals for the plant's equipment.
- In 2014, the Chinese hacker "Ugly Gorilla" infiltrated the network of a US public utility company.³²
- In 2013, a computer virus attacked a turbine control system at a US power company after a technician inserted an infected USB drive into a computer on the network. The incident kept a plant off-line for three weeks.³³
- In 2012, Qatar's RasGas, one of the world's largest producers of natural gas, was hit by a virus which infiltrated 30 000 of its computer workstations. The company isolated

³¹ <http://uk.reuters.com/article/us-nuclearpower-cyber-germany-idUKKCN0XN2OS>

³² <http://resources.infosecinstitute.com/cyber-security-policy-and-threat-assessment-for-the-energy-sector/>

³³ <http://www.reuters.com/article/us-cyber-security-powerplants-idUSBRE90F1F720130116>

all of its computer systems from outside access, which forced oil traders to revert to communicating by fax and telex, as even the company's external email services were inoperative. "It's like going back 20 years in time," a trader said about the use of the telex.

- In June 2010, the "Stuxnet" worm targeted Iran's Natanz nuclear facility, reportedly ruining a fifth of the country's nuclear centrifuges.

The range and variety of the above known attacks, is interesting as it points to the fact that the variety and range of vulnerabilities that existed and infers that such range and varieties are likely to continue to exist. When you take this together with the fact that it is very likely that this is a very small subset of the actual number of incidents that have occurred recently, the scale and complexity of the risk becomes apparent.

3.4. Investment Situation and Requirements

In order to perpetuate developments and innovation in the cyber security sector, vast public and private investments will be required. Technological and organisational advancements are needed to continuously improve efficiency of cyber security efforts, matching developments in complexity of cyber threats.

Potential damage from cyber threats is boosted by both developments in malware and the increasing dependency of CI upon ICT systems. Decisions on the level of cyber security investment should be therefore made in view of the potential costs of an attack. Research firm Cyber Security Ventures expects annual cybercrime costs to increase from USD3 trillion to USD6 trillion globally between 2015 and 2021, with losses resulting from "damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm".³⁴

Cyber security Ventures forecasts global spending on cyber security products and services to exceed USD1 trillion cumulatively between 2017 and 2021, representing 12-15% year-on-year growth. This strong forecast reflects recent rapid increase in cyber security spend across the world; for instance, the US Government has increased its annual cyber security budget by 35%, from USD14 billion budgeted in 2016 to USD19 billion in 2017.³⁵ On the European side, the EC has pledged to invest EUR450 million into a public-private partnership on cyber security that is expected to further trigger EUR1.8 billion of investment.³⁶

As mentioned in our discussion of legislation and policy (see Section 4), there are virtually no regulatory stimuli to cyber security investment in place within the EU, although some spending on innovation, research and development has been forthcoming. In order to provide the necessary incentive for investment, it is vital to communicate the level of potential damages from cyber-crime to public and private stakeholders, and to make clear the importance and urgency of action.

3.5. Market innovations addressing Cyber security

In addition to policy and legislation instruments, efforts of public and private organisations to develop innovative solutions and approached to address challenges outlined above to improve the overall state and functionality of energy cyber security. We have developed a

³⁴ Cyber security Ventures – 2016 Cybercrime Report

³⁵ Cyber security Ventures – Cyber security Market Report, Q3 2016

³⁶ http://www.theregister.co.uk/2016/07/05/eu_cyber_security_investment_plan/

broad classification of primary functions carried out by organisations and initiatives involved in introducing developments and innovations in the area:

- *Analytical function* – analysing existing cyber security protection and standardisation practices, identify gaps in the frameworks and provide commentary and strategic suggestions;
- *Technological function* – introducing new technological solutions for the purpose of cyber security enhancement;
- *Collaborative function* – aiming to bring together multiple stakeholders and foster cooperation and information sharing among them.

The above functions can be performed by public bodies and private vendors alike, and an organisation can embody more than one function. Investment is being made to address cyber security challenges, but it is unclear whether such activities are sufficient and whether a market will emerge to sustainably address the ever growing number of threats. Figure 7 which can be found in Annex 2 shows a snapshot of some of the public and private projects that driving innovation in energy cyber security.

