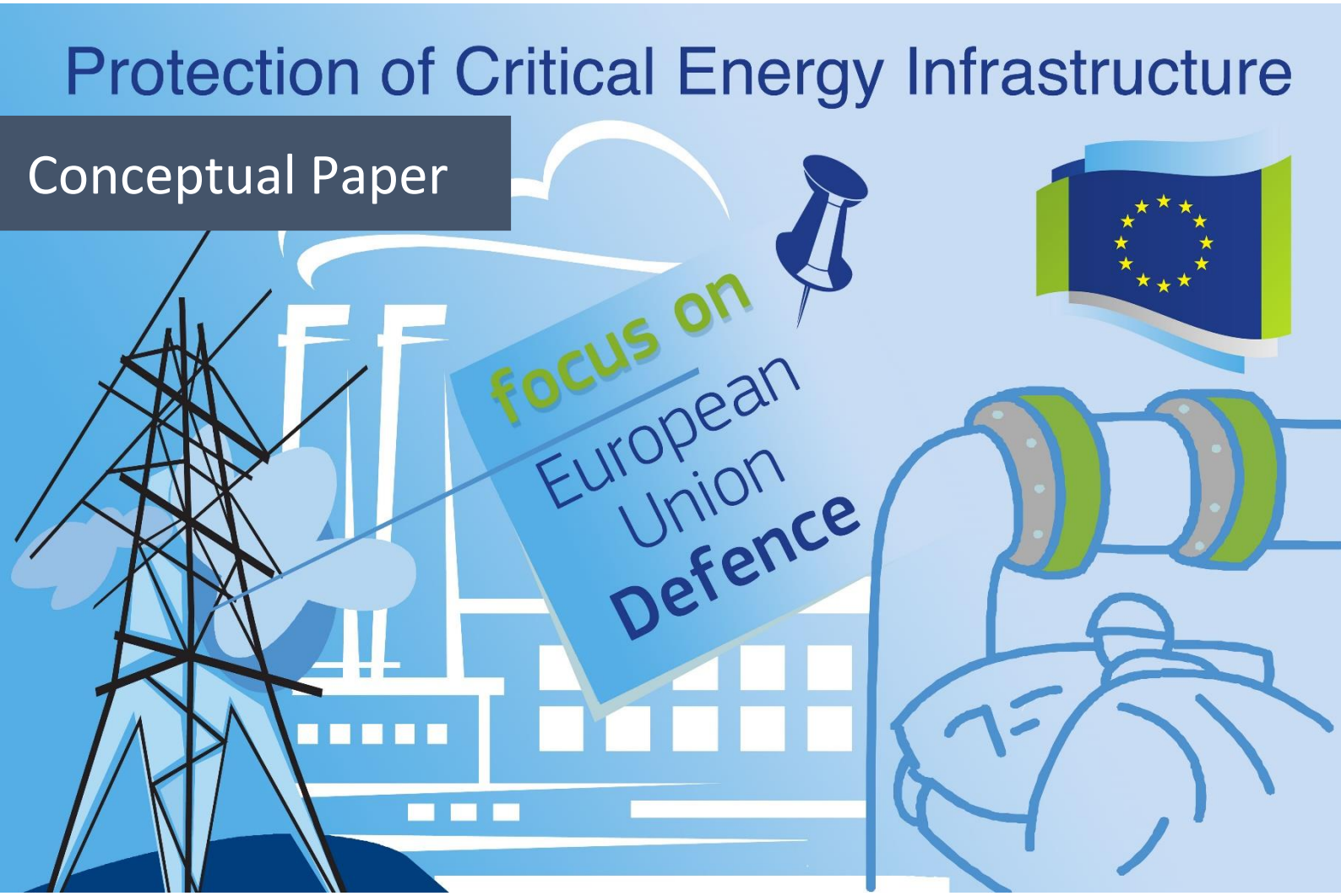
EUROPEAN DEFENCE AGENCY

CONSULTATION FORUM FOR SUSTAINABLE ENERGY IN THE DEFENCE AND SECURITY SECTOR

Protection of Critical Energy Infrastructure

Conceptual Paper



EUROPEAN DEFENCE AGENCY

PROTECTION OF CRITICAL ENERGY INFRASTRUCTURE (PCEI) EXPERTS GROUP

BRUSSELS, OCTOBER 2017

Protection of Critical Energy Infrastructure (PCEI) Conceptual Paper

PCEI Conceptual Paper
October 2017

This "Protection of Critical Energy Infrastructure (PCEI) Conceptual Paper" is developed by the PCEI Experts Group as part of the final deliverable of the European Commission-funded and EDA-led Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS).

PCEI Experts Group Contributors

Lead Member States:
Cyprus and Greece Ministries of Defence (MoDs)

Contributing Member States:
Bulgaria, Estonia and Ireland (MODs)

Academia and Research Centres:
Centre for Research & Technology Hellas (CERTH)
Cyprus University of Technology
European University Cyprus
KIOS Research and Innovation Center of Excellence, University of Cyprus
National Technical University of Athens (NTUA)

EU Institutions and Agencies:
European Commission: DG Energy and Joint Research Centre (JRC)
European Defence Agency (EDA)

Brussels, October 2017

Preface

This Conceptual Paper developed by the Protection of Critical Energy Infrastructure (PCEI) Experts Group, as part of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS), has identified the substantial role that PCEI can play in securing strategic energy autonomy within the European Defence Sector. Establishing a PCEI network in defence from scratch in a domain where cooperation hardly exists has been a remarkable achievement and reflects the determination to transit to a more sustainable energy future in the defence and security sectors. The engagement within this Group of the participating EU Member States, academia and research centres, and supported by the solid cross-institutional cooperation between the European Commission and the European Defence Agency, has demonstrated the commitment of the EU as a whole to enhance further the resilience and protection of defence related Critical Energy Infrastructure (CEI).

"Protecting the Union and its citizens" is one of the three strategic priorities of the new EU Level of Ambition, with the need for "strengthening the protection and resilience of its networks and critical infrastructure". The EU will be called upon to strengthen its engagement and solidarity mechanism in the protection of Member States and its citizens, including in the case of significant attacks or disruptions against Critical Infrastructure. Increased vigilance by the EU and its Member States will be required as disruption in the operation of CEI has the potential to hamper basic social and economic functions as well to adversely impact on the defence and security sectors.

There is an opportunity to foster an EU culture in protection and resilience of CEI in European defence. This momentum will help to initiate and develop cooperative defence related CEI projects for instance on joint training and exercises. It is our belief that by adapting and implementing EU policy, based on Sustainable Energy and Environmental Security priorities, the Union will ensure a pathway which leads towards a Sustainable Defence Sector. Building on this Conceptual Paper Member States supported by EU can move towards a broad consensus on how to invest in resilience and protection of CEI in a structured and collaborative manner.

Jorge DOMECQ
Chief Executive

Dominique RISTORI
Director-General

Abbreviations

CAT	**C**apability, **A**rmament & **T**echnology **D**irectorate.
CBRN	**C**hemical, **B**iological, **R**adiological and **N**uclear
CDI	**C**ritical **D**efence **I**nfrastructure
CEI	**C**ritical **E**nergy **I**nfrastructure
CF	**C**onsultation **F**orum
CI	**C**ritical **I**nfrastructure
CII	**C**ritical **I**nformation **I**nfrastructure
CIIP	**C**ritical **I**nformation **I**nfrastructure **P**rotection
CIP	**C**ritical **I**nfrastructure **P**rotection
CIR	**C**ritical **I**nfrastructure **R**esilience
CSDP	**C**ommon **S**ecurity and **D**efence **P**olicy
EC	**E**uropean **C**ommission
ECI	**E**uropean **C**ritical **I**nfrastructure
EDA	**E**uropean **D**efence **A**gency
EDEN	**E**uropean **D**efence **E**nergy **N**etwork
EDTIB	**E**uropean **D**efence **T**echnological and **I**ndustrial **B**ase
ESI	**E**uropean **S**ynergies & **I**nnovation **D**irectorate (EDA).
ESA	**E**uropean **S**pace **A**gency
EU	**E**uropean **U**nion
EUGS	**E**uropean **U**nion **G**lobal **S**trategy
ICT	**I**nformation and **C**ommunication **T**echnology
MS	**M**ember **S**tates
MOD	**M**inistries of **D**efence
pMS	**P**articipating **M**ember **S**tates
PCEI	**P**rotection of **C**ritical **E**nergy **I**nfrastructure
RES	**R**enewable **E**nergy **S**ources
SATCEN	**S**atellite **C**entre
SDU	**S**ecurity and **D**efence **U**nion
SEDSS	**S**ustainable **E**nergy in the **D**efence and **S**ecurity **S**ector
SESAED	**S**ecuring **E**nergy **S**trategic **A**utonomy for **E**uropean **D**efence

Contents

Executive Summary

As part of its work on improving the resilience of the defence and security sector, the European Defence Agency (EDA), through the Protection of Critical Energy Infrastructure (PCEI) Experts Group which is part of the Consultation Forum for Sustainable Energy in the Defence and Security Sector (CF SEDSS, has been exploring options for protecting defence related Critical Energy Infrastructure (CEI) from existing and emerging risk and threats, including hybrid and asymmetrical warfare, climate change and natural hazards. To help to maintain the European defence sector at the required levels of effectiveness and readiness, the aim is to identify both common capabilities (synergies) and research shortfalls and to develop plans for addressing collectively the challenges arising from the nexus of defence, energy infrastructure, resources, the future operating environment, and defence capabilities. This Conceptual Paper has been developed as part of the final deliverable of the first phase of the European Commission-funded and EDA-led CF SEDSS and is intended to support further expert analyses and the development of specific actions for elaborating comprehensive methodologies and tools for the protection of defence related CEI, both in the civilian and military domain.

The changing security and energy environment makes it necessary for CEI to serve both civilian and military operations and, in case of a severe crisis, be ready to switch from civilian to military *modus operandi* at short notice. Due to limited resources and the need to reduce operational costs we cannot afford critical infrastructures operating only for the defence sector and as a consequence closer collaboration between civil and military domains is paramount. The challenge is unprecedented since most often there are different procedures, regulations and *modus operandi* during a crisis. Apart from technological issues, the establishment of a common understanding between military and civilian staff is essential before, during and after an event. This requirement has become more evident as Europe has been struck by a number of adverse events in recent years. Terrorist attacks in EU capitals, huge refugee and migration flows, natural disasters, and a range of complex armed conflicts throughout the world have had a significant impact on the Defence and Security sectors. In addition, the impacts of climate change – including an increase in the frequency of extreme weather events, together with second and third order consequences such as drought, famine, and loss of livelihood and land – can be considered a threat multiplier. Armed forces have been asked to perform additional tasks to support police and civil protection, for instance by guarding strategic points, providing security and resources to refugee camps, or to contribute in search and rescue operations and in clearing and repairing damaged roads and other communications routes.

While the EU has put a lot of effort into making European Critical Infrastructure (ECI) more secure, the dependency of Defence on CEI has not been addressed yet within the Union. Given that the functionality of the Defence and security sectors relies either partially or entirely on CEI, any disruption, damage or failure can have adverse consequences beyond the public domain. Despite the fact that Member States (MS) have the primary responsibility for PCEI, a European framework is needed to provide direct assistance or coordinated solidarity during such events. This support is essential as the consequences of energy disruption can extend across national borders putting at risk not only the well-being of EU citizens but also causing negative impacts to the defence and security sector. To address the existing and emerging security and defence challenges, the European Commission has recently initiated the discussion on an enhanced defence capability for Europe. In this respect, President Juncker proposed three scenarios ranging from security and defence co-operation through a shared security and defence option to a fully-fledged common defence and security architecture for the EU. All three scenarios require the defence and security sector to do more including with regard to the protection and resilience of critical infrastructures (CI) in areas such as energy.

