EasyChair Preprint

№ 10622

Critical Energy Infrastructures: Geopolitical Vulnerabilities and Strategies of Securitization

Matteo Gerlini and Fabio Indeo

July 25, 2023

Matteo Gerlini, Assistant Professor (Tenured) at the University of Siena (Italy), ISEG Italian PoC, NATO SPS.

Fabio Indeo, Research Fellow at University of Siena (Italy) and analyst NATO Defense College Foundation (Rome, Italy)

Critical Energy Infrastructures: geopolitical vulnerabilities and strategies of securitization

Protecting Critical Energy Infrastructures (CEI) represents a key priority for global energy suppliers and consumers to preserve the energy security condition, namely "the uninterrupted availability of energy sources at an affordable price". As a matter of fact, the high relevance of energy in the global economy implies that CEI infrastructures have progressively become an attractive target for terrorist attacks – both physical and cyber-attacks – aimed at provoking energy disruptions and economic damages, highlighting the condition of the high vulnerability of the affected country in security terms.

Not only gas and oil pipelines but all CEI - including the RES-based infrastructures such as solar plants, wind farms and hydrogen industries, which will be the cornerstone of the energy transition - represent a vulnerable asset which is necessary to protect in order to preserve a condition of energy security without disruptions, ensuring the regularity of supply to the markets.

In the last years, we can observe that mainly Middle East producers and Ukraine have suffered terrorist attacks aimed at destroying CEI, while the European Union has been recently affected in the case of North Stream gas pipeline's sabotage in September 2022.

The EU Council defines 'ECI' as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".[1]

CEI's protection is one of the main tasks for the EU, mainly for two key interlinked reasons: firstly, CEI (power generation plants, pipelines, LNG terminals, refineries, solar parks, wind farms, power transmission systems and power distribution grid) appear highly vulnerable, because they are characterized by a vast, geographically-dispersed, widely-diverse infrastructure of assets.

1 Official Journal of the European Union. (2008). *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Brussels, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

European critical infrastructures are deeply interconnected and highly interdependent, clearly highlighting their profound vulnerability to systemic risks and the possibility of unpredictable and extensive disruption, failure or destruction. Given this interdependence, the widespread cascade effect is one of the main feared consequences: as a matter of fact, threats to a single critical infrastructure can significantly impact a broad range of actors in different infrastructures, also spanning a number of European countries. One such example is the European high-voltage electricity grid, composed of the interconnected national high-voltage electricity grids, as well as the interstate gas interconnections among EU countries in order to ensure reverse energy flows in the case of disruption.

Secondly, the preservation of energy infrastructures is a strategic priority in order to preserve EU energy security; because of the combination of high demand for energy and decreasing domestic production, the EU is strongly dependent on oil and gas imports (more than half of EU energy needs are covered by imports) drawing up a condition of extreme vulnerability in the case of a potential disruption of the regular supply, which represents a threat to its energy security.

The Nord Stream pipelines' sabotage in September 2022 represents the first direct attack affecting EU's CEI, depriving Germany and other EU Western countries of relevant gas imports coming from Russia: the implementation of prevention's tailored strategies and the achievement of a concrete diversification could help to manage and to prevent potential future disruptions mainly in the interconnected electricity grid.

Middle East countries are among the largest oil suppliers in the world, but they strongly depend on the sensitive energy chokepoint of Hormuz to deliver oil and gas exports to the markets: Hormuz is daily crossed by more than 21 million barrels of oil representing about 30 per cent of all seaborne-traded oil and is used for 25 per cent of global LNG trade.[2]

In this chokepoint, increasing tensions and instability have affected the regular transit along this strategic energy bottleneck. In May 2019, for instance, four oil tankers anchored off Fujairah Port (UAE) were sabotaged, while in June, two other tankers were attacked in the Gulf of Oman: in 2022, too, UAE suffered two missile attacks launched by Yemen' Houthi militant group which did not affect energy infrastructures of this OPEC's third-largest oil producer. Given the strategic relevance of the energy sector for the Saudi economy, national oil infrastructures (pipelines and refineries) have progressively become an attractive target for terrorist attacks aimed at provoking supply disruptions and economic losses and exhibiting the political vulnerability of the Kingdom. In September

2 US Energy Information Administration, The Strait of Hormuz is the world's most important oil transit chokepoint, June 2019, https://www.eia.gov/todayinenergy/detail.php?id=39932

2019, Saudi Aramco oil facilities at Abqaiq were struck by aerial attacks, which provoked temporary Saudi production cuts by 50 per cent of the daily production or nearly 5.7 million BPD, which accounts for around 5 per cent of the global oil supplies. There was a 20 per cent increase in oil prices after the attack, even after Saudi Aramco declared the restoration of supplies to the previous level. It was not the first terrorist attack on the Saudi energy facilities; in 2006, al-Qaeda carried out a failed suicide attack on the Abqaiq refinery complex, while in 2012, a cyberattack (allegedly by Iran) affected the Khurais facility, pushing Saudi authorities to increase security measures. In 2022 Houthi militias launched several drone and missile attacks targeting Saudi energy facilities (also in the Red Sea), a concrete threat to global energy security which was already undermined by the Russian-Ukraine conflict and the disruption of the energy flows to the European Union.