To be up to the challenge of growing diversity and complexity of threats, the market will require at a minimum sufficient incentive means and capability to address these threats. The potential damages highlighted in Section 4 would certainly support the view that there is sufficient incentive for significant investment in preventative actions. However, for such a market to be able to respond effectively would require the means to respond and this would require access to relevant incident information which at the present time is extremely difficult to obtain. Providing a clearly defined method and process to share such information in a timely, secure and efficient manner will require a systemically equivalent institutional response to the threat. It seems clear that the EC should prioritise action to identify and empower the appropriate organisation to coordinate and implement knowledge sharing and learning processes between existing stakeholder institutions, and Member States focussed specifically on the needs of the energy sector.

Figure 8 in Annex 3 shows the various information sharing platforms currently in operation, and highlight the importance of knowledge sharing to address cyber security challenges.

4. LEGISLATIVE AND POLICY SITUATION

4.1. Existing instruments

4.1.1 EU-wide policy

The protection of CI was first put on the EU agenda in June 2004. In November 2005, the European Commission adopted a green paper on the European Programme for Critical Infrastructure Protection (EPCIP). It sets the overall legislative framework for activities aimed at improving the protection of CI. This has resulted in range of activities both at a national and EU level to address the issues related to CI. The adoption of the Network Information Security (NIS) Directive strengthens the EPCIP.

Despite these various efforts and as mentioned during the 12th EU-US Energy Regulators' Roundtable, the numerous European and national initiatives have produced, a variety of guidelines and frameworks, in mostly uncoordinated fashion.³⁷ We have examined several of these in relation to policy, to provide an overview of the current energy cyber security situation in the EU. This assessment is aligned with the NIS Directive, seeking to understand the situation in terms of the three key pillars:

1. Improve Member State resilience based on the implementation of cyber security standards
2. Confirm EU minimum capabilities through audits/tests and sanctions for failure as assessed by competent authorities at national and sector level
3. Support and augment information sharing and collaboration through obligatory reporting – cross-border and between different parties nationally (public-private).

Policy frameworks for cyber security in the energy sector includes regulatory mechanisms that span several policy topics. This report looks at the following distinct (but overlapping) areas:

- *Cyber security*, viewed in detail in Section 3.1, is broadly concerned with all ICT-related security issues
- *CIP* encompasses policy and legislation for preserving vital services, such as energy, transportation and finance, in view of all types of hazards, including natural disasters, terrorist attacks and criminal activity
- *Critical information infrastructure protection (CIIP)* framework is created as an overlap of the above policies and focuses on protection of the both tangible and intangible information infrastructure.

Cyber security

The 2013 Cyber security Strategy of the European Union outlines overarching principles and priorities for EU cyber security. The strategy emphasises the need to establish a co-ordinated international cyberspace policy, develop capabilities and allocate resources in a way that enhances the Member States' ability to anticipate and handle cyberattacks and facilitates a reduction in cybercrime.³⁸

The strategy is supported by the NIS Directive, which requires Member States to develop national strategies on network and information security, specifies legislative elements to be

³⁷ Council of European Energy Regulators – Session V: Cyber security, 26 April 2016

³⁸ European Commission – Cyber security Strategy of the European Union: An open, Safe and Secure Cyberspace, 7 February 2013

included in these strategies, provides guidelines for setting up national security authorities and incident response teams and promotes international co-operation.³⁹

CI

On the European level, guidelines for CIP are outlined in the EU's Programme for EPCIP, which aims to identify European CI and interdependencies between them, set up CIP expert groups and the Critical Infrastructure Warning Information Network, facilitate CIP information-sharing and fund CIP-related projects. The most recent implementation of EPCIP, contained within the 2013 Staff Working Document⁴⁰, builds on the 2008 European Critical Infrastructures Directive, which establishes the procedure of CI identification for the energy and transport sectors.

CII

The regulatory basis for CIIP is predominately formed from a combination of cyber security and CIP policy instruments. Additionally, the 2013/40/EU directive defines criminal offences and relevant sanctions in the area of information systems.⁴¹

Smart grids with their close interdependencies between CI and ICT systems represent a crucial focus of CIIP. In 2009, the EC set up the Smart Grids Task Force (SGTF) consisting of five expert groups⁴²:

- Expert Group 1: Smart grid standard development
- Expert Group 2: Regulatory recommendations for privacy, data protection and cyber security in the smart grid environment
- Expert Group 3: Regulatory recommendations for smart grid deployment
- Expert Group 4: Smart grid infrastructure deployment
- Expert Group 5: Implementation of smart grid industrial policy.