Capacity building and enhanced capabilities are vital to supporting armed forces in carrying out their tasks. A defence research budget has been already put aside within Horizon 2020 and is likely to continue beyond. Notably, for the first time in the EU's history the Commission is proposing through a European Defence Fund to boost collaborative projects and research to better address current and emerging challenges in the defence sector. The 2016 Global Strategy for the European Union's Foreign and Security Policy acknowledges the need arising from Europe's security environment for a stronger EU, able to promote peace, guarantee its security and protect its MS and citizens, including through increased civil-military cooperation, through Common Security and Defence Policy (CSDP) and in cooperation with its partners. Most significantly the Strategy underlines the need for the EU "to support the swift recovery of Members States in the event of attacks" through enhanced efforts on the protection of critical infrastructure.

The objectives above place a higher priority on decreasing dependencies and achieving autonomy, in particular operational energy autonomy. The increasing demand for energy by both the defence and the civilian sectors as well as the new threats that will arise from emerging technologies, natural hazards and the impact of climate change are sources of concern and alarm. Although defence does have its own energy resources it depends to a great extent on civilian resources. This raises some serious questions: *What happens if these civilian resources are compromised? How far will a cyber-attack to a series of civil power plants of Europe compromise the capability of EU national defence sectors to operate? Would a lack of energy supply to the EU undermine its capability to provide*

security? Will the armed forces still provide security to civilians when their own security of supply is threatened? Furthermore, how can the EU be prepared for hybrid threats which show a clear increasing tendency in magnitude and complexity? These are questions that need to be addressed and resolved in order to reinforce EU defence capabilities and to address existing and emerging challenges in the field of PCEI.

This Conceptual Paper concludes that there is a need to ensure the protection and resilience of defence and security sectors in times of crisis. In this respect, the Paper aims at providing the framework which could lead to the identification of best management practices, including an EU policy based on Sustainable Energy and Environmental Security priorities, to support MS further in strengthening the protection of all defence related CEI from threats, risks or vulnerabilities. To address these challenges the PCEI Experts Group proposes to Secure Energy Strategic Autonomy for European Defence through cooperation and practical assistance among MS. The Group recommends a number of steps that will help the EU MoDs to identify concrete actions for developing appropriate methodologies and tools, and initiating projects of mutual interest with the support of the EU. It is expected that the PCEI Conceptual Paper will support the efforts of the EU and its Member States in enhancing the resilience of defence related CEI and to provide an impetus for future work on the issue.

1. Introduction

The future security environment is expected to be increasingly affected by key environmental and resource constraints, including health risks and societal factors, climate change, water scarcity and energy needs. In addition to those constraints, natural hazards, physical and cyber threats, terrorism, criminal activity, hybrid and asymmetrical warfare are among the issues which may amplify vulnerabilities to CEI affecting negatively the defence and security sector. It is therefore imperative to Secure Energy Strategic Autonomy for European Defence (SESAED) to ensure national and international security and resilience. In this respect, PCEI is becoming an essential element of the European defence landscape[1] and consequently to economic prosperity.

[1] European External Action Service (2016) Shared Vision, Common Action: A Stronger Europe A Global Strategy for the European Union's Foreign And Security Policy (Brussels, June 2016), https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf, T. M. Jopling, "Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures", (157 CDS 08 E rev 1 NATO Parliamentary Assembly Special Report, 2008), OSCE, "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", (Organization for Security and Co-operation in Europe, 2013), A, Niglia, "The Protection of Critical Energy Infrastructure Against Emerging Security Challenges", (IOS Press, Amsterdam, 2015), Y. Zabyelina & I. Kustova, "Energy and Conflict: Security Outsourcing in the Protection of Critical Energy Infrastructures", Cooperation and Conflict, 50 (2015) 531– 549,

The importance of PCEI is acknowledged in recent Strategies and policy papers both at the EU intergovernmental and institutional level. In 2014 the European Commission's *European Energy Security Strategy* highlighted the high degree of dependency of the EU on external suppliers of energy with the EU importing 53% of the energy it consumes; including an import dependency of 90% for crude oil and 66% for natural gas.[2] This dependency is a matter of concern for every MS affecting significantly the energy strategic autonomy of the Union as a whole. In November 2016, the Council of the EU adopted conclusions on the implementation of an *EU Global Strategy in the area of Security and Defence*. "Protecting the Union and its citizens" is one of the three strategic priorities of this new EU Level of Ambition, with the need for "strengthening the protection and resilience of its networks and critical infrastructure" with the role of defence explicitly addressed.[3] In June 2017 the Commissions' *Reflection Paper on the future of European Defence* presented three different scenarios[4] for moving towards a **Security and Defence Union (SDU)**. In all scenarios, the contribution of the EU in enhancing the protection and resilience of CI in areas such as energy was highlighted.

Finally, in July 2017, in their *Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats -a European Union response*[5] the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy placed a great emphasis on the need for increasing resilience, strengthening and protecting critical (energy) infrastructures. As the Report indicates, in the implementing steps related to the building of resilience, the "Commission, in cooperation with Member States and stakeholders, will identify common tools, including indicators, with a view to improve protection and resilience of critical infrastructure against hybrid threats in relevant sectors". Notably, the Report acknowledges the development of the PCEI Conceptual Paper as one of the building blocks to support collective efforts in enhancing the resilience of the defence related CEI and countering hybrid threats.

---

https://www.eda.europa.eu/info-hub/press-centre/latest-news/2016/10/17/expert-group-looks-into-protection-of-critical-energy-infrastructures-for-defence (assessed on May 20, 2017).

[2] European Commission, "European Energy Security Strategy" (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Brussels, 28.5.2014, COM(2014) 330 final), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

[3] Council of the European Union, "Council conclusions on implementing the EU Global Strategy in the area of Security and Defence"(General Secretariat of the Council, Brussels, 14 November 2016, 14149/16) http://www.consilium.europa.eu/en/meetings/fac/2016/11/14-15/

[4] The three scenarios are, a) Security and Defence Cooperation, b) Shared Security and Defence and c) Common Defence and Security, see European Commission, "Reflection Paper on the future of European Defence" (COM(2017) 315, 7 June 2017), https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

[5] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats -a European Union response", Brussels, 19 July 2017, https://ec.europa.eu/docsroom/documents/24601

It is envisioned that in the future the SDU may be called upon to strengthen its direct engagement (i.e. through sectoral policies, solidarity mechanisms, risk or threat assessments)[6] in the protection of MS and EU citizens, including in the case of significant attacks or disruptions against CI. An increased role for the Union may be required as disruption in the operation of CI has the potential to hamper basic social and economic functions. Prevention, detection, response and mitigation measures are required that need to consider specific technical, economic, political and social/cultural aspects. Despite the fact that risk management plans are already in place to ensure that CEI are well protected against a variety of hazards and threats, adverse events may still occur. In such circumstances, CEI operators must be equipped with the appropriate tools to minimise downtime and allow CEI to bounce back quickly enabling essential operations to continue at an acceptable level of functionality. Building capacities in resilience will enable CEI to absorb, recover and bounce back from a disruptive event thus minimising the impact to the whole society including to the defence sector.

While the European Commission has put a lot of effort[7] into making ECI more secure, the dependency of defence on CEI has not been addressed at the EU level. Despite the fact that MS have the primary responsibility for PCEI, the EU should consider measures including through direct assistance or coordinated solidarity among MS. **To address challenges related to the defence – energy nexus** the **European Defence Agency**[8] has **identified the following related drivers**:

- Operational Security (Managing Energy Saves Lives while Diversifying energy sources reduces the need for resupply convoys);
- Economic Impact (Managing Energy Saves Money year on year and Money that can be reinvested in new equipment and technology);
- **Energy Resilience & Autonomy** (Managing Energy is key to European Strategic Autonomy);

[6] European Commission, "Reflection Paper on the future of European Defence" (COM(2017) 315, 7 June 2017 and European Commission, Energy Security Strategy, https://ec.europa.eu/energy/en/topics/energy-strategy-and-energy-union/energy-security-strategy

[7] For example through the "European Programme for European Critical Infrastructure Protection" (EPCIP), "The Thematic Network on Critical Energy Infrastructure Protection" (TNCEIP), the "European Reference Network for Critical Infrastructure Protection (ERN-CIP)", the "Critical Infrastructure Warning Information Network" (CIWIN), and the Council Directive "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection" (2008/114/EC, 8 December 2008), see European Commission, Energy "Protection of critical infrastructure", https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure, the European Commission, Migration and Home Affairs, "Critical infrastructure", https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en and COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

[8] http://ecde.info/sites/default/files/docs/01_presentation_roger.pdf (assessed on May 20, 2017).

- High Import Dependency, Arc of instability surrounding Europe – Security of Supply Freedom of Action on operations.

Against this background, EDA has concluded that a comprehensive approach is required to significantly improve energy security and resilience in the defence sector and in particular in the protection of defence related CEI. In this context, the European Commission has identified PCEI as one of the areas to be examined as part of the CF SEDSS[9] and initially required that there should be a specific working group to examine this topic. Taking into account that the PCEI is a cross-dimensional domain it was agreed that a dedicated Expert Group within the Consultation Forum should be set up. The Cyprus and Hellenic Ministries of Defence (MoDs) offered to take the lead along with their national academia and research centres[10] on exploring PCEI from a military perspective. As a result, the EDA cross Directorate CAT[11] - ESI[12] PCEI Experts Group was established with its 1st meeting held at EDA in May 2016. Since extending the invitation to all EDA participating Member States (pMS) Bulgaria, Ireland and Estonia have joined the Group (at its third meeting in January 2017). The European Commission DG Energy and Joint Research Centre (JRC) as well as the NATO accredited Energy Security Centre of Excellence (ENSEC COE – as observer) support the work of the PCEI Experts Group through sharing their expertise.

To implement its objectives the PCEI Experts Group has agreed to:

- assess how EU legislation on the PCEI can be applied by the defence sector in a holistic way;
- identify those components of CEI that are pertinent to the defence sector;
- maintain or/and improve regional energy strategic autonomy,[13] security and sustainability within the EU;
- identify modalities of how to ensure the uninterrupted availability of safe, secure and sustainable energy supplies;
- define ways of protecting each and every part of defence-related critical infrastructures, ensuring the uninterrupted functioning of the overall energy supply chain;
- identify common capability and research shortfalls which could be addressed collectively to help achieve resilience in the CEI that have a direct or indirect impact on European Defence.

[9] This Forum, launched last October 2015, aspires to highlight the importance of energy and energy security as a defence capability and to assess how the EU energy legislation can be applied by the defence sector, including in due course, access to EU funding.

[10] Academic and research support is provided by the Centre for Research & Technology Hellas (CERTH), the Cyprus University of Technology, the European University Cyprus, the KIOS Research and Innovation Center of Excellence - University of Cyprus and the National Technical University of Athens (NTUA).

[11] Capability, Armament & Technology Directorate.

[12] European Synergies & Innovation Directorate.

[13] i.e. locally nationwide or between adjacent EU pMS within the same geographical Region.

To address the above-mentioned objectives the PCEI Experts Group has developed the present PCEI Conceptual Paper, as part of the final deliverable of the Commission-funded and EDA-led Consultation Forum – SEDSS, to support the development of pilot actions for developing the requisite holistic approach with the necessary methodologies and tools. This initiative, addressed through the PCEI Experts Group, aims at identifying common needs, shortfalls and opportunities related to the PCEI in the defence and security sector, leading to increased protection and resilience in CEI and also to contribute to SESAED.