The main problem is the lack of alternative export corridors bypassing Hormuz: among the Middle Eastern exporters, only Saudi Arabia and the UAE have developed alternative export routes, while Qatar (and in general LNG exports from the region) cannot reach the markets in the case of Hormuz closure, provoking an interruption of the energy flows.

The main aim of this proposal is to evaluate the existing threats to CEI and how efficiently prevent, contain and downplay the negative impact on global energy security: considering the sharing interest of both energy suppliers and consumers to preserve the regularity of the energy flows to the markets, a joint engagement which could be profitable to improve the security conditions and to avoid dangerous geopolitical unbalances.

If the Council Directive 2008 establishes procedures for identifying and designating CEI and introduces a common approach for assessing their protection (but only limited to the energy and transport sectors), the EU Program to protect CEI has been further revised in 2013, developing a new approach to take account of increasing cross-border interdependencies as well as to increase CEI resilience against threats and hazards, so minimising the consequences of loss of services to society as a whole.

The focus on the improvement of infrastructure resilience shows the EU’s engagement in providing service continuity following a sudden and non-predictable destructive event. Infrastructure resilience is defined as “the ability to reduce the magnitude and/or duration of disruptive events. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event. In this reshaped approach, prevention, preparedness, and response are coordinated initiatives to develop a more comprehensive European Program to increase the protection of CEI.

From this angle, the energy diversification outlined by the EU taxonomy implies a renewal of nuclear power production from plants placed in the EU. This will mitigate possible disruption in foreign energy supplies. But this will imply a renewed effort to strengthen the nuclear security framework in the EU members.

In the prevention sphere, the implementation of an efficient risk management programme could allow dealing with the vulnerability factor represented by the interdependence of the energy infrastructures, mitigating negative implications of the “cascading events”. A risk management programme must include the analysis of the possible threats and vulnerabilities, the risk assessment, and the implementation of initiatives to mitigate the negative impact of these threats.

The increasing digitalisation of the energy system has pushed the EU to reinforce its approach to prevent and tackle cybersecurity threats, one of the main dangerous challenges which can affect CEI.

In February 2013, the Commission issued a cybersecurity strategy that outlined the EU's vision for building cybersecurity capabilities. In 2016 the EU adopted the Network and Information Systems (NIS) Directive, which represents the first regional-wide effort to harmonize cybersecurity and notification requirements. NIS Directive imposes that EU member states should adopt national cybersecurity strategies and create a Cooperation Group to increase cooperation and promote the exchange of information. Moreover NIS Directive supports the creation of computer-security incident response teams (‘CSIRTs network’) in order to promote swift and effective operational cooperation.

The so-called Cybersecurity Act – which entered into force in June 2019 – reflects the EU’s revised approach aimed at strengthening the EU's response to cyber-attacks and improving cyber-resilience, underlining that the electricity grid needs a dedicated sectoral approach because of real-time requirements. Moreover, EU Commission attributed ENISA (the European Union Agency for Cybersecurity) the role of improving coordination and cooperation in cybersecurity across EU Member States and EU institutions, agencies and bodies.

Selected bibliography

European Commission. (2013). *Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructure more secure*. SWD (2013) 318 final. Brussels.

Indeo Fabio (2019), *European critical infrastructures: vulnerabilities and securitisation strategies,* in M. Brunelli (ed)., "Understanding radicalization, terrorism and deradicalization", Rubbettino editore

Lazari Alessandro (2014). *European Critical Infrastructure Protection*, Springer: Switzerland, DOIhttps://doi.org/10.1007/978-3-319-07497-9

Melchiorre Tiziana (2019). *Recommendations on the importance of critical energy infrastructure (CEI) stakeholder engagement, coordination and understanding of responsibilities in order to improve security.* NATO Energy Security Centre of Excellence, Vilnius, pp. 17-18, 22-24

Official Journal of the European Union. (2008). *Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. Brussels, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF

Official Journal of the European Union (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

Official Journal of the European Union (2019). *REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN

US Energy Information Administration (2019), The Strait of Hormuz is the world's most important oil transit chokepoint, June 2019, https://www.eia.gov/todayinenergy/detail.php?id=39932

US National Infrastructure Advisory Council (2009). *Critical Infrastructure Resilience Final Report and Recommendations*. Washington, pp. 12-13, https://www.cisa.gov/sites/default/files/publications/niac-critical-infrastructure-resilience-final-report-09-08-09-508.pdf