4.1.2. National governance structure

In its 2016 CIIP report, ENISA differentiates between three government profiles which broadly describe relationships among public and private agencies involved in CIIP and the structure of relevant decision-making processes.⁴³ This classification aims to enhance understanding of procedures to be followed to implement policy changes in individual member countries and to facilitate expertise exchange between them.

Decentralised approach

This approach is characterised by a lack of a centralised authority, and responsibility for CIIP is placed either on sector-specific agencies or CII operators. Although Member States utilising this approach tend to facilitate co-operation between various stakeholders, the benefits of information exchange can be offset by significant variance among sector-specific policies and initiatives. Examples of countries adhering to the decentralised approach include Austria, Cyprus, Finland, Switzerland and Sweden.

³⁹ Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016

⁴⁰ European Commission – Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, 28 August 2013

⁴¹ Directive 2013/40/EU of the European Parliament and of the Council on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 12 August 2013

⁴² European Commission website

⁴³ European Union Agency for Network and Information Security – Stocktaking, Analysis and Recommendations on the Protection of CIIs

Centralised approach

Under this approach, CIIP responsibility is assigned to a centralised agency, with authority spanning across multiple sectors. This allows for creation of comprehensive legislation that governs a large share of stakeholders. France has implemented the centralised approach, and separate elements of it have been adopted by other countries (central authority in the Czech Republic and comprehensive legislation in Germany).

PPPs

The PPP approach implies that the decision-making process is carried out through co-operation between public and private actors. This enables governments to incorporate private-sector expertise into regulation. The Netherlands is an example of a country adopting a PPP approach.

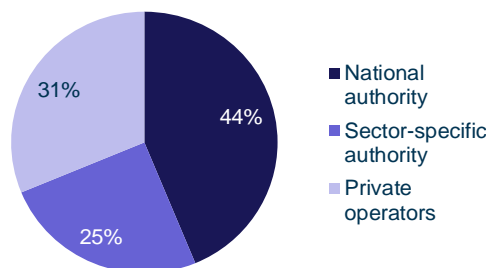
4.1.3 National CIIP measures

National regulatory and executive authorities, the make-up of which varies depending on the selected governance approach, are responsible for implementing specific CIIP measures. ENISA has conducted a survey of 15 EU Member States and Australia, examining existing practices across all aspects of cyber security.⁴⁴

Threat assessment

Threat assessment includes identification of potential threats, as well as their probability and consequence. It can be carried out by national authorities, sector-specific authorities (particularly under the decentralised approach) or CI or CII operators. Figure 5 shows survey results on the current or planned choice of the practice among examined Member States.

Figure 5: Actors responsible for threat assessment



Source: Analysys Mason, ENISA (2015)

Incident handling and reporting

While most Member States have introduced mandatory incident reporting for only specific sectors, five countries surveyed have adopted it throughout the economy. Ten other countries surveyed mandate incident reporting in the telecommunications sector, with efforts also being made in such sectors as energy, finance and public administration. Computer security response teams (CSIRTs), required under NIS Directive, are widely established to address cyber security incidents and can be governmental (offering services to public agencies), national (serving private CI operators), sector-specific or combined in nature.

⁴⁴ European Union Agency for Network and Information Security – Stocktaking, Analysis and Recommendations on the Protection of CIIs

Security measures and audits

The same five Member States that have mandated incident reporting across all sectors, have also implemented mandatory security measures across all sectors, as well as mandatory security audits. While security audits appear to be less of a priority (or harder to implement) for the Member States, security measures tend to be mandated at least in the most crucial sectors – telecommunications, energy and finance.

Investment incentives

Among countries surveyed, only Finland has introduced a CII investment incentive, in the form of tax breaks for companies investing in operational security. ENISA states that some countries believe market pressure is sufficient to encourage CII investment in the future.

4.2 Challenges and opportunities**4.2.1 Capability development***Governance approach selection*

Section 5.1.2 outlined a broad classification of governance approaches available to and implemented in Member States. A centralised approach may be seen as most conducive to development of comprehensive legislation; a recommendation cannot be made for its ubiquitous adoption throughout all Member States. The choice of an appropriate approach – or a combination of several governance structures – would be influenced by existing governmental organisations and decision-making processes in place across a variety of sectors. It is important to tackle the challenge of setting up clear CIIP governance mechanisms in Member States in the interest of facilitating information and expertise sharing among them. ENISA notes that countries with similar CIIP governance structures may be better suited for the exchange of practices and measures.⁴⁵

Audits and penalties

As mentioned in Section 5.1.3, few Member States have adopted mandatory security auditing practices, and we have identified no reference to penalties issued for any non-compliance with cyber security policy defined on either the EU or national level. The NIS Directive obliges Member States to “ensure that the competent authorities...require operators of essential services to provide...evidence of the effective implementation of security policies, such as the results of a security audit”.⁴⁶ RAND points out that activities of CII operators can be difficult to audit, and this might have contributed to the low adoption of mandatory security auditing.⁴⁷ Establishing EU-wide and national auditing practices can potentially allow the identification of gaps and challenges in legislation and standardisation efforts, as well as assessment of their efficiency.