The PCEI Experts Group considers important for the MS to undertake actions which will enable each to assess its level of energy autonomy. While the Defence sector's own infrastructure may be well protected, the interface and dependency with civilian energy infrastructures is another challenge. In a Europe where MS armed forces are required to work more closely together the question of who supplies energy gains urgency and in particular, in cases where the armed forces are engaged in civilian type operations such as search and rescue, fire-fighting etc. **As such, the following challenges need to be addressed:**

- The degree of energy independence of the armed forces;
- The civil-military interface in terms of agreements and arrangements that need to be performed during preparedness;
- Security and interoperability requirements that Defence puts on civilian energy infrastructure and projection of future needs;
- Introduction in civil energy infrastructure risk assessment and security plans related to Defence threat scenarios, in the framework of civil – military cooperation;
- Development of joint training and exercises throughout the whole prevention, preparedness and response cycle;
- Support of national activities which improve engagement by MS in investing in enhanced security and resilience of civil CEI relevant to Defence.

This **Conceptual Paper concludes** that there is an urgent need for promoting safety and security standards to increase the resilience of CEI related to the Defence domain. Securing Energy Strategic Autonomy for the MS and the EU as a whole is becoming more vital. Member States can increase their resilience and continued availability of secure and sustainable energy supplies by depending on the support of other States in times of crisis. In this respect, there may be a role for stronger collaboration between Defence and civilian CEI. Such collaboration could require for example at the *strategic level*

to work on a common language; at the *operational level* to develop common threat scenarios and security plans; and at the *tactical level* to provide the resources needed for crisis management and asset recovery. Similarly, investment plans should be agreed and the commitment of both MS and EU funds should be considered. In order to provide a comprehensive response to these challenges at MS level a Defence Strategy related to PCEI needs to be put in place in order to develop capacity, to make the necessary investments as well as research plans, to tackle gaps in knowledge and to prepare common threat scenarios for joined activities and training.

2. Scope, Objectives and Context

Scope – Objectives

The PCEI Conceptual Paper aims at contributing to Securing Energy Strategic Autonomy of European Defence by ensuring the protection of all EU Defence infrastructure elements[14] from threats, risks and vulnerabilities. The **scope** of this Conceptual Paper is to raise awareness of the significance of PCEI in the EU Defence and Security sector and to contribute to the enhancement of CEI protection and resilience. In particular, the paper aims to:

- identify common needs, including shortfalls and opportunities, related to PCEI in the defence and security sector;
- provide a framework for increasing resilience and for identifying how PCEI can contribute to ensuring Energy Strategic Autonomy in the European Defence and Security Sector.

The **objective** is to ensure the proper function of the critical path of the whole energy supply chain and life cycle, in the EU defence and security sector, by maintaining and improving energy security and sustainability within the EU.

PCEI Context

While the concept of CEI for the civilian sector has received considerable attention, this has not been the case in the defence sector. This is not surprising considering that the defence sector relies to a large extent on civilian energy infrastructure; it has however resulted in a need for further investigation related to the CEI for European Defence. Thus, a definition of CI for the defence sector in the EU should be devised before the necessary measures and policies can be developed to mitigate disruptions in the operation of such energy critical defence relevant infrastructures. This forms the motivation and provides the rationale for **a deeper analysis** of the issue, **considering challenges** such as:

- Diversity of hazards and threats (e.g. natural, physical, cyber, hybrid, multidimensional);
- The presence of interdependent networks of infrastructures (telecommunications, internet, transportation, water, sewage, etc.) that are impacting the energy network which itself

[14] Including structures, platforms, services, human capital, telecommunications, data, etc.

consists of many (sub-)networks (e.g. electric power, oil pipelines and logistic chains, gas pipelines and logistic chains);

- The emergence of complex behaviours due to the non-linear dynamics of networks and their interactions;

- The need to secure the integrity and maintain the robustness of existing and future defence relevant installations, bearing in mind the increasingly interconnected and interdependent nature of the systems;

- The need for efficient and cost-effective (including dual-use) solutions consistent with the current global financial reality;

- The global struggle for resources which are interlinked through the "Energy-Environment /Climate-Water-Food-Raw Materials" Resource nexus and which sets limits to global growth and prosperity;

- The fact that Energy is the fundamental "currency" of transactions occurring on the nexus where technical (energy, environmental, IT/Cyber), economic (financial and logistics), political (including geopolitical/geostrategic) and social/cultural aspects are colliding in the search for an optimized solution.[15]

- The need to enhance Resilience[16] within the Defence[17] and security sector by minimizing interruption of energy supplies and ensuring the protection of relevant CEI.

[15] Research has traditionally targeted the development of technologies that enable the transformation, reuse and management of all elements of the nexus in a sustainable manner, towards the realization of a Circular Economy and past work (i.e., A. G. Konstandopoulos & S. Lorentzou, "Novel Monolithic Reactors for Solar Thermochemical Water Splitting", in On Solar Hydrogen and Nanotechnology, (ed.) L. Vayssieres, (John Wiley & Sons New York 2010) 623-639, A. G. Konstandopoulos, C. Pagkoura & S. Lorentzou, "Solar Fuel and Industrial Solar Chemistry", in Concentrating Solar Power Technology: Principles, Developments and Applications, Part 3 Optimisation, Improvements and Applications, (eds.) K. Lovegrove & W. Stein, (Woodhead Publishing Series in Energy No. 21, Oxford 2012) 620-661, O. Deutchmann & A. G. Konstandopoulos, "Catalytic Technology for Soot and Gaseous Pollution Control", in Handbook of Combustion Vol. 2: Combustion Diagnostics and Pollutants, (eds.) M. Lackner, F. Winter & A. K. Agarwal, (Wiley VCH, 2010) 465-509) has contributed to the development of such enabling technologies. However, this alone is not sufficient to prevent the generation of additional volatility, instability and eventually vulnerability of our world;

[16] Resilience is broadly interpreted as the ability to rebound fast from a failure event, see J. Gao, B. Barzel & A-L. Barabási, "Universal Resilience Patterns in Complex Networks", Nature 530 (2016) 307-312, A. Garas, Interconnected Networks (Springer, New York 2016), L. M. Shekhtman, M. M. Danziger & S. Havlin, "Recent Advances on Failure and Recovery in Networks of Networks", Chaos, Solitons and Fractals, 90 (2016) 28–36.

[17] Resilience in the defence sector can be viewed as the ability to recover fast operational capacity in relation to any planned mission objectives. In the current context, resilience is an intrinsic attribute of the complex eco-system of the interacting networks of infrastructures and the defence functions.

3. Geopolitical Context

Energy and geopolitics have always been closely linked. We need to assess whether, when and how energy can be used as an instrument of national security. Challenges of energy security impact all of Europe: including through diversification of energy routes and sources, the modernization of the existing energy infrastructure, the security of energy supply at competitive prices, and the defence element of CEI.

Energy security is a key element for Europe.[18] Member States support energy infrastructure projects in order to increase energy security and respond to the growing energy demand in EU. The protection of energy infrastructure is not new to Europe. As of 8 December 2008 the Council issued the 2008/114/EC directive[19] *on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. The European perspective is that of an ***all-hazard approach***- although countering threats ***from terrorism*** is seen as a priority.

The geopolitics of energy plays a key role in cementing better relationships with other countries and vice versa. Smooth relations among States contribute positively to excellent cooperation in the energy sector. It is also obvious that geographical location in itself turns out to be crucial in meeting the above-mentioned needs of security in the energy sector, and prosperity and stability in a wider geographical area. On the one hand, an important feature of the energy sector is the interdependence of energy infrastructure, as well as the dependence of the other sectors on energy. This means that the energy sector as such is uniquely critical for a MS and consequently, an extremely attractive target for enemy attack (including terrorist attacks and cyberwarfare). This is not a new threat. On the other hand, the transit countries could be well protected from threats from the countries supplying them with energy. In this way, there is stability and protection of CEI.

The energy security of MS may also be disrupted by attacks against CEI, both internally and abroad, transit disruptions in key "chokepoints", cyber threats, as well as CBRN (including CBRNe[20]) threats, both intentional and accidental. Such ***transnational risks*** to energy infrastructure, require not just

[18] EUROPEAN COMMISSION (2014) "European Energy Security Strategy", (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Brussels, 28.5.2014)l, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

[19] EU COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[20] Chemical, Biological, Radiological, Nuclear and Explosive.

national-level coordination and intelligence-sharing among government agencies, industrial players and local communities, but also harmonization of procedures, across national boundaries.

Geopolitical issues in the energy sector may also take the form of a country's *ability to contribute to the diversification of routes and sources*. Gas transit countries fall into this category. ***The more pipelines that are installed in a country, or are interconnected with each other, the more diversified and resilient the route.*** But an abundance of routes is not the only ingredient of energy security, and the availability of a multitude of sources must also be taken into account. Multiple energy sources in combination with additional routes constitute essential elements of energy security - and especially within volatile geopolitical contexts - because they imply that the EU energy market is not dependent on one primary source only, or on only one energy supplier. Such diversification leads also to stability of the market.

Diversification of energy supply requires sophisticated and complex infrastructure, with an emphasis on cross-border infrastructure projects, which meet international standards of energy security. These could include for example design specifications for natural disasters tolerance, technical and operational specifications which mitigate the threat of disastrous accidents, and security measures to deal with the threats of terrorist attacks or cyberwarfare. As a consequence, it is important, that a State's relations with its neighbours enhances the stability of the wider region, thus becoming a bridge of nations with common interests -at least in the energy sector. That might make a given State's energy infrastructure more sensitive (in the sense of being vital) but given smooth bilateral relations and participation of that State in multilateral mechanisms, it can reassure the energy community about the safety of energy business across and within that State's border.

Energy needs in European Defence: It is a fact that the public does not readily associate energy efficiency and environmental protection with military priorities. However, given that the MS Armed Forces are among the largest energy consumers in Europe, energy can become a significant vulnerability in military operations (peace and war) unless it is managed effectively. An increase in military equipment often leads to increases in energy use and thus energy dependence, which in turn increases the complexity and cost of utilising the equipment operationally. Therefore, energy efficiency can be critically important to improving military capabilities, and in maintaining unit autonomy and operational resilience on the battlefield.

Evolution of Energy Security: The concept of energy security is undergoing a rapid transformation. In the past, geopolitics and the supply of oil and gas were the dominant factors determining energy

security. Today, a broader and more complex spectrum of elements is interacting to both stabilize and threaten energy security. The availability of energy sources, both fossil fuels and renewables, is increasing. In particular, a major source of change is the strong growth in the production and integration of renewable and distributed energy, which offers opportunities to diversify the energy mix and thus improve energy security.

In recent years, global conditions have been challenging for the energy sector. Changes in energy prices and production, a slowdown in the growth of emerging economies and geopolitical instability have reshuffled energy demand and supply scenarios. Geopolitical adjustments around the world in response to these changes point to a potential shift in global energy consumption from a mix dominated by fossil fuels to one driven by low carbon technologies. An increase in the consumption of renewable energy may thus bring a shift in centres of geopolitical power. A highly significant opportunity for the EU to diversify in this changing environment arises also from the discovery of its own resources and the further development of its infrastructures thus increasing its energy security and enhancing its strategic autonomy.

For foreign and security policy analysts, pipelines tend to be the entry point into the world of energy. Pipelines however create dependencies between States, they have long lifetimes (decades) and a highly symbolic political value. This is mainly due to the growing flexibility of European—and partially global—natural gas markets in light of the massive increase in liquefied natural gas (LNG) supply, interconnectors, and spot market trade. This new market environment has not only changed the relationship between producers and consumers but has also altered the political and economic leverage of transit countries.

Digitalization is also necessary for the smooth and efficient functioning of modern energy infrastructures. However, this heightens cyberspace threats to energy systems, especially since modern grids have become more interoperable and remotely accessible with the aim of reducing costs and improving efficiency. Operators are aware of the cyber risks which could have far-ranging adverse effects on a transnational scale.

It is now clear that a MS by itself cannot ensure autonomy based on national capacities only but has to consider interactions within its network of strategic partners. In essence, it needs to realize that **strategic autonomy does not imply having access to infinite domestic resources but having a diversity of options and choices within the nexus of the European Energy eco-system including the European Defence dimension**. Decision makers must give priority to the security of energy supplies

and a reduction of dependence on imported energy when deciding on the energy mix of their country and especially when planning the energy mix of their defence sector. Diversifying energy supplies, increasing the contribution from alternative energy sources (i.e. Renewable Energy Sources -RES) and consuming less fuel by implementing energy efficiency measures, will reduce exposure of the sector to energy dependency and will reduce the risk of future energy instability.