Investment stimulation

There are two primary concerns in regard to CIIP investment in Member States. The first has to do with the general asymmetry in smart grid innovation and demonstration investment among different countries, illustrated for smart grid projects in Section 3.3. The CIIP investment discrepancy, which is most likely to appear between Western Europe on one side and Eastern Europe on the other, complicates cross-border collaboration due to varying

⁴⁵ European Union Agency for Network and Information Security – Stocktaking, Analysis and Recommendations on the Protection of CIIs

⁴⁶ Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union, 6 July 2016

⁴⁷ RAND Corporation – Cyber security in the European Union and beyond: Exploring the Threats and Policy Responses

capability levels, as well as development and adoption of comprehensive cyber security regulation. The second challenge is to incentivise CI and CII operators to invest in cyber security. As mentioned in Section 5.1.3, almost none of the Member States currently have any incentive schemes in place. Options for establishing them include provision of tax breaks or financial subsidies, as well as post-incident investigation and recovery support.

4.2.2 Standardisation

Definitions

Due to the relatively nascent nature of cyber security as an issue and the multitude of actors involved in the development of reports, guidelines and regulations on the topic, there exists a variety of definitions for crucial terms and metrics. For instance, the 2015 RAND Corporation report states that the absence of a commonly accepted definition for cyber security threats and the variation in threat assessment methodologies complicates comparison of threat assessments resulting in groupings of assessments that are not reliably comparable⁴⁸. Moreover, the lack of clarity may potentially lead to duplication of findings and directives.

Cyber security obligations standards

As pointed out in the 2015 standardisation governance report by ENISA, a number of European standardisation organisations – such as CEN, CENELEC and ETSI – are making progress in developing and updating CIP and CIIP standards. However, the report also identified several challenges in standardisation on both national and European levels that still need to be addressed:

- Risk of overlapping work, which may potentially complicate synchronisation of standardisation activities
- Lack of co-ordination of standardisation activities in the area of cyber security
- Relative rigidity of governance, which is currently based on a “request-response” protocol, with EC directing standardisation requests to ESOs, which can choose whether to fulfil those requests.

ENISA suggests that it can be beneficial for standardisation to be carried out in a co-ordinated manner, with appropriate directorates of the EC routinely collecting needs from stakeholders and a co-ordination body (such as the existing Cyber Security Co-ordination Group) reviewing standardisation requests in the first instance, maintaining a database of standards and standardisation activities and making a judgement on producing a concrete standardisation request. Decision-making models involving ESOs in standardisation request justification can also be considered.⁴⁹

4.2.3 Co-operation

PPPs

ENISA’s 2016 survey of 15 Member States revealed that only 8 of these had established institutionalised forms of public-private co-operation.⁵⁰ The public sector can therefore increase its participation in the development and auditing of CIIP practices, drawing from their data and expertise. As per the RAND report, non-institutionalised PPPs can prove difficult to foster, especially at an EU-wide level, as there is currently no single contact point for

⁴⁸ RAND Corporation – Cyber security in the European Union and beyond: Exploring the Threats and Policy Responses

⁴⁹ European Union Agency for Network and Information Security – Stocktaking, Analysis and Recommendations on the Protection of CIIs

⁵⁰ European Union Agency for Network and Information Security – Stocktaking, Analysis and Recommendations on the Protection of CIIs

private companies willing to share information – they would need to first identify the relevant Member State, from which the information is transferred to Europol and, subsequently, other Member States. This approach is especially inefficient from the standpoint of cyber security, as identification of the relevant Member State is not always straightforward.⁵¹ Fostering PPPS has also been identified as challenge in the area of smart grid security, primarily due to lack of clear governance structures.⁵²

Information sharing

Co-operation, both between actors within separate Member States and among organisations on the European level, is inseparable from the concept of data and information sharing. But in order to derive benefits from this process in a secure and sustainable way, a number of questions should be answered, such as:⁵³

- Availability of information: what kinds of information is available for sharing? What legislative and non-legislative barriers hinder the information-sharing process?
- Information-sharing process: what mechanisms should be employed for gathering and transferring data?
- Use of information: what limitations should be placed on how the shared information is used?

The cornerstone of the above questions is information privacy. The need for shared information to be collected, stored and used in a way that adds value to national and international cyber security efforts while preserving privacy rights of EU residents and legal entities defines the way information sharing should be regulated and organised.

⁵¹ RAND Corporation – Cyber security in the European Union and beyond: Exploring the Threats and Policy Responses

⁵² European Union Agency for Network and Information Security – Smart grid security governance models in Europe

⁵³ RAND Corporation – Cyber security in the European Union and beyond: Exploring the Threats and Policy Responses

5. FINDINGS AND RECOMMENDATIONS

Cyber security in the energy sector has become a critical multi-national and multi-stakeholder focal point for all EU Member States. The scale of the threat to energy cyber security is massively increasing as energy systems develop ubiquitous intelligence and communications capabilities throughout their operations. Global imperatives concerning climate change and carbon reduction have placed smart energy at the centre of developments across CI domains, integrating smart grids with public telecommunications operations, e-government, healthcare, and logistics. In addition, development of a cost effective low carbon energy system across the EU will require a more distributed energy system, whilst also employing increased inter-connection and co-operation across national boundaries.

These energy network and services are also critical for the daily operation of the internet and other digital information systems, which form the backbone of the European Society and the Digital Single Market.

Many EU Member States have therefore begun to develop and implement measures for the protection of energy and other CII. However, Member States are working from very different start points in terms of the status of existing assets, infrastructure, technical capabilities and national economic circumstances. Plans to co-ordinate and standardise the transformation of energy systems and the associated cyber security plans must therefore also take into account the necessity of Member States to exercise some flexibility in the implementation of local cyber security strategies.

It is likely that for some time therefore, a natural tension will exist between the individual reactive responses and the need to co-ordinate policy actions in order to promote valuable regional synergies. There already exists within the EU and in the actions of Member States, significant positive developments and advances. However, many of these activities happen in isolated 'silos', whilst in the key areas of experience learnings and information availability, there is an urgent need for sharing and coordination. This is particularly the case regarding the specific requirements within the Energy sector.

The NIS Directive has made significant progress in terms of setting direction in the general cyber security market and policy areas. The Directive's proposed cyber security information sharing platforms are certainly an appropriate long-term solution. These reflect a multi sector approach however and will take some time to implement and become effective. The energy sector however cannot afford to be 'playing catch-up' regarding this longer-term vision. The Energy industry requires urgent, clear and coordinated direction. Energy should also be one of the sectors that is able to address its own particular needs, whilst also playing a key role in developing wider CII cyber strategy development.

The challenges are such that all existing energy sector stakeholders will need to find and play an active role, building on their individual areas of skill and knowledge. These capabilities should be fully employed to ensure an effective cyber security strategy, but more importantly, to drive forward urgent execution of the strategy across the energy sector. In so doing, immediate cyber security benefits will accrue, which should also signpost best practice to be adopted across the EU.

In a world where new threats are constantly emerging and all aspects of the energy system are now becoming a potential target for cyber-attack, a more distributed system offers a very different landscape. A distributed energy system will undoubtedly have a higher number of potential access points and vulnerabilities. However, the effect of such attacks can potentially be reduced as the impacts can be more easily isolated to a specific part of the system. This should be a key aspect of security standards for the development of smart energy systems.

The future sustainable Energy system will therefore require new institutional modalities that can seamlessly respond to and grow with the nature and scale of threats. This may create tensions between securing European citizens' requirement for data privacy and the need for Member States to build a coordinated Energy focussed cyber security strategy.

Recommendations to enable implementation of an effective cyber security strategy in the EU

The recommendations of this research and analysis, have been built upon the concerted work of many specialists and organisations from across the EU and around the world. Many expert groups and associations have completed investigations into the issues summarised within this paper. Our objective is to build upon this and thereby identify the urgent need for policy action that is the consensus of the industry as a whole. The recommendations herein therefore point to policy prescriptions that will enable an effective cyber security strategy for energy in the EU and also identify whether these may require a legislative framing in law or if alternative approaches can be pursued.

Further work will be required to fully assess the manner in which legislation should be drafted, as the considerations of data privacy legislation and impact on individual Member States will not be a simple matter. The recommendations are presented in separate "Legislative" and "Non-legislative" categories. Each recommendation is listed in order of importance, priority and impact. Each is also assigned a score between 1 and 5 (5 being highest priority and impact) to provide further context regarding our assessment.