4. Aspects of Critical Infrastructure

As the economies of the world grow and societies develop, so does the importance of energy and the infrastructures. CEI provide the "building blocks" that keep the global economy moving and societies working. Energy resources guarantee our way of life and help to improve our standard of living. PCEI applies to peacetime routine functions. Its purpose is for the MS to be able to anticipate, identify, mitigate and recover from possible and likely attacks on CEI with minimum disruptive impact on MS social, political and military cohesion.

According to EU legislation (Council Directive)[21] the term 'critical infrastructure' means an asset, system or part thereof located in MS which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a MS as a result of the failure to maintain those functions. Although the Directive discusses the issue of CI, in fact it is restricted only to the energy and transportation sector. It is the responsibility of the MS to identify those infrastructures in energy and transport that if disrupted will also affect other MS and designate them as ECI. For those designated ECIs certain measures need to be taken in order to improve their level of protection.

Several MS have designated CI in the energy sector as ECI. Furthermore, many MS have taken advantage of the EU Directive to set-up their own national programmes for CIP with a particular focus on energy and transport. Whilst the criticality thresholds used in determining ECI differ among MS, nevertheless the Directive has aided MS in increasing their awareness of the risks and vulnerabilities of their critical systems. A broad range of energy infrastructure protection issues must be addressed for which comprehensive and regular assessments are necessary. Infrastructure situational awareness should be enhanced to the maximum extent possible and private owners and operators should regularly report to state authorities on the status of their infrastructures. In addition, state authorities could arguably do more to share threat information with the private sector.

The need to develop a "holistic approach"[22] has arisen, stemming from the EU "Comprehensive Approach". A PCEI strategy, can secure energy strategic autonomy of the European Defence sector, by protecting and strengthening the resilience of CI (such as structures, platforms, services, human

[21] Council Directive 2008/114/EC
[22] Centre for European Policy Studies (CEPS), Protecting Critical Infrastructure in the EU (2010), Brussels (CEPS TASK FORCE REPORT), http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

capital, telecommunications, data, etc.) from all possible threats, and by ensuring the smooth and unobstructed function of the energy supply chain of the EU Defence and Security sector.

This accords with the three strategic priorities of the EU Global Strategy corresponding to the EU's new level of ambition: *responding to external conflicts and crises, building the capacities of partners and protecting the EU and its citizens*. All of which set up PCEI as an important tool utilised to anticipate, identify, mitigate and recover from disruptive events with minimum impact on the social, political and military cohesion of the Union. PCEI underlines the need for the EU "to support the swift recovery of MS in the event of attacks" through enhanced efforts on the protection of critical infrastructure.

For the European community, energy security and CEI security presents both challenges and opportunities arising from the need to prepare, protect and respond to threats. In addressing Europe's current and future security and defence needs the EU ought to enhance its strategic autonomy in order to be able to act alone as well as with partners wherever necessary. The changing security landscape combined with the new political momentum ask for the EU to leverage existing capacities within the EU but also for investing in areas that require strengthening. Energy security and CEI security lie at the heart of the Union's ambition to protect the Union and its citizens, demonstrating the nexus in this respect, between internal and external security; where the EU's external policy and actions have a direct impact on its internal security and resilience of its infrastructure. The energy sector relies on a large number of diverse categories of infrastructure, all of which constitute different components of the energy chain.

There are strong reasons why energy infrastructure has become so important. In recent years the infrastructure of transportation, storage, recycling and management of energy sources have become the target of criminal acts committed by terrorist groups, which could negatively affect military operations. Recent research indicates that oil infrastructure is generally considered as the most likely terrorist target, due to both the high dependence of European States and the concentration of resources in a relatively small number of third countries.[23] On the other hand, the gas and the electricity sectors, which rely on regional infrastructure networks are less attractive targets as an attack would result in a localized and limited impact.

Europe is a major net importer of energy, and in the major sub-sector of oil and gas, it comes towards the end of the energy chain. That means that Europe is dependent on a lengthy energy infrastructure

[23] EAPC, Industrial Planning Committee, Report on the IPC work on the Protection of energy critical infrastructure, 14 Dec 2007.

the majority of which, is located abroad. Infrastructure located in third countries can be more attractive to terrorists, and could have major cascading effects. It is impossible to protect CEI fully against all types of threats. In this sense, CEI is actually a risk management exercise, the main goal of which, is on the one hand to reduce the risk to CEI to an acceptable level, on the other hand to increase the resilience, and to strike a balance between efficiency and resilience. As we cannot protect everything, resiliency (including recovery capacity) are paramount to ensuring continuity of service.

While in previous decades, energy companies used to belong to or be managed by national governments, nowadays the majority of those companies belong to the private sector. As an example, during the Cold War, the majority of these energy producing companies, including railways, ports, airfields, grids and airspace were in State hands and easily transferred to NATO control for those MS concerned, in a crisis or wartime situation. Today, by contrast, 90 per cent of NATO's supplies and logistics are moved by private companies and 75 per cent of the host nation support for NATO forces forward deployed on the territory of the eastern Allies comes from private sector contracts.[24]

This new situation in terms of CI governance needs to be seriously considered since it may hinder the capacity of the defence sector during a crisis. The objectives of CI operators may be different with respect to the objectives of the security and defence sector. In this case, increased protection of specific energy infrastructure may have a significant cost which the private sector might be reluctant to bear. It is however, the responsibility of the MS to demonstrate to infrastructure owners that **costs associated to protection and resilience is actually an investment** that may save several times more money down the road in the occurrence of adverse events. As mentioned by Commissioner for Humanitarian Aid and Crisis Management Stylianides in 2014 in his confirmation hearing to the European Parliament, ***1 euro invested in Resilience saves 7 euros in emergency***. In addition to this, asymmetric threats can make it hard to define when a "war state" exists which creates ambiguity with respect to rules of engagement.

International co-operation is essential with respect to the majority of the action areas identified above. Given the transnational character of the energy supply chain, MS have a vested interest in co-operating to ensure the integrity of the energy infrastructure system. More experienced and resourced States have a vested interest in sharing their expertise and providing assistance to other less well-resourced States. As the energy security of a particular State is closely linked to that of others, each State needs to know what others are doing. Compliance with existing international safety and security standards

[24] NATO Review Magazine, Resilience: a core element of collective defence, 2016 ,www.nato.int

is a key element of transparency and is essential to regional energy stability. International co-operation is obviously indispensable to further promote such compliance, including through the provision of assistance, expert advice and training. ***One should not forget that in highly interconnected sectors such as the energy sector the overall security and resilience of the energy networks is as high as that of its weakest link.***

Besides, many actors (e.g. operators, regulators, authorities) of the energy sector feel that as the energy infrastructure system is transnational, a need exists for international efforts towards the development of a uniform cross-border regulatory framework and a comprehensive set of international standards for energy infrastructure security. International organizations such as the European Network of Transmission System Operators for Electricity (ENTSOE) and Gas Infrastructure Europe (GIE) also have an important role to play, in their different field of expertise, where they can add value to existing efforts.

In conclusion, the following **needs** have been identified within the framework of the development of the PCEI Conceptual Paper, followed by **recommendations** on **how to enhance EU PCEI in EU defence and security sector**.

Needs[25]

- There must be an increased policy and operational focus on resilience and preparedness both at EU and National level.

- Integrate PCEI into EU policy-making processes. Develop policy validation methodologies. Also, methodologies to stress-test existing policies should be developed through public funding of *ad hoc* research projects.

- Build a long-term PCEI strategy for EU to address among other issues related to civil-military cooperation. The EU needs a forward looking well defined strategy, and strong political commitment. The fact that suppliers are often global players, while public policy-makers act at a local level, makes the policy dialogue more difficult and international coordination even more important.

[25] EU Global Strategy, Joint Communication to European Parliament and the Council, EC July 2017, After the EU Global Strategy *Building Resilience,* EUISS June 2016, (OSCE, http://www.osce.org/atu/33481?download=true, PCEI against terrorist attacks, Reinforced NATO Economic Committee Meeting, 22 Sep 2008).

Recommendations[26]

- The nature of subsidiarity in the coordination of PCEI policy at international level must be clarified. The EU should perform a thorough subsidiarity test to identify areas where joint action is more desirable, and areas that should remain under national competence.

- The EU needs to explore options to enhance civil-military cooperation among CEI stakeholders and exchange best practices. Also, it needs to examine all possible options and frameworks from *ad-hoc* voluntary collaboration to more structured schemes throughout the whole cycle of preparedness, prevention and response. Taking on board existing national initiatives, identify commonalities and further support them in the framework of EU *acquis* is paramount.

- Adopt a 'new approach' for industry-government cooperation. General principles on PCEI policy should remain EU MS responsibility while the best technical approaches to achieve the desired level of resilience should be decided by the industry itself.

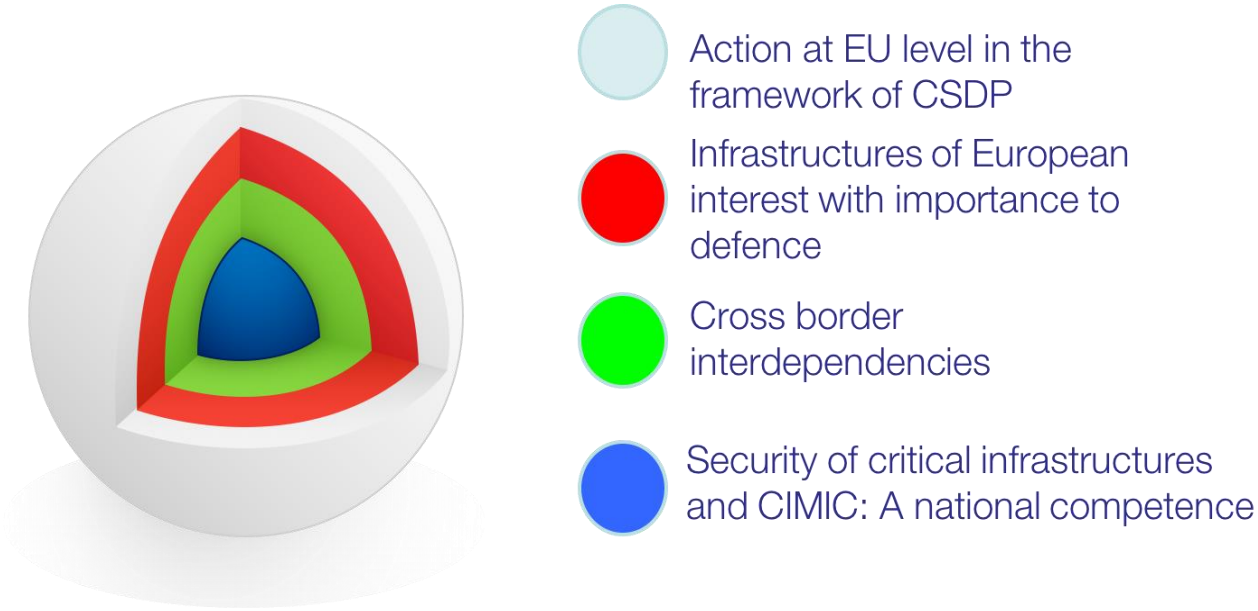


Figure 1: Layers of action in critical energy infrastructure protection and defence: From national competences to enhanced EU collaboration

[26] Ibid.

5. Facilities and Assets – Data Structure

Energy infrastructures are comprised of assets, systems, and functions of non-uniform "criticality" in nature, both at national and EU level. Yet it is necessary to develop an integrated methodological framework to efficiently identify facilities, systems, and functions of CI so as to easily monitor and enhance their preparedness.

During the evaluation of CI vulnerabilities to external threats, there are some particular energy assets and system parameters that deserve detailed consideration.[27] Identifying and prioritising which properties or attributes of an infrastructure are most essential to its function or have the most significant impact in case of threats or damage, is necessary for developing an effective protection strategy.[28] Among others, physical and location attributes of a CI (suppose a pipeline for example) will help to identify local particularities and develop protective strategies. Also, there are volumetric attributes that may refer to black spots caused by potential damage, functionality constraints or system incapacities and temporal attributes that consider operational fluctuations related to time or load constraints. Human capital constitutes another crucial energy asset, as highly qualified and skilled personnel are engaged in designing, constructing, monitoring, maintaining and restoring all CI. There are also economic assets in the military infrastructure as military logistic activities are indispensable in order to shape, control and monitor the procurement processes in the integrated energy supply chain especially in times of crisis.

Beyond the identification of individual critical assets, identification of their (inter)dependencies and the impact of those assets on other systems or other CI are also crucial given the complexity of energy CI, and the diversification of energy routes. For instance, a natural gas facility providing fuel for electric generation, will in the event of abrupt disruption of gas supplies, cause functionality problems through cascading effects to other CI as well. Other natural events (e.g. earthquakes, fires, volcanic activities), events of accidental nature (e.g. explosions), intentional criminal or terrorism acts against energy CI will also affect several energy or transportation CI in one or more States. Cyber attributes are equally important as complex networking systems link all previous energy system parameters and help control and monitor them through remote authorized use. This means that for some military infrastructure,

[27] Energy Sector-Specific Plan, an Annex to the National Infrastructure Protection Plan, United States Department of Energy, 2010.
[28] Moteff, J., Parfomak, P. Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, Congressional Research Service, the Library of Congress, October 2004.

the failure to reach sufficient resilience standards in one State can have a detrimental effect on many others.[29]

A complete record of military facilities and assets may have adverse results in terms of increased vulnerabilities in case of unintentional release. Instead, upon attempting to map CI assets, MS should prioritise in a harmonized manner which CI deserve detailed attention in the framework of protection planning based on a hierarchical approach with pre-defined criteria. A data request process for those CI should include data about CI current status, special particularities, capacity status, reporting on any past incidents, possible threats and vulnerabilities that can contribute to the development of a strategic protection plan based on strategic priorities. Supplementary data may include records regarding actual or potential interference with limited capabilities, including any past operational problems or maintenance actions and details from investigatory exercises, drills or other simulations during survey periods. Collecting non-sensitive information within a MS should help evaluate the efficiency and even restore functionality of military facilities. To that goal, potential existing information resources may be accessed through local governments, MoDs, industrial manufacturers of military technical equipment, and other relevant private sectors, owners and operators of CI, regarding for example the location and capacity of electrical grids, or oil and gas asset data, such as location or throughput data.

To facilitate the overall process and maximize the practical advantages of this effort each Member State is encouraged to collect required data in a standardized manner in order to ensure consistency in interpretation. A simple rating system (e.g. weak, low, moderate, high, very high) based on user-defined criteria or a performance based evaluation may be used to measure the assets value and potential impact of their loss. In a more complex management system, the value of an asset and impact of loss should be calculated in monetary units[30] based on predefined cost parameters (e.g. original construction or reconstruction costs, costs of increased regulatory oversight). Appropriate treatment of relevant information requires a-priori consideration of issues such as:[31] *which entities will be in charge of collecting data and how often (e.g. quarterly), what type of data will be collected, the availability of information, the information-sharing process and what would be the use of information.* To that extent, trust and confidence are crucial components due to the sensitivity of some data.

[29] Hämmerli, B., Renda, A., Protecting Critical Infrastructure in the EU, Centre for European Policy Studies, Brussels, 2010.
[30] Moteff, J., Parfomak, P. Critical Infrastructure and Key Assets: Definition and Identification, CRS Report for Congress, Congressional Research Service, the Library of Congress, October 2004.
[31] Cyber Security Strategy for the Energy Sector, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, ITRE: 2016-04, European Parliament, October 2016.

However, these are properties that only develop with time and mutual cooperation,[32] and therefore upfront regulation still remains challenging. A crucial aspect of facilities and data analysis is the verification and update of the collected data.[33] It may be fruitful to develop a rigorous data verification and validation framework through advanced programmes or procedures to meet mutually agreed-upon levels of accuracy and put in place safe-guards against unintentional release.

Given that a cyber-attack is another important threat for CI, yet less likely within defence, it would be an omission if not separately mentioned herein. This type of threat can cause great harm to CI (e.g. an abrupt disruption of the energy flow within the military infrastructure). So, there is a profound need to increase resilience of the Information and Communication Technology (ICT) factor or else the Critical Information Infrastructure (CII)[34]. ICT is known to be integral to the running of power systems, in particular modern power systems are dependent on ICT, e.g. Supervisory Control and Data Acquisition (SCADA) systems. Recent worldwide episodes have highlighted the need for an internationally coordinated CIP policy.[35] The heterogeneity in causes and magnitude of past disruptive events makes the all-hazards approach towards protection essential in order to account for both natural disasters and man-made attacks when designing prevention and remediation measures. Current experience from existing progress of EU cyber security policy will aid this effort. Indicative examples include the EU Agency for Network and Information Security (ENISA), the Network Information Security (NIS) Directive [36] and the Computer Emergency Response Team for the EU institutions (CERT-EU).[37]

To conclude, **recommendations**[38] for the development of effective methodologies towards data analysis procedures **governing the relations of defence related CEI** are set out below:

- Establish criteria and indicators to assess the outcomes of national and EU-wide information-sharing initiatives in order to allow the tracking of progress towards common, coordinated goals in PCEI policy.

[32] Perl, R.F., Protecting Critical Energy Infrastructures Against Terrorist Attacks: Threats, Challenges and Opportunities for International Co-operation, Organization for Security and Co-operation in Europe (OSCE).
[33] Energy Sector-Specific Plan, an Annex to the National Infrastructure Protection Plan, United States Department of Energy, 2010.
[34] European Commission, Strategy, Digital Single Market, Policy on Critical Information Infrastructure Protection (CIIP) 2013, https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip
[35] Hämmerli, B., Renda, A., Protecting Critical Infrastructure in the EU, Centre for European Policy Studies, Brussels, 2010.
[36] "European Commission, Strategy, Digital Single Market".
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[37] "Computer Agency Response Team EU", https://cert.europa.eu/cert/plainedition/en/cert_about.html
[38] (OSCE, http://www.osce.org/atu/33481?download=true, PCEI against terrorist attacks, Reinforced NATO Economic Committee Meeting, 22 Sep 2008).

- Foster trust between information-sharing partners. Time is needed along with well-defined rules, sector-specific arrangements and sharing units of limited size.

- Develop common approaches for PCEI risk assessment based on the ongoing production of data and relevant information. Defence aspects should be carefully considered through the development and adoption of EU common risk metrics and standardized approaches for risk identification, assessment and management.

- To utilize existing infrastructure (e.g. European Space Agency -ESA), EU Satellite Centre -EU SATCEN) for data collection, processing and interpretation purposes.

- To seek cooperation with ESA and/or EU SatCen in the framework of feasibility studies and demonstration projects on the use of space infrastructure and applications for protection of CEI.[39]

[39] Space based Positioning, Navigation, and Timing (PNT), Earth observation and Telecommunications infrastructure and (integrated) applications contribute to controlling CEI and increasing safety, security and efficiency. Space as a tool supports energy infrastructure resilience and protection, and has added value in observation and control over energy infrastructure and risk management.

6. Systems Complexity, (Inter)Dependencies, Cascading Effects

Energy infrastructures are complex systems with many parts that interact with each other within the energy sector and across other CI sectors, which may lead to cascading effects. In the EU, the CIP landscape is more complex due to the increasingly interconnected cross-border energy networks.

Modern energy infrastructures provide essential fuel to all other sectors of defence CI including transport, ICT, water, etc. Without energy, most of these sectors cannot operate properly. The energy sector initiates more cascades than any other sector. A disruptive event on defence related CEI can create cascading effects on other infrastructures dependent on them with impacts on these different sectors. This is due to the nature of modern CIs (including energy) which are now increasingly complex and more interconnected than ever and often operate as a system of systems. This interconnection gives rise to dependencies or interdependencies, whereby the effective operation of a CI relies more and more on the normal operation of other CIs. For example, electric power provides energy to pumping and compressor stations, storage facilities and control equipment for oil and natural gas. Power outages can affect oil and natural gas production and transportation whereby refineries may be shut down and oil terminals, gas tanks and pipelines may become inoperable due to electric power loss. Oil provides fuel and lubricants for electricity generators, and natural gas provides energy to generating stations, compressors and storage facilities. Power grids might also be affected by communication system disruptions as ICT is increasingly important in real-time monitoring of power production. Transport disruptions (road, rail, ports, aviation etc.) may lead to disruption of energy supply for fuels such as diesel. Water infrastructure also requires power to operate.

The following **types of (inter)dependencies** can be identified for **defence related CEI**:

- **Physical interdependency**: A physical interdependency arises from a physical linkage between the inputs and outputs of two infrastructures.
- **Cyber interdependency**: An infrastructure has a cyber-interdependency if its state depends on information transmitted through the information infrastructure.
- **Geographic interdependency**: A geographic interdependency occurs when elements of multiple infrastructures are in close spatial proximity, thus a local environmental event can create state changes in all of them.

- **Logical interdependency**: Two infrastructures are logically interdependent if the state of each depends on the state of the other via a mechanism that is not a physical, cyber, or geographic connection.

Interdependencies have been widely studied and demonstrated in several case studies, e.g. Schneidhofer,[40] Haraguchi and Kim,[41] Gordon and Dion,[42] Fleming.[43] **Annex B** lists a series of representative case studies of systems complexity and interdependencies.

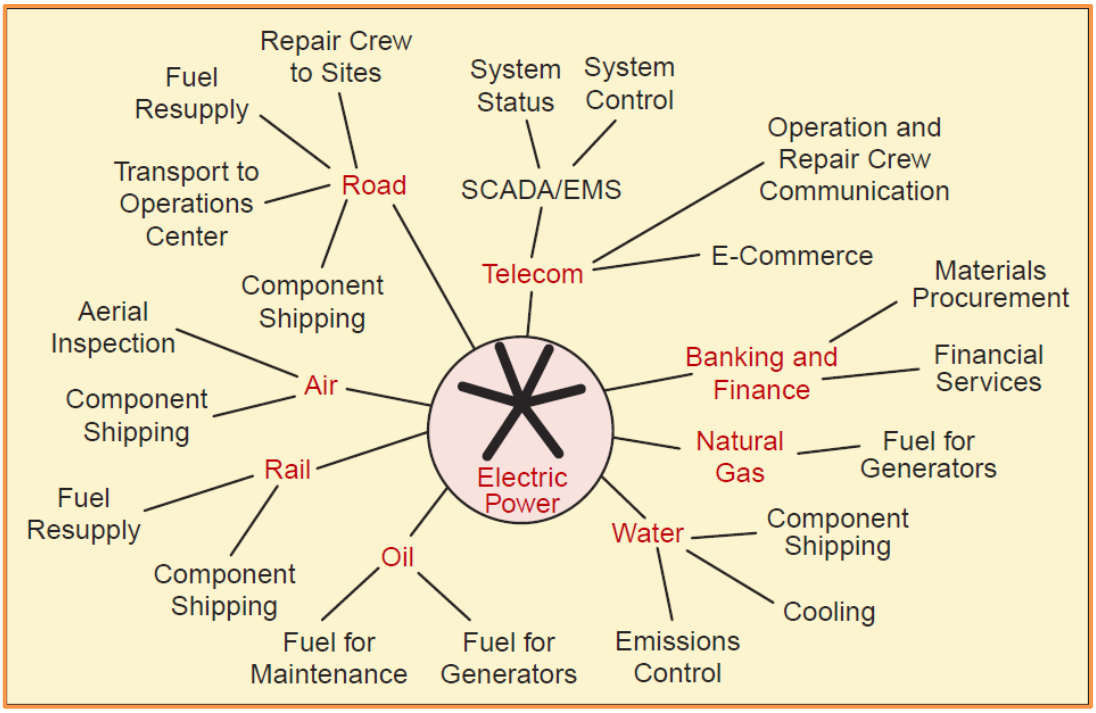


Figure 2: Example of Power System dependencies[44]

[40] Bernhard Schneidhofer, A case study in Critical Infrastructure Interdependency, Technical Report RHUL–ISG–2016–12 Royal Holloway University of London (2016).
[41] Masahiko Haraguchi Soojun Kim CRITICAL INFRASTRUCTURE SYSTEMS: A CASE STUDY OF THE INTERCONNECTEDNESS OF RISKS POSED BY HURRICANE SANDY FOR NEW YORK CITY, Global Assessment Report on Disaster Risk Reduction, The United Nations Office for Disaster Risk Reduction, 2015.
[42] Kathryn Gordon and Maeve Dion PROTECTION OF 'CRITICAL INFRASTRUCTURE' AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY Organisation for Economic Co-operation and Development Report 2008.
[43] Cherylne Fleming A Resilience Approach to Defence Critical Infrastructure21st International Congress on Modelling and Simulation, Gold Coast, Australia, 29 Nov to 4 Dec 2015, www.mssanz.org.au/modsim2015
[44] Rinaldi, S.M., Peerenboom, J.P., and Kelly, T.K. (2001) "Identifying, understanding, and analyzing critical infrastructure interdependencies", IEEE Control Systems Magazine, Vol.21, No.6, pp.11-25 .