Legislated implementation

1. **Appointment of a central authority** (5) – The formulation and appointment of a responsible body to take on an executive role to ensure compliance with all the proposed policy prescriptions and with a specific focus and responsibility for energy. This body should be aligned with and support cross-sector platforms. Being established as part of the NIS Directive, it will focus on co-operation in information sharing, incident reporting and other critical elements of energy cyber security in an expedited manner.
2. **Incident reporting** (5) – The European Commission should encourage Member States and all relevant smart energy stakeholders to coordinate incident reporting and sharing of relevant incident related information. This should include information concerning attack patterns and other contextual data. This will help operators and relevant stakeholders to act effectively to thereby protect energy system operation and develop effective countermeasures.
3. **Information Sharing** (5) – The standardisation and facilitation of information sharing primarily within the energy industry should be made a priority. This should also include other CII sectors across Member States. This must include ICS-SCADA operators and incident handlers in standardising information sharing concerning both best practices and also known threats across critical sectors including energy.
4. **Alignment of cyber security activities** (3) - At present ICS-SCADA cyber security is not aligned with national cyber security strategies and CII protection efforts. The European Commission and Member State authorities should require that all activities be aligned and fully integrated with national cyber security and CIIP strategies and operations.
5. **Security standards** (3) – The European Commission should work with utility suppliers, smart energy operators and stakeholders to develop a set of minimum security requirements to be applied in all cases where communication and control

devices are implemented within a smart energy network. This should include the following:

- a. Require smart grid operators to implement mandatory security risk assessments
 - b. Require manufacturers, integrators, services providers and grid operators to comply with specific security certifications
 - c. Establish regulatory sanctions (e.g. significant fines) for non-compliance;
 - d. The compliance results should be made publicly available.
6. **Certification board** (3) – Create a certification board made up of public and private stakeholders to coordinate smart grid / energy cyber security certification and compliance activities. This group should:
- a. Provide oversight for the creation of smart grid / energy cyber security requirements and develop the operational capability to effect smart grid security certification. Also, to facilitate and support national certification schemes.
 - b. Disseminate transparent information and best practices on smart grid / energy certification process and practices.
 - c. Provide regular monitoring and revision of smart energy cyber security needs
 - d. Responsibility to ensure that standards and certification processes remain relevant and aligned with other bodies within the EC and internationally
 - e. Provide all necessary administration functions to enable a Pan-European certification standard and where appropriate, support expansion of the certification function internationally.

Non-legislated implementation – executed through other means

1. **Harmonise requirements** (3) – The EC should facilitate agreement between Member States regarding a minimum level of harmonisation on security and resiliency requirements and standards. This should establish the basis for national regulatory authorities to effectively measure security and assess the current state of overall energy system security. This will also enable effective assessment and comparison of solutions provided by different organisations.
2. **Consumer awareness and engagement** (2) – promotion of end user awareness and education on the changes to the energy system should be compulsory for energy companies. Even if the energy system is technically secure, damage and financial loss can be incurred through social engineering attacks and similar manipulation.
3. **Stakeholder network** (2) – A proactive and empowered network of relevant stakeholders should be identified and actively managed at the European level. Representation should include relevant EC Directorates such as DG ENER, DG CONNECT and others, DSOs, TSOs and relevant standards bodies. This stakeholder group should employ a secretariat that is enabled to facilitate establishment of appropriate working groups and thereby develop propositions to address relevant matters including the following:
 - a. relevant regulatory or market issues that impact energy cyber security.
 - b. development of strategies for implementation of changes to relevant market or regulatory arrangements,
 - c. preparation and proposing of relevant policy documents including EC communications and Directives
4. **Communications systems for smart energy** (2) – The EC should look to align relevant policy approaches across Member States to establish a common approach for smart energy communication system design and integration. This should include the possible implementation of appropriate standards for smart energy communications systems and devices. The current lack of standards increases the vulnerability of

communications networks to cyber-attacks. Such standards and guidelines should in turn provide a basis for the development of a European certification scheme. These communication standards should include:

- a. a common reference architecture,
- b. technical and operational requirements for smart energy / grid applications and systems,
- c. remote updates and reconfiguration – providing for smart energy / grid communications systems that utilise updatable devices to dynamically and remotely update security applications,
- d. a reference risk assessment framework and methodology.