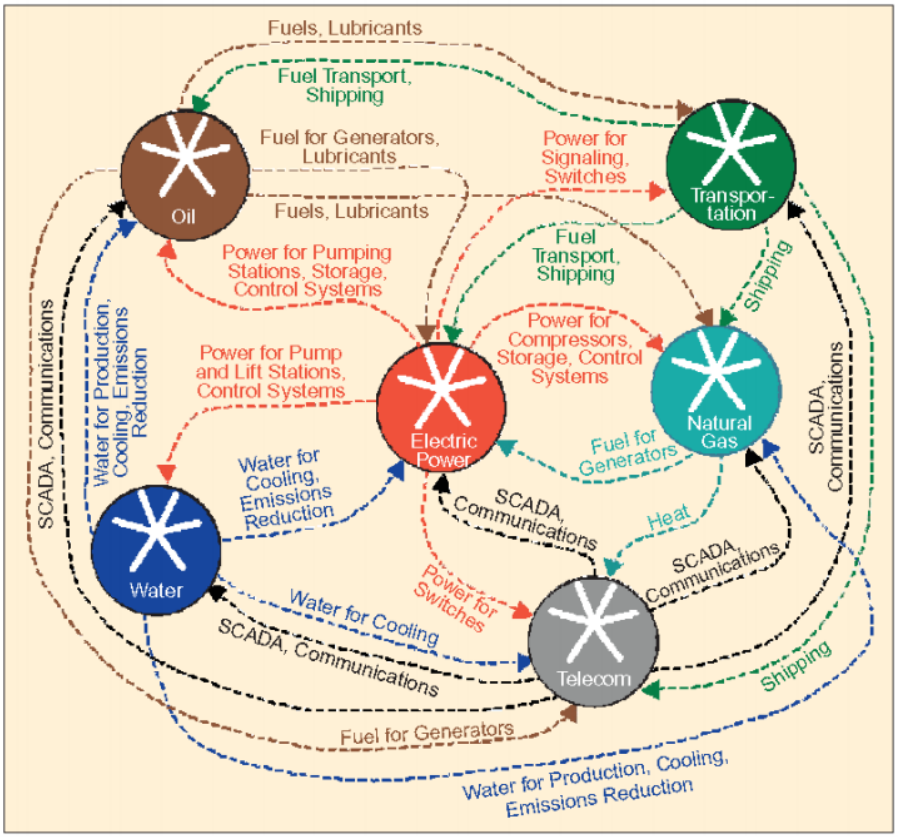


Figure. 3: Interacting energy critical infrastructures viewed as a complex system[45]

As CI are complex, interdependent systems and the consequences of their disruptions may extend beyond the geographical borders of a MS, modelling and simulation is essential to manage the complexity of CI.[46] Network theory is a powerful tool for modelling which can describe, analyse and understand in a unifying manner the complex interactions that occur in such systems. The network approach to a complex system (or to the set of interacting infrastructure systems) involves a set of basically simple actions based on a desired set of criteria. These actions include: *identifying the elements of the system and treating these as "nodes", mapping out all interactions with other elements and treating these as "links" and assigning "weights" that describe the "strength" of each link.* The approach in principle can be adapted also to interacting networks (Figure 3) such as those describing CEI of concern to European defence.

[45] NATO, Energy Security and Security Policy: NATO and the Role of International Security Actors in Achieving Energy Security, (NATO School Research, 2007) and National Institute of Standards and Technology, https://www.nist.gov/sites/default/files/documents/el/building_materials/resilience/Chapter4_75-_11Feb2015-3.pdf

[46] Setola R., Rosato V., Kyriakides E., Rome E. (Eds.): "Managing the Complexity of Critical Infrastructures A Modelling and Simulation Approach", Series: Studies in Systems, Decision and Control, Vol. 90, Springer, ISBN 978-3-319-51042-2, 2017.

7. Risk Assessment Framework

Risk assessment according to ISO 31010:2009 involves identification of the threats posed to European Defence CEI; estimation of their frequency/likelihood; estimation of their consequences; and the evaluation of the risks by combining consequences and likelihood; and implementing risk control strategies to manage and treat (reduce or mitigate) those risks.

Risk is assessed as a combination of threat likelihood (expressed as the probability that a given action, attack, or incident will occur), **vulnerability** (expressed as the probability that a given attack will succeed, given that the action, attack or incident occurs), and **consequence** (expressed as some measure of loss, such as loss of operation, euro cost, programmatic impact, etc.). Risk can be presented conceptually with the following equation:

$$\boldsymbol{Risk = Threat \times Vulnerability \times Consequence}$$

Threats to European Defence CEI include accidental human/technological threats, intentional human/technological threats and natural threats (Table 1).

A complete Risk Assessment Framework for CEI includes:

- **Risk Identification**: includes the identification of CEI assets and the threats by asset type, ranking by asset criticality, and development of a threat directory.

- **Risk Analysis**: combines the consequences and likelihood for all credible threats to provide a measure of risk. Risk analysis includes threat characterisation (type of threat, extent, intensity, probability, thresholds, time period); vulnerability assessment (identification of CEI assets, identification of interdependencies, how prone CEI are to the specific threat, definition of damage states and the probability of occurrence); impact/consequence analysis as shown in Table 2 below (e.g. disruption of energy supply to European Defence, cost of repair etc.); estimation of likelihood of occurrence of threat scenario(s), and the matrix of impact *vs.* likelihood.

- **Risk Evaluation**: includes the classification of risk based on asset per threat type.

- **Risk Management**: includes the guidelines of protection (external protection, internal protection, vulnerability mitigation process, personnel security, as well as training and awareness), recovery and resilience.

The above approach is scenario-based and considers known or foreseen threats. However, risk management should also consider unknown threats, which is more in line with the current approach of resilience. This means that countermeasures should not only focus on preventing a specific threat or protecting an asset, but also on enhancing the absorptive, adaptive and recovery capabilities of a CEI.

CEI Risk Assessment Methodologies can be divided in two major categories:

- ***Sectoral Methodologies***, whereby the energy sector is treated separately with its own risks and ranking; and

- ***Systems Approaches***, that assess CEI as an interconnected network and take into account interdependencies to and with other CIs.

Table 1: Threat matrix

Threats/Hazards	Examples	Direct	Indirect
Natural	Earthquake, tsunami, volcanic eruption, landslide, flood, storms, lightning, wildfires etc.	Extreme/severe weather conditions	Climate change
Human/Technological Accidental	Nuclear/chemical accidents, water/soil/air industrial pollution etc.	Physical fault Operational fault Connection failure	Communication failure Vulnerability by system design
Human/Technological Intentional	Armed conflict, terrorism, criminal attacks, politically motivated attacks etc.	Physical attack	Cyber attack Cyber-physical attack

Table 2: Impact to Critical Energy Infrastructure

Threat/Hazards	Asset of CEI affected	Impact
Flood	Power stations, electricity transmission and major distribution substations	Physical damage
Extreme winds from storms	Thermal power infrastructure, transmission and distribution lines electric grid	Physical damage
Wildfires	Thermal power infrastructure, transmission and distribution lines electric grid	Physical damage Decreased power transmission capacity Decreased power distribution capacity
Earthquakes	Failures on transmission poles equipment failures on (sub-)stations	Landslides
CBRN	Electrical power production	Contamination Pollution
Tsunami	Power stations, transmission towers and lines	Physical damage
Cyber-attack	SCADA	Power disruptions
Sabotage	Oil and gas pipe-lines Transmission lines	Physical damage Leakage
Terrorism	Oil and gas pipe-lines Transmission lines Power station	Physical damage

Where one or more of the risks assessed are deemed to be unacceptable Risk Management Options are identified, selected and implemented, taking into account the cost of implementing each risk management option against the benefits derived from it.

Risk Management is a tool that can enhance resilience of CEI by:

1. reducing the likelihood of occurrence of a threat;
2. reducing the impacts/consequences;
3. transferring in full or partly the risk;
4. avoiding the risk.

Resiliency of energy critical infrastructure consists of the following characteristics, listed below:

Robustness	withstanding a given level of stress without degradation/loss of function.
Autonomy	being able to function in a stand-alone operational mode.
Redundancy	sustain functional requirements during disruption/degradation/loss of functionality.
Responsiveness	being prepared to rapidly achieve goals in a timely manner to avoid future disruption.
Preparedness	evaluation of PCEI to anticipate and prepare against possible threats.
Resourcefulness	identifying problems, priorities and resources that are at risk of being disrupted.

Figure 4: Factors towards resilience

8. Key Research Topics

The research areas associated with PCEI can be classified in four main categories: monitoring; security; control and; interoperability. However, some research topics lie across two or more categories. These research areas will be further explored from the defence point of view as a following phase after the development of this Conceptual Paper.

The research topics could target technologies, tools and/or services in one of the following areas, to enhance:

Resilience: through Energy Autonomy, via integration of sustainable technologies. The development of an optimised energy mix to supply electrical power by combined generation and storage technologies for remote grids, camps and other military needs. Energy efficient design of the grid which allows for longer autonomy during standalone operation improving the robustness of the grid.

Protection: enhancing protection through Cyber-Physical Security. Development of sensor/actuator measurement techniques with adequate redundancy for defence needs and of resilient methods for identifying if these have been affected by an attack or a fault. Application of smart cameras for monitoring, and emergency response along with the development of algorithms for their optimised operation. Design of new methods for accommodating sensor/actuator failures; sensor/actuator faults, and system faults. Development of new methods for maintaining system stability under severe weather, unexpected conditions and attacks on the system.

Observability: through Real-time Monitoring and Control. Development of new methods for monitoring the state of a power grid and to detect direct or indirect attacks. Design of new methods for accommodating sensor/actuator failures; sensor/actuator faults, and system faults for enhanced Defence resilience.

Risk Management: development of customised risk assessment framework for dual-use purposes considering military realities. Classification of metrics for risk evaluation and identify the significance of (inter)dependencies, interconnections and risk communication.

9. Programme Initiatives

The prevailing approach in protecting energy related CI in the defence sector is to address weaknesses and threats and transform them into strengths and opportunities. The defence sector is now facing challenges to maximize defence capabilities and outputs through the adoption of relevant initiatives towards moving from PCEI concept to PCEI consensus. PCEI initiatives should consider the diversification of energy systems and motivate new research to ensure smart monitoring systems such that no individual disruption of the energy chain can affect the whole energy system.