ANNEX

Annex 1

Below is a list of some of the known technical threats used by attackers⁵⁴ that could potentially threaten smart energy networks within the EU;

- Spreading of malware
- Identity theft
- Database exploit of business and control systems
- Compromising of communication equipment
- Web attacks
- Web application attacks
- Network Availability
- Eavesdropping and traffic analysis
- Botnets
- Phishing
- Modbus security issue

Annex 2

We have developed a broad classification of primary functions carried out by organisations and initiatives involved in introducing developments and innovations in the area:

- **Analytical function** – analysing existing cyber security protection and standardisation practices, identify gaps in the frameworks and provide commentary and strategic suggestions;
- **Technological function** – introducing new technological solutions for the purpose of cyber security enhancement;
- **Collaborative function** – aiming to bring together multiple stakeholders and foster cooperation and information sharing among them.




Figure 6 shows a snapshot of some of the public and private projects that are driving innovation in energy cyber security.

Figure 6: Development and innovation organisations

Organisation	Description	Functions		
		A	T	C
ESMIG	The European Smart Metering Industry Group represents smart energy solution providers and publishes frameworks and standards aimed to ensure efficient integration of new energy management systems	●		●
SPARKS	The EU-funded Smart Grid Protection Against Cyber-attacks project conducts analysis of smart grid security measures, publishes standards and develops technological tools, such as an intrusion detection mechanism for SCADA systems	●	●	
SEGRID	The EU-funded Security for Smart Electricity Grids project brings together DSO manufacturers to conduct smart grid risk management analysis, employing a	●	●	●

⁵⁴ Aloula f., Al-AliaA R., Al-Dalkya R., Al-Mardinia M., El-Hajj M., Smart Grid Security: Threats, Vulnerabilities and Solutions (2012), International Journal of Smart Grid and Clean Energy vol. 1, no. 1

technologically innovative realistic test environment and produce recommendations

DENSEK	The EC-funded Distributed Energy Security Knowledge project is a consortium of energy supply chain actors which serves as an information-sharing platform and situation awareness network	
Scissor	The Scissor project is an EU-funded consortium designing a new generation SCADA security monitoring framework	
Edison	South California Edison is a private company providing cyber security protection for electricity grids on an enterprise level, with a tool based on technologies used in the defence and intelligence sectors	

Source: [Analysys Mason 2016]

Annex 3

Figure 7 shows the various information sharing platforms currently in operation, and highlight the importance of knowledge sharing to address cyber security challenges.

Figure 7: Current information-sharing platforms and initiatives

Name	Run by	activity	Focus	Web site
ERNCIP (European Reference Network for Critical Infrastructure Protection)	JRC	Testing and certification of IACS devices	all	https://erncip-project.jrc.ec.europa.eu/networks/tgs/ics-use-cases
TNCEIP (Thematic Network on Critical Energy Infrastructure Protection)	JRC	Information sharing	TSOs (electric + gas)	Web site: https://itis.jrc.ec.europa.eu/ by invitation only
EE-ISAC (European Energy Information Sharing and Analysis Center)	EE-ISAC	Information sharing	all	http://www.ee-isac.eu/membership required
NISP – Network and information security platform	CNET	Public private platform working on Strategic Research Agenda, risk management, information sharing.	All (cross sectoral)	https://resilience.enisa.europa.eu/nis-platform
ENISA ICS Security Stakeholder Group	ENISA	Information sharing on ICS SCADA security	all	https://resilience.enisa.europa.eu/ics-security by invitation only

Source: [Analysys Mason 2016]