Ad hoc case studies and in particular investigation scenarios should be initiated to detect structural or functional deficiencies of defence CI and energy shortfalls that occur at the construction phase as well as in the operation and maintenance phase in the service life of CEI. Methodologies to test existing policies with respect to CIP should be developed through such ad hoc research projects. In particular, these projects should look at how to model interdependencies between defence CI and potential cascading effects triggered by failures of some infrastructure based on smart models or "simulation games".[47] Specialized actions for example should be devoted to supervising thousands of kilometres of pipelines and power lines cutting across either wide open or dense urban areas with several critical junctions and transportation routes. A simulation process will help evaluate military operational reliability in conditions of normality and subsequently, develop predictive models for accurate estimations in unexpected severe situations. A subsequent step will be the identification and prioritization of needs and requirements to ensure uninterrupted functionality of CI. Among potential needs, these may include the development of a smart and decarbonized energy system coupled with targeted efforts to mitigate climate change effects[48]. The trend of making the energy network system more decentralized will provide benefits, as it will be easier to regionally isolate the impacts of a particular threat or attack. Currently, several MS adhere to the decentralized approach in terms of the energy network system.[49]

Energy security ought to be comprised of five dimensions related to availability, affordability, technology development, sustainability, and regulation.[50] This is also highly anticipated to be achieved

[47] Hämmerli, B., Renda, A. 2010. Protecting Critical Infrastructure in the EU, Centre for European Policy Studies, Brussels.
[48] Military Green, Energy & Environment: A European step beyond Reducing the Footprint, European Defence Agency.
[49] Cyber Security Strategy for the Energy Sector, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, ITRE: 2016-04, European Parliament, October 2016.
http://www.europarl.europa.eu/RegData/etudes/STUD/2016/587333/IPOL_STU(2016)587333_EN.pdf
[50] Sovacool, B.K., Mukherjee, I. 2011, Conceptualizing and measuring energy security: A synthesized approach, *Energy* 36 (2011): 5343-5355.

in the defence sector as well. In the framework of technological development and sustainability, the need for new research should be coupled with environmental concerns or constraints, including the increased energy demands that will affect the future security and operational planning in EU Defence. In light of the above, considering the effects of global warming as well as the magnitude or rate of long-term climate change, focus should be put on green procurement methods and green military equipment[51] with a lower carbon footprint that will provide increased operational, environmental and cost-effective reliability.

Moving towards the determination of challenges and opportunities, these should include attempts for increasing capability development[52] through an appropriate combination of several governance structures that will be responsible for a consistent threat assessment across EU, rigorous decision making, information sharing among relevant trusted stakeholders, establishment of an advanced monitoring system including the potential adoption of mandatory security auditing and relevant penalties for non-compliance with cyber security recommendations. Governments and MoDs need to be adaptive to new opportunities and risks stemming from technological developments in the energy sector in order to continuously adjust their strategy towards ensuring energy security. In the framework of reassessment of energy CI threats, investors, owners, manufacturers and operators of energy infrastructure need to be aware of benefits from new technologies and approaches that will continuously require increased collaboration between all relevant stakeholders to deal with natural or cyber threats. **PCEI initiatives should aim to propose recommendations, standardize guidelines, form potential regulations and set integrated procedures based on MS past and current experience.**
Investment motivation (in the means of tax breaks or financial subsidies) and motivation for new research constitute another big challenge as well. Such tax breaks exist in some MS for companies investing in the domain of operational security.[53] Above all, focusing on operational reliability within the defence is necessary in order to examine cross-sector approaches and opportunities and support scalable national and community infrastructure protection programs. In pursuit of that, the participation of any interested stakeholder (including international organizations such as the Organization for Security and Co-operation in Europe – OSCE – and others Centres of Excellence) may be considered as an additional asset given the important role they can play based on special fields of expertise. Also, any new research should focus on the development of alternative means rather than

[51] European Armaments Co-operation strategy, European Defence Agency, Brussels, 2008.
[52] Solana, J., 2008, Future Trends from the Capability Development Plan (CDP), European Defence Agency, Brussels.
[53] Cyber Security Strategy for the Energy Sector, Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, ITRE: 2016-04, European Parliament, October 2016.

on endless analysis of existing systems. It should also aim in defining interactions among several alternatives and determining potential constraints and bottlenecks in existing techniques with a view to improving them. In this respect optimal multidisciplinary efforts should be used to develop solutions with acceptable efficiency levels.

Initiatives for new and innovative research from a defence point of view require adequate funding given the strong financial impact of disruptions to CI. Fortunately, the EU invests several billion Euros for research in CIP. A number of schemes are targeted towards providing more security, such as the European Reference Network for Critical Infrastructure Protection (ERNCIP) that has particular thematic groups. **Securing energy in the defence sector constitutes an investment opportunity through making available technologies and promoting innovation.** A further opportunity could be the development of a funding programme that will stimulate national or community level PCEI projects with rational allocation of funds and human resources in order to achieve **a continuous infrastructure monitoring** and establish **alternative supply systems in the framework of contingency planning** (e.g. fuel cells in case of energy grid supply failure).

Implementation of pilot projects should be recognized as a promising starting point as MS will become more acquainted with PCEI concept. This will develop initiatives for mature and scalable future proposals based on “lessons learned” experience. The overall goal aims at strengthening PCEI related consciousness, as innovative ideas will be generated towards increasing resilience and energy strategic autonomy in EU Defence, with an increased level of CI protection in a way that defence CI will be enough flexible and responsive to changing requirements.

10. Recommendations and Way Ahead

From PCEI Concept to PCEI Consensus

This Conceptual Paper concludes that there is a need to ensure the resilience of defence and security sectors in times of crisis and one of the aspects of resilience is the continued availability of secure and sustainable energy supplies. The PCEI Experts Group with the support of interested EU MS, academia and national centres as well as the contribution of the Commission's DG Energy and DG JRC has developed this Paper. It aims at providing the framework which could lead to the identification of best management practices, in line with the EU policy framework, to further support MS in strengthening the protection of all defence related CEI from any kind of failures, risks, hazards, disasters and threats including terrorist or cyber-attacks.

To address these challenges the PCEI Group proposes to support **Securing Energy Strategic Autonomy for European Defence** through cooperation and practical assistance among MS and in particular the MS most vulnerable to severe energy supply disruptions and infrastructure failures. This Paper intends to lead to concrete actions for developing holistic methodologies and tools. The most cost-efficient way to implement these objectives is through cooperative projects of mutual interest with the support of the EU. In addition, MS need to foster an EU culture in protection and resilience of PCEI in European defence, for instance, through civ-mil training or exercises. Building on this PCEI Conceptual Paper MS supported by EU institutions (Commission) and Agencies (EDA) ***can move to a broad consensus on how to improve the resilience of defence related CEI, and thus protect our common interests***.

Recommendations:

- Address identified shortfalls in critical energy infrastructure protection and resilience by developing projects of mutual interest for the defence and security sector.

- Develop Short-, Medium- and Long-term strategy for the PCEI Initiative.

- Establish a network of experts as a platform for enabling broader collaboration across EU MS MoDs and relevant civil sectors.

Way Ahead

The following steps are recommended to achieve ***'PCEI Consensus'*** among EU MS MODs and other stakeholders (organisations, public, industry, academia, etc.):

- Disseminate the PCEI Conceptual Paper throughout the EU (all EU MS/MODs and other stakeholders, decision-makers, academia, industry, etc.) via any available tools (e.g. conducting conferences/workshops, publishing papers/articles, presentations, etc.) by EDA/ pMS and partners;

- Raise awareness through education and potential training within EU MS on the "PCEI Conceptual Paper" to build a common view and collaborative objectives among all stakeholders via respective EDA initiative;

The **second phase of the CF SEDSS** will include inter alia:

- Working to achieve the above objectives;
- Consideration of defence related PCEI projects;
- Identification of appropriate EU financial instruments for funding such projects;
- Enhanced cooperation between defence and civil sectors and exchange of experiences and best practices;

Annexes

Annex A

Glossary of Terms[54]

Critical Infrastructure	An asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.
Critical Defence Infrastructure	Assets, services and facilities essential to protect support, and sustain military forces and operations
Critical Energy Infrastructure Protection	Measures which aim to reduce the vulnerabilities of critical energy infrastructure in order to minimize the probability and potential impact of a successful attack.
Energy	All forms of energy products, combustible fuels, heat, renewable energy, electricity, or any other form of energy, as defined in Article 2(d) of Regulation (EC) No 1099/2008 of the European Parliament and of the Council of 22 October 2008 on energy statistics.
Defence Related Critical Energy Infrastructure	Critical Energy infrastructure, owned by the public or private sectors, that is essential to the functioning and the operations of the defence sector.
Participating Member States	EDA Member States participating in the PCEI Project

[54] The definitions of the terms of this section are based on several references:
COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, DIRECTIVE 2012/27/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012, European Climate Adaptation Platform (CLIMATE-ADAPT)
Definition from DIRECTIVE 2012/27/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 October 2012
Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information
"Defense Critical Infrastructure" definition by the US "Homeland Defense" joint publication 3-27 (http://www.dtic.mil/doctrine/new_pubs/jp3_27.pdf), NATO Parliamentary 157 CDS 08 E rev 1 - Energy Security: Co-operating to Enhance the Protection of Critical Energy Infrastructures, www.nato-pa.int/default.asp?SHORTCUT=1478
Glossaryhttp://climate-adapt.eea.europa.eu/help/glossary/index_html/#linkResilience, CIPedia©, www.cipedia.eu, "EUROPEAN DEFENCE MATTERS" magazine, Issue 11, 2016; https://www.eda.europa.eu/images/default-source/interface/edm11cover_web.jpg?MaxWidth=280&MaxHeight=&ScaleUp=false&Quality=High&Method=Resize
FitToAreaArguments&Signature=D879E517D6B7A1874B85EDA5571163B4, Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

Protection	All activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability.
Resilience	The ability to absorb disturbances while retaining the same basic structure and ways of functioning; the capacity for self-organisation; the capacity to adapt to stress; and the capacity to change and rebound.
Threat	A potential cause of an unwanted incident which may result in harm to an organisation or any of the systems it uses; such threats may be natural, accidental or deliberate (malicious) and are characterised by threatening elements, potential targets and attack methods.
Strategic Autonomy in Defence	The ability of the EU to develop the appropriate defence policies, capacities and capabilities in order to guarantee the security and the protection of the Union and its citizens.

Annex B

List of Figures and Tables

Annex C

Case Studies

In the present section a certain number of different representative case studies [1-10] have been selected, from the literature, to form a general frame of reference. These case studies are indicating of how the defence sector can contribute in enhancing the resilience and protection of the PCEI ecosystem at the EU cross-border level.

It is anticipated that the below examples will provide the motivation for setting up a mechanism to generate relevant case studies for the defence sector as well. Such case studies can be used to develop a tool box with relevant "problems and solutions" and targeted validation actions leading to the potential necessity for establishing a suitable entity to further elaborate the PCEI perspective within the EU Defence and Security Sector as well to promote synergies between EDA, the European Commission and any other stakeholders; from the military and the civil sectors, the industry or the academia through current and future framework programs (Horizon 2020, European Defence Fund). In this respect, it is noted that the south eastern part of the European Union presents a sufficiently rich but also manageable theatre for such case studies and validation actions.

Indicative Case Studies

1. Bernhard Schneidhofer, **A case study in Critical Infrastructure Interdependency**, Technical Report RHUL–ISG–2016–12 Royal Holloway University of London (2016)

This report provides an introduction into the topic of Critical Infrastructure Protection and an overview of a case study that examines regional Critical Infrastructures and the security vulnerabilities discovered during the investigation.

2. David Riedman, **Questioning the Criticality of Critical Infrastructure: A Case Study Analysis** Homeland Security Affairs, Volume 12 Essay 3 (May 2016) Assessed on www.hsaj.org on May 20, 2017)

This paper advocates an approach that reduces the scope of infrastructure protection missions from protecting all facilities against all threats and hazards. It takes into account the emergence of resilience within a complex systems perspective and realizes that not all infrastructures

designated as critical meet the definition of criticality, when such (especially commercial) infrastructures are supposedly damaged or destroyed.

3. Troy Nash, **An Undirected Attack Against Critical Infrastructure. A Case Study for Improving Your Control System Security**, Lawrence Livermore National Laboratory Report UCRL-MI-217620 (2005)

This report concerns an early case study for a water treatment facility, where control systems were repeatedly compromised by malware.

4. Masahiko Haraguchi Soojun Kim, **Critical Infrastructure Systems: A case study of the interconnectedness of risks posed by hurricane sandy for new Nork city**, Global Assessment Report on Disaster Risk Reduction, The United Nations Office for Disaster Risk Reduction, 2015

This report studies the impact of Hurricane Sandy from the perspective of interdependence among different sectors of critical infrastructure in New York City and assesses the interconnected nature of risks posed by such a hurricane. The main findings are that initiatives that focus primarily on building hard infrastructures to decrease direct damages, understate the importance of interdependent risk across sectors, while disaster risk reduction strategies need to address interdependent infrastructures in order to reduce indirect damages.

5. Mike Harrop, **Creating Trust in Critical Network Infrastructures: Canadian Case Study**, presented at INTERNATIONAL TELECOMMUNICATION UNIONITU WORKSHOP ON CREATING TRUST IN CRITICALNETWORK INFRASTRUCTURES, Document: CNI/0720 May 2002, Seoul, Republic of Korea, 20 - 22 May 2002

This report presents an overview of the Canadian environment relating to the operation and use of telecommunications, particularly data communications, together with a look at critical infrastructures, their interdependencies and the organizations involved in their protection.

6. Kathryn Gordon and Maeve Dion, **Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security,** Organisation for Economic Co-operation and Development Report, 2008

This report reviews the role of investment policies in broader national strategies for protecting critical infrastructure and policies that attempt to coordinate the role of private operators of such infrastructures

7. Nathan J. Edwards, Jason R. Hamlet, John Bailon and Shane F. Liptak, **Supply Chain Decision Analytics: Application and Case Study for Critical Infrastructure Security**, Sandia National Labs Report, SAND2015-2587C (2015)

This case study considers application of a decision analytics framework to the supply chain of a critical infrastructure construction project and illustrates how the framework can be used to identify supply chain threats and suggest mitigations for addressing those threats.

8. Cherylne Fleming, **A Resilience Approach to Defence Critical Infrastructure,** 21st International Congress on Modelling and Simulation, Gold Coast, Australia, 29 Nov to 4 Dec 2015, www.mssanz.org.au/modsim2015

This paper describes an approach to understand the dependencies and fragilities which impact defence resilience. It demonstrates the impact of critical infrastructure on Defence capability, and highlights their importance of a resilient infrastructure and how resilience should be treated as an integral part of the defence to accommodate the fact that changes occur in an interlinked way.

9. Katri Pynnöniemi (ed.), **Russian Critical Infrastructures: Vulnerabilities and Policies,** The Finnish Institute of International Affairs Report 35, (2012) (assessed on www.fiia.fi on May 20, 2017).

This report addresses the situational and conceptual factors underlying Russian policies on critical infrastructure protection and their evolution in the context of the national security policy, including political implications of critical infrastructure vulnerability in Russia and the impact of climate change.

10. Australian Government, **Critical Infrastructure Resilience Strategy** (2012) (assessed on http://ccpic.mai.gov.ro/docs/ on May 20, 2017)

This report provides the Australian Government's approach to critical infrastructure resilience and it has a strong focus on business-government partnerships fostering a shared responsibility

across governments and the owners and operators of critical infrastructure, instead of a more traditional approach of developing plans to deal with a finite set of scenarios, especially in the context of an increasingly complex environment.

11. References

[1] COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[2] European Commission/Energy "Protection of critical infrastructure", https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

[3] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, "Joint Report to the European Parliament and the Council on the implementation of the Joint Framework on countering hybrid threats -a European Union response", Brussels, 19 July 2017, https://ec.europa.eu/docsroom/documents/24601

[4] European Defence Agency, "European Defence Energy Network (EDEN)", https://www.eda.europa.eu/european-defence-energy-network

[5] European Defence Agency, "EDA in Single European Sky", https://www.eda.europa.eu/what-we-do/activities/activities-search/single-european-sky

[6] EUROCONTROL, "More collaboration between airports to reduce carbon footprint" (28 October 2016", https://www.eurocontrol.int/news/more-collaboration-between-airports-reduce-carbon-footprint

[7] NATO Review Magazine, "Resilience: a core element of collective defence", http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm

[8] NATO Review Magazine, "NATO's energy security agenda", http://www.nato.int/docu/review/2014/NATO-Energy-security-running-on-empty/NATO-energy-security-agenda/EN/index.htm

[9] European Defence Agency, "Energy and Environment Programme" https://www.eda.europa.eu/what-we-do/activities/activities-search/energy-and-environment-programme

[10] 'Protecting Critical Energy Infrastructures against terrorist attacks: threats, challenges and opportunities for international co-operation'. Address in the Reinforced NATO Economic Committee Meeting (22 September 2008, Brussels) by Dr. Raphael F. Perl; Head of the OSCE Action against Terrorism Unit.

[11] 'To Protect Critical Energy Infrastructure: Gaining Critical Insights and Discussing the Role, Strategic Objectives and Practical Measure Initiated by the Organization for Security and Co-Operation in Europe via Their Action against Terrorism Programme'. Address in Oil & Gas Critical Infrastructure & Asset Security Forum (19-21 September 2012) by Mr. Thomas Wuchte Head/Action against Terrorism Unit Transnational Threats Department OSCE.

[12] European Defence Agency, "Military Green", https://www.eda.europa.eu/docs/default-source/news/military-green-leaflet.pdf

[13] "Critical Infrastructure and Key Assets: Definition and Identification" (October 1, 2004), by John Moteff and Paul Parfomak), https://www.fas.org/sgp/crs/RL32631.pdf

[14] OSCE “Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks: Focusing on Threats Emanating from Cyberspace” (2013) http://www.osce.org/secretariat/103500?download=true

[15] European Commission and TNCEIP, “Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012)”, https://ec.europa.eu/energy/sites/ener/files/documents/20121114_tnceip_eupolicy_position_paper.pdf

[16] COUNCIL DECISION 2014/415/EU Arrangements for the Implementation by the Union of the Solidarity Clause.

[17] S. Rinaldi, J. Peerenboom, T. Kelly, Identifying, understanding and analyzing critical infrastructure interdependencies, IEEE Control Syst. 21 (6) (2001) 11–25

[18] L. Comfort, K. Ko, A. Zagorecki, Coordination in rapidly evolving disaster response systems: the role of information, Am. Behav. Sci. 48 (3) (2004) 295–313.

[19] A. Lo¨ schel, U. Moslener, D. Ru¨ bbelke, Energy security – concepts and indicators, Energy Policy 38 (4) (2010) 1607–1608.

[20] S. Patterson, G. Apostolakis, Identification of critical locations across multiple infrastructures for terrorist actions, Reliab. Eng. Syst. Saf. 92 (9) (2007) 1183–1203.

[21] C. Chai, X. Liu, W. Zhang, Z. Baber, Application of social network theory to prioritizing oil and gas industries protection in a networked critical infrastructure system, J. Loss Prev. Process Ind. 24 (5) (2011) 688–694.

[22] U.S. Department of Energy, U.S. Energy Sector Vulnerabilities to Climate Change and Extreme Weather, U.S. Department of Energy, 2013.

[23] AS/NZS, 1999. Risk Management. 4360:1999., s.l.: s.n.

[24] Giannopoulos, G., Filippini, R. & Schimmer, M., 2012. Risk Assessment Methodologies for Critical Infrastructure Protection. Part I, Luxembourg: Publications Office.

[25] ISO, 2009. Risk management – Principles and guidelines. First edition of 2009., s.l.: s.n.

[26] Energy Critical Infrastructure and Key Resources Sector-Specific Plan as input to the National Infrastructure Protection Plan (Redacted)May 2007Departmentof Energy, Homeland Security

[27] EEAS/EUMS (2016) “The EU Global Strategy –Challenge or Opportunity for EU CSDP”, Impetus (Issue 22, Autumn/Winter 2016, Brussels: EUMS), https://eeas.europa.eu/headquarters/headquarters-homepage/8487/previous-issues-impetus_en

[28] General Secretariat of the Council (2016), “Council conclusions on implementing the EU Global Strategy in the area of Security and Defence - Council conclusions”, (Brussels, 14 November 2016, Doc.: 14149/16), http://www.consilium.europa.eu/en/press/press-releases/2016/11/14-conclusions-eu-global-strategy-security-defence/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Council+conclusions+on+implementing+the+EU+global+strategy+in+the+area+of+security+and+defence

[29] EUROPEAN COMMISSION (2014) “European Energy Security Strategy”, (COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL, Brussels, 28.5.2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52014DC0330&from=EN

[30] Carlos Pascual (2015) The new Geopolitics of Energy (COLUMBIA SIPA: Center on Global Energy Policy) http://energypolicy.columbia.edu/sites/default/files/energy/The%20New%20Geopolitics%20of%20Energy_September%202015.pdf

[31] Centre for European Policy Studies (CEPS), Protecting Critical Infrastructure in the EU (2010), Brussels (CEPS TASK FORCE REPORT), http://aei.pitt.edu/15445/1/Critical_Infrastructure_Protection_Final_A4.pdf

12. List of Contributors

Cyprus – Ministry of Defence Delegation	
Lt. Col Stylianos Antoniou	CY MOD, Head of Delegation
Ms Melivia Demetriou	CY MFA
Dr. Nikolas Flourentzou	KIOS Centre of Excellence, University of Cyprus
Dr. Christos Laoudias	KIOS Centre of Excellence, University of Cyprus
Dr. Nicolas Kyriakides	Cyprus University of Technology
Prof. George Boustras	European University Cyprus
Ms Louisa Marie Shakou	European University Cyprus
Ms Cleo Varianou	European University Cyprus
Greece – Ministry of Defence Delegation	
Col Georgios Drosos	EL MOD, PCEI Chairman
Prof. Athanasios Konstandopoulos	Centre for Research & Technology Hellas (CERTH), PCEI Co-chairman
LtC Ioannis Chatzialexandris	EL MOD, Head of Delegation
Cpt Georgios Xanthos	EL MOD
Ms Angeliki D. Boura	EL MFA
Prof. Andreas Loizos	National Technical University of Athens (NTUA)
Dr Christina Plati	National Technical University of Athens (NTUA)
Mr Konstantinos Gkyrtis	National Technical University of Athens (NTUA)
Ms. Rozina Metallinou	Centre for Research & Technology Hellas (CERTH)
Bulgaria - Ministry of Defence	
Dr Hristo Hristov	Defence Instutue
Estonia - Ministry of Defence	
Mr Karmo Kõrvek	Defence Investments Department
Ireland - Ministry of Defence	
Col Jim Burke	IE MoD
European Defence Agency	
Dr Constantinos Hadjisavvas	Project Officer Protect
Mr Richard Brewin	Project Officer Energy & Environment Systems
European Commission	
Mr Adam Szolyak	DG Energy
Dr Naouma Kourti	Joint Research Centre
Dr Georgios Giannopoulos	Joint Research Centre
NATO Energy Security Centre of Excellence (ENSEC COE)	
Dr Jaroslav Hajek	Subject Matter Expert (Observer)

Protection of Critical Energy Infrastructure (PCEI) Experts Group

@EDA, Brussels

October 2017