REFERENCES

- Agora Energiewende, *Energy Transition in the Power Sector in Europe: State of Affairs in 2015*.
- Aloula F., Al-AliaA R., Al-Dalkya R., Al-Mardinia M., El-Hajj M., *Smart Grid Security: Threats, Vulnerabilities and Solutions (2012)*, International Journal of Smart Grid and Clean Energy vol. 1, no. 1
- Burton, G., *'Dumb crypto in smart grids': Smart meter encryption standard fundamentally flawed, claim researchers*. Computing, 11 May 2015.
- Burton, G., *GCHQ forced to intervene to prevent catastrophically insecure smart metering plan*, Computing, 21 March 2016.
- CEN-CENELEC-ETSI Smart Grid Coordination Group, *CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture*, 2012.
- Cyber Security Agency of Singapore, *National Cyber Security Masterplan 2018*, April 2015.
- Cybersecurity Ventures, *Hackerpocalypse: A Cybercrime Revelation*. 2016 Cybercrime Report.
- Cybersecurity Ventures, *Cybersecurity Market Report, Q3 2016*.
- Council of European Energy Regulators, *Session V: Cyber Security*, 26 April 2016
- Electricity Information Sharing and Analysis Center (E-ISAC), *Analysis of the Cyber Attack on the Ukrainian Power Grid*, March 2016.
- European Commission, *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, 7 February 2013
- European Network of Transmission System Operators for Electricity (ENTSO-E), *ENTSO-E Position on European Union Policy Framework for Climate and Energy in the Period from 2020 to 2030*, 2014.
- *EU Directive 2013/40/EU On Attacks against Information Systems and Replacing Council Framework Decision 2005/222/JHA*, 12 August 2013
- *EU Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union*, 6 July 2016 ["NIS Directive"]
- *EU Regulation 2016/679 On the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, April 2016.
- European Commission, *Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure*, 28 August 2013
- European Commission, DG Migration and Home Affairs, *Critical Infrastructure*.
- European Union Agency for Network and Information Security, *Smart Grid Security Governance Models in Europe*
- European Union Agency for Network and Information Security (ENISA), *Analysis of ICA-SCADA Cyber Security Maturity Levels in Critical Sectors*, 2015
- ENISA, *The Cost of Incidents Affecting CIIs*, August 2016
- ENISA, *Smart Grid Threat Landscape and Good Practice Guide*, 2013.
- ENISA, *ENISA Threat Landscape 2015*, 2016.
- ENISA, *Stocktaking, Analysis and Recommendations on the Protection of CIIs*, 2016
- Finkle, J., *Malicious virus shuttered power plant: DHS*. Technology News, 16 January 2013.

- Joint Research Centre, *Smart Grid Projects Outlook 2014*, 2014.
- Joint Research Centre, online heat map tool. Available at
- Keay-Bright, S., *Capacity Mechanisms for Power System Reliability*, 2013.
- Kostadinov, D., *Cybersecurity Policy and Threat Assessment for the Energy Sector*. Infosec Institute, 4 August 2015.
- Leyden, J., *EU uncorks €1.8bn in cybersecurity investment. Thirsty, UK?* The Register, July 2016.
- Lloyd's, *Business Blackout: The insurance implications of a cyber attack on the US power grid*. Emerging Risk Report, 2015.
- Loeb, L., *ICS-CERT Reports Increase in FY2015 Infrastructure Attacks*. SecurityIntelligence, 21 January 2016.
- McKinsey&Company, *Transformation of Europe's Power System until 2050*, 2010.
- Motorola Solutions, *Cyber security: A growing threat to the energy sector – An Australian perspective*, March 2016
- National Cybersecurity and Communications Integration Center/ Industrial Control Systems Cyber Emergency Response Team, *NCCIC/ICS-CERT Year in Review, FY 2015*.
- National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity*, 12 February 2014.
- Office of the Press Secretary, *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity*, 12 February 2013. Available at
- Paganini, P., *Smart meters in Spain can be hacked to hit the national power network*. Security Affairs, 17 October 2014.
- Ponemon Institute, *2015 Cost of Cyber Crime Study: Global*, October 2015.
- RAND Corporation, *Cyber Security in the European Union and Beyond: Exploring the Threats and Policy Responses*, 2015
- Salvaterra, N., *Then and Now: How the Utility Industry Has Changed*. The Wall Street Journal, September 2016.
- Smart Grid Interoperability Panel Cyber Security Working Group, *Guidelines for Smart Grid Cyber Security*, NIST Interagency Report 7628, September 2010.
- Steitz, C., *German nuclear plant infected with computer viruses, operator says*, Technology News, 27 April 2016.
- Symantec, *Targeted Attacks Against the Energy Sector*, Symantec Security Response, Version 1.0, 2014
- U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, *Energy Sector Cyber Security Framework Implementation Guidance*, January 2015.
- Vingerhoets, P. et al., *The Digital Energy System 4.0*, 2016.

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT ECONOMIC AND SCIENTIFIC POLICY **A**

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website:
<http://www.europarl.europa.eu/supporting-analyses>

PHOTO CREDIT:
iStockphoto.com; Shutterstock/beboy



ISBN 978-92-846-0349-7 (paper)
ISBN 978-92-846-0348-0 (pdf)

doi: 10.2861/52802 (paper)
doi: 10.2861/984337 (pdf)

